



UNIS 入侵检测系统

命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

目 录

1 命令参考导读.....	1-1
1.1 适用款型.....	1-1
1.2 内容简介.....	1-1

1 命令参考导读

本命令参考介绍了入侵检测系统产品支持的各软件特性的配置命令，包括命令的视图、缺省情况、参数介绍、使用指导和使用举例等。

1.1 适用款型

入侵检测系统产品款型较多，形态丰富，本手册所描述的内容适用于如下产品款型：

表1-1 手册适用的产品款型

系列	款型
T5000-G系列入侵检测系统	T5000-G20/T5000-G30
T1000-G系列入侵检测系统	T1000-G20/T1000-G50/T1000-G60/T1000-G80
T1000-CN系列入侵检测系统	T1000-CN60/T1000-CN80

1.2 内容简介

本节以列表的形式介绍了入侵检测系统产品支持的特性，不同产品款型之间对于这些特性的支持情况有所差异，具体支持情况请参见相关的模块资料。本手册的内容如下：

手册名称	内容简介
基础命令参考	介绍登录及管理设备的基本配置命令，包括如下内容： • CLI 命令（快速了解命令行接口、命令行接口的进阶应用、命令行接口的高级应用） • RBAC 命令 • 登录设备命令（CLI 登录、登录用户配置和管理） • FTP 和 TFTP 命令 • 文件系统管理 • 配置文件管理命令 • 软件升级命令 • ISSU 命令 • 设备管理命令 • Tcl 命令 • License 管理命令
虚拟化技术命令参考	介绍配置虚拟化特性使用的命令，包括如下内容： • IRF 命令 • Context 命令
安全命令参考	介绍配置安全特性使用的命令，包括如下内容： • AAA 命令

手册名称	内容简介
	• Password Control 命令 • 公钥管理命令 • PKI 命令 • SSH 命令 • SSL 命令 • ASPF 命令 • APR 命令 • 会话管理命令 • 连接数限制命令 • 对象组命令 • 攻击检测与防范命令 • ARP 攻击防御命令 • uRPF 命令 • 加密引擎命令 • 安全域命令 • 安全策略命令 • 用户身份识别与管理命令 • ND 攻击防御命令 • keychain 命令 • IP-MAC 绑定命令 • IPoE 命令 • IP 信誉命令 • MAC 地址认证命令 • 服务器外联防护命令
DPI深度安全命令参考	介绍了如何配置DPI命令，包括如下内容： • 应用层检测引擎命令 • IPS 命令 • 防病毒命令 • 数据过滤命令 • 文件过滤命令 • WAF 命令 • 代理策略命令
带宽管理命令参考	介绍了配置带宽管理，包括如下内容： • 带宽管理命令 • 应用审计与管理命令
接口管理命令参考	介绍了引擎口、以太网接口、Loopback接口和Null接口等内容。包括如下内容： • 接口批量命令 • 以太网接口配命令 • LoopBack 接口、Null 接口和 InLoopBack 接口命令

手册名称	内容简介
二层技术-以太网交换命令参考	介绍配置以太网交换使用的命令，包括如下内容： • MAC 地址表命令 • 以太网链路聚合命令 • VLAN 命令 • LLDP 命令 • 二层转发命令 • 环路检测命令
三层技术-IP业务命令参考	介绍配置IP业务所使用的命令，包括如下内容： • ARP 命令（ARP、代理 ARP） • IP 地址配命令 • 域名解析命令 • IP 转发基础命令 • 快速转发命令 • 流分类命令 • 邻接表命令 • IP 性能优化命令 • IPv6 基础命令 • IPv6 快速转发命令
三层技术-IP路由命令参考	介绍了构建不同规模的网络所需要的路由信息学习及控制技术。包括：IPv4、IPv6网络的各种路由学习技术，影响路由选择或者路由表生成的策略，包括如下内容： • IP 路由基础命令 • 静态路由命令 • RIP 命令 • OSPF 命令 • 策略路由命令 • IPv6 静态路由命令 • RIPng 命令 • OSPFv3 命令 • 路由策略命令 • IPv6 策略路由命令
ACL命令参考	介绍配置 ACL 使用的命令，包括如下内容： • ACL 命令 • 时间段命令
可靠性命令参考	介绍配置可靠性使用的命令，包括如下内容： • 冗余备份命令 • BFD 命令 • Track 命令命令 • 进程分布优化命令 • 接口组联动命令命令

手册名称	内容简介
	• Monitor Link 命令
网络管理和监控命令参考	介绍设备监控和管理使用的命令，包括如下内容： • 系统维护与调试命令（Ping、Tracert、系统调试） • NQA 命令 • NTP 命令 • SNMP 命令命令 • RMON 命令 • NETCONF 命令 • 进程监控和维护命令 • 信息中心命令 • Event MIB 命令 • 报文捕获命令 • 快速日志输出命令
VPN实例命令参考	介绍VPN实例的相关配置命令



UNIS 入侵检测系统

基础配置命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《基础配置命令参考》主要介绍 CLI、RBAC、登录设备、FTP 和 TFTP、文件系统管理、配置文件管理、软件升级、ISSU、自动配置命令、设备管理、Tcl 和 License 管理相关的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用 “[]” 括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由 “#” 号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号 “< >” 表示按钮名，如 “单击<确定>按钮”。
[]	带方括号 “[]” 表示窗口名、菜单名和数据表，如 “弹出[新建用户]窗口”。

格 式	意 义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 CLI	1-1
1.1 CLI命令	1-1
1.1.1 alias	1-1
1.1.2 display { begin exclude include }	1-3
1.1.3 display by-linenum	1-3
1.1.4 display >	1-4
1.1.5 display >>	1-5
1.1.6 display alias	1-6
1.1.7 display history-command	1-7
1.1.8 display history-command all	1-8
1.1.9 display hotkey	1-9
1.1.10 hotkey	1-11
1.1.11 quit	1-12
1.1.12 repeat	1-13
1.1.13 return	1-14
1.1.14 screen-length disable	1-14
1.1.15 system-view	1-15

1 CLI

1.1 CLI命令

1.1.1 alias

alias 命令用来为命令或命令字符串配置别名。

undo alias 命令用来取消相应配置。

【命令】

alias *alias command*

undo alias *alias*

【缺省情况】

系统为部分常用命令定义了缺省别名，如 [表 1-1](#) 所示。

表1-1 系统定义的缺省别名

缺省别名	命令
access-list	acl
end	return
erase	delete
exit	quit
hostname	sysname
logging	info-center
no	undo
show	display
write	save

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

alias: 表示命令的别名，为 1~20 个字符的字符串，区分大小写。别名不能为“alias”，也不能包含空格。

command: 表示配置别名的命令，可以为任意字符串。请用户保证该命令字符串能够被设备识别并执行，否则执行别名命令时将会失败。

【使用指导】

系统定义的缺省别名无法取消。

通过本命令用户可以为命令行指定一个或多个别名，也可以为命令行开头的一个或多个关键字配置多个别名，使其符合用户的使用习惯。

本命令可以为某条命令行配置别名，当执行该命令时可以直接使用别名以简化输入。例如将命令 **display ip routing-table** 的别名配置为 **shiprt**，当需要使用 **display ip routing-table** 查看设备生效的配置时，直接输入 **shiprt** 即可。

本命令可以为命令行起始的一个或多个关键字配置别名，使其更符合用户习惯。所有使用该关键字开头的命令行都可以使用别名命令来执行。例如，为 **display ip** 命令定义的别名为 **ship**，在使用所有以 **display ip** 关键字开头的命令行时，都可以使用 **ship** 进行配置。例如：

- 输入 **ship routing-table** 可以执行命令 **display ip routing-table**。
- 输入 **ship interface** 可以执行命令 **display ip interface**。

配置别名时，可以使用 **\$n** 表示命令行中的参数或者关键字，这样既可以用别名替代部分关键字来简化输入，又可以根据实际需要指定不同的参数或者关键字，增加了灵活性。**\$n** 最多可以使用 9 次，**n** 为 1~9 的整数，表示参数或关键字出现的顺序。比如，将命令 **display ip \$1 | include \$2** 的别名配置为 **shinc** 后，如果需要执行 **display ip routing-table | include Static** 命令来筛选并查看路由表中的所有静态路由信息，可直接执行 **shinc routing-table Static**；同样如果需要执行 **display ip interface | include GigabitEthernet1/0/1**，则可直接执行 **shinc interface GigabitEthernet1/0/1**。

【举例】

配置命令 **display ip routing-table** 的别名为 **shiprt**。

```
<Sysname> system-view
```

```
[Sysname] alias shiprt display ip routing-table
```

```
[Sysname] shiprt
```

```
Destinations : 13          Routes : 13
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
3.3.3.3/32	Static	60	0	192.168.1.62	GE1/0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
169.254.0.0/24	Direct	0	0	169.254.0.188	GE1/0/1
169.254.0.0/32	Direct	0	0	169.254.0.188	GE1/0/1
169.254.0.188/32	Direct	0	0	127.0.0.1	InLoop0
169.254.0.255/32	Direct	0	0	169.254.0.188	GE1/0/1
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

配置命令 **display ip \$1 | include \$2** 的别名为 **shinc**，同时使用别名命令筛选并查看路由表中的所有静态路由信息。

```
[Sysname] alias shinc display ip $1 | include $2
```

```
[Sysname] shinc routing-table Static
```

```
3.3.3.3/32          Static  60  0          192.168.1.62      GE1/0/1
```

【相关命令】

- **display alias**

1.1.2 display { begin | exclude | include }

display { begin | exclude | include } 命令用来使用正则表达式对显示信息进行过滤。

【命令】

display command { begin | exclude | include } regular-expression

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

command: 命令关键字，取值可以通过输入?来获得。

begin: 从包含正则表达式的行开始显示。

exclude: 只显示不包含正则表达式的行。

include: 只显示包含正则表达式的行。

regular-expression: 表示正则表达式，为 1~256 个字符的字符串，区分大小写。

【使用指导】

用 **display** 命令查看显示信息时，用户可以使用正则表达式来过滤显示信息，以便快速的找到自己关注的信息。关于正则表达式的详细描述请参考“基础配置指导”中的“CLI”。

【举例】

查看包含 VLAN 的配置。

```
<Sysname> display current-configuration | include vlan  
vlan 1  
vlan 999  
port access vlan 999
```

1.1.3 display | by-linenum

display | by-linenum 命令用来查看带行号的显示信息。

【命令】

display command | by-linenum

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

command: 命令关键字，取值可以通过输入?来获得。

【使用指导】

使用本命令时，系统在显示信息的同时会自动在每行显示信息的前面添加行号，以便当显示信息较多时，能够迅速定位到某行信息。

行号占 5 个字符，通常行号后面接“:”。当 **by-linenum** 和 **begin** 参数一起使用时，行号后面还可能接“-”，其中“:”表示该行符合匹配规则，“-”表示该行不符合匹配规则。

【举例】

显示 VLAN 999 信息的同时显示行号。

```
<Sysname> display vlan 999 | by-linenum
 1: VLAN ID: 999
 2: VLAN type: Static
 3: Route interface: Configured
 4: IPv4 address: 192.168.2.1
 5: IPv4 subnet mask: 255.255.255.0
 6: Description: For LAN Access
 7: Name: VLAN 0999
 8: Tagged ports:   None
 9: Untagged ports:
10:   GigabitEthernet1/0/1
11:
```

查看当前配置，从包含“user-group”字符串的行开始到最后一行配置信息，并同时显示行号。（行号后为“:”表示该行包含“user-group”字符串，行号后为“-”表示该行不包含“user-group”字符串。）

```
<Sysname> display current-configuration | by-linenum begin user-group
114: user-group system
115: #
116: return
```

1.1.4 display >

display >命令用来将显示信息独立保存到文件。

【命令】

display command > filename

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

command: 命令关键字，取值可以通过输入?来获得。

filename: 文件名称，为 1~63 个字符的字符串。

【使用指导】

display 命令显示的内容通常是统计信息、功能是否使能以及功能的相关参数配置，这些信息在设备运行过程中会随着时间的变化或者用户的配置而改变。使用本命令可以将当前显示信息保存到文件，可供用户随时比对和查看。

执行本命令时，如果 **filename** 不存在，系统会先创建该文件，再保存；如果 **filename** 已存在，则会覆盖原文件的内容。

【举例】

将 display vlan 1 的显示信息保存到文件 vlan.txt。

```
<Sysname> display vlan 1 > vlan.txt
```

查看 vlan.txt 的内容，验证 **display >** 命令的执行效果。

```
<Sysname> more vlan.txt
```

```
VLAN ID: 1  
VLAN type: Static  
Route interface: Not configured  
Description: VLAN 0001  
Name: VLAN 0001  
Tagged ports:   None  
Untagged ports:  
    GigabitEthernet1/0/2
```

1.1.5 display >>

display >> 命令用来将显示信息以追加方式保存到文件。

【命令】

display command >> filename

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

command: 命令关键字，取值可以通过输入?来获得。

filename: 文件名称，为 1~63 个字符的字符串。

【使用指导】

display 命令显示的内容通常是统计信息、功能是否使能以及功能的相关参数配置，这些信息在设备运行过程中会随着时间或者用户的配置而改变。使用本命令可以将当前显示信息保存到文件，可供用户随时比对和查看。

执行本命令时，如果 **filename** 不存在，系统会先创建该文件，再保存。如果 **filename** 已存在，则新保存的内容会追加到文件 **filename** 的尾部。

【举例】

将 **display vlan 999** 的显示信息以追加方式保存到文件 **vlan.txt**。

```
<Sysname> display vlan 999 >> vlan.txt
```

查看 **vlan.txt** 的内容，验证 **display >>** 命令的执行效果。

```
<Sysname> more vlan.txt
```

```
VLAN ID: 1
```

```
VLAN type: Static
```

```
Route interface: Not configured
```

```
Description: VLAN 0001
```

```
Name: VLAN 0001
```

```
Tagged ports:   None
```

```
Untagged ports:
```

```
    GigabitEthernet1/0/2
```

```
VLAN ID: 999
```

```
VLAN type: Static
```

```
Route interface: Configured
```

```
IPv4 address: 192.168.2.1
```

```
IPv4 subnet mask: 255.255.255.0
```

```
Description: For LAN Access
```

```
Name: VLAN 0999
```

```
Tagged ports:   None
```

```
Untagged ports:
```

```
    GigabitEthernet1/0/2
```

1.1.6 display alias

display alias 命令用来查看命令别名的相关配置。

【命令】

```
display alias [ alias ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

alias: 表示配置的命令别名。不指定该参数，则显示所有的已配置的命令别名。

【举例】

查看系统中配置的所有命令别名。

```
<Sysname> display alias
```

Index	Alias	Command key
1	access-list	acl
2	end	return
3	erase	delete
4	exit	quit
5	hostname	sysname
6	logging	info-center
7	no	undo
8	shinc	display \$1 include \$2
9	show	display
10	sirt	display ip routing-table
11	write	save

查看别名命令 **shinc** 表示的命令字符串。

```
<Sysname> display alias shinc
```

Alias	Command key
shinc	display ip \$1 include \$2

表1-2 display alias 命令显示信息描述表

字段	描述
Index	索引号
Alias	别名
Command key	命令字符串

【相关命令】

- **alias**

1.1.7 display history-command

display history-command 命令用来显示当前登录用户历史命令缓冲区中的命令。

【命令】

display history-command

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

用户登录设备后，系统会给每个用户自动分配一个历史命令缓冲区，用于存放用户本次登录成功执行的命令行，以便用户查看和调用。历史命令缓存区有大小限制，缺省保存 10 条命令，用户也可以通过 **history-command max-size** 命令来修改大小。当数目达到上限时，系统会自动删除最早的记录，来保存最新成功执行的命令。

如果用户退出登录，系统会自动清除该历史命令缓存区的所有记录。

【举例】

显示历史命令缓存区内保存的命令。

```
<Sysname> display history-command  
system-view  
vlan 2  
quit
```

【相关命令】

- **history-command max-size**（基础配置命令参考/登录设备）

1.1.8 display history-command all

display history-command all 命令用来显示所有登录用户历史命令缓冲区中的命令。

【命令】

display history-command all

【视图】

任意视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

系统中有一个共享历史命令缓冲区，用于存放所有登录用户成功执行的命令行，以便用户查看（不能调用）。历史命令缓存区的大小固定为 1024 条，不可配置。当数目达到上限时，系统会自动删除最早的记录，来保存最新成功执行的命令。

即使用户退出登录，系统也不会清除共享历史命令缓存区中该用户的历史命令记录。

【举例】

显示所有登录用户成功执行的历史命令。

```
<Sysname> display history-command all  
Date           Time           Terminal  Ip           User
```

```
03/16/2017 20:03:33 vty0      192.168.1.26    **
Cmd:dis his all

03/16/2017 20:03:29 vty0      192.168.1.26    **
Cmd:sys
```

表1-3 display history-command all 命令显示信息描述表

字段	描述
Date	执行命令行的日期
Time	执行命令行的时间
Terminal	执行命令的用户使用的登录用户线
Ip	执行命令的用户使用的登录IP
User	如果用户使用scheme方式登录设备，该字段显示为执行命令的用户使用的登录用户名；如果使用其他方式登录设备，该字段显示为**
Cmd	执行的命令（和用户的输入保持一致）

【相关命令】

- **display history-command**

1.1.9 display hotkey

display hotkey 命令用来显示系统支持的快捷键及其含义。

【命令】

display hotkey

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【举例】

```
# 显示系统支持的快捷键及其含义。
<Sysname>display hotkey
----- Hotkeys -----
      -Defined command hotkeys-
CTRL_G display current-configuration
CTRL_L display ip routing-table
CTRL_O undo debugging all
      -Undefined command hotkeys-
CTRL_T NULL
```

CTRL_U NULL

-System-reserved hotkeys-

CTRL_A Move the cursor to the beginning of the line.

CTRL_B Move the cursor one character to the left.

CTRL_C Stop the current command.

CTRL_D Erase the character at the cursor.

CTRL_E Move the cursor to the end of the line.

CTRL_F Move the cursor one character to the right.

CTRL_H Erase the character to the left of the cursor.

CTRL_K Abort the connection request.

CTRL_N Display the next command in the history buffer.

CTRL_P Display the previous command in the history buffer.

CTRL_R Redisplay the current line.

CTRL_V Paste text from the clipboard.

CTRL_W Delete the word to the left of the cursor.

CTRL_X Delete all characters from the beginning of the line to the cursor.

CTRL_Y Delete all characters from the cursor to the end of the line.

CTRL_Z Return to the User View.

CTRL_] Kill incoming connection or redirect connection.

ESC_B Move the cursor back one word.

ESC_D Delete all characters from the cursor to the end of the word.

ESC_F Move the cursor forward one word.

ESC_N Move the cursor down a line.

ESC_P Move the cursor up a line.

ESC_< Move the cursor to the beginning of the clipboard.

ESC_> Move the cursor to the end of the clipboard.

表1-4 display hotkey 命令显示信息描述表

字段	描述
Defined command hotkeys	已定义的快捷键
Undefined command hotkeys	未定义的快捷键
System-reserved hotkeys	系统保留的快捷键。每个保留快捷键的作用请参见 表1-5

表1-5 系统保留的快捷键

快捷键	功能
<Ctrl+A>	将光标移动到当前行的开头
<Ctrl+B>	将光标向左移动一个字符
<Ctrl+C>	停止当前正在执行的功能
<Ctrl+D>	删除当前光标所在位置的字符
<Ctrl+E>	将光标移动到当前行的末尾
<Ctrl+F>	将光标向右移动一个字符
<Ctrl+H>	删除光标左侧的一个字符

快捷键	功能
<Ctrl+K>	终止呼出的连接
<Ctrl+N>	显示历史缓冲区中的下一条命令
<Ctrl+P>	显示历史缓冲区中的上一条命令
<Ctrl+R>	重新显示当前行信息
<Ctrl+V>	粘贴剪贴板的内容
<Ctrl+W>	删除光标左侧连续字符串内的所有字符
<Ctrl+X>	删除光标左侧所有的字符
<Ctrl+Y>	删除光标所在位置及其右侧所有的字符
<Ctrl+Z>	退回到用户视图
<Ctrl+]>	终止当前连接
<Esc+B>	将光标移动到左侧连续字符串的首字符处
<Esc+D>	删除光标所在位置及其右侧连续字符串内的所有字符
<Esc+F>	将光标向右移到下一个连续字符串之前
<Esc+N>	将光标向下移动一行（输入回车前有效）
<Esc+P>	将光标向上移动一行（输入回车前有效）
<Esc+<>	将光标所在位置指定为剪贴板的开始位置
<Esc+>>	将光标所在位置指定为剪贴板的结束位置

【相关命令】

- **hotkey**

1.1.10 hotkey

hotkey 命令用来为快捷键指定对应的命令行。

undo hotkey 命令用来恢复缺省情况。

【命令】

```
hotkey { ctrl_g | ctrl_l | ctrl_o | ctrl_t | ctrl_u } command
undo hotkey { ctrl_g | ctrl_l | ctrl_o | ctrl_t | ctrl_u }
```

【缺省情况】

<Ctrl+G>对应命令 **display current-configuration**（显示当前配置）。

<Ctrl+L>对应命令 **display ip routing-table**（显示 IPv4 路由表信息）。

<Ctrl+O>对应命令 **undo debugging all**（关闭设备支持的所有功能项的调试开关）。

<Ctrl+T>未关联任何命令行。

<Ctrl+U>未关联任何命令行。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ctrl_g: 表示为快捷键<Ctrl+G>指定一条命令。

ctrl_l: 表示为快捷键<Ctrl+L>指定一条命令。

ctrl_o: 表示为快捷键<Ctrl+O>指定一条命令。

ctrl_t: 表示为快捷键<Ctrl+T>指定一条命令。

ctrl_u: 表示为快捷键<Ctrl+U>指定一条命令。

command: 快捷键关联的命令行。

【使用指导】

通过快捷键用户可以简便、快捷的操作设备，使用 **display hotkey** 命令可以查看设备支持的所有快捷键及其含义。

【举例】

指定命令 **display tcp statistics** 的快捷键为<Ctrl+T>。

```
<Sysname> system-view
```

```
[Sysname] hotkey ctrl_t display tcp statistics
```

【相关命令】

- **display hotkey**

1.1.11 quit

quit 命令用来使用户从当前视图退回到上一层视图。

【命令】

quit

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【使用指导】

如果当前是用户视图，执行 **quit** 后，会断开当前连接，退出系统。

【举例】

从接口 GigabitEthernet1/0/1 视图退回到系统视图，再退回到用户视图。

```
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] quit
<Sysname>
```

1.1.12 repeat

repeat 命令用来重复执行历史记录命令。

【命令】

repeat [*number*] [*count times*] [*delay seconds*]

【视图】

任意视图

【缺省用户角色】

network-admin
context-admin

【参数】

number: 表示重复执行历史命令的条数，取值范围为 1~10，缺省值为 1。

count times: 表示重复执行历史命令的次数，取值范围为 0~4294967295，缺省值为 0。如不指定该参数，则历史命令一直重复执行，直到执行用户线视图下设置的终止当前运行任务的快捷键才能停止执行该命令，默认的终止快捷键为<Ctrl+C>。关于终止当前执行任务的快捷键的设置，请参见“基础配置命令”中的“登录设备”。

delay seconds: 表示重复执行历史命令的时间间隔，取值范围为 0~4294967295，单位为秒，缺省值为 1。

【使用指导】

重复执行历史命令时，系统将按照历史命令的下发顺序执行。例如，用户在某视图下依次执行命令 a、b 和 c 后，再执行 **repeat 3** 命令，则系统将按照 a、b 和 c 的顺序重复执行。

如果用户重复执行的历史命令中存在交互式命令，需要用户手动处理此交互式命令，直到交互式命令执行结束，历史命令才会继续被重复执行。

【举例】

重复执行最近 2 条历史命令 **display cpu-usage** 和 **display clock**，重复执行 3 次，时间间隔 10 秒。

```
<Sysname> repeat 2 count 3 delay 10
<Sysname> display cpu-usage
Unit CPU usage:
    33% in last 5 seconds
    32% in last 1 minute
    33% in last 5 minutes
<Sysname> display clock
07:02:18 UTC Thu 06/19/2017
<Sysname> display cpu-usage
Unit CPU usage:
    33% in last 5 seconds
    32% in last 1 minute
```

```
33% in last 5 minutes
<Sysname> display clock
07:02:28 UTC Thu 06/19/2017
<Sysname> display cpu-usage
Unit CPU usage:
33% in last 5 seconds
32% in last 1 minute
33% in last 5 minutes
<Sysname> display clock
07:02:38 UTC Thu 06/19/2017
```

【相关命令】

- **display history-command**
- **escape-key**（基础配置命令参考/登录设备）
- **history-command max-size**

1.1.13 return

return 命令用来从当前视图（除 Tcl 配置视图和 Python shell 外的任意非用户视图）直接退回到用户视图。

【命令】

return

【视图】

除 Tcl 配置视图和 Python shell 外的任意非用户视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

在除 Tcl 配置视图和 Python shell 外的任意非用户视图下，也可以按快捷键<Ctrl+Z>退回到用户视图，功能等同于 **return** 命令。

Tcl 配置视图和 Python shell 下退回到用户视图的方式分别为：

- Tcl 配置视图下请使用 **tclquit** 返回用户视图。
- 在 Python shell 下请通过执行 **exit()**命令，从 Python shell 退回到用户视图。

【举例】

```
# 从接口 GigabitEthernet1/0/1 视图退回到用户视图。
[Sysname-GigabitEthernet1/0/1] return
<Sysname>
```

1.1.14 screen-length disable

screen-length disable 命令用来关闭当前用户的分屏显示功能。

undo screen-length disable 命令用来开启当前用户的分屏显示功能。

【命令】

```
screen-length disable
undo screen-length disable
```

【缺省情况】

用户登录后将遵循用户线下的 **screen-length** 设置。**screen-length** 设置的缺省情况为：允许分屏显示，下一屏显示 24 行数据。

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

分屏显示功能处于关闭状态时，会一次显示所有信息，如果信息较多，则会连续刷屏，不方便立即查看。

该配置只对当前用户本次登录有效，用户重新登录后将恢复到缺省情况。

【举例】

```
# 关闭当前用户的分屏显示功能。
<Sysname> screen-length disable
```

【相关命令】

- **screen-length** （基础配置命令参考/登录设备）

1.1.15 system-view

system-view 命令用来从用户视图进入系统视图。

【命令】

```
system-view
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【举例】

```
# 从用户视图进入系统视图。
<Sysname> system-view
System View: return to User View with Ctrl+Z.
```


[Sysname]

目 录

1 RBAC	1-1
1.1 RBAC配置命令	1-1
1.1.1 description	1-1
1.1.2 display role.....	1-1
1.1.3 display role feature.....	1-16
1.1.4 display role feature-group	1-18
1.1.5 feature	1-20
1.1.6 interface policy deny.....	1-21
1.1.7 permit interface	1-22
1.1.8 permit security-zone	1-24
1.1.9 permit vlan	1-25
1.1.10 role	1-27
1.1.11 role default-role enable.....	1-28
1.1.12 role feature-group	1-28
1.1.13 rule	1-29
1.1.14 security-zone policy deny.....	1-33
1.1.15 super.....	1-34
1.1.16 super authentication-mode	1-35
1.1.17 super default role	1-36
1.1.18 super password	1-37
1.1.19 super use-login-username	1-38
1.1.20 vlan policy deny	1-39
1.1.21 vpn-instance policy deny	1-40

1 RBAC

1.1 RBAC配置命令

1.1.1 description

description 命令用来配置用户角色的描述信息，用来方便管理员对用户角色进行管理。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

未定义用户角色描述信息。

【视图】

用户角色视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: 用户角色描述信息，为 1~128 个字符的字符串，区分大小写。

【举例】

为用户角色 **role1** 配置描述信息为 “labVIP”。

```
<Sysname> system-view
```

```
[Sysname] role name role1
```

```
[Sysname-role-role1] description labVIP
```

【相关命令】

- **display role**
- **role**

1.1.2 display role

display role 命令用来显示用户角色信息。

【命令】

display role [**name** *role-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

name *role-name*: 用户角色名称，为 1~63 个字符的字符串，区分大小写。如果不指定用户角色名称，则表示显示所有用户角色的信息，包括系统缺省存在的用户角色的信息。

【举例】

显示用户角色 123 的信息。

<Sysname> display role name 123

Role: 123

Description: new role

VLAN policy: Deny

Permitted VLANs: 1 to 5, 7 to 8

Interface policy: Deny

Permitted interfaces: GigabitEthernet1/0/1 to GigabitEthernet1/0/3, Vlan-interface1 to Vlan-interface20

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

显示所有用户角色的信息。

<Sysname> display role

Role: network-admin

Description: Predefined network admin role has access to all commands on the device

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	permit		command	*
sys-2	permit	RWX	web-menu	-
sys-3	permit	RWX	xml-element	-
sys-4	deny		command	display security-logfile summary
sys-5	deny		command	system-view ; info-center security-logfile directory *
sys-6	deny		command	security-logfile save
sys-7	permit	RW-	oid	1

R:Read W:Write X:Execute

Role: network-operator

Description: Predefined network operator role has access to all read commands on the device

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)
 Security zone policy: Permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	permit		command	display *
sys-2	permit		command	xml
sys-3	deny		command	display history-command all
sys-4	deny		command	display exception *
sys-5	deny		command	display cpu-usage configuration *
sys-6	deny		command	display kernel exception *
sys-7	deny		command	display kernel deadlock *
sys-8	deny		command	display kernel starvation *
sys-9	deny		command	display kernel reboot *
sys-12	permit		command	system-view ; local-user *
sys-13	permit		command	system-view ; switchto *
sys-14	permit R--		web-menu	-
sys-15	permit RW-		web-menu	m_device/m_maintenance/m_change password
sys-16	permit R--		xml-element	-
sys-17	deny		command	display security-logfile summary
sys-18	deny		command	system-view ; info-center security-logfile directory *
sys-19	deny		command	security-logfile save
sys-20	deny		command	system-view ; local-user-import *
sys-21	deny		command	system-view ; local-user-export *
sys-22	permit R--		oid	1

R:Read W:Write X:Execute

Role: context-admin

Description: Predefined context admin role has access to all commands within a context

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	permit		command	*
sys-2	permit RWX		web-menu	-
sys-3	permit RWX		xml-element	-
sys-4	deny RWX		feature	context
sys-5	permit		command	display context *
sys-6	deny		command	display security-logfile summary
sys-7	deny		command	system-view ; info-center security

```

ty-logfile directory *
sys-8  deny      command security-logfile save
sys-9  permit RW- oid      1
R:Read W:Write X:Execute

```

Role: context-operator

Description: Predefined context operator role has access to all read commands within a context

```

VLAN policy: Permit (default)
Interface policy: Permit (default)
VPN instance policy: Permit (default)
Security zone policy: Permit (default)

```

Rule	Perm	Type	Scope	Entity
sys-1	permit		command	display *
sys-2	permit		command	xml
sys-3	deny		command	display history-command all
sys-4	deny		command	display exception *
sys-5	deny		command	display cpu-usage configuration *
sys-6	deny		command	display kernel exception *
sys-7	deny		command	display kernel deadlock *
sys-8	deny		command	display kernel starvation *
sys-9	deny		command	display kernel reboot *
sys-12	permit		command	system-view ; local-user *
sys-13	permit R--		web-menu	-
sys-14	permit RW-		web-menu	m_device/m_maintenance/m_changepassword
sys-15	permit R--		xml-element	-
sys-16	deny		command	display security-logfile summary
sys-17	deny		command	system-view ; info-center security-logfile directory *
sys-18	deny		command	security-logfile save
sys-19	permit R--		oid	1

R:Read W:Write X:Execute

Role: level-0

Description: Predefined level-0 role

```

VLAN policy: Permit (default)
Interface policy: Permit (default)
VPN instance policy: Permit (default)
Security zone policy: Permit (default)

```

Rule	Perm	Type	Scope	Entity
sys-1	permit		command	tracert *
sys-2	permit		command	telnet *
sys-3	permit		command	ping *

```

sys-4  permit      command      ssh2 *
sys-5  permit      command      super *
R:Read W:Write X:Execute

```

Role: level-1

```

Description: Predefined level-1 role
VLAN policy: Permit (default)
Interface policy: Permit (default)
VPN instance policy: Permit (default)
Security zone policy: Permit (default)

```

```

-----
Rule    Perm   Type  Scope      Entity
-----
sys-1   permit      command    tracert *
sys-2   permit      command    telnet *
sys-3   permit      command    ping *
sys-4   permit      command    ssh2 *
sys-5   permit      command    display *
sys-6   permit      command    super *
sys-7   deny        command    display history-command all
R:Read W:Write X:Execute

```

Role: level-2

```

Description: Predefined level-2 role
VLAN policy: Permit (default)
Interface policy: Permit (default)
VPN instance policy: Permit (default)
Security zone policy: Permit (default)

```

Role: level-3

```

Description: Predefined level-3 role
VLAN policy: Permit (default)
Interface policy: Permit (default)
VPN instance policy: Permit (default)
Security zone policy: Permit (default)

```

Role: level-4

```

Description: Predefined level-4 role
VLAN policy: Permit (default)
Interface policy: Permit (default)
VPN instance policy: Permit (default)
Security zone policy: Permit (default)

```

Role: level-5

```

Description: Predefined level-5 role
VLAN policy: Permit (default)
Interface policy: Permit (default)
VPN instance policy: Permit (default)

```

Security zone policy: Permit (default)

Role: level-6

Description: Predefined level-6 role

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

Role: level-7

Description: Predefined level-7 role

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

Role: level-8

Description: Predefined level-8 role

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

Role: level-9

Description: Predefined level-9 role

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	permit	RWX	feature	-
sys-2	deny	RWX	feature	device
sys-3	deny	RWX	feature	filesystem
sys-4	permit		command	display *
sys-5	deny		command	display history-command all

R:Read W:Write X:Execute

Role: level-10

Description: Predefined level-10 role

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

Role: level-11

Description: Predefined level-11 role

VLAN policy: Permit (default)
 Interface policy: Permit (default)
 VPN instance policy: Permit (default)
 Security zone policy: Permit (default)

Role: level-12

Description: Predefined level-12 role
 VLAN policy: Permit (default)
 Interface policy: Permit (default)
 VPN instance policy: Permit (default)
 Security zone policy: Permit (default)

Role: level-13

Description: Predefined level-13 role
 VLAN policy: Permit (default)
 Interface policy: Permit (default)
 VPN instance policy: Permit (default)
 Security zone policy: Permit (default)

Role: level-14

Description: Predefined level-14 role
 VLAN policy: Permit (default)
 Interface policy: Permit (default)
 VPN instance policy: Permit (default)
 Security zone policy: Permit (default)

Role: level-15

Description: Predefined level-15 role
 VLAN policy: Permit (default)
 Interface policy: Permit (default)
 VPN instance policy: Permit (default)
 Security zone policy: Permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	permit		command	*
sys-2	permit	RWX	web-menu	-
sys-3	permit	RWX	xml-element	-
sys-4	deny		command	display security-logfile summary
sys-5	deny		command	system-view ; info-center security-logfile directory *
sys-6	deny		command	security-logfile save
sys-7	permit	RW-	oid	1
R:Read W:Write X:Execute				

Role: security-audit

Description: Predefined security audit role only has access to commands for the security log administrator
 VLAN policy: Permit (default)

Interface policy: Permit (default)
 VPN instance policy: Permit (default)
 Security zone policy: Permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	deny		command	*
sys-2	permit		command	display security-logfile summary
sys-3	permit		command	system-view ; info-center security-logfile directory *
sys-4	permit		command	security-logfile save
sys-5	permit		command	cd *
sys-6	permit		command	copy *
sys-7	permit		command	delete *
sys-8	permit		command	dir *
sys-9	permit		command	mkdir *
sys-10	permit		command	more *
sys-11	permit		command	move *
sys-12	permit		command	rmdir *
sys-13	permit		command	pwd
sys-14	permit		command	rename *
sys-15	permit		command	undelete *
sys-16	permit		command	ftp *
sys-17	permit		command	sftp *

R:Read W:Write X:Execute

Role: guest-manager

Description: Predefined guest manager role can't access to commands
 VLAN policy: Permit (default)
 Interface policy: Permit (default)
 VPN instance policy: Permit (default)
 Security zone policy: Permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	permit	RWX	xml-element	useraccounts/approveguest/
sys-2	permit	RWX	xml-element	useraccounts/exportguestaccount/
sys-3	permit	RWX	xml-element	useraccounts/generateguestaccount/
sys-4	permit	RWX	xml-element	useraccounts/guest/
sys-5	permit	RWX	xml-element	useraccounts/guestconfigure/
sys-6	permit	RWX	xml-element	useraccounts/importguestaccount/
sys-7	permit	RWX	xml-element	useraccounts/exportguesttemplet/
sys-8	permit	RWX	xml-element	rpc/
sys-9	permit	RWX	web-menu	m_global/m_networksecurity/m_guestmanage/m_guestlist/
sys-10	permit	RWX	web-menu	m_global/m_networksecurity/m_guestmanage/m_importguest/

sys-11	permit	RWX	web-menu	m_global/m_networksecurity/m_gue stmanage/m_generateguest/
sys-12	permit	RWX	web-menu	m_global/m_networksecurity/m_gue stmanage/m_approveguest/
sys-13	deny		command	*

R:Read W:Write X:Execute

Role: system-admin

Description: Predefined system admin role only has access to commands for the system administrator

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	permit	RWX	web-menu	dashboard/
sys-2	permit	RWX	web-menu	m_monitor/m_monitorlog/m_syslog
sys-3	permit	RWX	web-menu	m_device/m_virtualdevice/m_clust er
sys-4	permit	RWX	web-menu	m_device/m_virtualdevice/m_conte xt/
sys-5	permit	RWX	web-menu	m_device/m_highavailability/m_ho tbackup
sys-6	permit	RWX	web-menu	m_device/m_highavailability/m_vr rp
sys-7	permit	RWX	web-menu	m_device/m_highavailability/m_vr rpinterface
sys-8	permit	RWX	web-menu	m_device/m_logconf/m_basiclog
sys-9	permit	RWX	web-menu	m_device/m_logconf/m_natlog
sys-10	permit	RWX	web-menu	m_device/m_logconf/m_sessionlog
sys-11	permit	RWX	web-menu	m_device/m_logconf/m_atkadvancel og
sys-12	permit	RWX	web-menu	m_device/m_logconf/m_threatenlog
sys-13	permit	RWX	web-menu	m_device/m_logconf/m_urlfilterlo g
sys-14	permit	RWX	web-menu	m_device/m_logconf/m_auditlog
sys-15	permit	RWX	web-menu	m_device/m_logconf/m_cfgadvancel og
sys-16	permit	RWX	web-menu	m_device/m_reportconf/m_reportsu bscription
sys-17	permit	RWX	web-menu	m_device/m_reportconf/m_mailserv erconfig
sys-18	permit	RWX	web-menu	m_device/m_persistdisk
sys-19	permit	RWX	web-menu	m_device/m_sessionagingtimeset/m _protocolstatesessionagingtime
sys-20	permit	RWX	web-menu	m_device/m_sessionagingtimeset/m _appagingtime

sys-21	permit	RWX	web-menu	m_device/m_sessionagingtimeset/m_sessionsettings
sys-22	permit	RWX	web-menu	m_device/m_signatureupgrade/m_upgradecenter
sys-23	permit	RWX	web-menu	m_device/m_signatureupgrade/m_upgrade
sys-24	permit	RWX	web-menu	m_device/m_license
sys-25	permit	RWX	web-menu	m_device/m_maintenance/m_devicesettings/
sys-26	permit	RWX	web-menu	m_device/m_maintenance/m_config
sys-27	permit	RWX	web-menu	m_device/m_maintenance/m_diagnostic
sys-28	permit	RWX	web-menu	m_device/m_maintenance/m_pcapware
sys-29	permit	RWX	web-menu	m_device/m_maintenance/m_reboot
sys-30	permit	RWX	web-menu	m_device/m_maintenance/m_about/
sys-31	permit	RWX	web-menu	m_device/m_maintenance/m_changepassword
sys-32	permit	RWX	web-menu	m_device/m_adminuser/m_admin
sys-33	permit	RWX	web-menu	m_device/m_adminuser/m_rbacrole
sys-34	permit		command	tracert *
sys-35	permit		command	ping *

R:Read W:Write X:Execute

Role: security-admin

Description: Predefined security admin role only has access to commands for the security administrator

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	permit	RWX	web-menu	m_monitor/m_atklog/m_blacklistlog
sys-2	permit	RWX	web-menu	m_monitor/m_atklog/m_singleatk
sys-3	permit	RWX	web-menu	m_monitor/m_atklog/m_scanatk
sys-4	permit	RWX	web-menu	m_monitor/m_atklog/m_floodatk
sys-5	permit	RWX	web-menu	m_monitor/m_atklog/m_threatlog
sys-6	permit	RWX	web-menu	m_monitor/m_atklog/m_urllog
sys-7	permit	RWX	web-menu	m_monitor/m_atklog/m_filefilterlog
sys-8	permit	RWX	web-menu	m_monitor/m_atklog/m_zonepairlog
sys-9	permit	RWX	web-menu	m_monitor/m_auditlogs/m_auditimchatlog
sys-10	permit	RWX	web-menu	m_monitor/m_auditlogs/m_auditcommunitylog
sys-11	permit	RWX	web-menu	m_monitor/m_auditlogs/m_auditsea

				rchengine.log
sys-12	permit	RWX	web-menu	m_monitor/m_auditlogs/m_auditmai llog
sys-13	permit	RWX	web-menu	m_monitor/m_auditlogs/m_auditfil etransferlog
sys-14	permit	RWX	web-menu	m_monitor/m_auditlogs/m_auditrel axstocklog
sys-15	permit	RWX	web-menu	m_monitor/m_auditlogs/m_auditoth erapplog
sys-16	permit	RWX	web-menu	m_monitor/m_monitorlog/m_traffic log
sys-17	permit	RWX	web-menu	m_monitor/m_rank/m_trafficrank/
sys-18	permit	RWX	web-menu	m_monitor/m_rank/m_threadrank/
sys-19	permit	RWX	web-menu	m_monitor/m_rank/m_urlfilterrank /
sys-20	permit	RWX	web-menu	m_monitor/m_rank/m_ffilterrank/
sys-21	permit	RWX	web-menu	m_monitor/m_rank/m_securityaudit /
sys-22	permit	RWX	web-menu	m_monitor/m_rank/m_lb_serverrepo rt/
sys-23	permit	RWX	web-menu	m_monitor/m_rank/m_lb_linkreport /
sys-24	permit	RWX	web-menu	m_monitor/m_rank/m_lb_dnsproxyre port/
sys-25	permit	RWX	web-menu	m_monitor/m_rank/m_dropstats
sys-26	permit	RWX	web-menu	m_monitor/m_trend/m_traffictrend /
sys-27	permit	RWX	web-menu	m_monitor/m_trend/m_threadtrend/
sys-28	permit	RWX	web-menu	m_monitor/m_trend/m_urlfiltertre nd/
sys-29	permit	RWX	web-menu	m_monitor/m_trend/m_ffiltertrend /
sys-30	permit	RWX	web-menu	m_monitor/m_trend/m_lb_urltrend
sys-31	permit	RWX	web-menu	m_monitor/m_report
sys-32	permit	RWX	web-menu	m_monitor/m_session
sys-33	permit	RWX	web-menu	m_monitor/m_userinfocenter
sys-34	permit	RWX	web-menu	m_monitor/m_lb_dnscaches
sys-35	permit	RWX	web-menu	m_policy/m_firewall/m_secpolicy
sys-36	permit	RWX	web-menu	m_policy/m_firewall/m_targetpoli cy
sys-37	permit	RWX	web-menu	m_policy/m_firewall/m_redundancy rules
sys-38	permit	RWX	web-menu	m_policy/m_attackdefense/m_atkpo licy
sys-39	permit	RWX	web-menu	m_policy/m_attackdefense/m_clien tverifyprotectip
sys-40	permit	RWX	web-menu	m_policy/m_attackdefense/m_black listmanual

sys-41	permit	RWX	web-menu	m_policy/m_attackdefense/m_white listmanual
sys-42	permit	RWX	web-menu	m_policy/m_attackdefense/m_clien tverifyzone
sys-43	permit	RWX	web-menu	m_policy/m_attackdefense/m_connl imitpolicies
sys-44	permit	RWX	web-menu	m_policy/m_attackdefense/m_urpf/
sys-45	permit	RWX	web-menu	m_policy/m_nat/m_natbasicchange
sys-46	permit	RWX	web-menu	m_policy/m_nat/m_natoutboundconf ig/
sys-47	permit	RWX	web-menu	m_policy/m_nat/m_natserverconfig /
sys-48	permit	RWX	web-menu	m_policy/m_nat/m_natstaticchange /
sys-49	permit	RWX	web-menu	m_policy/m_nat/m_natoutbound444c onfig/
sys-50	permit	RWX	web-menu	m_policy/m_nat/m_natoutboundstat ic444config/
sys-51	permit	RWX	web-menu	m_policy/m_nat/m_natsettings/
sys-52	permit	RWX	web-menu	m_policy/m_appaudit/m_auditpolic y
sys-53	permit	RWX	web-menu	m_policy/m_appaudit/m_keywordgro ups
sys-54	permit	RWX	web-menu	m_policy/m_bandwidthmanagement/m _bandwidthpolicy
sys-55	permit	RWX	web-menu	m_policy/m_bandwidthmanagement/m _bandwidthchannel
sys-56	permit	RWX	web-menu	m_policy/m_bandwidthmanagement/m _interfacebandwidth
sys-57	permit	RWX	web-menu	m_policy/m_loadbalance/m_lb_glob alconfig/
sys-58	permit	RWX	web-menu	m_policy/m_loadbalance/m_lb_serv er/
sys-59	permit	RWX	web-menu	m_policy/m_loadbalance/m_lb_link /
sys-60	permit	RWX	web-menu	m_resource/m_healthmonitor
sys-61	permit	RWX	web-menu	m_policy/m_netshare/m_netsharepo licy
sys-62	permit	RWX	web-menu	m_policy/m_netshare/m_netsharest atus
sys-63	permit	RWX	web-menu	m_resource/m_user/m_usercontrol/
sys-64	permit	RWX	web-menu	m_resource/m_user/m_authenticati on/
sys-65	permit	RWX	web-menu	m_resource/m_user/m_access/
sys-66	permit	RWX	web-menu	m_resource/m_dpi/m_ipscfg/
sys-67	permit	RWX	web-menu	m_resource/m_dpi/m_antiviruscfg/
sys-68	permit	RWX	web-menu	m_resource/m_dpi/m_dfltcfg/
sys-69	permit	RWX	web-menu	m_resource/m_dpi/m_ufltcfg/

sys-70	permit	RWX	web-menu	m_resource/m_dpi/m_ffltcfg/
sys-71	permit	RWX	web-menu	m_resource/m_dpi/m_apprecognition/
sys-72	permit	RWX	web-menu	m_resource/m_dpi/m_securityaction/
sys-73	permit	RWX	web-menu	m_resource/m_dpi/m_dpifcfg
sys-74	permit	RWX	web-menu	m_resource/m_objectgroup/m_ipv4objectgroup
sys-75	permit	RWX	web-menu	m_resource/m_objectgroup/m_ipv6objectgroup
sys-76	permit	RWX	web-menu	m_resource/m_objectgroup/m_macobjectgroup
sys-77	permit	RWX	web-menu	m_resource/m_objectgroup/m_serviceobjectgroup
sys-78	permit	RWX	web-menu	m_resource/m_objectgroup/m_timerange
sys-79	permit	RWX	web-menu	m_resource/m_acl/m_ipv4acl
sys-80	permit	RWX	web-menu	m_resource/m_acl/m_ipv6acl
sys-81	permit	RWX	web-menu	m_resource/m_acl/m_macacl
sys-82	permit	RWX	web-menu	m_resource/m_ssl/m_sslserver
sys-83	permit	RWX	web-menu	m_resource/m_ssl/m_sslclient
sys-84	permit	RWX	web-menu	m_resource/m_ssl/m_ssladvancesetting
sys-85	permit	RWX	web-menu	m_resource/m_publickey/m_publickeylocal
sys-86	permit	RWX	web-menu	m_resource/m_publickey/m_publickeypeer
sys-87	permit	RWX	web-menu	m_resource/m_pki_cert/m_pki
sys-88	permit	RWX	web-menu	m_resource/m_pki_cert/m_certificatepolicy
sys-89	permit	RWX	web-menu	m_resource/m_pki_cert/m_certificatesubject
sys-90	permit	RWX	web-menu	m_network/m_vrf
sys-91	permit	RWX	web-menu	m_network/m_if/m_interface
sys-92	permit	RWX	web-menu	m_network/m_if/m_inline
sys-93	permit	RWX	web-menu	m_network/m_if/m_collaborations
sys-94	permit	RWX	web-menu	m_network/m_if/m_lagg
sys-95	permit	RWX	web-menu	m_network/m_seczone
sys-96	permit	RWX	web-menu	m_network/m_link/m_vlan
sys-97	permit	RWX	web-menu	m_network/m_link/m_mac
sys-98	permit	RWX	web-menu	m_network/m_dns_sum/m_dnshosts
sys-99	permit	RWX	web-menu	m_network/m_dns_sum/m_dns
sys-100	permit	RWX	web-menu	m_network/m_dns_sum/m_ddns
sys-101	permit	RWX	web-menu	m_network/m_dns_sum/m_dnsadvance
sys-102	permit	RWX	web-menu	m_network/m_ip_net/m_ip
sys-103	permit	RWX	web-menu	m_network/m_ip_net/m_arp
sys-104	permit	RWX	web-menu	m_network/m_ipv6_net/m_ipv6
sys-105	permit	RWX	web-menu	m_network/m_ipv6_net/m_nd

sys-106	permit	RWX	web-menu	m_network/m_vpn/m_gre
sys-107	permit	RWX	web-menu	m_network/m_vpn/m_ipsec/
sys-108	permit	RWX	web-menu	m_network/m_vpn/m_advpn/
sys-109	permit	RWX	web-menu	m_network/m_vpn/m_l2tp/
sys-110	permit	RWX	web-menu	m_network/m_sslvpn/m_sslvpn_cont ext
sys-111	permit	RWX	web-menu	m_network/m_sslvpn/m_sslvpn_gate way
sys-112	permit	RWX	web-menu	m_network/m_sslvpn/m_sslvpn_ipv4 addrpool
sys-113	permit	RWX	web-menu	m_network/m_sslvpn/m_sslvpn_acif
sys-114	permit	RWX	web-menu	m_network/m_sslvpn/m_sslvpn_stat istics
sys-115	permit	RWX	web-menu	m_network/m_routing/m_routingtab le
sys-116	permit	RWX	web-menu	m_network/m_routing/m_staticrout ing
sys-117	permit	RWX	web-menu	m_network/m_routing/m_policyrout ing/
sys-118	permit	RWX	web-menu	m_network/m_routing/m_ospf
sys-119	permit	RWX	web-menu	m_network/m_routing/m_bgp
sys-120	permit	RWX	web-menu	m_network/m_routing/m_rip
sys-121	permit	RWX	web-menu	m_network/m_multicast/m_multicas trouting
sys-122	permit	RWX	web-menu	m_network/m_multicast/m_pim
sys-123	permit	RWX	web-menu	m_network/m_multicast/m_igmp
sys-124	permit	RWX	web-menu	m_network/m_dhcp/m_dhcpservice
sys-125	permit	RWX	web-menu	m_network/m_dhcp/m_dhcpool
sys-126	permit	RWX	web-menu	m_network/m_ipservice/m_http
sys-127	permit	RWX	web-menu	m_network/m_ipservice/m_ssh
sys-128	permit	RWX	web-menu	m_network/m_ipservice/m_ntp
sys-129	permit	RWX	web-menu	m_network/m_ipservice/m_ftp
sys-130	permit	RWX	web-menu	m_network/m_ipservice/m_telnet
sys-131	permit	RWX	web-menu	m_network/m_probe/m_ping
sys-132	permit	RWX	web-menu	m_network/m_probe/m_tracert
sys-133	permit	RWX	web-menu	m_device/m_maintenance/m_changep assword
sys-134	permit		command	tracert *
sys-135	permit		command	ping *

R:Read W:Write X:Execute

Role: audit-admin

Description: Predefined audit admin role only has access to commands for the audit administrator

VLAN policy: Permit (default)

Interface policy: Permit (default)

VPN instance policy: Permit (default)

Security zone policy: Permit (default)

Rule	Perm	Type	Scope	Entity
sys-1	permit	RWX	web-menu	m_monitor/m_monitorlog/m_operati onlog
sys-2	permit	RWX	web-menu	m_device/m_maintenance/m_changep assword
sys-3	permit		command	tracert *
sys-4	permit		command	ping *

R:Read W:Write X:Execute

表1-1 display role 命令显示信息描述表

字段	描述
Role	用户角色名称，其中系统预定义的用户角色名称分别为network-admin、network-operator、context-admin、context-operator、level- n （ n 为0~15）、security-audit、guest-manager、system-admin、security-admin、audit-admin
Description	用户角色描述信息
VLAN policy	配置的VLAN策略： - Deny：表示除允许操作指定的 VLAN 外，其它 VLAN 均不能被用户操作 - Permit (default)：表示系统缺省允许用户操作任何 VLAN
Permitted VLANs	允许用户操作的VLAN
Interface policy	配置的接口策略： - Deny：表示除允许操作指定的接口外，其它接口均不能被用户操作 - Permit (default)：表示系统缺省允许用户操作任何接口
Permitted interfaces	允许用户操作的接口
VPN-instance policy	配置的VPN策略： - Deny：表示除允许操作指定的 VPN 实例外，其它 VPN 实例均不能被用户操作 - Permit (default)：表示系统缺省允许用户操作任何 VPN 实例
Permitted VPN instances	允许用户操作的VPN实例
Security zone policy	配置的安全域策略： - Deny：表示除允许操作指定的安全域外，其它安全域均不能被用户操作 - Permit (default)：表示系统缺省允许用户操作任何安全域
Permitted security zones	允许用户操作的安全域
Rule	用户角色规则编号（系统预定义的权限规则通过sys-n标识）
Perm	对命令行的操作许可： - Permit：允许操作 - Deny：禁止操作

字段	描述
Type	命令行类型： • R: 读类型 • W: 写类型 • X: 执行类型
Scope	用户角色规则的类型： • command: 基于命令行的规则 • feature: 基于特性的规则 • feature-group: 基于特性组规则 • web-menu: 基于 Web 菜单的规则 • xml-element: 基于 XML 元素的规则 • oid: 基于 OID 元素的规则
Entity	用户角色规则中定义的具体内容（命令特征字符串、特性名称、特性组名称、Web菜单、XML元素或OID） • “-” 表示所有特性 • “*” 为通配符，表示 0 个或多个任意字符

【相关命令】

- role

1.1.3 display role feature

display role feature 命令用来显示特性相关信息。

【命令】

display role feature [name *feature-name* | verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

name *feature-name*: 显示指定特性的详细信息，*feature-name* 表示系统中的特性名称，且所有特性名称中的字母均为小写。

verbose: 显示所有特性的详细信息，即显示特性内包含的所有命令行列表。

【使用指导】

如果不指定任何关键字，则显示系统中所有特性的名称列表。

【举例】

显示系统中所有特性的名称列表。

```
<Sysname> display role feature
Feature: device          (Device configuration related commands)
Feature: interface       (Interface related commands)
Feature: syslog          (Syslog related commands)
..... (略)
```

显示所有特性的详细信息。

```
<Sysname> display role feature verbose
Feature: device          (Device configuration related commands)
    display clock        (R)
    debugging dev        (W)
    display debugging dev (R)
    display device *      (R)
    display diagnostic-information (R)
    display environment * (R)
    display fan *         (R)
    display alarm *       (R)
    display power *       (R)
    display rps *         (R)
    display current-configuration * (R)
    display saved-configuration * (R)
    display default-configuration * (R)
    display startup       (R)
    display xbar *        (R)
    display this *        (R)
..... (略)
```

显示特性 **aaa** 的详细信息。

```
<Sysname> display role feature name aaa
Feature: aaa            (AAA related commands)
    system-view ; domain * (W)
    system-view ; header * (W)
    system-view ; aaa *    (W)
    display domain *       (R)
    system-view ; user-group * (W)
    system-view ; local-user * (W)
    display local-user *    (R)
    display user-group *    (R)
    display debugging local-server (R)
    debugging local-server * (W)
    super *                (X)
    display password-control * (R)
    reset password-control * (W)
    system-view ; password-control * (W)
..... (略)
```

表1-2 display role feature 命令显示信息描述表(以 display role feature name aaa 的显示字段为例)

字段	描述
Feature	特性名称以及功能简介
system-view ; domain *	系统视图下以 domain 开头的所有命令，以及ISP域视图下的所有命令
system-view ; header *	系统视图下以 header 开头的所有命令
system-view ; aaa *	系统视图下以 aaa 开头的所有命令
display domain *	用户视图下以 display domain 开头的所有命令
system-view ; user-group *	系统视图下以 user-group 开头的所有命令，以及用户组视图下的所有命令
system-view ; local-user *	系统视图下以 local-user 开头的所有命令，以及本地用户视图下的所有命令
display local-user *	用户视图下以 display local-user 开头的所有命令
display user-group *	用户视图下以 display user-group 开头的所有命令
display debugging local-server	用户视图下以命令 display debugging local-server 开头的所有命令
debugging local-server *	用户视图下以 debugging local-server 开头的所有命令
super *	用户视图下以 super 开头的所有命令
display password-control *	用户视图下以 display password-control 开头的所有命令
reset password-control *	用户视图下以 reset password-control 开头的所有命令
system-view ; password-control *	系统视图下以 password-control 开头的所有命令
(W)	命令行的类型为写命令，本类型的命令用于对系统进行配置
(R)	命令行的类型为读命令，本类型的命令仅能显示系统配置信息和维护信息
(X)	命令行的类型为执行命令，本类型的命令用于执行特定的功能

【相关命令】

- **feature**

1.1.4 display role feature-group

display role feature-group 命令用来显示特性组信息。

【命令】

display role feature-group [*name feature-group-name*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

context-admin
context-operator

【参数】

name *feature-group-name*: 显示指定特性组包含的特性名称列表。*feature-group-name* 表示特性组名称，为 1~31 个字符的字符串，区分大小写。如果不指定本参数，则表示显示所有特性组的相关信息。

verbose: 显示特性组的详细信息，即显示特性组内的特性所包含的命令行列表。如果不指定本参数，则表示显示特性组中的特性名称列表。

【使用指导】

特性组 L2 和 L3 为系统预定义的两个特性组。

【举例】

显示所有特性组内的特性名称列表。

```
<Sysname> display role feature-group
Feature group: L2
Feature: lacp          (LACP related commands)
Feature: stp           (STP related commands)
Feature: lldp          (LLDP related commands)
Feature: dldp          (DLDP related commands)
Feature: smart-link    (Smart-link related commands)
Feature: monitor-link  (Monitor-link related commands)
Feature: loopbk-detect (Loopback-detection related commands)
Feature: vlan          (Virtual LAN related commands)
Feature: evb           (EVB related commands)
Feature: ofp           (OFP related commands)

Feature group: L3
Feature: route          (Route management related commands)
Feature: usr            (Unicast static route related commands)
Feature: ospf           (Open Shortest Path First protocol related commands)
Feature: rip            (Routing Information Protocol related commands)
Feature: isis           (ISIS protocol related commands)
Feature: lisp           (LISP protocol related commands)
Feature: l3vpn          (Layer 3 Virtual Private Network related commands)
Feature: route-policy   (Routing Policy related commands)
```

显示所有特性组的详细信息。

```
<Sysname> display role feature-group verbose
Feature group: L2
Feature: lacp          (LACP related commands)
  display link-aggregation *    (R)
  display lacp *           (R)
  system-view ; interface Bridge-Aggregation *    (W)
  system-view ; interface Route-Aggregation *     (W)
  system-view ; link-aggregation *    (W)
  system-view ; lacp *        (W)
  system-view ; interface * ; link-aggregation *   (W)
```

```

system-view ; interface * ; port link-aggregation *      (W)
system-view ; interface * ; lacp *                      (W)
system-view ; probe ; display system internal link-aggregation *      (R)
system-view ; probe ; debugging system internal link-aggregation *      (W)
reset lacp *      (W)
debugging link-aggregation *      (W)
display debugging link-aggregation *      (R)
display irf-port load-sharing mode *      (R)
system-view ; interface * ; mad enable      (W)
system-view ; irf-port * ; irf-port load-sharing mode *      (W)
Feature: stp      (STP related commands)
display stp *      (R)
system-view ; stp *      (W)
system-view ; interface * ; stp *      (W)
..... (略)

```

显示特性组 L3 的特性名称列表。

```
<Sysname> display role feature-group name L3
```

```
Feature group: L3
```

```

Feature: route      (Route management related commands)
Feature: usr        (Unicast static route related commands)
Feature: ospf       (Open Shortest Path First protocol related commands)
Feature: rip        (Routing Information Protocol related commands)
Feature: isis       (ISIS protocol related commands)
Feature: lisp       (LISP protocol related commands)
Feature: l3vpn      (Layer 3 Virtual Private Network related commands)
Feature: route-policy (Routing Policy related commands)

```

表1-3 display role feature-group 命令显示信息描述表

字段	描述
Feature group	特性组名称，其中L2和L3为系统预定义的两个特性组
Feature	特性名称以及功能简介 关于特性内具体命令的详细介绍请参考 表1-2

【相关命令】

- **feature**
- **role feature-group**

1.1.5 feature

feature 命令用来向特性组中添加一个特性。

undo feature 命令用来删除特性组中的指定特性。

【命令】

```
feature feature-name
```

```
undo feature feature-name
```

【缺省情况】

自定义特性组中不包括任何特性。

【视图】

特性组视图

【缺省用户角色】

network-admin

context-admin

【参数】

feature-name: 系统支持的特性名称，所有特性名称中的字母均为小写。

【使用指导】

可通过多次执行本命令，向特性组中添加多个特性。

【举例】

```
# 向特性组 security-features 中添加特性 AAA 和 ACL。
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features] feature aaa
[Sysname-featuregrp-security-features] feature acl
```

【相关命令】

- **display role feature**
- **display role feature-group**
- **role feature-group**

1.1.6 interface policy deny

interface policy deny 命令用来进入接口策略视图。

undo interface policy deny 命令用来恢复缺省情况。

【命令】

```
interface policy deny
undo interface policy deny
```

【缺省情况】

用户具有操作任何接口的权限。

【视图】

用户角色视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

进入接口策略视图后，如果不配置允许操作的接口列表，则用户将没有操作任何接口的权限；如果需要限制或区分用户对接口资源的使用权限，则还应该通过 **permit interface** 命令配置允许用户操作的接口列表。若接口策略视图中未配置允许操作的接口列表，则表示不允许用户操作所有的接口。对接口的操作指的是创建接口并进入接口视图、删除和应用接口。其中，创建和删除接口，仅针对逻辑接口。

允许修改用户角色的接口策略，但修改后的策略只在被授权该角色的用户重新登录时才会生效。

【举例】

在用户角色 **role1** 中，进入接口策略视图，并禁止角色为 **role1** 的用户操作任何接口。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] quit
```

在用户角色 **role1** 中，进入接口策略视图，允许角色为 **role1** 的用户操作接口 **GigabitEthernet1/0/1** 到 **GigabitEthernet1/0/4**。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

【相关命令】

- **display role**
- **permit interface**
- **role**

1.1.7 permit interface

permit interface 命令用来配置允许用户操作的接口列表。

undo permit interface 命令用来禁止用户操作指定的或所有的接口。

【命令】

```
permit interface interface-list
undo permit interface [interface-list ]
```

【缺省情况】

接口策略视图下未定义允许操作的接口列表，用户没有操作任何接口的权限。

【视图】

接口策略视图

【缺省用户角色】

```
network-admin
context-admin
```


【参数】

interface interface-list: 允许用户操作的接口列表，表示多个接口，表示方式为 **interface-list = { interface-type interface-number [to interface-type interface-number] }&<1-10>**。其中，**interface-type** 为接口类型，**interface-number** 为接口编号。**&<1-10>**表示前面的参数最多可以输入 10 次。起始接口类型必须和终止接口类型一致，并且终止接口编号必须大于起始接口编号。

【使用指导】

通过 **interface policy deny** 命令进入接口策略视图后，必须要通过本命令配置允许操作的接口列表，用户才能具有操作相应接口的权限。

对接口的操作指的是创建并进入接口视图、删除和应用接口。其中，创建和删除接口，只针对逻辑接口。

可通过多次执行此命令向接口列表中添加允许用户操作的接口。

undo permit interface 命令如果不指定 **interface-list** 参数，则表示禁止用户操作所有接口。

修改后的接口资源控制策略对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。

【举例】

创建用户角色 **role1** 并进入其视图。

```
<Sysname> system-view
```

```
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行进入接口视图以及接口视图下的相关命令。

```
[Sysname-role-role1] rule 1 permit command system-view ; interface *
```

配置用户角色规则 2，允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令。

```
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

配置用户角色 **role1** 仅可以对接口 **GigabitEthernet1/0/1** 进行操作。

```
[Sysname-role-role1] interface policy deny
```

```
[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1
```

当拥有用户角色 **role1** 的用户登录设备后，仅可以操作接口 **GigabitEthernet1/0/1**，不能操作其它接口。

配置结果验证如下：

- 进入接口 **GigabitEthernet1/0/1** 视图。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1]
```

- 将接口 **GigabitEthernet1/0/1** 加入到 VLAN 10。

```
<Sysname> system-view
```

```
[Sysname] vlan 10
```

```
[Sysname-vlan10] port gigabitethernet 1/0/1
```

- 无法进入接口 **GigabitEthernet1/0/2** 视图。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/2
```

```
Permission denied.
```

【相关命令】

- **display role**
- **interface policy deny**
- **role**

1.1.8 permit security-zone

permit security-zone 命令用来配置允许用户操作的安全域列表。

undo permit security-zone 命令用来禁止用户操作指定的或所有的安全域实例。

【命令】

permit security-zone *security-zone-name*&<1-10>

undo permit security-zone [*security-zone-name*&<1-10>]

【缺省情况】

安全域策略视图下未定义允许操作的安全域列表，用户没有操作任何安全域的权限。

【视图】

安全域策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

security-zone-name&<1-10>: 表示允许用户操作的安全域的名称，为1~31个字符的字符串，区分大小写。&<1-10>表示前面的参数最多可以输入 10 次。

【使用指导】

通过 **security-zone policy deny** 命令进入安全域策略视图后，必须要通过本命令配置允许操作的安全域列表，用户才能具有操作相应安全域的权限。

对安全域的“操作”指的是创建安全域并进入其视图、删除和应用安全域。

可通过多次执行此本命令向安全域列表中添加允许用户操作的安全域。

undo permit security-zone 命令如果不指定 *security-zone-name* 参数，则表示禁止用户操作所有安全域。

修改后的安全域资源控制策略对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。

【举例】

创建用户角色 role1 并进入其视图。

```
<Sysname> system-view
```

```
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行系统视图下的所有命令以及所有子视图下的命令。

```
[Sysname-role-role1] rule 1 permit command system-view ; *
```

配置用户角色 role1 仅可以对安全域 trust 和 abc 进行操作。

```
[Sysname-role-role1] security-zone policy deny
```

```
[Sysname-role-role1-zonepolicy] permit security-zone trust abc
```

拥有用户角色 **role1** 的用户登录设备后，可以操作安全域 **abc**，但不能操作其它安全域。

配置结果验证如下：

- 创建并进入名称为 **abc** 的安全域视图。

```
<Sysname> system-view
```

```
[Sysname] security-zone name abc
```

```
[Sysname-security-zone-abc]
```

- 创建源安全域 **trust** 到目的安全域 **abc** 的域间实例。

```
<Sysname> system-view
```

```
[Sysname] zone-pair security source trust destination abc
```

```
[Sysname-zone-pair-security-Trust-abc]
```

- 无法创建名称为 **local** 的安全域或进入其视图。

```
<Sysname> system-view
```

```
[Sysname] security-zone name local
```

```
Permission denied.
```

【相关命令】

- **display role**
- **role**
- **security-zone policy deny**

1.1.9 permit vlan

permit vlan 命令用来配置允许用户操作的 VLAN 列表。

undo permit vlan 命令用来禁止用户操作指定的或所有的 VLAN。

【命令】

```
permit vlan vlan-id-list
```

```
undo permit vlan [ vlan-id-list ]
```

【缺省情况】

VLAN 接口视图下未定义允许操作的 VLAN 列表，用户没有操作任何 VLAN 的权限。

【视图】

VLAN 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

vlan-id-list：允许用户操作的 VLAN 列表，表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] }&<1-10>**，**vlan-id** 取值范围为 1~4094，&<1-10>表示前面的参数最多可以重复输入 10 次。终止 VLAN 编号必须大于起始 VLAN 编号。

【使用指导】

通过 **vlan policy deny** 命令进入 VLAN 策略视图后，必须要通过本命令配置允许操作的 VLAN 列表，用户才能具有操作相应 VLAN 的权限。

对 VLAN 的操作指的是创建 VLAN 并进入 VLAN 视图、删除和应用 VLAN。

可通过多次执行此命令向 VLAN 列表中添加多个允许用户操作的 VLAN。

undo permit vlan 命令如果不指定 *vlan-id-list* 参数，则表示禁止用户操作所有 VLAN。

修改后的 VLAN 资源控制策略对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。

缺省情况下，设备上所有的 access 端口都属于 VLAN 1。使用 **port access vlan** 命令将 access 端口加入到其它指定 VLAN 中时，该角色必须同时具备 VLAN 1 的操作权限(通过命令 **permit vlan 1** 配置)。

【举例】

创建用户角色 role1 并进入其视图。

```
<Sysname> system-view
```

```
[Sysname] role name role1
```

配置用户角色规则 1，允许用户执行进入接口视图以及接口视图下的相关命令。

```
[Sysname-role-role1] rule 1 permit command system-view ; interface *
```

配置用户角色规则 2，允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令。

```
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

配置用户角色 role1 仅可以操作 VLAN 1、VLAN 2、VLAN 4、VLAN 50~VLAN 100。

```
[Sysname-role-role1] vlan policy deny
```

```
[Sysname-role-role1-vlanpolicy] permit vlan 1 2 4 50 to 100
```

当拥有用户角色 role1 的用户登录设备后，可以操作 VLAN 1、VLAN 2、VLAN 4、VLAN 50~VLAN 100，但不能操作其它 VLAN。

配置结果验证如下：

- 创建并进入 VLAN 100 视图。

```
<Sysname> system-view
```

```
[Sysname] vlan 100
```

```
[Sysname-vlan100]
```

- 向 VLAN 100 中添加 Access 类型的端口 GigabitEthernet1/0/1。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port access vlan 100
```

- 无法创建 VLAN 101 或进入其视图。

```
<Sysname> system-view
```

```
[Sysname] vlan 101
```

```
Permission denied.
```

【相关命令】

- **display role**
- **role**
- **vlan policy deny**

1.1.10 role

role 命令用来创建用户角色，并进入用户角色视图。如果指定的用户角色已经存在，则直接进入用户角色视图。

undo role 命令用来删除指定的用户角色。

【命令】

role name *role-name*

undo role name *role-name*

【缺省情况】

存在系统预定义的用户角色：**network-admin**、**network-operator**、**context-admin**、**context-operator**、**level-*n***（*n* 为 0~15 的整数）、**security-audit**、**guest-manager**、**system-admin**、**security-admin**、**audit-admin**。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

name *role-name*: 用户角色名称，*role-name* 为 1~63 个字符的字符串，区分大小写。

【使用指导】

除系统预定义的缺省用户角色之外，系统中最多允许创建 64 个用户角色。

缺省的用户角色不能被删除，而且其中的 **network-admin**、**network-operator**、**context-admin**、**context-operator**、**level-15**、**security-audit**、**guest-manager**、**system-admin**、**security-admin**、**audit-admin** 这些用户角色内定义的所有权限均不能被修改；用户角色 **level-0~level-14** 可以通过自定义规则和资源控制策略调整自身的权限，但这种修改对于 **display history-command all** 命令不生效，即不能通过添加对应的规则来更改它的缺省执行权限。

非 AAA 认证用户不能被授予安全日志管理员角色。

【举例】

创建用户角色 **role1**，并进入用户角色视图。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1]
```

【相关命令】

- **display role**
- **interface policy deny**
- **rule**
- **vlan policy deny**
- **vpn-instance policy deny**

1.1.11 role default-role enable

role default-role enable 命令用来使能缺省用户角色授权功能。

undo role default-role enable 命令用来恢复缺省情况。

【命令】

```
role default-role enable [ role-name ]  
undo role default-role enable
```

【缺省情况】

缺省用户角色授权功能处于关闭状态，没有被 AAA 授权用户角色的用户不能登录设备。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

role-name: 缺省用户角色名称，为 1~63 个字符的字符串，区分大小写，可以是系统中已存在的任意用户角色。

【使用指导】

对于通过 AAA 认证登录设备的用户，由服务器（远程认证服务器或本地认证服务器）为其授权对应的用户角色。如果用户没有被授权任何用户角色，将无法成功登录设备。若未通过 **authorization-attribute** 命令配置本地用户或用户组的授权属性，则必须使能缺省用户角色授权功能。使能该功能后，用户将在没有被服务器授权任何用户角色的情况下，具有一个缺省的用户角色。

若用户通过 AAA 认证且被授予了具体的用户角色，则用户不具有缺省的用户角色。

若不指定 **role-name** 参数，如果用户登录于缺省 Context，则缺省用户角色为 **network-operator**；如果用户登录于非缺省 Context，则缺省用户角色为 **context-operator**。

【举例】

```
# 使能缺省用户角色授权功能。  
<Sysname> system-view  
[Sysname] role default-role enable
```

【相关命令】

- **role**

1.1.12 role feature-group

role feature-group 命令用来创建特性组，并进入特性组视图。如果指定的特性组已经存在，则直接进入特性组视图。

undo role feature-group 命令用来删除指定的特性组。

【命令】

```
role feature-group name feature-group-name  
undo role feature-group name feature-group-name
```

【缺省情况】

存在两个特性组，名称分别为 L2 和 L3。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

name *feature-group-name*: 特性组名称, *feature-group-name* 为 1~31 个字符的字符串, 区分大小写。

【使用指导】

除系统预定义的特性组 L2 和 L3 之外，系统中最多允许创建 64 个特性组。

不能修改和删除系统预定义的特性组 L2 和 L3。L2 中包含了所有的二层协议相关功能的命令，L3 中包含了所有三层协议相关功能的命令。

【举例】

```
# 创建特性组 security-features，并进入特性组视图。  
<Sysname> system-view  
[Sysname] role feature-group name security-features  
[Sysname-featuregrp-security-features]
```

【相关命令】

- **display role feature**
- **display role feature-group**
- **feature**

1.1.13 rule

rule 命令用来为用户角色创建一条规则。

undo rule 命令用来为用户角色删除规则。

【命令】

```
rule number { deny | permit } { command command-string | { execute | read | write } * { feature [ feature-name ] | feature-group feature-group-name | oid oid-string | web-menu [ web-string ] | xml-element [ xml-string ] } }  
undo rule { number | all }
```

【缺省情况】

新建的用户角色中未定义规则，即当前用户角色无任何权限。

【视图】

用户角色视图

【缺省用户角色】

network-admin

context-admin

【参数】

number: 权限规则编号，取值范围为 1~256。

deny: 禁止执行指定的命令、Web 菜单、XML 元素或 MIB 节点 OID。

permit: 允许执行指定的命令、Web 菜单、XML 元素或 MIB 节点 OID。

command *command-string*: 配置基于命令的规则。*command-string* 表示命令特征字符串，为 1~128 个字符的字符串，区分大小写，可以是特定的一条命令行，也可以是用星号 (*) 通配符表示的一批命令，可包含空格、Tab（它们用于分隔关键字、参数以及输入的字符），以及所有可打印字符。

execute: 表示执行类型的命令、Web 菜单、XML 元素或 MIB 节点 OID。用于执行特定的程序或功能，执行类型的命令如 **ping** 命令。

read: 表示读类型的命令、Web 菜单、XML 元素或 MIB 节点 OID，用于显示系统配置和维护信息。读类型的命令如 **display**、**dir**、**more** 和 **pwd** 命令。

write: 表示写类型的命令、Web 菜单、XML 元素或 MIB 节点 OID，用于对系统进行配置。写类型的命令如 **ssh server enable** 命令。

feature [*feature-name*]: 配置基于特性的规则。*feature-name* 表示系统预定义的特性名称，区分大小写。若不指定特性名称，则表示所有特性。

feature-group *feature-group-name*: 配置基于特性组的规则。*feature-group-name* 表示特性组名称，为 1~31 个字符的字符串，区分大小写。只有特性组创建后，基于特性组的规则才能生效。使用 **display role feature-group** 命令可以查看已创建的特性组信息。

oid *oid-string*: 配置基于 MIB 节点 OID (Object Identifier, 对象标识符) 的规则。*oid-string* 表示允许操作的 OID，为 1~255 个字符的字符串，不区分大小写。OID 是由一系列的整数组成，标明节点在 MIB 树中的位置，它能唯一地标识一个 MIB 库中的对象。例如：1.3.6.1.4.1.25506.8.35.14.19.1.1。

web-menu [*web-string*]: 配置基于 Web 菜单的规则。*web-string* 表示允许操作的 Web 菜单选项的 ID 路径，为 1~255 个字符的字符串，不区分大小写，以 “/” 为分隔符来分隔不同级别的菜单。合法的 *web-string* 为通过 **display web menu** 命令显示的 ID 路径，例如：M_DEVICE/I_BASIC_INFO/I_reboot；若不指定 *web-string* 参数，则表示对所有菜单选项生效。

xml-element [*xml-string*]: 配置基于 XML 元素的规则。*xml-string* 表示允许操作的 XML 元素的 XPath，为 1~255 个字符的字符串，不区分大小写，以 “/” 为分隔符来分隔不同级别的菜单，例如：Interfaces/Index/Name；若不指定 *xml-string* 参数，则表示对所有 XML 元素生效。

all: 指定所有权限规则。

【使用指导】

可为一个用户角色定义以下几种类型的规则：

- 禁止或允许执行特定的命令行。
- 禁止或允许执行指定或所有特性的某一类或某几类命令。

- 禁止或允许执行某个特性组中所有特性的某一类或某几类命令。
- 禁止或允许执行指定所有或指定的 MIB 节点 OID。
- 禁止或允许执行 Web 页面中所有菜单选项或某几类菜单选项。
- 禁止或允许执行所有 XML 元素或某几类 XML 元素。

每个用户角色中最多可以配置 256 条规则，系统中可以配置的用户角色规则总数不能超过 1024。

访问文件系统的命令，受基于文件系统特性规则以及具体命令规则的双重控制。

对于需要将输出信息重定向到文件中保存的命令，只有在用户角色被授权了文件系统写权限后才允许执行。

为用户角色定义规则时，需要注意的是：

- 如果指定编号的规则不存在，则表示创建一条新的规则；如果指定编号的规则已存在，则表示对已有的规则进行修改。修改后的规则对于当前已经在线的用户不生效，对于之后使用该角色登录设备的用户生效。
- 一个用户角色中允许创建多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。
- 在同时存在系统预定义规则（以 sys-x 为权限规则编号，x 为整数值）和自定义规则的用户角色中，若预定义规则定义的权限内容与自定义规则定义的权限内容有冲突，则以自定义规则为准。

输入命令特征字符串时，需要遵循以下规则：

(1) 段（segment）的划分

- 若要描述多级视图下的命令，则需要使用分号（;）将命令特征字符串分成多个段，每一个段代表一个或一系列命令，后一个段中的命令是执行前一个段中命令所进入视图下的命令。一个段中可以包含多个星号（*），每个星号（*）代表了 0 个或多个任意字符。例如：命令特征字符串“**system ; interface * ; ip * ;**”代表从系统视图进入到任意接口视图后，以 **ip** 开头的命令。
- 除最后一个段外，其余段中的命令应为描述如何进入子视图的命令特征字符串。
- 一个段中必须至少出现一个可打印字符，不能全部为空格或 Tab。

(2) 分号的使用

- 在输入命令特征字符串时必须指定该命令所在的视图，进入各视图的命令特征字符串由分号分隔。但是，对于能在任意视图下执行的命令（例如 **display** 命令）以及用户视图下的命令（例如 **dir** 命令），在配置包含此类命令的规则时，不需要在规则的命令匹配字符串中指定其所在的视图。
- 当最后一个段中的最后一个可见字符为分号时，表示所指的命令范围不再扩展，否则将向子视图中的命令扩展。例如：命令特征字符串“**system ; radius scheme * ;**”代表系统视图下以 **radius scheme** 开头的命令；命令特征字符串“**system ; radius scheme ***”代表系统视图下以 **radius scheme** 开头的命令，以及进入子视图（RADIUS 方案视图）下的所有命令。

(3) 星号的使用

- 当星号（*）出现在一个段的首部时，其后面不能再出现其它可打印字符，且该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“**system ; ***”就代表了系统视图下的所有命令，以及所有子视图下的命令。
- 当星号（*）出现在一个段的中间时，该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“**debugging * event**”就代表了用户视图下所有模块的事件调试信息开关命令。

(4) 前缀匹配

- 命令关键字与命令特征字符串是采用前缀匹配算法进行匹配的，即只要命令行中关键字的首部若干连续字符或全部字符与规则中定义的关键字相匹配，就认为该命令行与此规则匹配。因此，命令特征字符串中可以包括完整的或部分的命令关键字。例如，若规则“**rule 1 deny command display arp source**”生效，则命令**display arp source-mac interface**和命令**display arp source-suppression**都会被禁止执行。

对于基于命令的规则，有以下使用注意事项：

- 基于命令的规则只对指定视图下的命令生效。若用户输入的命令在当前视图下不存在而在其父视图下被查找到时，用于控制当前视图下的命令的规则不会对其父视图下的命令执行权限进行控制。例如，定义一条规则“**rule 1 deny command system ; interface * ; ***”禁止用户执行接口视图下的任何命令。当用户在接口视图下输入命令**acl advanced 3000**时，该命令仍然可以成功执行，因为系统在接口视图下搜索不到指定的**acl**命令时，会回溯到系统视图（父视图）下执行，此时该规则对此命令不生效。
- **display**命令中的重定向符（“|”、“>”、“>>”）及其后面的关键字不被作为命令行关键字参与规则的匹配。例如，若规则“**rule 1 permit command display debugging**”生效，则命令**display debugging > log**是被允许执行的，其中的关键字**> log**将被忽略，RBAC只对重定向符前面的命令行**display debugging**进行匹配。但是，如果在规则中配置了重定向符，则RBAC会将其作为普通字符处理。例如，若规则“**rule 1 permit command display debugging > log**”生效，则命令**display debugging > log**将会匹配失败，因为其中的关键字**> log**被RBAC忽略了，最终是命令**display debugging**与规则进行匹配。因此，配置规则时不要使用重定向符。

进行基于OID的规则匹配时，遵循以下规则：

- 与用户访问的OID形成最长匹配的规则生效。例如用户访问的OID为1.3.6.1.4.1.25506.141.3.0.1，角色中存在“**rule 1 permit read write oid 1.3.6**”，“**rule 2 deny read write oid 1.3.6.1.4.1**”和“**rule 3 permit read write oid 1.3.6.1.4**”，其中rule 2与用户访问的OID形成最长匹配，则认为rule 2与OID匹配，匹配的结果为用户的此访问请求被拒绝。
- 对于定义的OID长度相同的规则，规则编号大的生效。例如用户访问的OID为1.3.6.1.4.1.25506.141.3.0.1，角色中存在“**rule 1 permit read write oid 1.3.6**”，“**rule 2 deny read write oid 1.3.6.1.4.1**”和“**rule 3 permit read write oid 1.3.6.1.4.1**”，其中rule 2和rule 3与访问的OID形成最长匹配，则rule 3生效，匹配的结果为用户的访问请求被允许。

【举例】

为用户角色role1创建一条规则，允许用户执行命令**display acl**。

```
<Sysname> system-view
```

```
[Sysname] role name role1
```

```
[Sysname-role-role1] rule 1 permit command display acl
```

为用户角色role1添加一条权限规则，允许用户执行所有以**display**开头的命令。

```
[Sysname-role-role1] rule 2 permit command display *
```

为用户角色 **role1** 添加一条权限规则，允许用户执行系统视图下的 **radius scheme aaa** 命令，以及使用该命令进入子视图后的所有命令。

```
[Sysname-role-role1] rule 3 permit command system ; radius scheme aaa
```

为用户角色 **role1** 添加一条权限规则，禁止用户执行所有特性中读类型和写类型的命令。

```
[Sysname-role-role1] rule 4 deny read write feature
```

为用户角色 **role1** 添加一条权限规则，禁止用户执行特性 **aaa** 中所有读类型的命令。

```
[Sysname-role-role1] rule 5 deny read feature aaa
```

为用户角色 **role1** 添加一条权限规则，允许执行特性组 **security-features** 中所有特性的读类型、写类型以及执行类型的命令。

```
[Sysname-role-role1] rule 6 permit read write execute feature-group security-features
```

为用户角色 **role1** 添加一条基于 **OID** 的规则，允许对 **OID** 为 **1.1.2** 的 **MIB** 节点进行读、写操作。

```
[Sysname-role-role1] rule 7 permit read write oid 1.1.2
```

【相关命令】

- **display role**
- **display role feature**
- **display role feature-group**
- **display web menu**（基础配置命令参考/登录设备）
- **role**

1.1.14 security-zone policy deny

security-zone policy deny 命令用来进入安全域策略视图。

undo security-zone policy deny 命令用来恢复缺省情况。

【命令】

```
security-zone policy deny
```

```
undo security-zone policy deny
```

【缺省情况】

用户具有操作任何安全域的权限。

【视图】

用户角色视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

进入安全域策略视图后，如果不配置允许操作的安全域列表，则用户将没有操作任何安全域的权限；如果需要限制或区分用户对安全域资源的使用权限，则还应该通过 **permit security-zone** 命令配置允许用户操作的安全域列表。若安全域策略视图中未配置允许操作的安全域列表，则表示不允许用户操作所有安全域。对安全域的“操作”指的是创建并进入安全域视图、删除和应用安全域。

允许修改用户角色的安全域策略，但修改后的策略只对被授权该角色的用户重新登录时才会生效。

【举例】

在用户角色 **role1** 中，进入安全域策略视图，禁止角色为 **role1** 的用户操作任意安全域。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] security-zone policy deny
[Sysname-role-role1-zonepolicy] quit
```

在用户角色 **role1** 中，进入安全域策略视图，允许角色为 **role1** 的用户操作安全域 **trust** 和 **abc**。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] security-zone policy deny
[Sysname-role-role1-zonepolicy] permit security-zone trust abc
```

【相关命令】

- **display role**
- **permit security-zone**
- **role**

1.1.15 super

super 命令用来使用户从当前角色切换到指定的用户角色。

【命令】

```
super [ role-name ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

role-name: 待切换的用户角色名称，为 1~63 个字符的字符串，区分大小写，可以是系统中已存在的除 **security-audit**、**guest-manager** 之外的任意用户角色。若不指定本参数，则切换到当前缺省的目的用户角色。缺省的目的用户角色由 **super default role** 命令指定。

【使用指导】

切换后的用户角色只对当前登录生效，用户重新登录后，又会恢复到原有角色。

为了保证操作的安全性，通常用户进行用户角色切换时，均需要输入用户角色切换密码。切换到不同的用户角色时，需要输入相应切换密码。如果服务器没有响应或者没有配置用户角色切换密码，则切换操作失败，若还有备份认证方案，则转而进行备份认证。因此，在进行切换操作前，请先保证配置了正确的用户角色切换密码。

在切换用户角色时，需要注意的是：

- 若级别切换认证方式为 **local**，在设备上未配置切换密码的情况下，对于 **Console** 用户，设备不关心用户是否输入切换密码以及输入切换密码的内容，可允许用户成功切换用户角色。

- 若级别切换认证方式为 **local scheme**，在设备上未配置切换密码的情况下，对于 Console 或 VTY 用户，则转为远程 AAA 认证。

【举例】

将用户角色切换到 **network-operator**。（假设用户当前的角色为 **network-admin**，切换认证方式为 **local**，切换密码已经设置）

```
<Sysname> super network-operator
```

```
Password:
```

```
User privilege role is network-operator, and only those commands that authorized to the role can be used.
```

【相关命令】

- **authentication super**（安全命令参考/AAA）
- **super authentication-mode**
- **super password**

1.1.16 super authentication-mode

super authentication-mode 命令用来设置切换用户角色时使用的认证方式。

undo super authentication-mode 命令用来恢复缺省情况。

【命令】

```
super authentication-mode { local | scheme } *
```

```
undo super authentication-mode
```

【缺省情况】

采用 **local** 认证方式。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

local：使用本地配置的用户角色切换密码进行认证。

scheme：使用 AAA 配置进行认证。

【使用指导】

使用本地密码认证时，需要通过 **super password** 命令在设备上配置用户角色切换的密码。

使用远程 AAA 认证时，需要在 RADIUS 或 HWTACACS 服务器上配置用户名和用户角色切换密码。

用户可以选择使用 **local** 或者 **scheme** 方式认证，也可以同时选择 **local** 和 **scheme** 方式，多选时根据配置顺序依次认证。

- **local scheme** 方式：先进行本地密码认证，若设备上未设置本地用户角色切换密码，使用 Console 或 VTY 用户线登录的用户则转为远程 AAA 认证。

- **scheme local** 方式：先进行远程 AAA 认证，远程 HWTACACS/RADIUS 服务器无响应或设备上的 AAA 远程认证配置无效时，转为本地密码认证。

scheme 认证方式需要与 AAA 的认证方案相配合，具体请参考“安全配置指导”中的“AAA”。

【举例】

```
# 配置切换用户角色时采用 local 认证方式。
<Sysname> system-view
[Sysname] super authentication-mode local
# 配置切换用户角色时采用先 scheme 后 local 的认证方式。
<Sysname> system-view
[Sysname] super authentication-mode scheme local
```

【相关命令】

- **authentication super**（安全命令参考/AAA）
- **super password**

1.1.17 super default role

super default role 命令用来配置用户角色切换的缺省目的角色。

undo super default role 命令用来恢复缺省情况。

【命令】

```
super default role role-name
undo super default role
```

【缺省情况】

对于登录缺省 Context 的用户，用户角色切换的缺省目的角色为 **network-admin**；对于登录非缺省 Context 的用户，用户角色切换的缺省目的角色为 **context-admin**。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

role-name：待切换的用户角色名称，为 1~63 个字符的字符串，区分大小写，可以是系统中已存在的除 **security-audit**、**guest-manager** 之外的任意用户角色。

【使用指导】

当执行 **super** 命令切换用户角色时，或配置用户角色切换的密码时，如不指定目的切换的角色名称，则表示使用 **super default role** 命令配置的缺省用户角色。

【举例】

```
# 配置用户切换角色的缺省目的角色为 network-operator。
<Sysname> system-view
[Sysname] super default role network-operator
```

【相关命令】

- **super**
- **super password**

1.1.18 super password

super password 命令用来设置用户角色切换的密码。

undo super password 命令用来删除用户角色切换密码。

【命令】

```
super password [ role role-name ] [ { hash | simple } string ]  
undo super password [ role role-name ]
```

【缺省情况】

未设置用户角色切换密码。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

role role-name: 待切换的用户角色的名称，为 1~63 个字符的字符串，区分大小写，可以为系统中已存在的除 **security-audit**、**guest-manager** 之外的任意用户角色。如果不指定角色名称，则表示设置的是切换到当前缺省目的用户角色的密码。缺省的目的用户角色由 **super default role** 命令指定。

hash: 以哈希方式设置密码。

simple: 以明文方式设置密码，该密码将以哈希计算后的密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串；哈希密码为 1~110 个字符的字符串。

【使用指导】

如果不指定 **hash** 或 **simple** 参数，**super password** [*role role-name*] 命令将以交互式方式设置本地用户密码，涵义与指定 **simple** 关键字相同。

当用户切换认证方式为 **local** 或包含 **local** (**local scheme**、**scheme local**) 时，才需要本命令指定的用户角色切换密码。

为保证权限控制更加安全，推荐给不同的用户角色指定不同的切换密码。

在全局 **Password Control** 功能处于开启的情况下，需要注意的是：

- 所有历史密码都以哈希方式存储。
- 以明文方式设置新的用户角色切换密码时，需要保证新密码与所有历史密码和当前密码不同；以哈希方式设置新的用户角色切换密码时，不与历史密码和当前密码进行比较。

【举例】

配置将用户角色切换到 **network-operator** 时使用的密码为明文密码 123456TESTplat!。

```
<Sysname> system-view
[Sysname] super password role network-operator simple 123456TESTplat&!
# 以交互式方式设置将用户角色切换到 network-operator 时使用的密码为明文密码
123456TESTplat&!.
<Sysname> system-view
[Sysname] super password role network-operator
Password:
Confirm :
Updating user information. Please wait.....
```

【相关命令】

- **super authentication-mode**
- **super default role**

1.1.19 super use-login-username

super use-login-username 命令用来配置用户角色切换认证时使用用户登录的用户名进行认证。

undo super use-login-username 命令用来恢复缺省情况。

【命令】

```
super use-login-username
undo super use-login-username
```

【缺省情况】

用户角色切换认证时系统提示用户输入用户名进行认证。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

通过开启本功能，在设备采用远程 AAA 认证方案进行用户角色切换认证，且用户采用用户名和密码方式登录设备的情况下，用户切换用户角色时，设备会自动获取用户登录使用的用户名作为角色切换认证的用户名，不再提示用户输入用户名。

开启本功能后，若设备采用远程 AAA 认证方案进行用户角色切换认证，但用户未采用用户名和密码方式登录设备，则用户角色切换失败。

若设备未采用远程 AAA 认证方案进行用户角色切换认证，则本功能配置无效。

【举例】

配置用户角色切换认证时使用用户登录的用户名进行认证。

```
<Sysname> system-view
[Sysname] super use-login-username
```


【相关命令】

- **authentication super**（安全命令参考/AAA）
- **super authentication-mode**
- **super password**

1.1.20 vlan policy deny

vlan policy deny 命令用来进入 VLAN 策略视图。

undo vlan policy deny 命令用来恢复缺省情况。

【命令】

vlan policy deny
undo vlan policy deny

【缺省情况】

用户具有操作任何 VLAN 的权限。

【视图】

用户角色视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

进入 VLAN 策略视图后,如果不配置允许操作的 VLAN 列表,则用户将没有操作任何 VLAN 的权限;如果需要限制或区分用户对 VLAN 资源的使用权限,则还应该通过 **permit vlan** 命令配置允许用户操作的 VLAN 列表。若 VLAN 策略视图中未配置允许操作的 VLAN 列表,则表示不允许用户操作所有的 VLAN。对 VLAN 的“操作”指的是创建并进入 VLAN 视图、删除和应用 VLAN。

允许修改用户角色的 VLAN 策略,但修改后的策略只对被授权该角色的用户重新登录时才会生效。

【举例】

在用户角色 role1 中,进入 VLAN 策略视图,禁止角色为 role1 的用户操作任意 VLAN。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] quit
```

在用户角色 role1 中,进入 VLAN 策略视图,允许角色为 role1 的用户操作 VLAN 50~VLAN 100。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 50 to 100
```

【相关命令】

- **display role**
- **permit vlan**
- **role**

1.1.21 vpn-instance policy deny

vpn-instance policy deny 命令用来进入 VPN 策略视图。

undo vpn-instance policy deny 命令用来恢复缺省情况。

【命令】

```
vpn-instance policy deny
undo vpn-instance policy deny
```

【缺省情况】

用户具有操作任何 VPN 实例的权限。

【视图】

用户角色视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

进入 VPN 策略视图后，如果不配置允许操作的 VPN 实例列表，则用户将没有操作任何 VPN 实例的权限；如果需要限制或区分用户对 VPN 资源的使用权限，则还应该通过 **permit vpn-instance** 命令配置允许用户操作的 VPN 实例列表。若 VPN 策略视图中未配置允许操作的 VPN 实例列表，则表示不允许用户操作所有的 VPN 实例。对 VPN 实例的“操作”指的是创建 MPLS L3VPN 实例并进入其视图、删除和应用 VPN 实例。

允许修改用户角色的 VPN 策略，但修改后的策略只对被授权该角色的用户重新登录时才会生效。

【举例】

在用户角色 role1 中，创建并进入一个 VPN 策略视图，并禁止角色为 role1 的用户操作任意 VPN 实例。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vpn-instance policy deny
[Sysname-role-role1-vpnpolicy] quit
```

在用户角色 role1 中，创建并进入一个 VPN 策略视图，允许角色为 role1 的用户操作 VPN 实例 vpn2。

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vpn-instance policy deny
[Sysname-role-role1-vpnpolicy] permit vpn-instance vpn2
```

【相关命令】

- **display role**
- **permit vpn-instance**
- **role**

目 录

1 登录设备	1-1
1.1 登录设备命令	1-1
1.1.1 activation-key	1-1
1.1.2 authentication-mode	1-3
1.1.3 auto-execute command	1-4
1.1.4 command accounting	1-6
1.1.5 command authorization	1-7
1.1.6 databits	1-7
1.1.7 display ip http	1-8
1.1.8 display ip https	1-9
1.1.9 display line	1-10
1.1.10 display telnet client	1-12
1.1.11 display user-interface	1-13
1.1.12 display users	1-15
1.1.13 display web menu	1-16
1.1.14 display web users	1-22
1.1.15 escape-key	1-23
1.1.16 flow-control	1-24
1.1.17 free line	1-25
1.1.18 free user-interface	1-26
1.1.19 free web users	1-27
1.1.20 history-command max-size	1-28
1.1.21 http method	1-28
1.1.22 idle-timeout	1-29
1.1.23 ip http acl	1-30
1.1.24 ip http enable	1-31
1.1.25 ip http port	1-32
1.1.26 ip https acl	1-33
1.1.27 ip https certificate access-control-policy	1-34
1.1.28 ip https enable	1-35
1.1.29 ip https port	1-35
1.1.30 ip https ssl-server-policy	1-36
1.1.31 line	1-37

1.1.32 line class	1-38
1.1.33 lock	1-39
1.1.34 lock reauthentication	1-40
1.1.35 lock-key	1-42
1.1.36 parity	1-43
1.1.37 protocol inbound	1-44
1.1.38 restful http enable	1-46
1.1.39 restful https enable	1-46
1.1.40 screen-length	1-47
1.1.41 send	1-48
1.1.42 set authentication password	1-49
1.1.43 shell	1-50
1.1.44 speed	1-51
1.1.45 stopbits	1-51
1.1.46 telnet	1-52
1.1.47 telnet client source	1-53
1.1.48 telnet ipv6	1-54
1.1.49 telnet server acl	1-55
1.1.50 telnet server acl-deny-log enable	1-56
1.1.51 telnet server dscp	1-57
1.1.52 telnet server enable	1-58
1.1.53 telnet server ipv6 acl	1-58
1.1.54 telnet server ipv6 dscp	1-59
1.1.55 telnet server ipv6 port	1-60
1.1.56 telnet server port	1-61
1.1.57 terminal type	1-61
1.1.58 user-interface	1-62
1.1.59 user-interface class	1-63
1.1.60 user-role	1-65
1.1.61 web captcha	1-66
1.1.62 web https-authorization mode	1-67
1.1.63 web https-authorization username	1-67
1.1.64 web idle-timeout	1-68
1.1.65 webui log enable	1-69

1 登录设备

1.1 登录设备命令

对于同时支持用户线视图和用户线类视图的命令，本文中的命令描述只描述用户线视图下命令的作用，对于用户线类视图下该命令的作用，请按照下列规则进行类推：

- 用户线视图下的配置只对该用户线生效，用户线类视图下的配置对该类用户线生效。
- 非缺省配置优先于缺省配置。如果在用户线视图、用户线类视图下都是非缺省配置，则用户线视图下的配置优先于用户线类视图下的配置。
- 用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效。

1.1.1 activation-key

activation-key 命令用来配置启动终端会话的快捷键。

undo activation-key 命令用来恢复缺省情况。

【命令】

activation-key *key-string*

undo activation-key

【缺省情况】

按<Enter>键启动终端会话。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【参数】

key-string：定义启动终端会话的快捷键，可以是区分大小写的单个字符，也可以是单个字符或组合键对应的ASCII码（0~127）。比如设置**activation-key 1**，此时生效快捷键为Ctrl+A；如果设置**activation-key a**，生效的快捷键为a。单个字符的快捷键对应的ASCII码与标准的ASCII码表一致，组合键对应的ASCII码请参见 [表 1-1](#)。

【使用指导】

VTY 用户线视图/VTY 用户线类视图不支持该命令。

在用户线/用户线类视图下，该命令的配置结果将立即生效。

如果使用 **activation-key** 命令设置了其他快捷键，则新的快捷键将代替<Enter>键来启动终端会话。新设置的快捷键可以使用 **display current-configuration | include activation-key** 命令查看。

如果用户线视图下配置 **activation-key** 为缺省值，并且此时用户线类视图下配置了 **activation-key**，则用户线类视图下的配置生效；如果用户线类视图下未配置，则生效的为缺省值。

表1-1 Ctrl+X 组合键对应的 ASCII 码表

Ctrl+X 组合键	对应的 ASCII 码
CTRL+A	1
CTRL+B	2
CTRL+C	3
CTRL+D	4
CTRL+E	5
CTRL+F	6
CTRL+G	7
CTRL+H	8
CTRL+I	9
CTRL+J	10
CTRL+K	11
CTRL+L	12
CTRL+M	13
CTRL+N	14
CTRL+O	15
CTRL+P	16
CTRL+Q	17
CTRL+R	18
CTRL+S	19
CTRL+T	20
CTRL+U	21
CTRL+V	22
CTRL+W	23
CTRL+X	24
CTRL+Y	25
CTRL+Z	26

【举例】

指定启动 Console 用户线终端会话的快捷键为<s>。

```
<Sysname> system-view
```

```
[Sysname] line console 0
```

```
[Sysname-line-console0] activation-key s
```

验证过程如下：

- 退出终端会话。

```
[Sysname-line-console0] return  
<Sysname> quit
```

- 重新登录设备，能看到如下显示信息。

```
Press ENTER to get started.
```

- 此时，<Enter>键失效，需要按<s>键才能出现用户视图提示符，启动终端会话。
<Sysname>

1.1.2 authentication-mode

authentication-mode 命令用来设置用户登录设备时的认证方式。

undo authentication-mode 命令用来恢复缺省情况。

【命令】

```
authentication-mode { none | password | scheme }  
undo authentication-mode
```

【缺省情况】

设备采用出厂配置启动时，使用 VTY 用户线登录的用户的认证方式为 **scheme**，使用 Console 用户线登录的认证方式为 **scheme**。

设备采用空配置启动时，使用 VTY 用户线登录的用户的认证方式为 **password**，使用 Console 用户线登录的用户不需要认证。

关于出厂配置和空配置的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

none：不进行认证。

password：进行密码认证方式。

scheme：进行 AAA 认证方式。AAA 的相关内容请参见“安全配置指导”中的“AAA”。

【使用指导】

当认证方式设置为 **none** 时，用户不需要输入用户名和密码，就可以使用该用户线登录设备，存在安全隐患，请谨慎配置。

用户线视图下，**authentication-mode** 与 **protocol inbound** 相关联：

- 当这两条命令均配置为缺省值，此时该用户线视图下的这两条命令配置值均取该类用户线类视图下的相应的配置；若该类用户线类视图下没有进行相应的配置，则均取缺省值。
- 当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值。

- 当两条命令都配置成非缺省值，则均取用户线下的配置值。

仅具有 **network-admin**、**context-admin** 或者 **level-15** 用户角色的用户可以执行该命令。其他角色的用户，即使授权了该命令的操作权限，也不能执行该命令。

在用户线视图/用户线类视图下，该命令的配置结果将在下次登录设备时生效。

【举例】

设置用户使用 VTY 0 用户线登录设备时，不需要认证。

```
<Sysname> system-view
```

```
[Sysname] line vty 0
```

```
[Sysname-line-vty0] authentication-mode none
```

设置用户使用 VTY 0 用户线登录设备时，需要密码认证，认证密码为 321。

```
<Sysname> system-view
```

```
[Sysname] line vty 0
```

```
[Sysname-line-vty0] authentication-mode password
```

```
[Sysname-line-vty0] set authentication password simple 321
```

设置用户使用 VTY 0 用户线，采用 Telnet 方式登录设备时采用本地 AAA 认证，用户名为 123，认证密码为 321，服务类型为 Telnet，用户角色为 **network-admin**。

```
<Sysname> system-view
```

```
[Sysname] line vty 0
```

```
[Sysname-line-vty0] authentication-mode scheme
```

```
[Sysname-line-vty0] quit
```

```
[Sysname] local-user 123
```

```
[Sysname-luser-manage-123] password simple 321
```

```
[Sysname-luser-manage-123] service-type telnet
```

```
[Sysname-luser-manage-123] authorization-attribute user-role network-admin
```

【相关命令】

- **set authentication password**

1.1.3 auto-execute command

auto-execute command 命令用来设置自动执行命令。

undo auto-execute command 命令用来恢复缺省情况。

【命令】

auto-execute command *command*

undo auto-execute command

【缺省情况】

未配置自动执行命令。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【参数】

command: 需要自动执行的某条命令。

【使用指导】



注意

- 在配置 **auto-execute command** 命令之前，请确保可以通过其他用户线（例如 Console 用户线）登录系统，以便出现问题后，能删除该配置。
- 执行该命令后，可能导致用户不能通过该终端线对本系统进行配置，需谨慎使用。

用户在登录时设备会自动执行 **auto-execute command** 配置好的命令，执行完命令后，自动断开用户连接。

在用户线视图/用户线类视图下配置该命令时，需要注意：

- Console 用户线视图/Console 用户线类视图不支持该命令。
- 如果用户线视图下配置 **auto-execute command** 为缺省值，并且此时用户线类视图下配置了 **auto-execute command**，那么用户线类视图下的配置生效；如果用户线类视图下未配置，则用户线视图下的配置生效。

使用该命令设置的自动执行命令将在下次登录设备时生效。

【举例】

配置用户从 VTY0 登录本设备(IP 地址为 192.168.1.40)后,自动 Telnet 到 IP 地址为 192.168.1.41 的设备。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] auto-execute command telnet 192.168.1.41
This action will lead to configuration failure through line-vty0. Are you sure?
[Y/N]:y
[Sysname-line-vty0]
```

结果验证：

重新 Telnet 登录到本设备，设备会自动执行 telnet 192.168.1.41 命令，在 Telnet 客户端会看到以下显示信息。

```
C:\> telnet 192.168.1.40
*****
* Copyright (c) 2015-2019 Beijing UNIS Hengyue Technologies Co., Ltd.          *
* Without the owner's prior written consent,                                  *
* no decompiling or reverse-engineering shall be allowed.                     *
*****

<Sysname>
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
*****
```

```
* Copyright (c) 2015-2019 Beijing UNIS Hengyue Technologies Co., Ltd.      *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                  *
*****
<Sysname.41>
```

此时相当于用户直接登录了 192.168.1.41 设备。如果用户断开与 192.168.1.41 的 Telnet 连接，用户与 192.168.1.40 设备的 Telnet 连接也会同时自动断开。

1.1.4 command accounting

command accounting 命令用来开启命令行计费功能。

undo command accounting 命令用来关闭命令行计费功能。

【命令】

```
command accounting
undo command accounting
```

【缺省情况】

命令行计费功能处于关闭状态，即计费服务器不会记录用户执行的命令行。

【视图】

用户线视图
用户线类视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启命令行计费功能后，如果未配置命令行授权功能，则当前用户执行的每一条合法命令都会发送到 HWTACACS 服务器上做记录；如果配置了命令行授权功能，则当前用户执行的并且授权成功的命令都会发送到 HWTACACS 服务器上做记录。

在用户线视图/用户线类视图下，该命令的配置结果将在下次登录设备时生效。

如果在用户线类视图下使用 **command accounting** 命令使能了命令行计费功能，则该类型用户线视图都使能命令行计费功能，且用户线视图下无法使用 **undo command accounting** 恢复缺省情况。

【举例】

设置用户使用 VTY 0 用户线登录设备时，执行的命令需要在 HWTACACS 服务器上做记录。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] command accounting
```

【相关命令】

- **accounting command**（安全命令参考/AAA）
- **command authorization**

1.1.5 command authorization

command authorization 命令用来开启命令行授权功能。

undo command authorization 命令用来关闭命令行授权功能。

【命令】

command authorization

undo command authorization

【缺省情况】

命令行授权功能处于关闭状态，即用户登录后执行命令行不需要服务器授权。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启命令行授权功能后，使用该用户线登录的用户只能执行服务器授权的命令，服务器没有授权的命令不能执行。

在用户线视图/用户线类视图下该命令的配置结果将在下次登录设备时生效。

如果在用户线类视图下使用 **command authorization** 命令开启了命令行授权功能，则该类型用户线视图都开启命令行授权功能，且用户线视图下无法使用 **undo command authorization** 恢复缺省情况。

【举例】

设置用户使用 VTY 0 用户线登录设备时，需要服务器授权才能执行命令。

```
<Sysname> system-view
```

```
[Sysname] line vty 0
```

```
[Sysname-line-vty0] command authorization
```

【相关命令】

- **command accounting**
- **authorization command**（安全命令参考/AAA）

1.1.6 databits

databits 命令用来设置数据位的个数。

undo databits 命令用来恢复缺省情况。

【命令】

databits { 7 | 8 }

undo databits

【缺省情况】

用户线的数据位为 8 位。

【视图】

用户线视图

【缺省用户角色】

network-admin

context-admin

【参数】

7：数据位为 7 位，即使用 7 比特来表示一个字符。

8：数据位为 8 位，即使用 8 比特来表示一个字符。

【使用指导】

VTY 用户线类视图不支持该命令。

访问终端和设备相应用户线下数据位的设置必须一致，双方才能正常通信。

【举例】

设置数据位为 7 位。

```
<Sysname> system-view
```

```
[Sysname] line console 0
```

```
[Sysname-line-console0] databits 7
```

1.1.7 display ip http

display ip http 命令用来显示 HTTP 的状态信息。

【命令】

display ip http

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

显示 HTTP 的状态信息。

```
<Sysname> display ip http
```

```
HTTP port: 80
```

```
ACL: 2222(basic)
```

```
Operation status: Enabled
```

表1-2 display ip http 命令显示信息描述表

字段	描述
HTTP port	HTTP服务使用的端口号
ACL	与HTTP服务关联的基本访问控制列表号或名称 基本访问控制列表号为0表示未配置，有如下几种类型： • basic，表示基本 ACL • advanced，表示高级 ACL • layer 2，表示二层 ACL
Operation status	HTTP服务是否开启： Enabled：表示HTTP服务处于开启状态 Disabled：表示HTTP服务处于关闭状态

【相关命令】

- **ip http port**
- **ip http acl**
- **ip http enable**

1.1.8 display ip https

display ip https 命令用来显示 HTTPS 的状态信息。

【命令】

display ip https

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 显示 HTTPS 的状态信息。
<Sysname> display ip https
HTTPS port: 443
SSL server policy: test
Certificate access-control-policy: Not configured
ACL: 3333(advanced)
Operation status: Enabled
```

表1-3 display ip https 命令显示信息描述表

字段	描述
HTTPS port	HTTPS服务使用的端口号
SSL server policy	与HTTPS服务关联的SSL服务器端策略，Not configured表示未配置
Certificate access-control-policy	与HTTPS服务关联的证书属性访问控制策略，Not configured表示未配置
ACL	与HTTPS服务关联的基本访问控制列表号或名称，基本访问控制列表号为0表示未配置，有如下几种类型： • basic，表示基本 ACL • advanced，表示高级 ACL • layer 2，表示二层 ACL
Operation status	HTTPS服务是否开启： Enabled：表示HTTPS服务处于开启状态 Disabled：表示HTTPS服务处于关闭状态

【相关命令】

- **ip https port**
- **ip https acl**
- **ip https enable**
- **ip https ssl-server-policy**
- **ip https certificate access-control-policy**

1.1.9 display line

display line 命令用来显示用户线的相关信息。

【命令】

display line [*number1* | { **console** | **vty** } *number2*] [**summary**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

number1：用户线的编号（绝对编号方式）。

本参数的取值范围与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	取值范围为0~65
T5000-G30	取值范围为0~65
T1000-G20/T1000-G50/T1000-G60/T1000-G80	T1000-G20/T1000-G50/T1000-G60: 取值范围为0~69 T1000-G80: 取值范围为0~67
T1000-CN60/T1000-CN80	取值范围为0~65

console: Console 用户线。

vty: VTY 用户线。

number2: 用户线的编号（相对编号方式），对于 Console 用户线取值范围为 0~1，对于 VTY 用户线取值范围为 0~63。

summary: 显示用户线的摘要信息。不使用该参数时，将显示用户线类型、绝对/相对编号、传输速率、认证方式及接入接口；使用该参数时，将显示正在使用和未使用的用户线数目和类型。

【举例】

显示用户线 0 的相关信息。

```
<Sysname> display line 0
```

```
  Idx  Type    Tx/Rx      Modem Auth  Int           Location
+  0    CON 0    9600        -      N      -           1/0
```

```

+      : Line is active.
F      : Line is active and in async mode.
Idx    : Absolute index of line.
Type   : Type and relative index of line.
Auth   : Login authentication mode.
Int    : Physical port of the line.
A      : Authentication use AAA.
N      : No authentication is required.
P      : Password authentication.
```

表1-4 display line 命令显示信息描述表

字段	描述
+	表示当前正在使用的用户线
F	表示当前正在使用的用户线，且工作在异步方式
Idx	用户线的绝对编号
Type	用户线的类型及相对编号
Tx/Rx	用户线的速率
Modem	（暂不支持）Modem的呼入/呼出开关，取值有in（允许呼入）、out（允许呼出）、inout（允许呼入呼出），缺省显示“-”（表示未配置）
Auth	使用该用户线登录的用户的认证方式，取值有A、L、N和P四种方式

字段	描述
Int	用户线对应的物理接口的简称表示（Console口以及没有对应接口的用户线均显示“-”）
Location	用户线的物理位置，显示为“设备成员编号/CPU编号”
A	表示使用AAA认证方式，对应的 authentication-mode 为 scheme
N	表示无需认证，对应的 authentication-mode 为 none
P	表示使用当前用户线的密码进行认证，对应的 authentication-mode 为 password

显示所有用户线的摘要信息。

```
<Sysname> display line summary
  Line type : [CON]
             0:U
  Line type : [VTY]
             2:UXXX X
  2 lines used.      (U)
  5 lines not used.  (X)
```

表1-5 display line summary 命令显示信息描述表

字段	描述
Line type	用户线类型： - CON 表示 Console 用户线 - VTY 表示 VTY 用户线
0:UXXX XXXX XX	0表示用户线的绝对编号 X表示当前没有用户使用该用户线 U表示当前有用户使用该用户线
lines used. (U)	当前正在使用的用户线的数目（即U字符数量）
lines not used. (X)	当前未使用的用户线的数目（即X字符数量）

1.1.10 display telnet client

display telnet client 命令用来显示设备作为 Telnet 客户端的配置信息。

【命令】

display telnet client

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin

context-operator

【使用指导】

目前该命令显示的是 Telnet 客户端源 IPv4 地址或源接口的配置信息。用户可以使用 **telnet client source** 命令指定 Telnet 客户端源 IPv4 地址或源接口。

【举例】

显示设备作为 Telnet 客户端的相关配置信息。
<Sysname> display telnet client
The source IP address is 1.1.1.1.
以上显示信息表示设备作为 Telnet 客户端时，发送 Telnet 报文的源 IPv4 地址为 1.1.1.1。

【相关命令】

- **telnet client source**

1.1.11 display user-interface

display user-interface 命令用来显示用户线的相关信息。

【命令】

display user-interface [*number1* | { **console** | **vty** } *number2*] [**summary**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

number1：用户线的编号（绝对编号方式）。
本参数的取值范围与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	取值范围为0～65
T5000-G30	取值范围为0～65
T1000-G20/T1000-G50/T1000-G60/T1000-G80	T1000-G20/T1000-G50/T1000-G60：取值范围为0～69 T1000-G80：取值范围为0～67
T1000-CN60/T1000-CN80	取值范围为0～65

console：Console 用户线。
vty：VTY 用户线。

number2: 用户线的编号（相对编号方式），对于 Console 用户线取值范围为 0~1，对于 VTY 用户线取值范围为 0~63。

summary: 显示用户线的摘要信息。不使用该参数时，将显示用户线类型、绝对/相对编号、传输速率、认证方式及接入接口；使用该参数时，将显示正在使用和未使用的用户线数目和类型。

【使用指导】

该命令实现与 **display line** 一致，仅为与旧版本兼容保留，请使用 **display line**。

【举例】

```
# 显示用户线 0 的相关信息。
<Sysname> display user-interface 0
  Idx  Type   Tx/Rx      Modem Auth  Int       Location
+  0    CON 0    9600      -      N      -        1/0

+      : Line is active.
F      : Line is active and in async mode.
Idx    : Absolute index of line.
Type   : Type and relative index of line.
Auth   : Login authentication mode.
Int    : Physical port of the line.
A      : Authentication use AAA.
N      : No authentication is required.
P      : Password authentication.
```

表1-6 display user-interface 命令显示信息描述表

字段	描述
+	表示当前正在使用的用户线
F	表示当前正在使用的用户线，且工作在异步方式
Idx	用户线的绝对编号
Type	用户线的类型及相对编号
Tx/Rx	用户线的速率
Modem	（暂不支持）Modem的呼入/呼出开关，取值有in（允许呼入）、out（允许呼出）、inout（允许呼入呼出），缺省显示“-”（表示未配置）
Auth	使用该用户线登录的用户的认证方式，取值有A、L、N和P四种方式
Int	用户线对应的物理接口的简称表示（Console口以及没有对应接口的用户线均显示“-”）
Location	用户线的物理位置，显示为“设备成员编号/CPU编号”
A	表示使用AAA认证方式，对应的 authentication-mode 为 scheme
N	表示无需认证，对应的 authentication-mode 为 none
P	表示使用当前用户线的密码进行认证，对应的 authentication-mode 为 password

```
# 显示所有用户线的摘要信息。
<Sysname> display user-interface summary
```

```

Line type : [CON]
           0:U
Line type : [VTY]
           2:UXXX X
2 lines used.      (U)
5 lines not used.  (X)

```

表1-7 display user-interface summary 命令显示信息描述表

字段	描述
Line type	用户线类型： - CON 表示 Console 用户线 - VTY 表示 VTY 用户线
0:UXXX XXXX XX	0表示用户线的绝对编号 X表示当前没有用户使用该用户线 U表示当前有用户使用该用户线
lines used. (U)	当前正在使用的用户线的数目（即U字符数量）
lines not used. (X)	当前未使用的用户线的数目（即X字符数量）

1.1.12 display users

display users 命令用来显示正在使用的用户线以及用户的相关信息。

【命令】

display users [all]

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

all: 显示设备支持的所有用户线以及用户的相关信息。

【举例】

显示正在使用的用户线以及用户的相关信息。

```
<Sysname> display users
```

```

  Idx  Line   Idle      Time                Pid   Type
+ 10   VTY 0    00:00:00   Jan 01 00:33:10    484   TEL
  12   VTY 2    00:06:22   Jan 01 00:33:22    495   TEL

```

Following are more details.

```

VTY 0   :
        Location: 192.168.1.107
VTY 2   :
        Location: 192.168.1.134
+       : Current operation user.
F       : Current operation user works in async mode.

```

表1-8 display users 命令显示信息描述表

字段	描述
Idx	用户线的绝对编号
Line	用户线的相对编号，第一列（例如VTY）表示用户线的类型，第二列（例如0）表示用户线的相对编号
Idle	空闲时间，表明用户和设备没有报文交互的时间长度，格式为hh:mm:ss。当空闲时间大于等于24小时时，显示为old
Time	用户本次登录的时间
Pid	用户对应的进程ID（CLI用户登录时，系统会自动运行一个用户登录进程来监控用户的操作）
Type	显示用户的登录方式： • TEL 表示用户通过 Telnet 方式登录设备 • SSH 表示用户通过 SSH 方式登录设备 • Switchto User 表示用户通过 context 的 switchto 命令方式登录设备 • 无显示信息表示用户通过 Console 口方式登录设备
+	当前操作用户
User name	使用该用户线登录的用户的用户名，用户通过用户名和密码认证后登录设备的情况下会显示该字段
Location	使用该用户线登录的用户的位置信息（即用户的IP地址）
F	当前操作用户工作在异步模式

1.1.13 display web menu

display web menu 命令用来显示 Web 的页面菜单树。

【命令】

display web menu [chinese]

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

chinese: 显示 Web 的页面中文菜单树。不指定该参数时，显示 Web 的页面英文菜单树。

【使用指导】

配置用户角色对应的 Web 菜单项时，可以使用该命令查看系统支持的全部菜单树。

【举例】

显示全部 Web 菜单信息。

```
<Sysname> display web menu
```

```
.
|--Dashboard: ID = dashboard
|   |--Working monitor: ID = m_dashboard
|   |--Flowing monitor: ID = m_flowdetection
|   |--Threating monitor: ID = m_threatdetection
|   |--Url monitor: ID = m_urldetection
|   |--UserDefined monitor: ID = m_definedboard
|   `--Interface Information: ID = m_ifinfopanel
|--Monitor: ID = m_monitor
|   |--Attack Defense Logs: ID = m_atklog
|   |   |--Blacklist Logs: ID = m_blacklistlog
|   |   |--Blacklist Logs: ID = m_singleatk
|   |   |--Blacklist Logs: ID = m_scanatk
|   |   |--Blacklist Logs: ID = m_floodatk
|   |   |--Threat Log: ID = m_threatlog
|   |   |--URL Log: ID = m_urllog
|   |   |--Ffilter Log: ID = m_filefilterlog
|   |   `--Zonepair Logs: ID = m_zonepairlog
|   |--Application Audit Logs: ID = m_auditlogs
|   |   |--IM Chat Logs: ID = m_auditimchatlog
|   |   |--Community Logs: ID = m_auditcommunitylog
|   |   |--SearchEngine Logs: ID = m_auditsearchenginelog
|   |   |--Mail Logs: ID = m_auditmaillog
|   |   |--File Transfer Logs: ID = m_auditfiletransferlog
|   |   |--Relax/Stock Logs: ID = m_auditrelaxstocklog
|   |   `--Other Application Logs: ID = m_auditotherapplog
|   |--Log: ID = m_monitorlog
|   |   |--System Log: ID = m_syslog
|   |   |--Operation Log: ID = m_operationlog
|   |   `--Traffic Log: ID = m_trafficlog
|   |--Statistics: ID = m_rank
|   |   |--Traffic Rank: ID = m_trafficrank
|   |   |   |--User Rank: ID = m_usertrafficrank
|   |   |   |--App Rank: ID = m_apptrafficrank
|   |   |   |--SrcIP Rank: ID = m_srciprank
|   |   |   `--Virtual System Rank: ID = m_versysystrafficrank
|   |   |--Threat Rank: ID = m_threadrank
|   |   |   |--User Rank: ID = m_threaduserrank
|   |   |   |--App Rank: ID = m_threadapprank
```

```

|   |   |   |--Threat Type Rank: ID = m_threadtyperank
|   |   |   |--Attacker Rank: ID = m_attackerrank
|   |   |   |--Attack Target Rank: ID = m_attacktargetrank
|   |   |   `--Threat Name Rank: ID = m_threadnamerank
|   |   |--URLFilter Rank: ID = m_urlfilterrank
|   |   |   |--User Rank: ID = m_urluserrank
|   |   |   |--Category Rank: ID = m_urlcategoryrank
|   |   |   |--Website Rank: ID = m_urlwebsiterank
|   |   |   |--SrcIP Rank: ID = m_urlsrciprank
|   |   |   `--DstIP Rank: ID = m_urldstiprank
|   |   |--FFilter Rank: ID = m_ffilterrank
|   |   |   `--FileType Rank: ID = m_filetyperank
|   |   |--Security Audit: ID = m_securityaudit
|   |   |   |--Security Audit: ID = m_attackstatistics
|   |   |   |--Clientverify Protectrunning: ID = m_clientverifyprotectrunning
|   |   |   `--Blacklist Running: ID = m_blacklistrunning
|   |   `--Drop Stat: ID = m_dropstats
|   |--Trend: ID = m_trend
|   |   |--Traffic Trend: ID = m_traffictrend
|   |   |   |--User Trend: ID = m_appsorttraffictrend
|   |   |   |--App Category Trend: ID = m_appcategorytraffictrend
|   |   |   |--SrcIP Trend: ID = m_srciptrend
|   |   |   |--App Trend: ID = m_apptraffictrend
|   |   |   |--Virtual System Trend: ID = m_versysstraffictrend
|   |   |   |--BandWidth Trend: ID = m_tunneltraffictrend
|   |   |   |--Traffic Histogram: ID = m_traffichistogram
|   |   |   `--Traffic Distribution: ID = m_trafficdistribution
|   |   |--Thread Trend: ID = m_threadtrend
|   |   |   |--User Trend: ID = m_threadusertrend
|   |   |   |--App Trend: ID = m_threadapptrend
|   |   |   |--Threat Type Trend: ID = m_threadtypetrend
|   |   |   |--Attacker Trend: ID = m_attackertrend
|   |   |   |--Attack Target Trend: ID = m_attacktargettrend
|   |   |   `--Threat Name Trend: ID = m_threadnametrend
|   |   |--URLFilter Trend: ID = m_urlfiltertrend
|   |   |   |--User Trend: ID = m_urlusertrend
|   |   |   |--Category Trend: ID = m_urlcategorytrend
|   |   |   |--Website Trend: ID = m_urlwebsitetrend
|   |   |   |--SrcIP Trend: ID = m_urlsrciptrend
|   |   |   `--DstIP Trend: ID = m_urldstiptrend
|   |   `--FFilter Trend: ID = m_ffiltertrend
|   |       `--FileType Trend: ID = m_filetypetrend
|   |--Report: ID = m_report
|   |--Session Show: ID = m_session
|   `--User Information Center: ID = m_userinfocenter
|--Policy: ID = m_policy
|   |--Security Policy: ID = m_firewall
|   |   |--Security Policy: ID = m_secpolicy

```

```

|   |   |--Redundancy Rules: ID = m_redundancyrules
|   |   |--Targeted Policy: ID = m_targetpolicy
|   |--IPS: ID = m_ipscfg
|   |   |--Profile: ID = m_ips
|   |   |--Signature: ID = m_ipssignature
|   |--Anti-Virus: ID = m_antiviruscfg
|   |   |--Profile: ID = m_antivirus
|   |   |--Virus Family: ID = m_virusfamily
|   |--Attack Defense: ID = m_attackdefense
|   |   |--Attack Policy: ID = m_atkpolicy
|   |   |--Clientverify Protectip: ID = m_clientverifyprotectip
|   |   |--Blacklist Manual: ID = m_blacklistmanual
|   |   |--Whitelist Manual: ID = m_whitelistmanual
|   |   |--Clientverify Zone: ID = m_clientverifyzone
|   |   |--Attack Defense: ID = m_connlimitpolicies
|   |   |--Attack Defense: ID = m_urpf
|   |       |--IPv4 uRPF: ID = m_urpfzoneipv4
|   |       |--IPv6 uRPF: ID = m_urpfzoneipv6
|   |--Application Audit: ID = m_appaudit
|   |   |--Audit Policy: ID = m_auditpolicy
|   |   |--KeywordGroups: ID = m_keywordgroups
|   |--Bandwidth Management: ID = m_bandwidthmanagement
|   |   |--Traffic Policy: ID = m_bandwidthpolicy
|   |   |--Traffic Profile: ID = m_bandwidthchannel
|   |   |--Interface Bandwidth: ID = m_interfacebandwidth
|--Object: ID = m_resource
|   |--User: ID = m_user
|   |   |--User Control: ID = m_usercontrol
|   |   |   |--Local Users: ID = m_localuser
|   |   |   |--Identity Users: ID = m_identifyuser
|   |   |   |--Online Users: ID = m_onlineuser
|   |   |   |--ImportPolicy: ID = m_importpolicy
|   |   |--Authentication: ID = m_authentication
|   |       |--ISP Domains: ID = m_ispdomain
|   |       |--RADIUS: ID = m_radius
|   |       |--LDAP: ID = m_ldap
|   |           |--LDAPSchme: ID = m_ldapschme
|   |           |--LDAPMap: ID = m_ldapmap
|   |           |--RESTful Server: ID = m_restful
|   |           |--Sec Manage Server: ID = m_tsm
|--APPSecurity: ID = m_dpi
|   |   |--Data Filtering: ID = m_dfltcfg
|   |   |   |--Data Filtering: ID = m_dflt
|   |   |   |--Data Filtering: ID = m_keywordsgroup
|   |   |--URL Filtering: ID = m_ufltcfg
|   |   |   |--URL Category: ID = m_urlcategory
|   |   |   |--Profile: ID = m_uflt
|   |   |--File Filtering: ID = m_ffltcfg

```

```

|   |   |   |--Profile: ID = m_fflt
|   |   |   `--File Type Group: ID = m_filefiltergrp
|   |   |--Application Protocol Recognition: ID = m_apprecognition
|   |   |   |--Application Protocol Recognition: ID = m_applications
|   |   |   `--Application Protocol Recognition: ID = m_appgroup
|   |   |--Security Action: ID = m_securityaction
|   |   |   |--Block: ID = m_block
|   |   |   |--Redirect: ID = m_redirect
|   |   |   `--Capture: ID = m_capture
|   |   `--Advanced Configuration: ID = m_dpfcfg
|--Object Group: ID = m_objectgroup
|   |   |--IPv4: ID = m_ipv4objectgroup
|   |   |--IPv6: ID = m_ipv6objectgroup
|   |   |--IPv6: ID = m_macobjectgroup
|   |   |--Services: ID = m_serviceobjectgroup
|   |   `--Time Range: ID = m_timerange
|--ACL: ID = m_acl
|   |   |--IPv4: ID = m_ipv4acl
|   |   |--IPv6: ID = m_ipv6acl
|   |   `--Ethernet: ID = m_macacl
|--SSL: ID = m_ssl
|   |   |--SSLSERVER: ID = m_sslserver
|   |   |--SSLCLIENT: ID = m_sslclient
|   |   `--SSLADVANCED: ID = m_ssladvancesetting
|--Public Key: ID = m_publickey
|   |   |--Local Keys: ID = m_publickeylocal
|   |   `--Peer Public Key: ID = m_publickeypeer
|--PKI: ID = m_pki_cert
|   |   |--Certificate: ID = m_pki
|   |   |--Certificate Access Control: ID = m_certificatepolicy
|   |   `--Certificate Subject: ID = m_certificatesubject
|--Network: ID = m_network
|   |--VRF: ID = m_vrf
|   |--Interfaces: ID = m_if
|   |   |--Interfaces: ID = m_interface
|   |   |--Interface Pair: ID = m_inline
|   |   |--Interface Collaboration: ID = m_collaborations
|   |   `--Aggregation: ID = m_lagg
|--Security Zone: ID = m_seczone
|--Link: ID = m_link
|   |--VLAN: ID = m_vlan
|   `--MAC: ID = m_mac
|--DNS: ID = m_dns_sum
|   |--Resolution: ID = m_dnshosts
|   |--DNS Client: ID = m_dns
|   `--DNS Advanced Setting: ID = m_dnsadvance
|--IP: ID = m_ip_net
|   |--IP: ID = m_ip

```



```

|   |   |--ARP: ID = m_arp
|   |--IPv6: ID = m_ipv6_net
|   |   |--IPv6: ID = m_ipv6
|   |   |--ND: ID = m_nd
|   |--Routing: ID = m_routing
|   |   |--Routing Table: ID = m_routingtable
|   |   |--Static Routing: ID = m_staticrouting
|   |   |--PolicyRouting: ID = m_policyrouting
|   |   |   |--IPv4 Policy-Based Routing: ID = m_ipv4policy
|   |   |   |--IPv6 Policy-Based Routing: ID = m_ipv6policy
|   |   |--OSPF: ID = m_ospf
|   |   |--RIP: ID = m_rip
|   |--Service: ID = m_ipservice
|       |--HTTP/HTTPS: ID = m_http
|       |--SSH: ID = m_ssh
|       |--NTP: ID = m_ntp
|       |--FTP: ID = m_ftp
|       |--Telnet: ID = m_telnet
|--System: ID = m_device
    |--Virtualization: ID = m_virtualdevice
    |   |--IRF: ID = m_cluster
    |   |--Context: ID = m_context
    |       |--Context: ID = m_contextcontext
    |       |--Context Interface: ID = m_contextinterface
    |       |--Context Resource: ID = m_contextresource
    |       |--Context Usage: ID = m_contextusage
    |--High Availability: ID = m_highavailability
    |   |--Hot Backup: ID = m_hotbackup
    |--Log Settings: ID = m_logconf
    |   |--Basic Setting: ID = m_basiclog
    |   |--Session Log: ID = m_sessionlog
    |   |--Threaten Log: ID = m_threatenlog
    |   |--Audit Log: ID = m_auditlog
    |   |--Url Filter Log: ID = m_urlfilterlog
    |   |--Attack Advance Log: ID = m_atkadvancelog
    |   |--Bandwidth Settings: ID = m_bandwidthalarm
    |   |--Configuration Advance Log: ID = m_cfgadvancelog
    |--Report Settings: ID = m_reportconf
    |   |--Report Subscription: ID = m_reportsubscription
    |   |--Mail Server Config: ID = m_mailserverconfig
    |--Session Aging Time Settings: ID = m_sessionagingtimeset
    |   |--The Aging Time Of The Protocol State Session: ID =
m_protocolstatesessionagingtime
    |   |--Aging Time For Sessions Of An Application Layer Protocol: ID = m_appagingtime
    |   |--Advanced Setting: ID = m_sessionsettings
    |--Signature Upgrade: ID = m_signatureupgrade
    |   |--Signature Upgrade: ID = m_upgradecenter
    |   |--Upgrade: ID = m_upgrade
    |--LicenseConfig: ID = m_license

```

```

|--Administrators: ID = m_adminuser
|   |--Administrators: ID = m_admin
|   `--Role: ID = m_rbacrole
|--Maintenance: ID = m_maintenance
|   |--Settings: ID = m_devicesettings
|   |   |--Device Info: ID = m_basicdevinfo
|   |   |--Datetime: ID = m_basicdatetime
|   |   `--SNMP: ID = m_snmp
|   |--Configuration: ID = m_config
|   |--Reboot: ID = m_reboot
|   `--About: ID = m_about
|       |--DeviceInfo: ID = m_aboutdeviceinfo
|       |--Version: ID = m_aboutversion
|       |--Electronic: ID = m_aboutelectronic
|       `--Legal: ID = m_aboutlegal
`--Diagnosis Center: ID = m_diagnosis
    |--Ping: ID = m_ping
    |--Tracert: ID = m_tracert
    |--Packet Capture: ID = m_pcapware
    |--Web Diagnosis: ID = m_webdiag
    |--Diagnostics: ID = m_diagnostic
    `--Packet Trace: ID = m_troubleshoot

```

1.1.14 display web users

display web users 命令用来显示 Web 用户的相关信息。

【命令】

display web users

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【举例】

显示当前 Web 用户的相关信息。

```
<Sysname> display web users
```

UserID	Name	Type	Language	JobCount	LoginTime	LastOperation
AB2039483271293	Administrator	HTTP	Chinese	3	12:00:23	14:10:05
F09382BA2014AC8	user	HTTPS	English	1	13:05:00	14:11:00

表1-9 display web users 命令显示信息描述表

字段	描述
UserID	Web用户的ID号，用来唯一标识一个登录用户
Name	Web用户的登录用户名
Type	Web用户登录使用的协议类型： • HTTP 表示 Hypertext Transfer Protocol • HTTPS 表示基于安全套接字的 Hypertext Transfer Protocol
Language	Web用户登录时使用的语言： • Chinese 表示中文 • English 表示英文
JobCount	Web用户建立的连接数量
LoginTime	Web用户的登录时间
LastOperation	Web用户的最后操作时间

1.1.15 escape-key

escape-key 命令用来配置终止运行任务（比如 **ping** 命令等）的快捷键。

undo escape-key 命令用来取消快捷键的配置，包括缺省快捷键。

【命令】

escape-key { *key-string* | **default** }

undo escape-key

【缺省情况】

按<Ctrl+C>组合键终止运行的任务。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【参数】

key-string: 定义终止运行任务的快捷键，可以是区分大小写的单个字符（字符“d”和“D”除外），也可以是单个字符或组合键对应的ASCII码（0~127）。比如设置**escape-key 1**，此时生效快捷键为Ctrl+A；如果设置**escape-key a**，生效的快捷键为a。配置字符“d”和“D”作为终止运行任务的快捷键时系统不会生效，此时<Ctrl+C>为实际的生效快捷键。如确实需要使用字符“d”和“D”作为终止运行任务的快捷键，可以配置**key-string**为字符“d”和“D”对应的ASCII码。单个字符的快捷键对应的ASCII码与标准的ASCII码表一致，组合键对应的ASCII码请参见 [表 1-1](#)。

default: 恢复为缺省的快捷键<Ctrl+C>。

【使用指导】

用户可以按<Ctrl+C>组合键来终止 ping、tracert 等正在执行的任务，以便输入新的命令。如果配置了 **escape-key**，则用户可以用新配置的快捷键来代替<Ctrl+C>。命令行是否支持<Ctrl+C>终止与功能模块的软件实现有关，请参见相关命令行的描述。

如果设置的快捷键为单个字符，且有任务可终止，则输入快捷键会终止命令的执行；如果没有任务可终止，则输入的快捷键会作为普通的编辑字符。

如果在 Device A 某用户线设置了单个字符 **key-string** 为任务终止快捷键，当使用该用户线登录到 Device A，又通过 Device A 以 telnet 方式到 Device B，这时的 **key-string** 在 Device B 上将被视为编辑字符进行输入。如果 telnet 到 Device B 时所使用的用户线下配置了相同的 **key-string**，此时 **key-string** 在有任务运行时可以中止任务。

新设置的快捷键可以使用 **display current-configuration | include escape-key** 命令来查看。

如果用户线视图下配置 **escape-key** 为缺省值，并且此时用户线类视图下配置了 **escape-key**，则用户线类视图下的配置生效；如果用户线类视图下未配置，则生效的为缺省值。

用户线视图下使用本命令配置的快捷键立即生效；用户线类视图下配置的快捷键将在下次登录时生效。

【举例】

配置 VTY0 终止运行任务的快捷键为 a。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] escape-key a
```

验证过程如下：

- 使用 **ping** 命令检查 IP 地址为 192.168.1.49 的设备是否可达，并用 **-c** 参数指定发送 ICMP 回显请求报文的数目为 20。

```
<Sysname> ping -c 20 192.168.1.49
  PING 192.168.1.49: 56 data bytes, press a to break
    Reply from 192.168.1.49: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 192.168.1.49: bytes=56 Sequence=2 ttl=255 time=3 ms
```

- 键入 a，任务立即终止，并返回到当前视图。

```
--- 192.168.1.49 ping statistics ---
  2 packet(s) transmitted
  2 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 3/3/3 ms
<Sysname>
```

1.1.16 flow-control

flow-control 命令用来配置流量控制方式。

undo flow-control 命令用来恢复缺省情况。

【命令】

```
flow-control { hardware | none | software }
undo flow-control
```

【缺省情况】

没有配置流量控制方式。

【视图】

用户线视图

【缺省用户角色】

network-admin
context-admin

【参数】

hardware: 进行硬件方式的流量控制。
none: 不进行流量控制。
software: 进行软件方式的流量控制。

【使用指导】

VTY 用户线视图不支持该命令。
流量控制分为入方向和出方向，入方向表示本设备能够接受远端设备的流量控制，出方向表示本设备能够对远端设备进行流量控制。配置该命令后，流量控制方式对入方向和出方向都生效。
要使流量控制生效，双方才能正常通信，对端设备也要配置相同的流量控制方式。

【举例】

```
# 配置 Console 0 用户线视图下，入方向和出方向都采用软件流量控制方式。  
<Sysname> system-view  
[Sysname] line console 0  
[Sysname-line-console0] flow-control software
```

1.1.17 free line

free line 命令用来释放用户线上建立连接。

【命令】

free line { number1 | { console | vty } number2 }

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

number1: 用户线的编号（绝对编号方式）。
本参数的取值范围与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	取值范围为0~65

型号	说明
T5000-G30	取值范围为0~65
T1000-G20/T1000-G50/T1000-G60/T1000-G80	T1000-G20/T1000-G50/T1000-G60: 取值范围为0~69 T1000-G80: 取值范围为0~67
T1000-CN60/T1000-CN80	取值范围为0~65

console: Console 用户线。

vty: VTY 用户线。

number2: 用户线的编号（相对编号方式），对于 Console 用户线取值范围为 0~1，对于 VTY 用户线取值范围为 0~63。

【使用指导】

用户不能使用该命令释放自己的连接。

【举例】

```
# 释放用户线上 VTY 1 建立的连接。
<Sysname> free line vty 1
Are you sure to free line vty1? [Y/N]:y
[OK]
```

1.1.18 free user-interface

free user-interface 命令用来释放用户线上建立的连接。

【命令】

free user-interface { *number1* | { **console** | **vty** } *number2* }

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

number1: 用户线的编号（绝对编号方式）。

本参数的取值范围与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	取值范围为0~65
T5000-G30	取值范围为0~65
T1000-G20/T1000-G50/T1000-G60/T1000-G80	T1000-G20/T1000-G50/T1000-G60: 取值范围为0~69 T1000-G80: 取值范围为0~67

型号	说明
T1000-CN60/T1000-CN80	取值范围为0~65

console: Console 用户线。

vty: VTY 用户线。

number2: 用户线的编号（相对编号方式），对于 Console 用户线取值范围为 0~1，对于 VTY 用户线取值范围为 0~63。

【使用指导】

用户不能使用该命令释放自己的连接。

该命令实现与 **free line** 一致，仅为与旧版本兼容保留，请使用 **free line**。

【举例】

```
# 释放用户线上 VTY 1 建立的连接。
<Sysname> free user-interface vty 1
Are you sure to free line vty1? [Y/N]:y
[OK]
```

1.1.19 free web users

free web users 命令用来强制在线 Web 用户下线。

【命令】

free web users { all | user-id user-id | user-name user-name }

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

all: 所有 Web 用户。

user-id user-id: Web 用户的 ID 号，为 15 位十六进制数。系统会自动为每位成功登录的 Web 用户分配一个用户 ID，用户 ID 用于唯一标识 Web 用户。

user-name user-name: Web 用户的用户名，为 1~255 个字符的字符串，区分大小写。

【举例】

```
# 强制所有在线 Web 用户下线。
<Sysname> free web users all
```

【相关命令】

- **display web users**

1.1.20 history-command max-size

history-command max-size 命令用来设置可以存储的当前用户线下历史命令的条数。

undo history-command max-size 命令用来恢复缺省情况。

【命令】

history-command max-size *size-value*

undo history-command max-size

【缺省情况】

历史命令缓冲区可存储 10 条历史命令。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【参数】

size-value: 可存储的历史命令的条数，取值范围为 0~256。

【使用指导】

每个用户线对应一个历史命令缓冲区，缓冲区里保存了当前用户最近执行成功的命令，缓冲区的容量决定了可以保存的历史命令的数目。用户使用 **display history-command** 命令、上光标键 ↑ 或下光标键 ↓ 可以随时了解近期成功执行了哪些操作（**display history-command** 命令的详细介绍请参见“基础配置命令参考”中的“CLI”）。同时登录设备的不同用户拥有不同的历史命令缓冲区，互不影响。

用户退出当前会话时，系统会自动清除相应历史命令缓冲区内保存的历史命令。

如果用户线视图下配置 **history-command max-size** 为缺省值，并且此时用户线类视图下配置了 **history-command max-size**，那么用户线视图下的生效配置值为用户线类视图下的配置；如果用户线类视图下未配置，则生效的为缺省值。

在用户线视图下使用本命令配置的当前用户线下可存储的历史命令条数立即生效；用户线类视图下配置的可存储的历史命令条数将在下次登录时生效。

【举例】

设置 VTY0 用户线下历史命令缓冲区最多可以存储 20 条历史命令。

```
<Sysname> system-view
```

```
[Sysname] line vty 0
```

```
[Sysname-line-vty0] history-command max-size 20
```

1.1.21 http method

http method 命令用来配置 HTTP 服务在响应 OPTIONS 请求时返回的方法列表。

undo http method 命令用来从响应 OPTIONS 请求的方法列表中删除指定的方法。

【命令】

```
http method { delete | get | head | options | post | put } *  
undo http method { delete | get | head | options | post | put } *
```

【缺省情况】

未配置任何方法。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

delete: 将 DELETE 方法添加到返回的方法列表中。
get: 将 GET 方法添加到返回的方法列表中。
head: 将 HEAD 方法添加到返回的方法列表中。
options: 将 OPTIONS 方法添加到返回的方法列表中。
post: 将 POST 方法添加到返回的方法列表中。
put: 将 PUT 方法添加到返回的方法列表中。

【使用指导】

用户通过向设备发送 HTTP OPTIONS 请求，以探测设备支持的 HTTP 方法。如果用户请求的 URL 资源中没有任何服务注册 OPTIONS 方法，则设备将会根据本配置响应用户请求，否则由被请求服务来响应这个请求。若由设备响应此 OPTIONS 请求，则响应方式如下：

- 若未配置 **options** 参数，则返回 405 Method Not Allowed。
- 若配置了 **options** 参数，则根据配置生成 OPTIONS 请求响应返回给用户。

本命令不影响除 OPTIONS 外的其他任何 HTTP 请求。

【举例】

```
# 配置 HTTP 服务在响应 OPTIONS 请求时返回的方法列表为 GET、HEAD、POST、OPTIONS。  
<Sysname> system-view  
[Sysname] http method get head post options
```

1.1.22 idle-timeout

idle-timeout 命令用来设置用户连接的超时时间。

undo idle-timeout 命令用来恢复缺省情况。

【命令】

```
idle-timeout minutes [seconds ]  
undo idle-timeout
```

【缺省情况】

超时时间为 10 分钟。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【参数】

minutes: 指定超时时间，取值范围为 0～35791，单位为分钟。

seconds: 指定超时时间，取值范围为 0～59，单位为秒，缺省值为 0。

【使用指导】

用户登录后，如果在超时时间内设备和用户间没有消息交互，则超时时间到达时设备会自动断开用户连接。

当超时时间设置为 0 时，表示设备不会因为超时自动断开用户连接。

如果用户线视图下配置 **idle-timeout** 为缺省值，并且此时用户线类视图下配置了 **idle-timeout**，那么用户线视图下的生效配置值为用户线类视图下的配置；如果用户线类视图下未配置，则生效的为缺省值。

用户线视图下使用本命令配置的连接超时时间立即生效；用户线类视图下配置的连接超时时间将在下次登录时生效。

【举例】

设置 VTY0 用户线下用户连接超时时间为 1 分钟 30 秒。

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] idle-timeout 1 30
```

1.1.23 ip http acl

ip http acl 命令用来配置 HTTP 服务与 ACL 关联。

undo ip http acl 命令用来恢复缺省情况。

【命令】

```
ip http acl [ advanced | mac ] { acl-number | name acl-name }
undo ip http acl
```

【缺省情况】

HTTP 服务没有与 ACL 关联。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

advanced: 指定高级 ACL。

mac: 指定二层 ACL。

acl-number: 指定 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

name acl-name: 指定 ACL 的名称。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 **all**。仅当指定名称的 ACL 存在时生效。

【使用指导】

如果未指定 **advanced** 和 **mac** 参数，则表示指定 IPv4 基本 ACL。

目前，对于高级 ACL，仅针对源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议设置的匹配条件才能生效；对于二层 ACL，仅针对源 MAC 地址设置的匹配条件才能生效。

配置 ACL 限制 HTTP 客户端时：

- 当未引用 ACL 时，允许所有 HTTP 客户端通过 web 方式登录设备；
- 当引用的 ACL 不存在或者为空时，允许所有 HTTP 客户端通过 web 方式登录设备；
- 当引用的 ACL 非空时，则只有 ACL 中 **permit** 的用户才能访问设备，禁止其他用户访问设备，以避免非法用户访问设备；
- 如果多次使用该命令配置 HTTP 服务与 ACL 关联，最新配置生效。

关于 ACL 的详细描述和介绍请参见“ACL 配置指导”中的“ACL”。

【举例】

配置 HTTP 服务与 ACL 2001 关联，只允许 10.10.0.0/16 网段的客户端通过 Web 访问设备。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ip http acl 2001
```

【相关命令】

- **acl** (ACL 命令参考/ACL)

1.1.24 ip http enable

ip http enable 命令用来开启 HTTP 服务。

undo ip http enable 命令用来关闭 HTTP 服务。

【命令】

ip http enable

undo ip http enable

【缺省情况】

HTTP 服务处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启 HTTP 服务后，用户才能通过 Web 使用 HTTP 方式登录设备。

开启 HTTP 服务后，为了增强设备的安全性，HTTPS 服务的端口号也会被自动打开，且在 HTTP 服务开启的状态下无法通过 **undo ip https enable** 命令关闭。

【举例】

使能 HTTP 服务。

```
<Sysname> system-view  
[Sysname] ip http enable
```

【相关命令】

- **ip https enable**

1.1.25 ip http port

ip http port 命令用来配置 HTTP 服务的端口号。

undo ip http port 命令用来恢复缺省情况。

【命令】

```
ip http port port-number  
undo ip http port
```

【缺省情况】

HTTP 服务的端口号为 80。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

port-number：HTTP 服务的端口号，取值范围为 1~65535。

【使用指导】

如果修改端口号前 HTTP 服务是开启的，则修改端口号后系统会自动重启 HTTP 服务，正在访问的用户将被断开，用户需要在浏览器的地址栏中重新输入新的地址后才可以继续访问。

【举例】

配置 HTTP 服务的端口号为 80。

```
<Sysname> system-view
```

[Sysname] ip http port 80

1.1.26 ip https acl

ip https acl 命令用来配置 HTTPS 服务与 ACL 关联。

undo ip https acl 命令用来恢复缺省情况。

【命令】

```
ip https acl [ advanced | mac ] {acl-number | name acl-name }  
undo ip https acl
```

【缺省情况】

HTTPS 服务未与 ACL 关联。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

advanced: 指定高级 ACL。

mac: 指定二层 ACL。

acl-number: ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999: 表示基本 ACL。
- 3000～3999: 表示高级 ACL。
- 4000～4999: 表示二层 ACL。

name acl-name: 指定 ACL 的名称。**acl-name** 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 **a～z** 或 **A～Z** 开头。为避免混淆，ACL 的名称不允许使用英文单词 **all**。仅当指定名称的 ACL 存在时生效。

【使用指导】

如果未指定 **advanced** 和 **mac** 参数，则表示指定 IPv4 基本 ACL。

目前，对于高级 ACL，仅针对源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议设置的匹配条件才能生效；对于二层 ACL，仅针对源 MAC 地址设置的匹配条件才能生效。

配置 ACL 限制 HTTPS 客户端时：

- 当未引用 ACL 时，允许所有 HTTPS 客户端通过 web 方式登录设备；
- 当引用的 ACL 不存在或者为空时，允许所有 HTTPS 客户端通过 web 方式登录设备；
- 当引用的 ACL 非空时，则只有 ACL 中 **permit** 的用户才能访问设备，禁止其他用户访问设备，以避免非法用户访问设备；
- 如果多次使用该命令配置 HTTPS 服务与 ACL 关联，最新配置生效。

关于 ACL 的详细描述和介绍请参见“ACL 配置指导”中的“ACL”。

Web 登录时用户输入的用户名和密码属于敏感信息，Web 登录请求采用 HTTPS 方式发送到 Web 服务器。所以，如果本命令中的 ACL 规则拒绝客户端通过 HTTPS 服务访问 Web 页面，那么该客户端也无法通过 HTTP 服务访问 Web 页面。

【举例】

配置 HTTPS 服务与 ACL 2001 关联，只允许 10.10.0.0/16 网段的客户端通过 Web 访问设备。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ip https acl 2001
```

【相关命令】

- **acl** (ACL 命令参考/ACL)

1.1.27 ip https certificate access-control-policy

ip https certificate access-control-policy 命令用来配置 HTTPS 服务与证书属性访问控制策略关联。

undo ip https certificate access-control-policy 命令用来恢复缺省情况。

【命令】

```
ip https certificate access-control-policy policy-name
undo ip https certificate access-control-policy
```

【缺省情况】

HTTPS 服务未与证书属性访问控制策略关联。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 证书属性访问控制策略名，为 1~31 个字符的字符串，区分大小写。

【使用指导】

通过将 HTTPS 服务与已配置的客户端证书属性访问控制策略关联，可以实现对客户端的访问权限进行控制。证书属性访问控制策略的相关介绍请参见“安全配置指导”中“PKI”。

【举例】

```
# 设置 HTTPS 服务使用的证书属性访问控制策略为 myacl。
<Sysname> system-view
[Sysname] ip https certificate access-control-policy myacl
```

【相关命令】

- **pki certificate access-control-policy** (PKI 命令参考/PKI)

1.1.28 ip https enable

ip https enable 命令用来开启 HTTPS 服务。

undo ip https enable 命令用来关闭 HTTPS 服务。

【命令】

ip https enable

undo ip https enable

【缺省情况】

设备采用出厂配置启动时，HTTPS 服务处于开启状态。

设备采用空配置启动时，HTTPS 服务处于关闭状态。

关于出厂配置和空配置的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

只有使能该功能后，用户才能通过 Web 方式使用 HTTPS 登录设备。

使能 HTTPS 服务，会触发 SSL 的握手协商过程。在 SSL 握手协商过程中，如果设备的本地证书已经存在，则 SSL 协商可以成功，HTTPS 服务可以正常启动；如果设备的本地证书不存在，则 SSL 协商过程会触发证书申请流程。由于证书申请需要较长的时间，会导致 SSL 协商不成功，从而无法正常启动 HTTPS 服务。因此，在这种情况下，需要多次执行 **ip https enable** 命令，这样 HTTPS 服务才能正常启动。

【举例】

使能 HTTPS 服务。

<Sysname> system-view

[Sysname] ip https enable

【相关命令】

- **ip https ssl-server-policy**
- **ip https certificate access-control-policy**

1.1.29 ip https port

ip https port 命令用来配置 HTTPS 服务的端口号。

undo ip https port 命令用来恢复缺省情况。

【命令】

ip https port *port-number*

undo ip https port

【缺省情况】

HTTPS 服务的端口号为 443。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

port-number: HTTPS 服务的端口号，取值范围为 1～65535。

【使用指导】

如果修改端口号前 HTTPS 服务是开启的，则修改端口号后系统会自动重启 HTTPS 服务，正在访问的用户将被断开，用户需要在浏览器的地址栏中重新输入新的地址后才可以继续访问。

【举例】

配置 HTTPS 服务的端口号为 8080。

```
<Sysname> system-view
[Sysname] ip https port 8080
```

1.1.30 ip https ssl-server-policy

ip https ssl-server-policy 命令用来配置 HTTPS 服务与 SSL 服务器端策略关联。

undo ip https ssl-server-policy 命令用来恢复缺省情况。

【命令】

```
ip https ssl-server-policy policy-name
undo ip https ssl-server-policy
```

【缺省情况】

HTTPS 服务未与 SSL 服务器端策略关联，HTTPS 使用自签名证书。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: SSL 服务器端策略名，为 1～31 个字符的字符串。

【使用指导】

HTTP 服务和 HTTPS 服务处于使能状态时，对与 HTTPS 服务关联的 SSL 服务器端策略进行的修改不会生效。如需修改 HTTPS 服务与 SSL 服务器端的关联策略，首先执行 **undo ip http enable** 和 **undo ip https enable** 两条命令，再执行 **ip https ssl-server-policy *policy-name*** 命令，最后重新使能 HTTP 服务和 HTTPS 服务，新的策略即可生效。

如需恢复缺省情况，必须先执行 **undo ip http enable** 和 **undo ip https enable** 两条命令，再执行 **undo ip https ssl-server-policy**，最后重新使能 HTTP 服务和 HTTPS 服务即可。

【举例】

```
# 设置 HTTPS 服务使用的 SSL 服务器端策略为 myssl。
<Sysname> system-view
[Sysname] ip https ssl-server-policy myssl
```

【相关命令】

- **ssl server-policy**（安全命令参考/SSL）

1.1.31 line

line 命令用来进入一个或多个用户线视图。

【命令】

```
line { first-number1 [ last-number1 ] | { console | vty } first-number2
[ last-number2 ] }
```

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

first-number1：第一个用户线的编号（绝对编号方式）。
本参数的取值范围与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	取值范围为0~65
T5000-G30	取值范围为0~65
T1000-G20/T1000-G50/T1000-G60/T1000-G80	T1000-G20/T1000-G50/T1000-G60：取值范围为0~69 T1000-G80：取值范围为0~67
T1000-CN60/T1000-CN80	取值范围为0~65

last-number1：最后一个用户线的编号（绝对编号方式），最大取值与 **first-number1** 取值相同，取值必须大于 **first-number1**。

console：Console 用户线。

vty：VTY 用户线。

first-number2：第一个用户线的编号（相对编号方式），对于 Console 用户线取值范围为 0~1，对于 VTY 用户线取值范围为 0~63。

last-number2：最后一个用户线的编号（相对编号方式），对于 Console 用户线取值为 1，对于 VTY 用户线取值范围为 1~63，取值必须大于 **first-number2**。

【举例】

```
# 进入 VTY 0 用户线视图。
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0]
# 进入 VTY 0~63 用户线视图。
<Sysname> system-view
[Sysname] line vty 0 63
[Sysname-line-vty0-63]
```

【相关命令】

- **line class**

1.1.32 line class

line class 命令用来进入用户线类视图。

【命令】

```
line class { console | vty }
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

console: Console 用户线类。

vty: VTY 用户线类。

【使用指导】

用户线视图下的配置只对该用户线生效。

用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效。

line class 命令用来进入用户线类视图，**line** 命令用来进入一个或多个用户线视图。对于同时支持这两种视图的命令：

- 用户线视图下的配置优先于用户线类视图下的配置。
- 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值。

用户线类视图下支持的命令有：

- **activation-key**
- **auto-execute command**
- **authentication-mode**
- **command accounting**
- **command authorization**

- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

【举例】

在 VTY 用户线类视图下，将用户连接的超时时间的缺省值设置为 15 分钟。

```
<Sysname> system-view
[Sysname] line class vty
[Sysname-line-class-vty] idle-timeout 15
```

在 Console 用户线类视图下，将终端会话的快捷键设置为<s>。

```
<Sysname> system-view
[Sysname] line class console
[Sysname-line-class-console] activation-key s
[Sysname-line-class-console] quit
```

- 在 Console 用户线视图下，将终端会话的快捷键设置为缺省值（可以使用 **undo activation-key** 或者直接使用 **activation-key 13** 进行配置）。

```
[Sysname] line console 0
[Sysname-line-console0] undo activation-key
```

- 此时生效的快捷键为用户线类视图下的配置，验证过程如下：
- 退出终端会话。

```
[Sysname-line-console0] return
<Sysname> quit
```

- 重新登录设备，能看到如下显示信息。

Press ENTER to get started.

- 此时，<Enter>键失效，需要按<s>键才能出现用户视图提示符，启动终端会话。

```
<Sysname>
```

【相关命令】

- **line**

1.1.33 lock

lock 命令用来锁定当前用户线并配置解锁密码，防止未授权的用户操作该用户线。

【命令】

lock

【缺省情况】

系统不会自动锁定当前用户线。

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

用户输入 **lock** 命令后，系统提示输入密码（密码最大长度为 16 个字符），并提示再次输入密码，只有两次输入的密码相同，**Lock** 操作才能成功。如果用户线被锁定，用户需要输入解锁密码才能结束锁定，进入系统。

【举例】

锁住当前用户线然后解锁。

```
<Sysname> lock
```

```
Please input password<1 to 16> to lock current line:
```

```
Password:
```

```
Again:
```

```
locked !
```

此时，命令行用户线被锁定。键入回车，并输入正确的密码后，可以解锁。

```
Password:
```

```
<Sysname>
```

1.1.34 lock reauthentication

lock reauthentication 命令用来锁定当前用户线并对其进行重新认证。

【命令】

lock reauthentication

【缺省情况】

系统不会对当前用户线进行重新认证。

【视图】

任意视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

执行该命令后，当前用户线会被锁定。用户需要输入设备登录密码对当前用户线进行重新认证才能结束锁定，进入系统。如果设备未配置登录密码，用户按回车键后将直接进入系统。

需要注意的是，如果在设备登录后修改了登录设备的认证方式或密码，那么锁定用户线后的解锁过程将使用新配置的认证方式及密码。

【举例】

输入命令锁定当前用户线，并使用设备登录密码重新登录设备。

```
<Sysname> lock reauthentication
```

```
Please press Enter to unlock the screen.
```

按回车键后，提示输入密码对当前用户线进行重新认证并登录设备。

```
Password:
```

```
<Sysname>
```

【相关命令】

- **lock-key**

1.1.35 lock-key

lock-key 命令用来配置对当前用户线进行锁定并重新认证的快捷键。

undo lock-key 命令用来恢复缺省情况。

【命令】

lock-key *key-string*

undo lock-key

【缺省情况】

未设置对当前用户线进行锁定并重新认证的快捷键。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【参数】

key-string: 指定对当前用户线进行重新认证的快捷键。可以是区分大小写的单个字符，也可以是单个字符或组合键对应的ASCII码（0~127）。例如设置**lock-key 1**，则快捷键为Ctrl+A；如设置**lock-key a**，生效的快捷键为a。使用ASCII码设置快捷键时，单个字符对应的ASCII码与标准ASCII码表一致，组合键对应的ASCII码请参照 [表 1-1](#)。

【使用指导】

通常情况下，建议用户使用组合键而不使用单个字符作为快捷键，避免用户在输入命令时输入完快捷键字符后出现锁定，影响正常命令行的输入。用户设置了快捷键之后，可以输入对应的快捷键代替 **lock reauthentication** 命令完成对当前用户线进行锁定并重新认证的操作。

在用户线/用户线类视图下，该命令的配置的快捷键将立即生效。

新设置的快捷键可以使用 **display current-configuration | include lock-key** 命令来查看。

【举例】

配置锁定当前用户线的快捷键为 Ctrl+A。

```
<Sysname> system-view
```

```
[Sysname] line vty 0
```

```
[Sysname-line-vty0] lock-key 1
```

```
[Sysname-line-vty] quit
```

验证过程如下：

- 用户键入 Ctrl+A 组合键后，系统锁定当前用户线并切换到重新认证界面：

```
[Sysname]
```

Please press Enter to unlock the screen.

- 按回车键后，系统提示输入密码对当前用户线进行重新认证并登录设备。

Password:

[Sysname]

【相关命令】

- **lock reauthentication**

1.1.36 parity

parity 命令用来设置校验位的解析和生成方式。

undo parity 命令用来恢复缺省情况。

【命令】

```
parity { even | mark | none | odd | space }  
undo parity
```

【缺省情况】

设备校验位的校验方式为 **none**，即不进行校验。

【视图】

用户线视图

【缺省用户角色】

network-admin
context-admin

【参数】

even: 进行偶校验。
mark: 进行标记校验。
none: 无校验。
odd: 进行奇校验。
space: 进行空格校验。

【使用指导】

VTY 用户线视图不支持该命令。

访问终端和设备相应用户线下校验位的设置必须一致，双方才能正常通信。

【举例】

```
# 将 Console 用户线传输校验位设为奇校验。  
<Sysname> system-view  
[Sysname] line console 0  
[Sysname-line-console0] parity odd
```

1.1.37 protocol inbound

protocol inbound 命令用来指定所在用户线支持的协议。

undo protocol inbound 命令用来恢复缺省情况。

【命令】

```
protocol inbound { all | ssh | telnet }  
undo protocol inbound
```

【缺省情况】

系统支持所有协议。

【视图】

VTY 用户线视图
VTY 用户线类视图

【缺省用户角色】

network-admin
context-admin

【参数】

all: 支持所有的协议，包括 Telnet 和 SSH。
ssh: 支持 SSH 协议。
telnet: 支持 Telnet 协议。

【使用指导】

用户线视图下，该命令的配置结果将在下次登录时生效。

如果要配置用户线支持 SSH 协议，必须先将该用户的认证方式配置为 **scheme**，否则 **protocol inbound ssh** 命令会执行失败。

用户线视图下，对 **authentication-mode** 和 **protocol inbound** 进行关联绑定。

- 当这两条命令均配置为缺省值，此时该用户线视图下的这两条命令配置值均取该类用户线类视图下的相应的配置；若该类用户线类视图下没有进行相应的配置，则均取缺省值。
- 当两条命令中的任意一条配置了非缺省值，那么另外一条取缺省值。当两条命令都配置成非缺省值，则均取用户线下的配置值。

仅具有 **network-admin**、**context-admin** 或者 **level-15** 用户角色的用户可以执行该命令。其他角色的用户，即使授权了该命令的操作权限，也不能执行该命令。

【举例】

设置用户线 VTY 0 到 VTY 4 只支持 SSH 协议。

```
<Sysname> system-view
[Sysname] line vty 0 4
[Sysname-line-vty0-4] authentication-mode scheme
[Sysname-line-vty0-4] protocol inbound ssh
```

设置 VTY 用户线类支持 SSH 协议，认证方式为 **scheme**。同时设置用户线 VTY 0 到 VTY 4 不进行登录认证，支持所有的协议。

```
<Sysname> system-view
[Sysname] line class vty
[Sysname-line-class-vty] authentication-mode scheme
[Sysname-line-class-vty] protocol inbound ssh
[Sysname-line-class-vty] line vty 0 4
[Sysname-line-vty0-4] authentication-mode none
```

验证过程如下：

- 使用 Telnet 方式登录，无需认证即可成功登录。

```
<Client> telnet 192.168.1.241
Trying 192.168.1.241 ...
Press CTRL+K to abort
Connected to 192.168.1.241 ...
```

```
*****
* Copyright (c) 2015-2019 Beijing UNIS Hengyue Technologies Co., Ltd.          *
* Without the owner's prior written consent,                                  *
* no decompiling or reverse-engineering shall be allowed.                    *
*****
```

```
<Server>
```

- 查看当前正在使用的用户线以及用户的相关信息，用户线为 **line 0**，则证明该配置下用户线下配置生效。

```
<Server> display users

  Idx  Line   Idle       Time           Pid    Type
+ 50   VTY 0   00:00:00   Jan 17 15:29:27   189    TEL
```

```
Following are more details.  
VTY 0 :  
      Location: 192.168.1.186  
+      : Current operation user.  
F      : Current operation user works in async mode.
```

【相关命令】

- **authentication-mode**

1.1.38 restful http enable

restful http enable 命令用来开启基于 HTTP 的 RESTful 功能。

undo restful http enable 命令用来关闭基于 HTTP 的 RESTful 功能。

【命令】

```
restful http enable  
undo restful http enable
```

【缺省情况】

基于 HTTP 的 RESTful 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

开启该功能后，用户才可以通过 RESTful HTTP 方式登录设备并采用 RESTful API 对设备进行配置和维护。

【举例】

```
# 开启基于 HTTP 的 RESTful 功能。  
<Sysname> system-view  
[Sysname] restful http enable
```

1.1.39 restful https enable

restful https enable 命令用来开启基于 HTTPS 的 RESTful 功能。

undo restful https enable 命令用来关闭基于 HTTPS 的 RESTful 功能。

【命令】

```
restful https enable  
undo restful https enable
```

【缺省情况】

基于 HTTPS 的 RESTful 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启该功能后，用户才可以通过 RESTful HTTPS 方式登录设备并采用 RESTful API 对设备进行配置和维护。

【举例】

开启基于 HTTPS 的 RESTful 功能。

```
<Sysname> system-view
```

```
[Sysname] restful https enable
```

1.1.40 screen-length

screen-length 命令用来设置分屏显示时，每屏所显示的行数。

undo screen-length 命令用来恢复缺省情况。

【命令】

screen-length *screen-length*

undo screen-length

【缺省情况】

每屏显示 24 行数据。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【参数】

screen-length: 指定每屏所显示的行数，取值范围为 0~512。0 表示一次性显示全部信息，即不进行分屏显示，此时与执行 **screen-length disable** 命令效果相同。

【使用指导】

该命令设置的是每一屏所显示的行数，但显示终端实际显示的行数由终端的规格决定。比如，设置 **screen-length** 的值为 40，但显示终端的规格为 24 行，当暂停显示按空格键时，设备发送给显示终端的信息为 40 行，但当前屏幕显示的是第 18~第 40 行的信息，前面的 17 行信息，需要通过 <Page Up>/<Page Down>键来翻看。

设备支持分屏显示信息，在暂停显示时按空格键，能继续显示下一屏信息。

缺省情况下，分屏显示功能处于开启状态。

如果用户线视图下配置 **screen-length** 为缺省值，并且此时用户线类视图下配置了 **screen-length**，则用户线类视图下的配置生效；如果用户线类视图下未配置，则生效的为缺省值。

用户线视图下使用本命令配置的分屏显示信息行数立即生效；在用户线类视图下配置的分屏显示信息行数将在下次登录时生效。

【举例】

```
# 设置 VTY 用户线分屏显示时，每屏显示 30 行数据。
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] screen-length 30
```

【相关命令】

- **screen-length disable**（基础配置指导/CLI）

1.1.41 send

send 命令用来向用户线发送消息。

【命令】

```
send { all | number1 | { console | vty } number2 }
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

all：所有的用户线。

number1：用户线的编号（绝对编号方式）。

本参数的取值范围与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	取值范围为0~65
T5000-G30	取值范围为0~65
T1000-G20/T1000-G50/T1000-G60/T1000-G80	T1000-G20/T1000-G50/T1000-G60：取值范围为0~69 T1000-G80：取值范围为0~67
T1000-CN60/T1000-CN80	取值范围为0~65

console：Console 用户线。

vtty：VTY 用户线。

number2：用户线的编号（相对编号方式），对于 Console 用户线取值范围为 0~1，对于 VTY 用户线取值范围为 0~63。

【使用指导】

输入本命令后回车，系统会提示您可以输入消息内容。在输入消息内容时，按<Enter>键结束输入，按<Ctrl+C>组合键取消此次操作。

【举例】

使用 VTY 0 用户线上线的用户想重启设备，于是发信息 “Note please, I will reboot the system in 3 minutes.” 来提醒 VTY 1。

```
<Sysname> send vty 1
```

Input message, end with Enter; abort with CTRL+C:

Your attention, please. I will reboot the system in 3 minutes.

Send message? [Y/N]:y

使用 VTY 1 用户线登录的用户将收到如下消息：

```
[Sysname]
```

```
***
```

```
***
```

```
***Message from vty0 to vty1
```

```
***
```

```
Your attention, please. I will reboot the system in 3 minutes.
```

1.1.42 set authentication password

set authentication password 命令用来设置认证密码。

undo set authentication password 命令用来恢复缺省情况。

【命令】

set authentication password { hash | simple } *string*

undo set authentication password

【缺省情况】

未配置认证密码。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【参数】

hash：以哈希方式设置密码。

simple：以明文方式设置密码，该密码将以密文方式存储。

string：密码字符串，区分大小写。明文密码为 1~16 个字符的字符串，哈希密码为 1~110 个字符的字符串。

【使用指导】

以明文或哈希方式设置的密码，均以哈希计算后的密文形式保存在配置文件中。

如果用户线视图下配置 **set authentication password** 为缺省值，并且此时用户线类视图下配置了 **set authentication password**，则用户线类视图下的配置生效；如果用户线类视图下未配置，则生效的为缺省值。

仅具有 **network-admin**、**context-admin** 或者 **level-15** 用户角色的用户可以执行该命令。其他角色的用户，即使授权了该命令的操作权限，也不能执行该命令。

在用户线视图/用户线类视图下，使用该命令设置的认证密码将在下次登录设备时生效。

【举例】

设置用户线 VTY 0 的认证密码为 hello。

```
<Sysname> system-view
```

```
[Sysname] line vty 0
```

```
[Sysname-line-vty0] authentication-mode password
```

```
[Sysname-line-vty0] set authentication password simple hello
```

设置完后如果退出系统，则只有在密码提示信息后输入 **hello** 字符串才能再进入系统。

【相关配置】

- **authentication-mode**

1.1.43 shell

shell 命令用来在当前用户线上开启终端服务。

undo shell 命令用来在当前用户线上关闭终端服务。

【命令】

shell

undo shell

【缺省情况】

所有用户线的终端服务功能处于开启状态。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

Console 用户线视图/Console 用户线类视图不支持 **undo shell** 命令。

用户不能在自己登录的用户线上使用 **undo shell** 命令。

当设备作为 Telnet/SSH 服务器的时候，不能配置 **undo shell** 命令。

如果在用户线类视图下使用 **undo shell** 命令关闭了终端服务，那么用户线视图下无法使用 **shell** 启动终端服务。

【举例】

在 VTY0 到 VTY4 上终止终端服务（用户将不能通过 VTY0~4 登录设备）。

```
<Sysname> system-view
[Sysname] line vty 0 4
[Sysname-line-vty0-4] undo shell
Disable line-vty0-4 , are you sure? [Y/N]:y
[Sysname-line-vty0-4]
```

1.1.44 speed

speed 命令用来设置用户线的传输速率。

undo speed 命令用来恢复缺省情况。

【命令】

speed *speed-value*

undo speed

【缺省情况】

用户线的传输速率为 9600bps。

【视图】

用户线视图

【缺省用户角色】

network-admin

context-admin

【参数】

speed-value: 传输速率，单位为 bps。异步串口的传输速率有：300bps、600bps、1200bps、2400bps、4800bps、9600bps、19200bps、38400bps、57600bps 和 115200bps。异步串口的传输速率和配置时的网络环境相关，请根据网络环境配置异步串口的传输速率。

【使用指导】

VTY 用户线视图不支持该命令。

访问终端和设备相应用户线下传输速率的设置必须一致，双方才能正常通信。

【举例】

将用户线 Console 0 的传输速率设置为 19200bps。

```
<Sysname> system-view
[Sysname] line console 0
[Sysname-line-console0] speed 19200
```

1.1.45 stopbits

stopbits 命令用来设置停止位的个数。

undo stopbits 命令用来恢复缺省情况。

【命令】

```
stopbits { 1 | 1.5 | 2 }  
undo stopbits
```

【缺省情况】

停止位为 1 比特。

【视图】

用户线视图

【缺省用户角色】

network-admin
context-admin

【参数】

1: 停止位为 1 比特。

1.5: 停止位为 1.5 比特。目前，设备不支持该参数，配置后实际生效的是命令行 **stopbits 2**。

2: 停止位为 2 比特。

【使用指导】

VTY 用户线视图不支持该命令。

访问终端和设备相应用户线下停止位的设置必须一致，双方才能正常通信。

【举例】

设置 Console 用户线的停止位为 1 比特。

```
<Sysname> system-view  
[Sysname] line console 0  
[Sysname-line-console0] stopbits 1
```

1.1.46 telnet

telnet 命令用于 Telnet 登录到远端设备，以便进行远程管理。

【命令】

```
telnet remote-host [ service-port ] [ vpn-instance vpn-instance-name ]  
[ source { interface interface-type interface-number | ip ip-address } ]  
[ dscp dscp-value ] [ escape character ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

remote-host: 远端设备的 IPv4 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

service-port: 远端设备提供 Telnet 服务的 TCP 端口号, 取值范围为 0~65535, 缺省值为 23。

vpn-instance vpn-instance-name: 指定远端设备所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示远端设备位于公网中。

source: 指定 Telnet 报文的源接口或源 IPv4 地址。如果未指定本参数, 则使用路由出接口的主 IP 地址作为设备发送的 Telnet 报文的源 IPv4 地址。

interface interface-type interface-number: 指定源接口, 发送的 Telnet 报文的源 IPv4 地址为该接口的地址。*interface-type interface-number* 为接口类型和接口编号。

ip ip-address: 指定 Telnet 报文的源 IPv4 地址。

dscp-value: Telnet 客户端向服务器端发送 Telnet 报文的 DSCP 优先级, 取值范围为 0~63, 缺省值为 48。

escape character: 指定退出字符, 该退出字符需要与字符“.”配合使用来断开当前 Telnet 连接, 并返回到上一级连接。*character* 为一个字符, 区分大小写。退出字符不能与登录用户名相同, 建议使用~, 即输入~.来中断当前连接。

【使用指导】

用户可以使用<Ctrl+K>组合键、**quit** 命令或指定退出字符来中断当前 Telnet 连接。这三种方式的使用如下:

- <Ctrl+K>组合键: 断开所有的连接。可在任意情况下使用。
- **quit**: 断开当前连接, 并返回到上一级连接。在服务器端重启或发生异常时该命令无法使用。
- 退出字符: 断开当前连接, 并返回到上一级连接。可在任意情况下使用。

如果指定了退出字符, <Ctrl+K>组合键将失效。

使用退出字符时, 必须在一行中首先输入退出字符和., 该操作才能生效。若该行中曾经输入过其它字符或执行了其它操作 (比如退格), 则需要重新换行输入才能生效。

本命令指定的源 IPv4 地址或源接口只对当前 Telnet 连接有效。

【举例】

Telnet 登录到远程主机 (IP 地址为 1.1.1.2), 并指定发送 Telnet 报文的源 IP 地址为 1.1.1.1。

```
<Sysname> telnet 1.1.1.2 source ip 1.1.1.1
```

【相关命令】

- **telnet client source**

1.1.47 telnet client source

telnet client source 命令用来指定设备作为 Telnet 客户端时, 发送 Telnet 报文的源 IPv4 地址或源接口。

undo telnet client source 命令用来恢复缺省情况。

【命令】

```
telnet client source { interface interface-type interface-number | ip  
ip-address }
```

```
undo telnet client source
```

【缺省情况】

未指定发送 Telnet 报文的源 IPv4 地址和源接口，使用报文路由出接口的主 IPv4 地址作为 Telnet 报文的源地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface interface-type interface-number: 指定源接口，发送的 Telnet 报文的源 IPv4 地址为该接口的地址。*interface-type interface-number* 为接口类型和接口编号。

ip ip-address: 指定发送 Telnet 报文的源 IPv4 地址。

【使用指导】

本命令指定的源 IPv4 地址或源接口对所有 Telnet 连接有效。

若同时使用本命令和 **telnet** 命令指定源 IPv4 地址或源接口，则以 **telnet** 命令指定的源 IP 地址或源接口为准。

【举例】

设备作为 Telnet 客户端时，指定发送的 Telnet 报文的源 IP 地址为 1.1.1.1。

```
<Sysname> system-view
```

```
[Sysname] telnet client source ip 1.1.1.1
```

【相关命令】

- **display telnet client**

1.1.48 telnet ipv6

telnet ipv6 命令用于 IPv6 组网环境下，Telnet 登录到远程主机，以便进行远程管理。

【命令】

```
telnet ipv6 remote-host [ -i interface-type interface-number ] [ port-number ]  
[ vpn-instance vpn-instance-name ] [ source { interface interface-type  
interface-number | ipv6 ipv6-address } ] [ dscp dscp-value ] [ escape  
character ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

remote-host: 远端设备的 IPv6 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

-i interface-type interface-number: 指定 Telnet 报文的出接口。*interface-type interface-number* 为接口类型和接口编号。当 Telnet 指定的服务端 IPv6 地址是全球单播地址时，则不能指定该参数；当指定的服务端 IPv6 地址为链路本地地址时，必须指定该参数。

port-number: 远端设备提供 Telnet 服务的 TCP 端口号，取值范围为 0~65535，缺省值为 23。

vpn-instance vpn-instance-name: 指定远端设备所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示远端设备位于公网中。

source: 指定 Telnet 报文的源接口或源 IPv6 地址。如果未指定本参数，则使用路由出接口的主 IPv6 地址作为 Telnet 报文的源 IPv6 地址。

interface interface-type interface-number: 指定源接口，发送的 Telnet 报文的源 IPv6 地址为该接口的主地址。*interface-type interface-number* 为接口类型和接口编号。

ipv6 ipv6-address: 指定 Telnet 报文的源 IPv6 地址。

dscp-value: IPv6 Telnet 客户端向服务器端发送 Telnet 报文的 DSCP 优先级，取值范围为 0~63，缺省值为 48。

escape character: 指定退出字符，该退出字符需要与字符“.”配合使用来断开当前 Telnet 连接，并返回到上一级连接。*character* 为一个字符，区分大小写。退出字符不能与登录用户名相同，建议使用~，即输入~.来中断当前连接。

【使用指导】

用户可以使用<Ctrl+K>组合键、**quit** 命令或指定退出字符来中断当前 Telnet 连接。这三种方式的使用如下：

- <Ctrl+K>组合键：断开所有的连接。可在任意情况下使用。
- quit：断开当前连接，并返回到上一级连接。在服务器端重启或发生异常时该命令无法使用。
- 退出字符：断开当前连接，并返回到上一级连接。可在任意情况下使用。

如果指定了退出字符，<Ctrl+K>组合键将失效。

使用退出字符时，必须在一行中首先输入退出字符和.，该操作才能生效。若该行中曾经输入过其它字符或执行了其它操作（比如退格），则需要重新换行输入才能生效。

【举例】

Telnet 登录到远程主机，IPv6 地址为 5000::1。

```
<Sysname> telnet ipv6 5000::1
```

Telnet 登录到远程主机，IPv6 地址为 2000::1，并指定 Telnet 报文的源 IPv6 地址为 1000::1。

```
<Sysname> telnet ipv6 2000::1 source ipv6 1000::1
```

1.1.49 telnet server acl

telnet server acl 命令用来使用 ACL（Access Controle List，访问控制列表）限制哪些 Telnet 客户端可以访问设备。

undo telnet server acl 命令用来恢复缺省情况。

【命令】

```
telnet server acl [ mac ] acl-number  
undo telnet server acl
```

【缺省情况】

未使用 ACL 限制 Telnet 客户端。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

mac: 指定二层 ACL。若不指定该关键字，则表示 IPv4 ACL。

acl-number: ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999: 表示 IPv4 基本 ACL。
- 3000～3999: 表示 IPv4 高级 ACL。
- 4000～4999: 需指定 **mac** 关键字，表示二层 ACL。

【使用指导】

配置 ACL 限制 Telnet 客户端时：

- 当未引用 ACL 时，允许所有登录用户访问设备；
- 当引用的 ACL 不存在、或者引用的 ACL 为空时，禁止所有登录用户访问设备；
- 当引用的 ACL 非空时，则只有 ACL 中 **permit** 的用户才能访问设备，其他用户不允许访问设备，以免非法用户使用 Telnet 访问设备。
- 如果多次使用该命令配置 Telnet 服务与 ACL 关联，最新配置生效。

关于 ACL 的详细描述和介绍请参见“ACL 配置指导”中的“ACL”。

该配置只过滤新建立的 Telnet 连接，不会对已建立的 Telnet 连接和操作造成影响。

【举例】

仅允许地址为 1.1.1.1 的用户通过 Telnet 访问本设备。

```
<Sysname> system-view  
[Sysname] acl basic 2001  
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0  
[Sysname-acl-ipv4-basic-2001] quit  
[Sysname] telnet server acl 2001
```

1.1.50 telnet server acl-deny-log enable

telnet server acl-deny-log enable 命令用来开启匹配 ACL deny 规则后打印日志信息功能。

undo telnet server acl-deny-log enable 命令用来关闭匹配 ACL deny 规则后打印日志信息功能。

【命令】

```
telnet server acl-deny-log enable
undo telnet server acl-deny-log enable
```

【缺省情况】

匹配 ACL deny 规则后打印日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

通过配置 **telnet server acl** 或 **telnet server ipv6 acl** 命令，可限制 Telnet 客户端对设备的访问。此时，可通过开启 Telnet 客户端匹配 ACL deny 规则后打印日志信息功能，记录访问 Telnet 服务器受限的 Telnet 客户端信息。

执行本配置后，Telnet 客户端匹配 ACL deny 规则时，将产生日志信息。生成的日志信息将被发送到设备的信息中心，通过设置信息中心的参数，决定日志信息的输出规则（即是否允许输出以及输出方向）。

【举例】

开启 Telnet 客户端匹配 ACL deny 规则后打印日志信息功能。

```
<Sysname> system-view
[Sysname] telnet server acl-deny-log enable
```

【相关命令】

- **telnet server acl**
- **telnet server ipv6 acl**

1.1.51 telnet server dscp

telnet server dscp 命令用来配置 Telnet 服务器发送 Telnet 报文的 DSCP 优先级。

undo telnet server dscp 命令用来恢复缺省情况。

【命令】

```
telnet server dscp dscp-value
undo telnet server dscp
```

【缺省情况】

Telnet 服务器发送 Telnet 报文的 DSCP 优先级为 48。

【视图】

系统视图

【缺省用户角色】

```
network-admin
```

context-admin

【参数】

dscp-value: Telnet 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 Telnet 服务器发送报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] telnet server dscp 30
```

1.1.52 telnet server enable

telnet server enable 命令用来开启 Telnet 服务。

undo telnet server enable 命令用来关闭 Telnet 服务。

【命令】

```
telnet server enable
undo telnet server enable
```

【缺省情况】

Telnet 服务处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

只有使能 Telnet 服务后，才允许网络管理员通过 Telnet 协议登录设备。

【举例】

```
# 使能 Telnet 服务。
<Sysname> system-view
[Sysname] telnet server enable
```

1.1.53 telnet server ipv6 acl

telnet server ipv6 acl 命令用来使用 ACL 限制哪些 IPv6 Telnet 客户端可以访问设备。

undo telnet server ipv6 acl 命令用来恢复缺省情况。

【命令】

```
telnet server ipv6 acl { ipv6 | mac } acl-number
undo telnet server ipv6 acl
```

【缺省情况】

未使用 ACL 限制 Telnet 客户端。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6: 指定 IPv6 ACL。

mac: 指定二层 ACL。

acl-number: ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999: 需指定 **ipv6** 关键字，表示 IPv6 基本 ACL。
- 3000～3999: 需指定 **ipv6** 关键字，表示 IPv6 高级 ACL。
- 4000～4999: 需指定 **mac** 关键字，表示二层 ACL。

【使用指导】

配置 ACL 限制 IPv6 Telnet 客户端时：

- 当未引用 ACL 时，允许所有登录用户访问设备；
- 当引用的 ACL 不存在、或者引用的 ACL 为空时，禁止所有登录用户访问设备；
- 当引用的 ACL 非空时，则只有 ACL 中 **permit** 的用户才能访问设备，其他用户不允许访问设备，以免非法用户使用 Telnet 访问设备。
- 如果多次使用该命令配置 Telnet 服务与 ACL 关联，最新配置生效。

关于 ACL 的详细描述和介绍请参见“ACL 配置指导”中的“ACL”。

该配置只过滤新建立的 Telnet 连接，不会对已建立的 Telnet 连接和操作造成影响。

【举例】

仅允许地址为 2000::1 的用户通过 Telnet 访问本设备。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl6-ipv6-basic-2001] rule permit source 2000::1 128
[Sysname-acl6-ipv6-basic-2001] quit
[Sysname] telnet server ipv6 acl ipv6 2001
```

1.1.54 telnet server ipv6 dscp

telnet server ipv6 dscp 命令用来配置 IPv6 Telnet 服务器发送报文的 DSCP 优先级。

undo telnet server ipv6 dscp 命令用来恢复缺省情况。

【命令】

```
telnet server ipv6 dscp dscp-value
undo telnet server ipv6 dscp
```

【缺省情况】

IPv6 Telnet 服务器发送 IPv6 Telnet 报文的 DSCP 优先级为 48。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value: IPv6 Telnet 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 IPv6 Telnet 服务器发送的报文的 DSCP 优先级为 30。

```
<Sysname> system-view
```

```
[Sysname] telnet server ipv6 dscp 30
```

1.1.55 telnet server ipv6 port

telnet server ipv6 port 命令用来配置 IPv6 网络 Telnet 协议的端口号。

undo telnet server ipv6 port 命令用来恢复缺省情况。

【命令】

telnet server ipv6 port *port-number*

undo telnet server ipv6 port

【缺省情况】

IPv6 网络 Telnet 协议的端口号为 23。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

port-number: IPv6 网络 Telnet 协议端口号，取值范围为 23 或 1025~65535。

【使用指导】

配置 IPv6 网络 Telnet 协议的端口号后，当前所有与 Telnet 服务器的 IPv6 网络 Telnet 连接将被断开，此时需要重新建立 Telnet 连接。

【举例】

```
# 配置 IPv6 网络 Telnet 协议的端口号为 1026。  
<Sysname> system-view  
[Sysname] telnet server ipv6 port 1026
```

1.1.56 telnet server port

telnet server port 命令用来配置 IPv4 网络 Telnet 协议的端口号。
undo telnet server port 命令用来恢复缺省情况。

【命令】

```
telnet server port port-number  
undo telnet server port
```

【缺省情况】

IPv4 网络 Telnet 协议的端口号为 23。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

port-number: IPv4 网络 Telnet 协议的端口号，取值范围为 23 或 1025～65535。

【使用指导】

配置 IPv4 网络 Telnet 协议的端口号后，当前所有与 Telnet 服务器的 IPv4 网络 Telnet 连接将被断开，此时需要重新建立 Telnet 连接。

【举例】

```
# 配置 IPv4 网络 Telnet 协议的端口号为 1025。  
<Sysname> system-view  
[Sysname] telnet server port 1025
```

1.1.57 terminal type

terminal type 命令用来设置当前用户线下的终端显示类型。
undo terminal type 命令用来恢复缺省情况。

【命令】

```
terminal type { ansi | vt100 }  
undo terminal type
```

【缺省情况】

终端显示类型为 ANSI。

【视图】

用户线视图
用户线类视图

【缺省用户角色】

network-admin
context-admin

【参数】

ansi: 终端显示类型为 ANSI 类型。
vt100: 终端显示类型为 VT100 类型。

【使用指导】

设备支持 ANSI 和 VT100 两种终端显示类型。当设备的终端类型与客户端（如超级终端或者 Telnet 客户端等）的终端类型不一致，或者均设置为 ANSI 时，并且当前编辑行的总字符数超过 80 个字符时，客户端会出现光标错位、终端屏幕不能正常显示的现象。建议两端都设置为 VT100 类型。

当用户线视图下的配置为缺省值时，将采用用户线类视图下配置的值；如果用户线类视图下的属性配置也为缺省值时，则采用该用户线下配置的缺省值。

用户线视图/用户线类视图下配置的终端显示类型都在下次登录时生效。

【举例】

```
# 设置终端显示类型为 VT100 类型。  
<Sysname> system-view  
[Sysname] line vty 0  
[Sysname-line-vty0] terminal type vt100
```

1.1.58 user-interface

user-interface 命令用来进入一个或多个用户线视图。

【命令】

```
user-interface { first-number1 [ last-number1 ] | { console | vty }  
first-number2 [ last-number2 ] }
```

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

first-number1: 第一个用户线的编号（绝对编号方式）。
本参数的取值范围与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	取值范围为0~65

型号	说明
T5000-G30	取值范围为0~65
T1000-G20/T1000-G50/T1000-G60/T1000-G80	T1000-G20/T1000-G50/T1000-G60: 取值范围为0~69 T1000-G80: 取值范围为0~67
T1000-CN60/T1000-CN80	取值范围为0~65

last-number1: 最后一个用户线的编号（绝对编号方式），最大取值与 **first-number1** 取值相同，该参数取值必须大于 **first-number1**。

console: Console 用户线。

vty: VTY 用户线。

first-number2: 第一个用户线的编号（相对编号方式），对于 Console 用户线取值范围为 0~1，对于 VTY 用户线取值范围为 0~63。

last-number2: 最后一个用户线的编号（相对编号方式），对于 Console 用户线取值为 1，对于 VTY 用户线取值范围为 1~63，该参数取值必须大于 **first-number2**。

【使用指导】

该命令实现与 **line** 一致，仅为与旧版本兼容保留，请使用 **line**。

进入一个用户线视图进行配置后，该配置只对该用户视图有效。

进入多个用户线视图进行配置后，该配置对这些用户视图均有效。

【举例】

```
# 进入 Console 0 用户线视图。
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-line-console0]
# 进入 VTY 0~4 用户线视图。
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-line-vty0-4]
```

【相关命令】

- **user-interface class**

1.1.59 user-interface class

user-interface class 命令用来进入用户线类视图。

【命令】

```
user-interface class { console | vty }
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

console: Console 用户线类。

vtty: VTY 用户线类。

【使用指导】

该命令实现与 **line class** 一致，仅为与旧版本兼容保留，请使用 **line class**。

用户线视图下的配置只对该用户线生效。

用户线类视图下的配置修改不会立即生效，当用户下次登录后所修改的配置值才会生效。

user-interface class 命令用来进入用户线类视图，**user-interface** 命令用来进入一个或多个用户线视图。对于同时支持这两种视图的命令：

- 用户线视图下的配置优先于用户线类视图下的配置。
- 用户线视图下的属性配置为缺省值时，将采用用户线类视图下配置的值。如果用户线类视图下的属性配置也为缺省值时，则直接采用该属性的缺省值。

用户线类视图下支持的命令有：

- **activation-key**
- **auto-execute command**
- **authentication-mode**
- **command accounting**
- **command authorization**
- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

【举例】

在 VTY 用户线类视图下，将用户连接的超时时间的缺省值设置为 15 分钟。

```
<Sysname> system-view
[Sysname] user-interface class vty
[Sysname-line-class-vty] idle-timeout 15
```

在 Console 用户线类视图下，将终端会话的快捷键设置为<S>。

```
<Sysname> system-view
[Sysname] user-interface class console
[Sysname-line-class-console] activation-key s
[Sysname-line-class-console] quit
```

- 在 Console 用户线视图下，将终端会话的快捷键设置为缺省值（可以使用 **undo activation-key** 或者直接使用 **activation-key 13** 进行配置）。

```
[Sysname] user-interface console 0
```

```
[Sysname-line-console0] undo activation-key
```

- 此时生效的快捷键为用户线类视图下的配置，验证过程如下：

- 退出终端会话。

```
[Sysname-line-console0] return
```

```
<Sysname> quit
```

- 重新登录设备，能看到如下显示信息。

```
Press ENTER to get started.
```

- 此时，<Enter>键失效，需要按<s>键才能出现用户视图提示符，启动终端会话。

```
<Sysname>
```

【相关命令】

- **user-interface**

1.1.60 user-role

user-role 命令用来配置从当前用户线登录系统的用户角色。

undo user-role 命令用来删除用户角色或恢复缺省情况。

【命令】

```
user-role role-name
```

```
undo user-role [role-name ]
```

【缺省情况】

如果用户登录于缺省 Context，通过 Console 口登录系统的缺省用户角色为 **network-admin**，通过其他方式登录系统的用户角色为 **network-operator**；如果用户登录于非缺省 Context，则缺省用户角色均为 **context-operator**。

【视图】

用户线视图

用户线类视图

【缺省用户角色】

network-admin

context-admin

【参数】

role-name：用户角色名称，为 1~63 个字符的字符串，区分大小写。可以是系统预定义的角色名称，包括 **network-admin**、**network-operator**、**context-admin**、**context-operator**、**level-0**~**level-15**，也可以是自定义的用户角色名称。不指定该参数时，表示恢复到缺省情况。系统预定义角色 **security-audit** 和 **guest-manager** 不支持在用户线/用户线类视图下进行配置。

【使用指导】

在用户线视图/用户线类视图下使用该命令设置的用户角色将在下次登录设备时生效。

当用户线视图下的属性配置为缺省值时，将采用该用户线类视图下配置的用户角色。如果用户线类视图下配置的用户角色也为缺省值时，则直接采用该用户线下的缺省值。

仅具有 **network-admin**、**context-admin** 或者 **level-15** 用户角色的用户可以执行该命令。其他角色的用户，即使授权了该命令的操作权限，也不能执行该命令。

可通过多次执行本命令，配置多个用户角色，最多可配置 **64** 个。用户登录后具有的权限是这些角色权限的集合。

关于用户角色的详细介绍请参见“基础配置指导”中的“RBAC”。

【举例】

设置从 VTY 用户线登录系统的用户角色为 **network-admin**。

```
<Sysname> system-view
[Sysname] line vty 0 63
[Sysname-line-vty0-63] user-role network-admin
```

1.1.61 web captcha

web captcha 命令用来配置用户访问 Web 的固定校验码。

undo web captcha 命令用来恢复缺省情况。

【命令】

```
web captcha verification-code
undo web captcha
```

【缺省情况】

用户只能使用 Web 页面显示的校验码访问 Web。

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

verification-code: 访问 Web 的固定校验码，为 4 个字符的字符串，区分大小写。

【使用指导】

配置该命令后，不管 Web 登录页面显示的校验码是什么，用户只要输入该固定的校验码，即可访问设备。本命令主要用于测试环境，当需要对设备的 Web 功能进行测试时，可以配置一个固定的校验码，使用脚本即可登录设备，以免每次测试都要手工输入变化的校验码，影响测试效率。

设备在网络中正常使用的时候，建议不要配置该命令，以免降低 Web 访问的安全性。

多次配置该命令，最新配置生效。

该命令不能保存到配置文件，设备重启后失效。

【举例】

设置访问 Web 的固定校验码为 **test**。

```
<Sysname> web captcha test
```

1.1.62 web https-authorization mode

web https-authorization mode 命令用来设置使用 HTTPS 登录设备时的方式。

undo web https-authorization mode 命令用来恢复缺省情况。

【命令】

web https-authorization mode { manual | certificate | certificate-manual }

undo web https-authorization mode

【缺省情况】

使用 HTTPS 登录设备时的方式为 **manual**。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

manual: 表示用户只能使用用户名和密码登录方式。

certificate: 表示用户只能使用数字证书登录方式。

certificate-manual: 表示用户必须使用用户名和密码登录方式，但是登录时会使用数字证书重新建立 HTTPS 连接。

【使用指导】

使用数字证书登录前，需要：

- 为 HTTPS 服务绑定 SSL 服务器端策略，并在策略中开启基于数字证书的身份验证功能。
- 配置 **web https-authorization username** 命令，并在本地创建同名的本地用户。
- 在建立 HTTPS 连接时，选择正确的数字证书。

【举例】

设置使用 HTTPS 登录设备时的方式为 **certificate**。

```
<Sysname> system-view
```

```
[Sysname] web https-authorization mode certificate
```

【相关命令】

- **web https-authorization username**

1.1.63 web https-authorization username

web https-authorization username 命令用来配置通过数字证书登录设备时使用的用户名。

undo web https-authorization username 命令用来恢复缺省情况。

【命令】

web https-authorization username { cn | email-prefix | oid oid-value }

undo web https-authorization username

【缺省情况】

使用数字证书中的 CN（Common Name，公用名称）字段，作为通过数字证书登录设备时使用的用户名。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

cn: 指定数字证书中的 CN 字段，作为通过数字证书登录设备时使用的用户名。

email-prefix: 指定数字证书中 emailAddress 字段 “@” 字符前的字符串，作为通过数字证书登录设备时使用的用户名。

oid oid-value: 指定数字证书中对象标识符 *oid-value* 对应的字段，作为通过数字证书登录设备时使用的用户名。对象标示符是以点分十进制形式表示的字符串，长度范围为 1~255。

【使用指导】

以下两种情况下，需要使用本命令指定的用户名进行登录：

- 设置通过 HTTPS 登录设备的方式为 **certificate**。
- 设置通过 HTTPS 登录设备的方式为 **auto**，且是使用数字证书登录方式。

【举例】

指定数字证书中对象标识符 1.2.840.113549.1.9.1 对应的字段，作为通过数字证书登录设备时使用的用户名。

```
<Sysname> system-view
```

```
[Sysname] web https-authorization username oid 1.2.840.113549.1.9.1
```

【相关命令】

- **web https-authorization mode**

1.1.64 web idle-timeout

web idle-timeout 命令用来设置 Web 闲置超时时间。

undo web idle-timeout 命令用来恢复缺省情况。

【命令】

web idle-timeout idle-time

undo web idle-timeout

【缺省情况】

Web 闲置超时时间为 10 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

idle-time: Web 闲置超时时间，取值范围为 1~999，单位为分钟。

【使用指导】

当某 Web 用户在 *idle-time* 内一直没有操作 Web 页面，包括点击鼠标或键盘操作（只是移动鼠标，不会延长用户的下线时间），则系统会强制断开该用户的 Web 链接，使该用户下线。从而尽量避免在用户离开登录终端期间，非法用户对设备进行配置。

需要注意的是，修改 Web 线的闲置超时时间，会影响正在访问的用户。

【举例】

设置 Web 闲置超时时间为 100 分钟。

```
<Sysname> system-view  
[Sysname] web idle-timeout 100
```

1.1.65 webui log enable

webui log enable 命令用来开启 Web 操作日志功能。

undo webui log enable 命令用来关闭 Web 操作日志功能。

【命令】

webui log enable
undo webui log enable

【缺省情况】

设备采用出厂配置启动时，Web 操作日志功能处于开启状态。

设备采用空配置启动时，Web 操作日志功能处于关闭状态。

关于空配置和出厂配置的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

开启 Web 操作日志功能，比较关键的 Web 操作（比如修改系统时间）会产生对应的 Web 操作日志，输出到信息中心。通过设置信息中心的参数，最终决定 Web 操作日志的输出规则（即是否允许输出以及输出方向）

Web 操作日志，采用固定的模块名“WEB”；日志助记符有统一的前缀“WEBOPT_”；同时 Web 操作日志还包含 Web 用户信息：Web 客户端 IP 地址和 Web 用户名。

【举例】

开启 Web 操作日志功能，Web 用户执行修改系统时间的操作。

```
<Sysname> system-view
```

```
[Sysname] webui log enable
```

当 Web 用户执行修改系统时间的操作时，设备上将输出如下日志：

```
%Mar 25 14:32:38:802 2013 UNIS WEB/6/WEBOPT_SET_TIME: -HostIP=192.168.100.235-User=Admin;  
Set the system date and time to 2013-05-27T10:00:00.
```

目 录

1 FTP	1-1
1.1 FTP服务器配置命令	1-1
1.1.1 display ftp-server	1-1
1.1.2 display ftp-user	1-1
1.1.3 free ftp user	1-2
1.1.4 free ftp user-ip	1-3
1.1.5 free ftp user-ip ipv6	1-3
1.1.6 ftp server acl	1-4
1.1.7 ftp server acl ipv6	1-5
1.1.8 ftp server acl-deny-log enable	1-6
1.1.9 ftp server dscp	1-7
1.1.10 ftp server enable	1-7
1.1.11 ftp server ipv6 dscp	1-8
1.1.12 ftp server ssl-server-policy	1-8
1.1.13 ftp timeout	1-9
1.2 FTP客户端配置命令	1-10
1.2.1 ?	1-10
1.2.2 append	1-11
1.2.3 ascii	1-11
1.2.4 binary	1-12
1.2.5 bye	1-13
1.2.6 cd	1-13
1.2.7 cdup	1-14
1.2.8 close	1-15
1.2.9 debug	1-15
1.2.10 delete	1-16
1.2.11 dir	1-16
1.2.12 disconnect	1-18
1.2.13 display ftp client source	1-18
1.2.14 ftp	1-19
1.2.15 ftp client ipv6 source	1-20
1.2.16 ftp client source	1-21
1.2.17 ftp ipv6	1-21

1.2.18 get	1-23
1.2.19 help	1-24
1.2.20 lcd	1-24
1.2.21 ls	1-25
1.2.22 mkdir	1-26
1.2.23 newer	1-27
1.2.24 open	1-27
1.2.25 passive	1-28
1.2.26 put	1-29
1.2.27 pwd	1-30
1.2.28 quit	1-30
1.2.29 reget	1-31
1.2.30 rename	1-32
1.2.31 reset	1-32
1.2.32 restart	1-33
1.2.33 rhelp	1-33
1.2.34 rmdir	1-35
1.2.35 rstatus	1-36
1.2.36 status	1-38
1.2.37 system	1-39
1.2.38 user	1-40
1.2.39 verbose	1-40

2 TFTP 2-1

2.1 TFTP服务器配置命令	2-1
2.1.1 tftp server enable	2-1
2.1.2 tftp server work-directory	2-1
2.2 TFTP客户端配置命令	2-2
2.2.1 tftp	2-2
2.2.2 tftp client ipv6 source	2-4
2.2.3 tftp client source	2-5
2.2.4 tftp ipv6	2-6
2.2.5 tftp-server acl	2-7
2.2.6 tftp-server ipv6 acl	2-8

1 FTP

1.1 FTP服务器配置命令

1.1.1 display ftp-server

display ftp-server 命令用来显示设备作为 FTP 服务器时的配置和运行情况。

【命令】

display ftp-server

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 FTP 服务器的配置和运行情况。

```
<Sysname> display ftp-server
```

```
FTP server is running.
```

```
User count: 1
```

```
Idle-timeout timer (in minutes): 30
```

表1-1 display ftp-server 命令显示信息描述表

字段	描述
FTP server is running	FTP服务器功能正在运行中
User count	当前登录的用户数
Idle-timeout timer (in minutes)	FTP连接自动断开前的空闲时间，如果在该时间段内，FTP客户端和FTP服务器之间没有报文交互，该FTP连接会被断开

【相关命令】

- **ftp server enable**
- **ftp timeout**

1.1.2 display ftp-user

display ftp-user 命令用来显示 FTP 用户的详细情况。

【命令】

display ftp-user

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 FTP 用户详细情况。

```
<Sysname> display ftp-user
UserName      HostIP          Port    HomeDir
root          192.168.20.184  46539   flash:

当登录用户名长度超过 10 位时，将换行并靠左对齐显示；当登录用户的 IP 地址长度超过 15 位时，
将换行并靠左对齐显示；当用户根路径长度超过 37 位时，将换行并靠左对齐显示。形如：

<Sysname> display ftp-user
UserName      HostIP          Port    HomeDir
user2         2000:2000:2000: 1499     flash:/user2
              2000:2000:2000:
              2000:2000
administra    100.100.100.100 10001    flash:/123456789/123456789/123456789/
tor                                                    123456789/123456789/123456789/1234567
                                                    89/123456789
```

表1-2 display ftp-user 命令显示信息描述表

字段	描述
UserName	当前登录的FTP用户名
HostIP	当前登录的FTP用户的IP地址
Port	当前登录的FTP用户使用的端口号
HomeDir	当前登录的FTP用户的授权路径

1.1.3 free ftp user

free ftp user 命令用来强制释放通过用户名建立的 FTP 连接。

【命令】

free ftp user username

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

username: 用户名。可以使用 **display ftp-user** 命令来查看当前 FTP 用户的信息。

【举例】

```
# 强制释放通过用户名 ftpuser 建立的 FTP 连接。
<Sysname> free ftp user ftpuser
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

1.1.4 free ftp user-ip

free ftp user-ip 命令用来强制释放通过 IPv4 地址建立的 FTP 连接。

【命令】

free ftp user-ip *ip-address* [**port** *port*]

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: 待释放的 FTP 连接的源 IP。可以使用 **display ftp-user** 命令来查看当前 FTP 连接的源 IP。

port port: 待释放的 FTP 连接的源端口, *port* 为源端口的端口号。可以使用 **display ftp-user** 命令来查看当前 FTP 连接的源端口。

【举例】

```
# 强制释放通过 IP 地址 192.168.20.184 建立的 FTP 连接。
<Sysname> free ftp user-ip 192.168.20.184
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

1.1.5 free ftp user-ip ipv6

free ftp user-ip 命令用来强制释放通过 IPv6 地址建立的 FTP 连接。

【命令】

free ftp user-ip ipv6 *ipv6-address* [**port** *port*]

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address: 待释放的 FTP 连接的源 IP。可以使用 **display ftp-user** 命令来查看当前 FTP 连接的源 IP。

port port: 待释放的 FTP 连接的源端口, *port* 为源端口的端口号。可以使用 **display ftp-user** 命令来查看当前 FTP 连接的源端口。

【举例】

强制释放通过 IP 地址 2000::154 建立的 FTP 连接。

```
<Sysname> free ftp user-ip ipv6 2000::154  
Are you sure to free FTP connection? [Y/N]:y  
<Sysname>
```

1.1.6 ftp server acl

ftp server acl 命令用来设置 IPv4 FTP 客户端对 FTP 服务器的访问限制。

undo ftp server acl 命令用来恢复缺省情况。

【命令】

```
ftp server acl { advanced-acl-number | basic-acl-number | mac  
mac-acl-number }  
undo ftp server acl
```

【缺省情况】

IPv4 FTP 客户端对 FTP 服务器的访问不受限制。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

advanced-acl-number: 指定 IPv4 高级 ACL，取值范围为 3000~3999。

basic-acl-number: 指定 IPv4 基本 ACL，取值范围为 2000~2999。

mac mac-acl-number: 指定二层 ACL。*mac-acl-number* 是二层 ACL 的编号，取值为 4000~4999。

【使用指导】

配置 ACL 限制 IPv4 FTP 客户端时：

- 当未引用 ACL 时，允许所有 IPv4 FTP 客户端访问设备；
- 当引用的 ACL 不存在或者为空时，禁止所有 IPv4 FTP 客户端访问设备；
- 当引用的 ACL 非空时，则只有 ACL 中 **permit** 的用户才能访问设备，禁止其他用户访问设备，以避免非法用户访问设备；

- 如果多次使用该命令配置 FTP 服务与 ACL 关联，最新配置生效。
- 关于 ACL 的详细描述和介绍请参见“ACL 配置指导”中的“ACL”。
- 该配置只过滤新建立的 FTP 连接，不会对已建立的 FTP 连接和操作造成影响。

【举例】

```
# 配置 FTP 服务与 ACL 关联，只允许 IPv4 FTP 客户端（1.1.1.1）通过 FTP 访问本设备。
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule 0 permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] rule 1 deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ftp server acl 2001
```

1.1.7 ftp server acl ipv6

ftp server acl ipv6 命令用来设置 IPv6 FTP 客户端对 FTP 服务器的访问限制。

undo ftp server acl ipv6 命令用来恢复缺省情况。

【命令】

```
ftp server acl ipv6 { advanced-acl-number | basic-acl-number | mac
mac-acl-number }
undo ftp server acl ipv6
```

【缺省情况】

IPv6 FTP 客户端对 FTP 服务器的访问不受限制。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

advanced-acl-number: 指定 IPv6 高级 ACL，取值范围为 3000～3999。

basic-acl-number: 指定 IPv6 基本 ACL，取值范围为 2000～2999。

mac *mac-acl-number*: 指定二层 ACL。*mac-acl-number* 是二层 ACL 的编号，取值为 4000～4999。

【使用指导】

配置 ACL 限制 IPv6 FTP 客户端时：

- 当未引用 ACL 时，允许所有 IPv6 FTP 客户端访问设备；
- 当引用的 ACL 不存在或者为空时，禁止所有 IPv6 FTP 客户端访问设备；
- 当引用的 ACL 非空时，则只有 ACL 中 permit 的用户才能访问设备，禁止其他用户访问设备，以避免非法用户访问设备；
- 如果多次使用该命令配置 FTP 服务与 ACL 关联，最新配置生效。

关于 ACL 的详细描述和介绍请参见“ACL 配置指导”中的“ACL”。

该配置只过滤新建立的 FTP 连接，不会对已建立的 FTP 连接和操作造成影响。

【举例】

配置 FTP 服务与 ACL 关联，只允许 IPv6 FTP 客户端（1:1::1:1/64）通过 FTP 访问本设备。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule 0 permit source 1:1::1:1 64
[Sysname-acl-ipv6-basic-2001] rule 1 deny source any
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] ftp server acl ipv6 2001
```

1.1.8 ftp server acl-deny-log enable

ftp server acl-deny-log enable 命令用来开启匹配 ACL deny 规则后打印日志信息功能。

undo ftp server acl-deny-log enable 命令用来关闭匹配 ACL deny 规则后打印日志信息功能。

【命令】

```
ftp server acl-deny-log enable
undo ftp server acl-deny-log enable
```

【缺省情况】

FTP 客户端匹配 ACL deny 规则后打印日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

通过配置 **ftp server acl** 或 **ftp server acl ipv6** 命令，可限制 FTP 客户端对设备的访问。此时，可通过开启 FTP 客户端匹配 ACL deny 规则后打印日志信息功能，记录访问 FTP 服务器受限的 FTP 客户端信息。

执行本命令后，FTP 客户端匹配 ACL deny 规则时，将产生日志信息。生成的日志信息将被发送到设备的信息中心，通过设置信息中心的参数，决定日志信息的输出规则（即是否允许输出以及输出方向）。

【举例】

开启匹配 ACL deny 规则后打印日志信息功能。

```
<Sysname> system-view
[Sysname] ftp server acl-deny-log enable
```

【相关命令】

- **ftp server acl**
- **ftp server acl ipv6**

1.1.9 ftp server dscp

ftp server dscp 命令用来配置 FTP 服务器发送的 FTP 报文的 DSCP 优先级。

undo ftp server dscp 命令用来恢复缺省情况。

【命令】

ftp server dscp *dscp-value*

undo ftp server dscp

【缺省情况】

FTP 服务器发送的 FTP 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value: 指定设备发送的 FTP 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 FTP 服务器发送的 FTP 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
```

```
[Sysname] ftp server dscp 30
```

1.1.10 ftp server enable

ftp server enable 命令用来开启设备的 FTP 服务器功能，允许 FTP 用户登录。

undo ftp server enable 命令用来关闭设备的 FTP 服务器功能。

【命令】

ftp server enable

undo ftp server enable

【缺省情况】

FTP 服务器功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【举例】

```
# 开启设备的 FTP 服务器功能。
<Sysname> system-view
[Sysname] ftp server enable
```

1.1.11 ftp server ipv6 dscp

ftp server ipv6 dscp 命令用来配置 FTP 服务器发送的 IPv6 FTP 报文的 DSCP 优先级。
undo ftp server ipv6 dscp 命令用来恢复缺省情况。

【命令】

```
ftp server ipv6 dscp dscp-value
undo ftp server ipv6 dscp
```

【缺省情况】

FTP 服务器发送的 IPv6 FTP 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

dscp-value: 指定设备发送的 IPv6 FTP 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

```
# 配置 FTP 服务器发送的 IPv6 FTP 报文的 DSCP 优先级为 30。
<Sysname> system-view
[Sysname] ftp server ipv6 dscp 30
```

1.1.12 ftp server ssl-server-policy

ftp server ssl-server-policy 命令用来配置 FTP 服务与 SSL 服务器端策略关联。
undo ftp server ssl-server-policy 命令用来恢复缺省情况。

【命令】

```
ftp server ssl-server-policy policy-name
undo ftp server ssl-server-policy
```

【缺省情况】

未配置 SSL 服务器端策略与 FTP 服务关联。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: SSL 服务器端策略名，为 1~31 个字符的字符串。

【使用指导】

当支持 FTP 安全扩展协议的两台设备建立 FTP 连接时，通过将 FTP 服务与 SSL 服务器端策略关联，可以建立一条安全的 SSL 连接来传输数据，保证 FTP 传输的安全性。

【举例】

设置 FTP 服务使用的 SSL 服务器端策略为 myssl。

```
<Sysname> system-view
```

```
[Sysname] ftp server ssl-server-policy myssl
```

【相关命令】

- **ftp server enable**
- **ssl server-policy**（安全命令参考/SSL）

1.1.13 ftp timeout

ftp timeout 命令用来设置 FTP 连接自动断开前的空闲时间。

undo ftp timeout 命令用来恢复缺省情况。

【命令】

ftp timeout *minute*

undo ftp timeout

【缺省情况】

FTP 连接自动断开前的空闲时间为 30 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

minute: FTP 连接自动断开前的空闲时间，取值范围为 1~35791，单位为分钟。

【使用指导】

如果在设置的连接空闲时间到期时，FTP 服务器和客户端一直没有信息交互，FTP 服务器将认为该连接已失效并断开该连接，从而避免系统资源被持续占用、其它 FTP 用户的登录受影响。

【举例】

```
# 设置 FTP 连接自动断开前的空闲时间为 36 分钟。
<Sysname> system-view
[Sysname] ftp timeout 36
```

1.2 FTP客户端配置命令



说明

- 为避免重复，在本节中对需要在FTP客户端视图下执行的命令进行举例时，将省略进入FTP客户端视图的配置过程。进入FTP客户端视图的命令请参考“[1.2.14](#)”。
- 在执行 FTP 客户端配置命令前，请确认在 FTP 服务器上是否为用户配置了相应的权限，例如：查询工作目录下的文件列表、读取/下载文件、创建目录/上传文件、以及对服务器上的文件进行重命名/删除等。
- 本节描述的是设备支持的 FTP 客户端配置命令，但命令能否执行成功，与服务器是否支持这些操作有关。
- 本节举例中各命令的显示信息与 FTP 服务器的类型有关，请以实际情况为准。

1.2.1 ?

?命令用来显示所有 FTP 客户端支持命令的名字。

? *command-name* 命令用来显示指定命令的帮助信息。

【命令】

? [*command-name*]

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

command-name：命令名。

【使用指导】

在 FTP 客户端视图下，?命令等同于 help 命令。

【举例】

显示 FTP 客户端支持的所有命令的名字。

```
ftp> ?
```

Commands may be abbreviated. Commands are:

append	delete	ls	quit	rmdir

ascii	debug	mkdir	reget	status
binary	dir	newer	rstatus	system
bye	disconnect	open	rhel	user
cd	get	passive	rename	verbose
cdup	help	put	reset	?
close	lcd	pwd	restart	

查看 **dir** 命令的帮助信息

```
ftp> ? dir
```

```
dir                list contents of remote directory
```

【相关命令】

- **help**

1.2.2 append

append 命令用来在原文件内容的后面添加新文件的内容。

【命令】

```
append localfile [ remotefile ]
```

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

localfile: 待添加的本地文件名称。

remotefile: 被添加的 FTP 服务器文件名称。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

【举例】

将本地 a.txt 文件内容添加到 FTP 服务器上的 b.txt 文件内容的后面。

```
ftp> append a.txt b.txt
```

```
local: a.txt remote: b.txt
```

```
150 Connecting to port 50190
```

```
226 File successfully transferred
```

```
1657 bytes sent in 0.000736 seconds (2.15 Mbyte/s)
```

1.2.3 ascii

ascii 命令用来设置文件传输的模式为 ASCII 模式。

【命令】

```
ascii
```

【缺省情况】

文件传输模式为二进制模式。

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

当设备作为 FTP 服务器时，使用的传输模式由 FTP 客户端决定。当设备作为 FTP 客户端时，使用的传输模式用户可通过命令行修改，缺省为二进制模式。

请使用二进制模式传输非文本文件，用 ASCII 模式传输文本文件。

【举例】

设置数据传输的模式为 ASCII 模式。

```
ftp> ascii
```

```
200 TYPE is now ASCII
```

【相关命令】

- **binary**

1.2.4 binary

binary 命令用来设置文件传输的模式为二进制模式（也称为流模式）。

【命令】

binary

【缺省情况】

文件传输模式为二进制模式。

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

当设备作为 FTP 服务器时，使用的传输模式由 FTP 客户端决定。当设备作为 FTP 客户端时，使用的传输模式用户可通过命令行修改，缺省为二进制模式。

请使用二进制模式传输非文本文件，用 ASCII 模式传输文本文件。

【举例】

```
# 设置文件传输类型为二进制模式。  
ftp> binary  
200 TYPE is now 8-bit binary
```

【相关命令】

- **ascii**

1.2.5 bye

bye 命令用来断开与 FTP 服务器的连接，并退回到用户视图。如果设备与 FTP 服务器没有建立连接，则直接退回到用户视图。

【命令】

bye

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 终止与 FTP 服务器的连接，并退回到用户视图。  
ftp> bye  
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.  
221 Logout.  
<Sysname>
```

【相关命令】

- **quit**

1.2.6 cd

cd 命令用来切换 FTP 服务器上的工作目录，即访问 FTP 服务器上的另一目录。

【命令】

cd { *directory* | .. | / }

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

directory: 指定目标工作目录。如果指定的工作目录不存在，则执行 **cd directory** 后保持当前工作目录不变。

..: 返回上一级目录，功能与 **cdup** 类似。如果当前工作目录已经是 FTP 根目录，则执行 **cd ..** 后保持当前工作目录不变。

/: 返回 FTP 根目录。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

用户可以访问的目录只能是 FTP 服务器对用户授权的目录。

【举例】

切换工作目录到当前工作目录的 **logfile** 子目录下。

```
ftp> cd logfile
```

```
250 OK. Current directory is /logfile
```

切换工作目录到 FTP 根目录的 **folder** 子目录下。

```
ftp> cd /folder
```

```
250 OK. Current directory is /folder
```

切换工作目录到当前工作目录的上层目录下。

```
ftp> cd ..
```

```
250 OK. Current directory is /
```

切换工作目录到 FTP 根目录下。

```
ftp> cd /
```

```
250 OK. Current directory is /
```

【相关命令】

- **cdup**
- **pwd**

1.2.7 cdup

cdup 命令用来退出 FTP 服务器的当前工作目录，并返回到 FTP 服务器的上一级目录。如果当前工作目录已经是 FTP 根目录，则执行该命令后，保持当前工作目录不变。

【命令】

cdup

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

【举例】

```
# 将工作目录改为上一级目录。
ftp> pwd
257 "/ftp/subdir" is your current location
ftp> cdup
250 OK. Current directory is /ftp
ftp> pwd
257 "/ftp" is your current location
```

【相关命令】

- **cd**
- **pwd**

1.2.8 close

close 命令用来在不退出 FTP 客户端视图的前提下，断开与 FTP 服务器的连接。

【命令】

close

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

【举例】

```
# 断开与 FTP 服务器的连接，并保持在 FTP 客户端视图。
ftp> close
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

【相关命令】

- **disconnect**

1.2.9 debug

debug 命令用来切换 FTP 客户端调试信息开关状态。

【命令】

debug

【缺省情况】

FTP 客户端调试信息开关处于关闭状态。

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

重复执行该命令，可以打开或者关闭 FTP 客户端调试信息开关。

【举例】

```
# 切换 FTP 客户端调试信息开关状态。
ftp> debug
Debugging on (debug=1).
ftp> debug
Debugging off (debug=0).
```

1.2.10 delete

delete 命令用来彻底删除 FTP 服务器上的文件。

【命令】

delete *remotefile*

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

remotefile: FTP 服务器上的文件的文件名。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

用户必须具有删除的权限才能执行该操作。

【举例】

```
# 删除文件 b.txt。
ftp> delete b.txt
250 Deleted b.txt
```

1.2.11 dir

dir 命令用来查看 FTP 服务器工作目录下的所有子目录及文件的详细信息。

【命令】

dir [*remotefile* [*localfile*]]

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

remotefile: 待查看的 FTP 服务器上的目录或文件名。

localfile: 用于保存查询信息的本地文件的名称。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

dir remotefile 命令用来查看 FTP 服务器上目录或文件的详细信息。

dir remotefile localfile 命令用来将 FTP 服务器上目录或文件的详细信息保存在本地以 *localfile* 命名的文件中。

在 FTP 客户端视图下，**dir** 命令等同于 **ls** 命令。

【举例】

显示当前 FTP 服务器工作目录下的所有文件夹以及文件的信息。

```
ftp> dir
150 Connecting to port 50201
-rwxr-xr-x   1 0          0                1481 Jul  7 15:36 a.txt
drwxr-xr-x   2 0          0                8192 Jul  2 14:33 diagfile
drwxr-xr-x   3 0          0                8192 Jul  7 15:21 ftp
drwxr-xr-x   2 0          0                8192 Jul  5 09:15 logfile
drwxr-xr-x   2 0          0                8192 Jul  2 14:33 seclog
-rwxr-xr-x   1 0          0            40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x   1 0          0                3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x   1 0          0            54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x   1 0          0                1481 Jul  7 12:34 x.cfg
```

226 9 matches total

将文件 a.txt 的查询结果保存在 s.txt 文件中。

```
ftp> dir a.txt s.txt
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: a.txt
查看 s.txt 文件的内容。
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Sysname> more s.txt
-rwxr-xr-x   1 0          0                1481 Jul  7 12:34 a.txt
```

【相关命令】

- **ls**

1.2.12 disconnect

disconnect 命令用来在不退出 FTP 客户端视图的前提下，断开与 FTP 服务器的连接。

【命令】

disconnect

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

【举例】

```
# 断开与 FTP 服务器的连接，保持在 FTP 客户端视图。  
ftp> disconnect  
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.  
221 Logout.  
ftp>
```

【相关命令】

- **close**

1.2.13 display ftp client source

display ftp client source 命令用来显示设备作为 FTP 客户端时的源地址的配置。

【命令】

display ftp client source

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 显示设备作为 FTP 客户端时的源地址的配置。  
<Sysname> display ftp client source  
The source IP address of the FTP client is 1.1.1.1.
```

1.2.14 ftp

ftp 命令用来登录 FTP 服务器，并进入 FTP 客户端视图。

【命令】

```
ftp [ ftp-server [ service-port ] [ vpn-instance vpn-instance-name ] [ dscp dscp-value | source { interface interface-type interface-number | ip source-ip-address } ] ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

ftp-server: FTP 服务器的主机名或 IP 地址。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

service-port: 远端设备提供 FTP 服务的 TCP 端口号，取值范围为 0~65535，缺省值为 21。

vpn-instance *vpn-instance-name*: 指定 FTP 服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 FTP 服务器位于公网中。

dscp *dscp-value*: 指定设备发送的 FTP 报文中携带的 DSCP 优先级的取值，取值范围为 0~63，缺省值为 0。

source { interface interface-type interface-number | ip source-ip-address }: 指定建立 FTP 连接时使用的源地址。其中：

- **interface interface-type interface-number**: 表示源接口的接口类型和接口编号。发送 FTP 协议报文时，设备将使用该接口下配置的主 IP 地址作为源地址。如果源接口下没有配置主地址，则不能建立连接。
- **ip source-ip-address**: 表示源 IP 地址。发送 FTP 协议报文时，设备将使用该 IP 地址作为源地址。该地址必须是设备上已配置的 IP 地址，否则不能建立连接。

【使用指导】

该命令仅适用于 IPv4 组网环境。

如果不指定任何参数，则只进入 FTP 客户端视图，不登录 FTP 服务器。

如果指定参数，系统会提示用户输入登录 FTP 服务器的用户名和密码。如果用户名和密码正确，则登录成功，并进入 FTP 客户端视图；否则，登录失败。

【举例】

使用 FTP 方式，从当前设备 Sysname 登录到设备 FTP Server (IP 地址为 192.168.0.211)，并且 FTP 发送报文的源 IP 地址为 192.168.0.212。

```
<Sysname> ftp 192.168.0.211 source ip 192.168.0.212
```

```
Press CTRL+C to abort.
```

```
Connected to 192.168.0.211 (192.168.0.211).
```

```
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
```

```
User (192.168.0.211:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

1.2.15 ftp client ipv6 source

ftp client ipv6 source 命令用来在 IPv6 组网环境下配置 FTP 客户端发送的 FTP 报文的源地址。

undo ftp client ipv6 source 命令用来恢复缺省情况。

【命令】

```
ftp client ipv6 source { interface interface-type interface-number | ipv6 source-ipv6-address }
undo ftp client ipv6 source
```

【缺省情况】

未配置源地址，设备自动选择 IPv6 FTP 报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface interface-type interface-number：表示源接口的类型和编号，此接口下配置的 IPv6 地址即为发送报文的源地址。请使用状态为 up 的接口作为源接口，否则，文件传输失败。

ipv6 source-ipv6-address：设置当前 FTP 客户端发送报文所使用的源 IPv6 地址。该地址必须是设备上已经配置的 IPv6 地址，并且地址所在接口状态为 up，否则，文件传输失败。

【使用指导】

多次执行本命令，最新一次执行的命令生效。

使用该命令指定了源地址后，又在 **ftp ipv6** 命令中指定了源地址，则采用 **ftp ipv6** 命令中指定的源地址进行通信。

本命令指定的源地址对所有的 FTP 传输有效，**ftp ipv6** 命令指定的源地址只对当前的 FTP 传输有效。

【举例】

```
# 配置设备发送的 FTP 报文的源 IPv6 地址为 2000::1。
<Sysname> system-view
[Sysname] ftp client ipv6 source ipv6 2000::1
```

【相关命令】

- **ftp ipv6**

1.2.16 ftp client source

ftp client source 命令用来在 IPv4 组网环境下配置 FTP 客户端发送的 FTP 报文的源地址。

undo ftp client source 命令用来恢复缺省情况。

【命令】

```
ftp client source { interface interface-type interface-number | ip
source-ip-address }
undo ftp client source
```

【缺省情况】

未配置源地址，使用路由出接口的主 IP 地址作为设备发送 FTP 报文的源 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface interface-type interface-number: 设置 FTP 传输使用的源接口，包括接口类型和接口编号，此接口下配置的主 IP 地址即为发送报文的源地址。请使用配置了主 IP 地址，并且状态为 up 的接口作为源接口，否则，文件传输失败。

ip source-ip-address: 设置当前 FTP 客户端发送报文所使用的源 IP 地址。该地址必须是设备上已经配置的 IP 地址，并且地址所在接口状态为 up，否则，文件传输失败。

【使用指导】

多次执行本命令，最新一次执行的命令生效。

使用本命令指定了源地址后，又在 **ftp** 命令中指定了源地址，则采用 **ftp** 命令中指定的源地址进行通信。

本命令指定的源地址对所有的 FTP 传输有效，**ftp** 命令指定的源地址只对当前的 FTP 传输有效。

【举例】

配置设备发送 FTP 报文的源 IP 地址为 192.168.20.222。

```
<Sysname> system-view
```

```
[Sysname] ftp client source ip 192.168.20.222
```

【相关命令】

- **ftp**

1.2.17 ftp ipv6

ftp ipv6 命令用来登录 FTP 服务器，并进入 FTP 客户端视图。

【命令】

```
ftp ipv6 [ ftp-server [ service-port ] [ vpn-instance vpn-instance-name ]
[ dscp dscp-value | source { ipv6 source-ipv6-address | interface
```

```
interface-type interface-number } ] * [ -i interface-type  
interface-number ] ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

ftp-server: 远端设备的 IPv6 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

service-port: 远端设备提供 FTP 服务的 TCP 端口号，取值范围为 0~65535，缺省值为 21。

dscp dscp-value: 指定设备发送的 IPv6 FTP 报文中携带的 DSCP 优先级的取值，取值范围为 0~63，缺省值为 0。

source { ipv6 source-ipv6-address | interface interface-type interface-number }: 指定建立 IPv6 FTP 连接时使用的源地址。其中：

- **interface interface-type interface-number**: 当前 FTP 客户端连接所使用的源接口的接口类型和接口编号。此参数主要用于 FTP 服务器的地址是链路本地地址的情况，而且指定的出接口必需具有链路本地地址。（链路本地地址的介绍和配置请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”）。
- **ipv6 source-ipv6-address**: 当前 FTP 客户端连接所使用的源 IPv6 地址。该地址必须是设备上已配置的 IPv6 地址。

vpn-instance vpn-instance-name: 指定目的端所属的 VPN 实例。**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的端位于公网中。

-i interface-type interface-number: 当前 FTP 客户端连接所使用的出接口的接口类型和接口编号。此参数主要用于 FTP 服务器的地址是链路本地地址的情况，而且指定的出接口必需具有链路本地地址。

【使用指导】

该命令仅适用于 IPv6 组网环境。

如果不指定任何参数，则只进入 FTP 客户端视图，不登录 FTP 服务器。

如果指定参数，系统会提示用户输入登录 FTP 服务器的用户名和密码。如果用户名和密码正确，则登录成功，并进入 FTP 客户端视图；否则，登录失败。

【举例】

登录到 IPv6 地址为 2000::154 的 FTP 服务器。

```
<Sysname> ftp ipv6 2000::154  
Press CTRL+C to abort.  
Connected to 2000::154 (2000::154).  
220 FTP service ready.  
User (2000::154): root  
331 Password required for root.
```

```
Password:
230 User logged in
Remote system type is UNIS
```

1.2.18 get

get 命令用来下载 FTP 服务器上的文件，并将下载的文件存储在本地。

【命令】

```
get remotefile [ localfile ]
```

【视图】

FTP 客户端视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

remotefile: 需要下载的文件名称。

localfile: 将文件下载到本地保存时使用的文件名称。当不使用该参数，将使用源文件名称作为本地文件名称保存。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

保存文件时：

- 如果要将文件保存到用户执行 **ftp** 命令时的当前工作目录，*localfile* 只能是文件的名称或者不输入，形如 **a.cfg**。
- 如果要将文件保存到用户执行 **ftp** 命令时的当前工作目录外的其它目录，则 *localfile* 必须是绝对路径形式，形如 **flash:/subdirectory/a.cfg**，否则，命令执行失败。

【举例】

下载 **a.txt** 文件，并以 **b.txt** 文件名保存到用户执行 **ftp** 命令时的当前工作目录。

```
ftp> get a.txt b.txt
local: b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

下载 **a.txt** 文件，并以 **b.txt** 文件名保存到用户执行 **ftp** 命令时的当前工作目录的子文件夹 **test**。

```
ftp> get a.txt flash:/test/b.txt
local: flash:/test/b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

下载 **a.txt** 文件到指定 **slot** 存储介质的根目录下，并以 **c.txt** 文件名保存。

```
ftp> get a.txt slot1#flash:/c.txt
local: slot1#flash:/c.txt remote: a.txt
150 Connecting to port 47460
```

```
226 File successfully transferred
1569 bytes received in 0.0564 seconds (27.2 kbyte/s)
```

【相关命令】

- **put**

1.2.19 help

help 命令用来显示所有 FTP 客户端支持的命令的名字。

help *command-name* 命令用来显示指定命令的帮助信息。

【命令】

help [*command-name*]

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

command-name: 命令名。

【使用指导】

在 FTP 客户端视图下，**help** 命令等同于 **?** 命令。

【举例】

显示所有 FTP 客户端支持的命令的名字。

```
ftp> help
```

Commands may be abbreviated. Commands are:

append	delete	ls	quit	rmdir
ascii	debug	mkdir	reget	status
binary	dir	newer	rstatus	system
bye	disconnect	open	rhel	user
cd	get	passive	rename	verbose
cdup	help	put	reset	?
close	lcd	pwd	restart	

查看 **dir** 命令的帮助信息

```
ftp> help dir
```

dir list contents of remote directory

【相关命令】

- **?**

1.2.20 lcd

lcd 命令用来显示或切换 FTP 客户端本地的工作目录。

【命令】

lcd [*directory* | /]

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

directory: 表示本设备上的目录。该参数用来将 FTP 客户端本地的工作目录切换到指定目录。请注意，存储介质名前面必须带“/”，形如“/flash:/logfile”。

/: 表示本设备的根目录。该参数用来将 FTP 客户端本地的工作目录切换到本设备的根目录。

【使用指导】

执行 **lcd** 命令，不指定任何参数时，用来显示 FTP 客户端本地的工作目录。

【举例】

```
# 显示 FTP 客户端本地的当前工作目录。
ftp> lcd
Local directory now /flash:
# 将 FTP 客户端本地的工作目录切换到 flash:/logfile。
ftp> lcd /flash:/logfile
Local directory now /flash:/logfile
```

1.2.21 ls

ls 命令用来查看 FTP 服务器工作目录下的所有子目录及文件的详细信息。

【命令】

ls [*remotefile* [*localfile*]]

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

remotefile: 待查看的 FTP 服务器上的目录或文件名。

localfile: 用于保存查询信息的本地文件的名称。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

ls remotefile 命令用来查看 FTP 服务器上目录或文件的详细信息。

ls remotefile localfile 命令用来将 FTP 服务器上目录或文件的详细信息保存在本地以 *localfile* 命名的文件中。

在 FTP 客户端视图下，**ls** 命令等同于 **dir** 命令。

【举例】

显示当前 FTP 服务器工作目录下的所有文件夹以及文件的信息。

```
ftp> ls
150 Connecting to port 50201
-rwxr-xr-x    1 0          0          1481 Jul  7 15:36 a.txt
drwxr-xr-x    2 0          0          8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0          0          8192 Jul  7 15:21 ftp
drwxr-xr-x    2 0          0          8192 Jul  5 09:15 logfile
drwxr-xr-x    2 0          0          8192 Jul  2 14:33 seclog
-rwxr-xr-x    1 0          0      40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x    1 0          0        3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x    1 0          0       54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0          0        1481 Jul  7 12:34 x.cfg
226 9 matches total
```

将文件 a.txt 的查询结果保存在 s.txt 文件中。

```
ftp> ls a.txt s.txt
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: a.txt
查看 s.txt 文件的内容。
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Sysname> more s.txt
-rwxr-xr-x    1 0          0          1481 Jul  7 12:34 a.txt
```

【相关命令】

- **dir**

1.2.22 mkdir

mkdir 命令用来在 FTP 服务器上当前工作目录下创建子目录。

【命令】

mkdir directory

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

directory: 待创建的目录名称。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

用户必须具有创建的权限才能执行此项操作。

【举例】

在 FTP 服务器的当前工作目录下创建子目录 newdir。

```
ftp> mkdir newdir
257 "newdir" : The directory was successfully created
```

1.2.23 newer

newer 命令用来更新本地文件。

【命令】

newer *remotefile* [*localfile*]

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

remotefile: 目标文件名称。

localfile: 需要更新的本地文件名称。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

如果本地文件不存在，一律视为目标文件比本地新，即本地文件需要更新。

如果目标文件不比本地文件新，则不更新本地文件。

【举例】

FTP 服务器的文件 a.txt 比本地的要新，更新本地文件。

```
ftp> newer a.txt
local: a.txt remote: a.txt
150 Connecting to port 63513
226 File successfully transferred
1573 bytes received in 0.0293 seconds (52.3 kbyte/s)
```

1.2.24 open

open 命令用来在 FTP 客户端视图下，登录 FTP 服务器。

【命令】

open *server-address* [*service-port*]

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

server-address: FTP 服务器的 IP 地址（IPv4 或 IPv6 地址）或主机名。

service-port: 远端设备提供 FTP 服务的 TCP 端口号，取值范围为 0～65535，缺省值为 21。

【使用指导】

登录时，系统会提示用户输入登录用户名和密码。如果用户名和密码正确，则登录成功；否则，登录失败。

如果已经登录到 FTP 服务器，则不能直接使用 **open** 命令连接到其他 FTP 服务器，需要中断与 FTP 服务器的连接后再重新连接。

【举例】

在 FTP 客户端视图下，登录 FTP 服务器（IP 地址为 192.168.40.7）。

```
<Sysname> ftp
ftp> open 192.168.40.7
Press CTRL+C to abort.
Connected to 192.168.40.7 (192.168.40.7).
220 FTP service ready.
User (192.168.40.7:(none)): root
331 Password required for root.
Password:
230 User logged in.
Remote system type is UNIS.
ftp>
```

1.2.25 passive

passive 命令用来切换 FTP 数据传输的主被动方式。

【命令】

passive

【缺省情况】

数据传输的方式为被动方式。

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

数据传输的方式分为主动方式和被动方式：

- 主动方式是指在建立数据连接时由 **FTP** 服务器主动发起连接请求。
- 被动方式是指在建立数据连接时由 **FTP** 客户端主动发起连接请求。

重复执行该命令，可以将 **FTP** 数据传输方式设置为主动方式或者被动方式。

该命令主要与防火墙功能配合使用，用来限制私网用户和公网用户之间建立 **FTP** 会话。

【举例】

切换数据传输的主被动方式。

```
ftp> passive
Passive mode on.
ftp> passive
Passive mode off.
```

1.2.26 put

put 命令用来将 **FTP** 客户端本地的文件上传到 **FTP** 服务器。

【命令】

put *localfile* [*remotefile*]

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

localfile：待上传的本地文件名称。

remotefile：文件上传完成后，在 **FTP** 服务器上保存时使用的文件名称。如果用户没有指定 **FTP** 服务器上的文件名，则系统缺省认为此文件名与本地文件名相同。

【使用指导】

只有成功登录 **FTP** 服务器后才能执行此项操作。

保存文件时：

- 如果要将用户执行 **ftp** 命令时的当前工作目录下的某文件上传，*localfile* 只能是文件的名称，形如 **a.cfg**。
- 如果要将用户执行 **ftp** 命令时的当前工作目录外的其它文件上传，则 *localfile* 必须是绝对路径形式，形如 **flash:/subdirectory/a.cfg**，否则，命令执行失败。

【举例】

上传用户执行 **ftp** 命令时的当前工作目录下的 **a.txt** 文件，并以 **b.txt** 文件名保存。

```
ftp> put a.txt b.txt
local: a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
```

```
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
# 上传用户执行 ftp 命令时的当前工作目录下子文件夹 test 下的 a.txt 文件, 并以 b.txt 文件名保存。
ftp> put flash:/test/a.txt b.txt
local: flash:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
# 上传指定 slot 存储介质 test 目录下的 a.txt 文件, 并以 b.txt 文件名保存。
ftp> put slot2#flash:/test/a.txt b.txt
local: slot2#flash:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

【相关命令】

- **get**

1.2.27 pwd

pwd 命令用来显示当前用户正在访问的 **FTP** 服务器上的目录。

【命令】

pwd

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

只有成功登录 **FTP** 服务器后才能执行此项操作。

【举例】

```
# 显示当前用户正在访问的 FTP 服务器上的目录。
ftp> cd subdir
250 OK. Current directory is /subdir
ftp> pwd
257 "/subdir" is your current location
```

1.2.28 quit

quit 命令用来断开与 **FTP** 服务器的连接, 并退回到用户视图。

【命令】

quit

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 终止与 FTP 服务器的连接，并退回到用户视图。  
ftp> quit  
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.  
221 Logout.  
<Sysname>
```

【相关命令】

- **bye**

1.2.29 reget

reget 命令用来实现断点续传。

【命令】

reget *remote file* [*local file*]

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

remote file: 目标文件名称。

local file: 内容保存不完整的本地文件名称。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

网络故障或者存储空间不足，可能导致正在进行的下载操作终止，下载的文件内容不完整。当网络故障排除或者存储空间恢复后，可执行 **reget** 命令继续下载文件剩余的内容。

【举例】

```
# 获取因传输中断而不完整的本地文件 s.bin 的剩余内容。  
ftp> reget s.bin  
local: s.bin remote: s.bin  
350 Restarting at 1749706  
150-Connecting to port 47429  
150 38143.3 kbytes to download  
226 File successfully transferred  
39058742 bytes received in 66.2 seconds (576.1 kbyte/s)
```

1.2.30 rename

rename 命令用来重命名文件。

【命令】

```
rename [ oldfilename [ newfilename ] ]
```

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

oldfilename: 原文件名。

newfilename: 新文件名。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

【举例】

将文件 a.txt 改名为 b.txt。

方法一：

```
ftp> rename  
(from-name) a.txt  
(to-name) b.txt  
350 RNFR accepted - file exists, ready for destination  
250 File successfully renamed or moved
```

方法二：

```
ftp> rename a.txt  
(to-name) b.txt  
350 RNFR accepted - file exists, ready for destination  
250 File successfully renamed or moved
```

方法三：

```
ftp> rename a.txt b.txt  
350 RNFR accepted - file exists, ready for destination  
250 File successfully renamed or moved
```

1.2.31 reset

reset 命令用来清除缓存中 FTP 服务器端发送回来的命令应答。

【命令】

```
reset
```

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【举例】

清除缓存中 FTP 服务器端发送回来的命令应答。
ftp> reset

1.2.32 restart

restart 命令用来指定重传点。

【命令】

restart *marker*

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

marker: 重传点，从文件首部开始的偏移量，单位为字节。

【使用指导】

在 FTP 文件传输过程中，如果发生了中断，执行该命令，则设备将从重传点开始重新传输文件。
只有成功登录 FTP 服务器后才能执行此项操作。
不同 FTP 服务器对本命令的支持情况可能不同，请以 FTP 服务器的实际情况为准。

【举例】

```
# 设置重传点的偏移量为 2 字节，将本地文件 h.c（大小 82 字节）上传。
ftp> restart 2
restarting at 2. execute get, put or append to initiate transfer
ftp> put h.c h.c
local: h.c remote: h.c
350 Restart position accepted (2).
150 Ok to send data.
226 File receive OK.
80 bytes sent in 0.000445 seconds (175.6 kbyte/s)
ftp> dir
150 Here comes the directory listing.
-rw-r--r--    1 0          0          82 Jul 18 02:58 h.c
```

1.2.33 rhelp

rhelP 命令用来显示 FTP 服务器支持的 FTP 相关协议命令字。

rhelP protocol-command 命令用来显示 FTP 服务器支持的 FTP 相关协议命令字的帮助信息。

【命令】

`rhel[ protocol-command ]`

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

protocol-command: FTP 协议命令字。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

【举例】

```
# 查看 FTP 服务器支持的 FTP 相关协议命令字。
ftp> rhel
214-The following FTP commands are recognized
USER PASS NOOP QUIT SYST TYPE
HELP CWD XCWD PWD CDUP XCUP
XPWD LIST NLST MLSD PORT EPRT
PASV EPSV REST RETR STOR APPE
DELE MKD XMKD RMD XRMD ABOR
SIZE RNFR RNT0
214 UNIX Type: L8
```

表1-3 rhel 命令显示信息描述表

字段	描述
214-The following FTP commands are recognized	以下是可用的FTP命令字列表
USER	用户名
PASS	用户口令
NOOP	空操作，表示当服务器收到无效命令时，不做任何操作
QUIT	退出
SYST	显示系统参数
TYPE	请求类型
HELP	帮助
CWD	改变当前工作目录
XCWD	扩展命令，含义同CWD
PWD	打印工作路径
CDUP	改变目录到父级目录

字段	描述
XCUP	扩展命令，含义同CDUP
XPWD	扩展命令，含义同PWD
LIST	列出文件
NLST	列出文件简单描述
MLSD	列出文件内容
PORT	主动模式（IPv4）
EPRT	主动模式（IPv6）
PASV	被动模式（IPv4）
EPSV	被动模式（IPv6）
REST	重启动
RETR	下载文件
STOR	上传文件
APPE	追加上传
DELE	删除文件
MKD	创建文件夹
XMKD	扩展命令，含义同MKD
RMD	删除文件夹
XRMD	扩展命令，含义同RMD
ABOR	中断传输
SIZE	获取文件的传输大小
RNFR	需要重命名的文件的原名称
RNTO	需要重命名的文件的新名称

1.2.34 rmdir

rmdir 命令用来彻底删除 FTP 服务器上的目录。

【命令】

rmdir *directory*

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

directory: FTP 服务器上的目录名。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

用户必须具有删除的权限才能执行此项操作。

被删除的目录必须为空目录（即删除目录前，必须先删除该目录下的所有文件及子目录，文件的删除请参见 **delete** 命令）。

成功执行 **rmdir** 命令后，FTP 服务器的回收站中原来属于该文件夹的文件不会被删除。

【举例】

```
# 删除空目录 subdir1。
ftp>rmdir subdir1
250 The directory was successfully removed
```

【相关命令】

- **delete**

1.2.35 rstatus

rstatus 命令用来显示 FTP 服务器的状态。

rstatus *remotefile* 命令用来显示 FTP 服务器上目录或文件的详细信息。

【命令】

rstatus [*remotefile*]

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

remotefile: 待查询的 FTP 服务器上的目录或文件名。

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

不同 FTP 服务器对本命令的支持情况可能不同，请以 FTP 服务器的实际情况为准。

【举例】

```
# 显示 FTP 服务器状态。
ftp> rstatus
211-FTP server status:
    Connected to 192.168.20.177
    Logged in as root
    TYPE: ASCII
    No session bandwidth limit
```



```

Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
At session startup, client count was 1
vsFTPD 2.0.6 - secure, fast, stable
211 End of status

```

表1-4 rstatus 命令显示信息描述表

字段	描述
211-FTP server status:	211: FTP命令字; 整个字段表示FTP服务器状态信息开始
Connected to 192.168.20.177	连接的FTP客户端IP地址: 192.168.20.177
Logged in as root	登入的用户名: root
TYPE: ASCII	文件传输模式: ASCII
No session bandwidth limit	无带宽限制
Session timeout in seconds is 300	超时时间: 300, 单位为秒
Control connection is plain text	控制连接类型: 纯文本
Data connections will be plain text	数据连接类型: 纯文本
At session startup, client count was 1	FTP客户端连接数: 1
vsFTPD 2.0.6 - secure, fast, stable	FTP版本号: 2.0.6; 可靠, 快速, 稳定
211 End of status	FTP服务器状态信息结束

```

# 查看文件 a.txt。
ftp> rstatus a.txt
213-Status follows:
-rw-r--r--    1 0      0          80 Jul 18 02:58 a.txt
213 End of status

```

表1-5 rstatus 命令显示文件信息描述表

字段	描述
213-Status follows:	213: FTP命令字; 整个字段表示文件信息开始

字段	描述
-rw-r--r--	第一位表示文件类型： • -: 普通文件 • b: 块设备文件 • c: 字符设备文件 • d: 目录 • l: 符号连接文件 • p: 命名管道文件 • s: socket 文件 第二位到第十位分为3组，每组3个字符，分别表示所有者、组和其他用户的访问权限： • -: 没有对应权限 • r: 有读权限 • w: 有写权限 • x: 有执行权限
1	表示文件的连接数
0	文件所有者的名字
0	文件所有者的组名
80	文件大小，单位为字节
Jul 18 02:58	文件最近一次修改的日期和时间
a.txt	文件名
213 End of status	文件信息结束

1.2.36 status

status 命令用来显示当前 FTP 状态。

【命令】

status

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【举例】

显示当前 FTP 状态。

```
ftp> status
```

```
Connected to 192.168.1.56.
```

```
No proxy connection.
```

```
Not using any security mechanism.
```

Mode: stream; Type: ascii; Form: non-print; Structure: file
Verbose: on; Bell: off; Prompting: on; Globbing: off
Store unique: off; Receive unique: off
Case: off; CR stripping: on
Ntrans: off
Nmap: off
Hash mark printing: off; Use of PORT cmds: on

表1-6 status 命令显示信息描述表

字段	描述
Connected to 192.168.1.56.	连接到的FTP服务器IP地址
No proxy connection.	不使用代理连接
Not using any security mechanism.	不使用安全机制
Mode: stream; Type: ascii; Form: non-print; Structure: file	文件传输模式：数据流；类型：ASCII；格式：非打印；组织结构：文件
Verbose: on; Bell: off; Prompting: on; Globbing: off	显示调试信息；操作完成后无蜂鸣提示；多文件操作时不需要每个文件进行确认；不能自动匹配文件名
Store unique: off; Receive unique: off	FTP服务器文件名唯一；本地接收文件名唯一
Case: off; CR stripping: on	不支持一次获取多个文件；文本环境下下载文件时，将“\r”删除
Ntrans: off	不使用输入输出传输表
Nmap: off	文件名不使用输入输出映射模板
Hash mark printing: off; Use of PORT cmds: on	不以“#”号结尾；使用“PORT”命令字作为数据传输连接

1.2.37 system

system 命令用来显示 FTP 服务器的系统信息。

【命令】

system

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

只有成功登录 FTP 服务器后才能执行此项操作。

【举例】

显示 FTP 服务器的系统信息。

```
ftp> system
215 UNIX Type: L8
```

1.2.38 user

user 命令用来在现有 FTP 连接上重新发起 FTP 认证。认证成功后，能访问当前的 FTP 服务器。

【命令】

```
user username [ password ]
```

【视图】

FTP 客户端视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

username: 登录用户名。

password: 登录密码。

【使用指导】

该命令通常用于用户登录 FTP 服务器失败，在 FTP 连接超时前，使用该命令重新登录当前访问的 FTP 服务器。

在使用该命令前，必须事先在 FTP 服务器上设置相应的用户名和密码，否则将导致登录失败，FTP 连接关闭。

【举例】

用户登录 FTP 服务器失败，在 FTP 连接超时前，重新登录当前访问的 FTP 服务器。

方法一：

```
ftp> user ftp 123456
331 Password required for ftp.
230 User logged in.
```

方法二：

```
ftp> user ftp
331 Password required for ftp.
Password:
230 User logged in.
```

1.2.39 verbose

verbose 命令用来允许或者禁止显示 FTP 操作过程中的详细信息。

【命令】

```
verbose
```

【缺省情况】

允许显示 FTP 操作过程中的详细信息。

【视图】

FTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

本配置只对当前会话生效。当用户重新登录后，本命令将恢复到缺省情况。

【举例】

禁止显示 FTP 操作过程中的详细信息时，执行 **get** 操作。

```
ftp> verbose
```

```
Verbose mode off.
```

```
ftp> get a.cfg 1.cfg
```

允许显示 FTP 操作过程中的详细信息时，执行 **get** 操作。

```
ftp> verbose
```

```
Verbose mode on.
```

```
ftp> get a.cfg 2.cfg
```

```
227 Entering Passive Mode (192,168,1,58,68,14)
```

```
150-Accepted data connection
```

```
150 The computer is your friend. Trust the computer
```

```
226 File successfully transferred
```

```
3796 bytes received in 0.00762 seconds (486.5 kbyte/s)
```

2 TFTP

2.1 TFTP服务器配置命令

2.1.1 tftp server enable

tftp server enable 命令用来开启设备的 TFTP 服务器功能。

undo tftp server 命令用来关闭设备的 TFTP 服务器功能。

【命令】

```
tftp server enable
undo tftp server enable
```

【缺省情况】

TFTP 服务器功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 开启设备的 TFTP 服务器功能。
<Sysname> system-view
[Sysname] tftp server enable
```

【相关命令】

- **tftp server work-directory**

2.1.2 tftp server work-directory

tftp server work-directory 命令用来配置 TFTP 服务器的工作路径。

undo tftp server work-directory 命令用来恢复缺省情况。

【命令】

```
tftp server work-directory directory
undo tftp server work-directory
```

【缺省情况】

TFTP 服务器的工作路径为缺省文件系统的根目录。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

directory: TFTP 服务器的工作路径，该路径必须是绝对路径。为 1~255 个字符的字符串，不区分大小写，且该目录必须已经存在。

【使用指导】

配置 TFTP 服务器的工作路径后，TFTP 用户登录设备后，可以读、写该路径及其子文件夹下的文件。

【举例】

```
# 配置 TFTP 服务器的工作路径为 flash:/tftp。  
<Sysname> system-view  
[Sysname] tftp server work-directory flash:/tftp
```

【相关命令】

- **tftp server enable**

2.2 TFTP客户端配置命令

2.2.1 tftp

tftp 命令用来在 IPv4 组网环境下执行下列操作：

- 下载文件：将 TFTP 服务器上的源文件下载到本地。
- 上传文件：将本地的源文件上传到 TFTP 服务器。

【命令】

```
tftp tftp-server { get | put | sget } source-filename [ destination-filename ]  
[ vpn-instance vpn-instance-name ] [ dscp dscp-value | source { interface  
interface-type interface-number | ip source-ip-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

tftp-server: TFTP 服务器的 IP 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

get: 执行下载文件操作。执行该操作时，设备直接将文件保存到存储介质中。如果下载前存储介质中已有同名文件，则先删除存储介质中的已有文件，再下载。如果下载失败，将导致已有文件被删除，不可恢复，因此，不安全。

put: 执行上传文件操作。

sget: 执行安全下载文件操作。执行该操作时，设备会先将文件保存到内存，保存成功后，再拷贝到存储介质中，并删除内存中的文件。比 **get** 方式更加安全。

source-filename: 源文件名，为 1~255 个字符的字符串，不区分大小写。

destination-filename: 目标文件名，为 1~255 个字符的字符串，不区分大小写。如果不指定该参数，则使用源文件名作为目标文件名。

vpn-instance vpn-instance-name: 指定 TFTP 服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果不指定该参数，则表示 TFTP 服务器位于公网中。

dscp dscp-value: 指定设备发送的 TFTP 报文中携带的 DSCP 优先级的取值，取值范围为 0~63，缺省值为 0。

source: 发送的 TFTP 报文的源 IP 地址。不指定该参数时，则使用路由出接口的主 IP 地址作为发送的 TFTP 报文的源 IP 地址。

interface interface-type interface-number: 表示源接口的类型和编号，此接口下配置的主 IP 地址将作为设备发送的 TFTP 报文的源 IP 地址。请使用配置了主 IP 地址，并且状态为 up 的接口作为源接口，否则，文件传输失败。

ip source-ip-address: 源 IP 地址，该地址将作为设备发送的 TFTP 报文的源 IP 地址。该地址必须是设备上已经配置的 IP 地址，并且地址所在接口状态为 up，否则，文件传输失败。

【使用指导】

使用 **tftp client source** 命令指定了源地址后，又在 **tftp** 命令中指定了源地址，则采用 **tftp** 命令中指定的源地址进行通信。

tftp client source 命令指定的源地址对所有的 TFTP 传输有效，**tftp** 命令指定的源地址只对当前的 TFTP 传输有效。

【举例】

将 TFTP 服务器上的 new.bin 文件下载到本地存储设备。TFTP 服务器的 IP 地址为 192.168.1.1，下载到本地后以文件名 new.bin 保存。

```
<Sysname> tftp 192.168.1.1 get new.bin
Press CTRL+C to abort.
    % Total      % Received % Xferd  Average Speed   Time    Time       Time   Current
                               Dload  Upload    Total   Spent    Left    Speed
100 13.9M  100 13.9M    0     0 1206k      0  0:00:11  0:00:11  --:--:-- 1206k
Writing file...Done.
<Sysname>
```

表2-1 tftp 命令显示信息描述表

字段	描述
%	文件传输的进度百分比
Total	要传输的文件大小，单位为字节
%	下载时已接收文件大小与文件总大小的百分比
Received	下载时已接收的文件大小，单位为字节
%	上传时已发送文件大小与文件总大小的百分比

字段	描述
Xferd	上传时已发送的文件大小，单位为字节
Average Dload	平均下载速度，单位为字节/秒
Speed Upload	平均上传速度，单位为字节/秒
Time Total	文件传输时已花费时间和剩余时间的总和，单位为秒
Time Spent	文件传输时已花费时间，单位为秒
Time Left	完成文件传输，还需要的时间，单位为秒
Current Speed	文件传输时的当前速度，单位为字节/秒
Writing file	正在将文件保存到存储介质中，成功会显示Done，失败显示Failed。执行get和sget操作时会显示该字段

【相关命令】

- **tftp client source**

2.2.2 tftp client ipv6 source

tftp client ipv6 source 命令用来在 IPv6 组网环境下配置 TFTP 客户端发送的 TFTP 报文的源地址。

undo tftp client ipv6 source 命令用来恢复缺省情况。

【命令】

```
tftp client ipv6 source { interface interface-type interface-number | ipv6
source-ipv6-address }
undo tftp client ipv6 source
```

【缺省情况】

未配置源地址，设备自动选择 IPv6 TFTP 报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface *interface-type interface-number*: 表示源接口的类型和编号，此接口下配置的 IPv6 地址即为发送报文的源地址。请使用状态为 up 的接口作为源接口，否则，文件传输失败。

ipv6 *source-ipv6-address*: 设置当前 TFTP 客户端发送报文所使用的源 IPv6 地址。该地址必须是设备上已经配置的 IPv6 地址，并且地址所在接口状态为 up，否则，文件传输失败。

【使用指导】

多次执行本命令，最新一次执行的命令生效。

使用该命令指定了源地址后，又在 **tftp ipv6** 命令中指定了源地址，则采用 **tftp ipv6** 命令中指定的源地址进行通信。

本命令指定的源地址对所有的 TFTP 传输有效，**tftp ipv6** 命令指定的源地址只对当前的 TFTP 传输有效。

【举例】

配置设备发送的 TFTP 报文的源 IPv6 地址为 2000::1。

```
<Sysname> system-view
```

```
[Sysname] tftp client ipv6 source ipv6 2000::1
```

【相关命令】

- **tftp ipv6**

2.2.3 tftp client source

tftp client source 命令用来在 IPv4 组网环境下配置 TFTP 客户端发送的 TFTP 报文的源地址。

undo tftp client source 命令用来恢复缺省情况。

【命令】

```
tftp client source { interface interface-type interface-number | ip  
source-ip-address }
```

```
undo tftp client source
```

【缺省情况】

未配置源地址，使用路由出接口的主 IP 地址作为设备发送 TFTP 报文的源 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface interface-type interface-number: 设置 TFTP 传输使用的源接口，包括接口类型和接口编号，此接口下配置的主 IP 地址即为发送报文的源地址。请使用配置了主 IP 地址，并且状态为 up 的接口作为源接口，否则，文件传输失败。

ip source-ip-address: 设置当前 TFTP 客户端发送报文所使用的源 IP 地址。该地址必须是设备上已经配置的 IP 地址，并且地址所在接口状态为 up，否则，文件传输失败。

【使用指导】

多次执行本命令，最新一次执行的命令生效。

使用本命令指定了源地址后，又在 **tftp** 命令中指定了源地址，则采用 **tftp** 命令中指定的源地址进行通信。

本命令指定的源地址对所有的 TFTP 传输有效，**tftp** 命令指定的源地址只对当前的 TFTP 传输有效。

【举例】

```
# 配置设备发送 TFTP 报文的源 IP 地址为 192.168.20.222。
<Sysname> system-view
[Sysname] tftp client source ip 192.168.20.222
```

【相关命令】

- **tftp**

2.2.4 tftp ipv6

tftp ipv6 命令用来在 IPv6 组网环境下执行下列操作：

- 下载文件：将 TFTP 服务器上的源文件下载到本地。
- 上传文件：将本地的源文件上传到 TFTP 服务器。

【命令】

```
tftp ipv6 tftp-server [ -i interface-type interface-number ] { get | put | sget } source-filename [ destination-filename ] [ vpn-instance vpn-instance-name ] [ dscp dscp-value | source { interface interface-type interface-number | ipv6 source-ipv6-address } ] *
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

tftp-server：TFTP 服务器的 IPv6 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

-i interface-type interface-number：表示出接口的接口类型和接口编号。如果 TFTP 服务器的地址是链路本地地址的情况，则必须指定出接口且出接口必须具有链路本地地址（链路本地地址的介绍和配置请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”）。

get：执行下载文件操作。执行该操作时，设备直接将文件保存到存储介质中。如果下载前存储介质中已有同名文件，则先删除存储介质中的已有文件，再下载。如果下载失败，将导致已有文件被删除，不可恢复，因此，不安全。

put：执行上传文件操作。

sget：执行安全下载文件操作。执行该操作时，设备会先将文件保存到内存，保存成功后，再拷贝到存储介质中，并删除内存中的文件。比 **get** 方式更加安全。

source-filename：源文件的名称，为 1~255 个字符的字符串，不区分大小写。

destination-filename：目的文件的名称，为 1~255 个字符的字符串，不区分大小写。如果不指定该参数，则目的文件的名称与源文件的名称相同。

vpn-instance vpn-instance-name：指定目的主机所属的 VPN 实例。**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的主机位于公网中。

dscp dscp-value: 指定设备发送的 IPv6 TFTP 报文中携带的 DSCP 优先级的取值, 取值范围为 0~63, 缺省值为 0。

source { interface interface-type interface-number | ipv6 source-ipv6-address }: 发送的 IPv6 TFTP 报文的源地址。不指定该参数时, 设备自动选择报文的源 IPv6 地址, 具体选择原则请参见 RFC 3484。其中:

- **interface interface-type interface-number**: 表示源接口的类型和编号, 此接口下配置的 IPv6 地址将作为设备发送的 TFTP 报文的源 IPv6 地址。请使用状态为 up、且已配置了 IPv6 地址的接口作为源接口, 否则, 文件传输失败。
- **ipv6 source-ipv6-address**: 源 IPv6 地址, 该地址将作为设备发送的 TFTP 报文的源 IPv6 地址。该地址必须是设备上已经配置的 IPv6 地址, 并且地址所在接口状态为 up, 否则, 文件传输失败。

【使用指导】

使用 **tftp client ipv6 source** 命令指定了源地址后, 又在 **tftp ipv6** 命令中指定了源地址, 则采用 **tftp ipv6** 命令中的源地址进行通信。

tftp client ipv6 source 命令指定的源地址对所有的 TFTP 传输有效, **tftp ipv6** 命令指定的源地址只对当前的 TFTP 传输有效。

【举例】

将 TFTP 服务器上的 new.bin 文件下载到本地存储设备。TFTP 服务器的 IPv6 地址为 2001::1, 下载到本地之后以文件名 new.bin 保存。

```
<Sysname> tftp ipv6 2001::1 get new.bin new.bin
```

Press CTRL+C to abort.

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload Upload	Total	Spent	Left	Speed
100 13.9M	100 13.9M	0 0	1206k	0 0:00:11	0:00:11	--:--:--	1206k

Writing file...Done.

本命令显示信息的详细描述请参见 [表 2-1](#)。

2.2.5 tftp-server acl

tftp-server acl 命令用来在 IPv4 组网环境下使用 ACL 限制设备可访问哪些 TFTP 服务器。

undo tftp-server acl 命令用来恢复缺省情况。

【命令】

```
tftp-server acl acl-number
undo tftp-server acl
```

【缺省情况】

未使用 ACL 对设备可访问的 TFTP 服务器进行限制。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

acl-number: 基本访问控制列表的编号，取值范围为 2000～2999。

【使用指导】

用户利用 ACL 中配置的规则可以允许或禁止设备对网络中特定 TFTP 服务器的访问。

【举例】

仅允许设备访问 IP 地址为 1.1.1.1 的 TFTP 服务器。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] tftp-server acl 2000
```

2.2.6 tftp-server ipv6 acl

tftp-server ipv6 acl 命令用来在 IPv6 组网环境下使用 ACL 限制设备可访问哪些 TFTP 服务器。

undo tftp-server ipv6 acl 命令用来恢复缺省情况。

【命令】

```
tftp-server ipv6 acl ipv6-acl-number
undo tftp-server ipv6 acl
```

【缺省情况】

未使用 ACL 对设备可访问的 IPv6 TFTP 服务器进行限制。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-acl-number: 基本访问控制列表的编号，取值范围为 2000～2999。

【使用指导】

用户利用 ACL 中配置的规则可以允许或禁止设备对网络中特定 TFTP 服务器的访问。

【举例】

仅允许设备访问 IP 地址为 2001::1 的 TFTP 服务器。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2001::1/128
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] tftp-server ipv6 acl 2001
```

目 录

1 文件系统管理.....	1-1
1.1 文件系统管理命令.....	1-1
1.1.1 cd.....	1-1
1.1.2 copy	1-2
1.1.3 delete.....	1-4
1.1.4 dir	1-5
1.1.5 fdisk.....	1-6
1.1.6 file prompt.....	1-8
1.1.7 fixdisk	1-9
1.1.8 format	1-10
1.1.9 fuser	1-11
1.1.10 gunzip	1-12
1.1.11 gzip.....	1-12
1.1.12 md5sum.....	1-13
1.1.13 mkdir.....	1-14
1.1.14 more	1-14
1.1.15 mount.....	1-15
1.1.16 move.....	1-16
1.1.17 pwd.....	1-16
1.1.18 rename	1-17
1.1.19 reset recycle-bin	1-17
1.1.20 rmdir	1-18
1.1.21 sha256sum.....	1-19
1.1.22 tar create	1-19
1.1.23 tar extract.....	1-20
1.1.24 tar list	1-21
1.1.25 umount	1-22
1.1.26 undelete.....	1-23

1 文件系统管理

1.1 文件系统管理命令



注意

- 请完全了解文件/文件夹作用后再执行各种文件/文件夹操作，以免误删重要文件/文件夹。
- 文件/文件夹分为隐藏、非隐藏两类。对于隐藏文件/文件夹，请勿修改或删除，以免影响对应功能。
- 给文件/文件夹命名时，首字母不能使用“.”。否则，系统将把名称首字母为“.”的文件/文件夹识别为隐藏文件/文件夹。

当需要对存储介质进行写操作，包括执行 **copy**、**delete**、**fixdisk**、**format**、**gunzip**、**gzip**、**mkdir**、**move**、**rename**、**rmdir**、**undelete** 命令，请确保没有将存储介质写保护。如果存储介质写保护了，这些命令将执行失败。执行其它命令行不受写保护开关影响。

存储介质的支持情况与设备型号有关，请以设备的实际情况为准。

型号	固定存储介质	可插拔存储介质
T5000-G20	CF卡	U盘
T5000-G30	SD卡	HD卡、U盘
T1000-G20/T1000-G50/T1000-G60/ T1000-G80	Flash	HD卡、U盘
T1000-CN60/T1000-CN80	Flash	HD卡、U盘

当用户对存储介质或文件系统执行 **fixdisk** 或 **format** 操作时，其他用户不能访问该存储介质或文件系统。需要等待这些操作结束后，通过以下方式来访问此存储介质或文件系统：

- 通过命令行参数直接指定绝对路径。例如，使用 **dir flash:/**命令来显示 Flash 中的文件。
- 通过 **cd** 命令切换到该存储介质或文件系统目录下后，再使用相对路径访问。例如，使用 **cd flash:/**进入 Flash，再使用 **dir** 命令显示 Flash 中的文件。

本命令手册中文件系统名称、目录名和文件名的参数输入规则必须符合文件系统命名规范，详细请参见“基础配置指导”中的“文件系统管理配置”。

1.1.1 cd

cd 命令用来修改工作路径。

【命令】

cd { *directory* | .. }

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

directory: 指定目标工作路径。

..: 返回上一级目录。如果当前的工作路径是根目录，则执行 **cd ..** 后提示出错。该参数不支持命令行在线帮助。

【举例】

登录设备后从根目录进入 **test** 文件夹。

<Sysname> cd test

返回上一级目录。

<Sysname> cd ..

1.1.2 copy

copy 命令用来复制文件。

【命令】

```
copy source-file { dest-file | dest-directory } [ vpn-instance  
vpn-instance-name ] [ source interface interface-type interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

source-file: 源文件名或者远程源文件 URL。若为 URL 格式，表示从远程文件服务器拷贝文件。远程源文件 URL 是否支持大小写遵循远程服务器端的规格。

dest-file: 目标文件名或远程目标文件 URL。若为 URL 格式，表示拷贝文件至远程的目标文件。远程目标文件 URL 是否支持大小写遵循远程服务器端规格。

dest-directory: 目标文件夹或远程目录 URL。若为 URL 格式，表示拷贝文件至远程的目标文件夹。远程目录 URL 是否支持大小写遵循远程服务器端规格。如果使用文件夹作为 **dest-directory**，则系统会将文件复制到文件夹，使用源文件名称作为文件名。

vpn-instance *vpn-instance-name* : 指定远程服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示远程服务器位于公网中。

source interface *interface-type* *interface-number*: 指定连接远程服务器时使用的源接口。指定源接口后，设备将使用源接口的主 IP 作为设备生成的连接报文的源 IP。不指定该参数时，则使用路由出接口作为源接口。

【使用指导】

指定 *source-file* 和 *dest-file* 时：

- 当 *source-file* 和 *dest-file* 均是本地路径时，可以实现本地文件间的拷贝。
- 当 *source-file* 是远程服务器上的路径（即为 URL 格式），*dest-file* 中指定的是本地路径时，可以实现将远程服务器上的文件拷贝到本地。
- 当 *source-file* 是本地路径，*dest-file* 是远程服务器上的路径（即为 URL 格式）时，可以实现将本地文件拷贝到远程服务器。

当进行远程拷贝时，支持使用FTP、TFTP协议，各协议的URL格式如 [表 1-1](#) 所示：

表1-1 FTP、TFTP 协议的 URL 格式

协议类型	URL 格式	说明
FTP	ftp://FTP用户名[:密码]@服务器地址[:端口号]/文件路径	用户名和密码必须和服务器的配置一致。例如 ftp://a:1@1.1.1.1/startup.cfg 表示地址为 1.1.1.1 的 FTP 服务器授权目录下的 startup.cfg 文件，用户名为 a、密码为 1。 如果服务器只对用户名进行认证，则无需输入密码
TFTP	tftp://服务器地址[:端口号]/文件路径	tftp://1.1.1.1/startup.cfg 表示地址为 1.1.1.1 的 TFTP 服务器工作目录下的 startup.cfg 文件

服务器地址为 IPv6 地址时，必须用中括号 “[]” 将 IPv6 地址括起来，以便将 IPv6 地址和端口号区分开。例如：ftp://test:test@[2001::1]:21/test.cfg，其中，2001::1 为 FTP 服务器的 IPv6 地址，21 为 FTP 协议的端口号。

【举例】

将文件 test.cfg 在当前文件夹下复制一份，并命名为 testbackup.cfg。

```
<Sysname> copy test.cfg testbackup.cfg
```

```
Copy flash:/test.cfg to flash:/testbackup.cfg? [Y/N]:y
```

```
Copying file flash:/test.cfg to flash:/testbackup.cfg...Done.
```

将 Flash 上文件夹 test 下的文件 1.cfg 复制到 U 盘指定分区下的文件夹 testbackup，并命名为 1backup.cfg。

```
<Sysname> copy flash:/test/1.cfg usba0:/testbackup/1backup.cfg
```

```
Copy flash:/test/1.cfg to usba0:/testbackup/1backup.cfg? [Y/N]:y
```

```
Copying file flash:/test/1.cfg to usba0:/testbackup/1backup.cfg...Done.
```

登录设备后将配置文件拷贝到指定 slot 的根目录下。

```
<Sysname> copy test.cfg slot2#flash:/
```

```
Copy flash:/test.cfg to slot2#flash:/test.cfg? [Y/N]:y
```

```
Copying file flash:/test.cfg to slot2#flash:/test.cfg...Done.
```

将 FTP 服务器 1.1.1.1 上的文件 test.cfg 拷贝到本地，并命名为 testbackup.cfg，FTP 服务器的登录用户名为 user，密码为 private。

```
<Sysname> copy ftp://user:private@1.1.1.1/test.cfg testbackup.cfg
```

```
Copy ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
```

```
Copying file ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

将文件 test.cfg 拷贝到 FTP 服务器 1.1.1.1 上，并命名为 testbackup.cfg，FTP 服务器的登录用户名为 user，密码为 private。

```
<Sysname> copy test.cfg ftp://user:private@1.1.1.1/testbackup.cfg
```

```

Copy flash:/test.cfg to ftp://user:private@1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to ftp://user:private@1.1.1.1/testbackup.cfg... Done.
# 将 TFTP 服务器 1.1.1.1 上的文件 test.cfg 拷贝到本地，并命名为 testbackup.cfg。
<Sysname> copy tftp://1.1.1.1/test.cfg testbackup.cfg
Copy tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
# 将文件 test.cfg 拷贝到 TFTP 服务器 1.1.1.1 上，并命名为 testbackup.cfg。
<Sysname> copy test.cfg tftp://1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to tftp://1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to tftp://1.1.1.1/testbackup.cfg... Done.
# 将 FTP 服务器 1.1.1.1 上的文件 test.cfg 拷贝到本地，并命名为 testbackup.cfg。FTP 服务器位于
VPN 实例（名称为 vpn1）中，登录用户名为 user，密码为 private。
<Sysname> copy ftp://user:private@1.1.1.1/test.cfg testbackup.cfg vpn-instance vpn1
Copy ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
# 将 TFTP 服务器 1.1.1.1 上的文件 test.cfg 拷贝到本地，并命名为 testbackup.cfg。TFTP 服务器
位于 VPN 实例（名称为 vpn1）中。
<Sysname> copy tftp://1.1.1.1/test.cfg testbackup.cfg vpn-instance vpn1
Copy tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
# 将 FTP 服务器 2001::1 上的文件 test.cfg 拷贝到本地，并命名为 testbackup.cfg，登录用户名为
user，密码为 private。
<Sysname> copy ftp://user:private@[2001::1]/test.cfg testbackup.cfg
Copy ftp://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
# 将 TFTP 服务器 2001::1 上的文件 test.cfg 拷贝到本地，并命名为 testbackup.cfg。
<Sysname> copy tftp://[2001::1]/test.cfg testbackup.cfg
Copy tftp://[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://[2001::1]/test.cfg to flash:/testbackup.cfg... Done.

```

1.1.3 delete

delete 命令用来删除文件。

【命令】

```
delete [ /unreserved ] file
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

/unreserved: 彻底删除该文件，如果不指定该参数，被删除的文件将被移至回收站中。

file: 要删除的文件名。**file** 参数支持通配符 “*” 进行匹配，例如 **delete *.txt** 可以删除当前目录下所有以 txt 为扩展名的文件。

【使用指导】

delete /unreserved file 命令用来永久删除文件，系统会将该文件从设备上彻底删除。被删除的文件不再存在，不能恢复。

delete file 命令用来暂时删除文件，被删除的文件存放在回收站中，可以使用 **undelete** 命令恢复：

当文件系统空间不足时，执行 **delete /unreserved file** 命令，系统将永久删除对应文件。

请不要对回收站中的文件执行 **delete** 命令，以免影响回收站功能。若要删除回收站中的文件，请使用 **reset recycle-bin** 命令。

在同一个目录下，如果先后删除了两个名称相同的文件，回收站中只保留最后一次删除的文件。不同目录下，如果先后删除了名称相同的文件，回收站中会保留这些删除的文件。

【举例】

删除当前目录下的文件 1.cfg。

```
<Sysname> delete 1.cfg
```

```
Delete flash:/1.cfg? [Y/N]:y
```

```
Deleting file flash:/1.cfg...Done.
```

永久删除当前目录下的文件 1.cfg。

```
<Sysname> delete /unreserved 1.cfg
```

```
The file cannot be restored. Delete flash:/1.cfg? [Y/N]:y
```

```
Deleting the file permanently will take a long time. Please wait...
```

```
Deleting file flash:/1.cfg...Done.
```

【相关命令】

- **undelete**
- **reset recycle-bin**

1.1.4 dir

dir 命令用来显示当前文件夹或文件信息。

【命令】

```
dir [ /all ] [ file | directory | /all-file systems ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

/all: 显示当前文件夹下所有的文件及文件夹信息，包括非隐藏文件、非隐藏文件夹、隐藏文件和隐藏文件夹。不指定该参数时，只显示非隐藏文件和非隐藏文件夹。

file: 显示指定的文件的信息。**file** 参数支持通配符“*”，例如 **dir *.txt** 可以显示当前文件夹下所有以 **txt** 为扩展名的文件。

directory: 显示指定的文件夹的信息。

/all-file systems: 显示设备上所有文件系统根目录下的文件及文件夹信息。

【使用指导】

不使用任何参数时，用来显示当前文件夹下所有可见文件及文件夹的信息。

回收站的文件夹名称为“.trash”，如需查看回收站内的文件，请用 **dir /all.trash**，或者 **cd .trash** 进入回收站文件夹后，再用 **dir** 命令查看。

对于 **EXT4** 类型的文件系统，1%的空间为系统保留空间，通过 **dir** 命令查看到的可用空间不包含保留空间。

多用户同时执行文件操作时，比如同时创建或删除文件或文件夹，可能导致该命令显示结果不准确。

【举例】

显示当前文件夹下所有的文件及文件夹信息。

```
<Sysname> dir /all
Directory of flash: (VFAT)
.....略.....
```

显示设备上所有文件系统根目录下的文件及文件夹信息。

```
<Sysname> dir /all-file systems
Directory of flash: (VFAT)
.....略.....
```

表1-2 dir 命令显示信息描述表

字段	说明
Directory of XX: (xx)	当前显示的目录： - XX 表示当前目录名 - xx 表示当前目录所在文件系统的类型
0 -rwh 3144 Apr 26 2014 13:45:28 xx.xx	文件或文件夹的信息： 0 表示编号，由系统自动分配 -rwh 表示属性。第一个字符如果是 d 表示文件夹，如果显示为“-”，则表示它是文件；第二个字符是 r，表示本文件或文件夹是可读的；第三个字符是 w，表示本文件或文件夹是可写的；第四个字符如果是 h，表示本文件或文件夹是隐藏的，如果显示为“-”，则表示它是非隐藏的（请不要修改或删除隐藏文件或文件夹，以免影响对应功能） 3144 表示文件大小，单位为 B。如果显示为“-”，则表示它是文件夹 - Apr 26 2014 13:45:28 表示最近一次修改的时间 - xx.xx 表示名称

1.1.5 fdisk

fdisk 命令用来对文件系统进行分区。

【命令】

fdisk medium [*partition-number*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

medium: 需要分区的存储介质的名称。

partition-number: 分区数，取值范围为 1~4。

- 如果指定分区数，则设备将存储介质平均分成指定数目的分区。
- 如果不指定分区数，则设备进入交互模式进行分区。

【使用指导】

本命令仅缺省 **Context** 支持。

Flash 不支持分区。

设备不支持对分区进行再分区。

如果要修改分区大小，需要重新对存储介质进行分区。

执行分区操作前，请做好如下准备：

- 请务必做好文件备份，分区操作会清除存储介质中的所有数据。
- 请确认分区过程中，无其他用户访问该存储介质，否则，系统会提示分区失败。
- 对存储介质分区前，请确保没有对存储介质设置写保护。否则会分区失败，此时需要重新挂载或者插拔存储介质后，才能正常访问存储介质。

对存储介质分区后，必须先对各分区格式化（例如，要格式化支持分区的 **CF** 卡，请逐个格式化各分区，不能执行 **format cfa**），再进行读写操作，否则，读写失败。

分区完成后，各分区的大小可能与用户指定的大小不一致，但误差小于存储介质总容量的 5%。

必须先卸载所有的分区才能安全的拔出存储介质，否则，可能会引起存储介质的损坏。

【举例】

将设备的 **CF** 卡平均分为 3 个分区。

```
<Sysname> fdisk cfa: 3
Capacity of cfa: : 256M bytes
cfa: will be divided into the following partitions:
DeviceName      Capacity
cfa0:           85MB
cfa1:           85MB
cfa2:           86MB
All data on cfa: will be lost, continue? [Y/N]:y
Partitioning cfa:...Done.
```

使用交互模式将设备的 **CF** 卡分为 1 个分区。

```
<Sysname> fdisk cfa:
The capacity of cfa: : 256M bytes
Partition 1 (32MB~224MB, 256MB. Press CTRL+C to quit or Enter to use all available space):
```

```
// 按<Enter>键或者输入 256。
cfa: will be divided into the following partition(s):
DeviceName      Capacity
cfa0:            256MB
All data on cfa: will be lost, continue? [Y/N]:y
Partitioning cfa:...Done.
# 将 CF 卡分为 3 个分区, 并分别指定 3 个分区的大小。
<Sysname> fdisk cfa:
The capacity of cfa: : 256M bytes
Partition 1 (32MB~224MB, 256MB, Press CTRL+C to quit or Enter to use all available space):128
// 将第一个分区的大小指定为128MB (输入 128 后回车)。
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available space):31
// 将第二个分区的大小指定为31MB (输入 31 后回车)。
The partition size must be greater than or equal to 32MB.
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available space):1000
// 将第二个分区的大小指定为1000MB (输入 1000 后回车)。
The partition size must be less than or equal to 128MB.
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available space):127
// 将第二个分区的大小指定为127MB (输入 127 后回车)。
The remaining space is less than 32MB. Please enter the size of partition 2 again.
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available space):
// 重新指定第二个分区的大小为56MB (输入 56 后回车)。
Partition 3 (32MB~40MB, 72MB, Press CTRL+C to quit or Enter to use all available space):
// 剩余的空间全部划分给第三个分区 (直接回车)。
cfa: will be divided into the following partition(s):
DeviceName      Capacity
cfa0:            128MB
cfa1:            56MB
cfa2:            72MB
All data on cfa: will be lost, continue? [Y/N]:y
Partitioning cfa:...Done.
```

1.1.6 file prompt

file prompt 命令用来设置系统对文件/文件夹操作的提示方式。

undo file prompt 命令用来恢复缺省情况。

【命令】

```
file prompt { alert | quiet }
```

```
undo file prompt
```

【缺省情况】

用户对文件进行有危险性的操作时, 系统会要求用户进行交互确认。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

alert: 当用户对文件/文件夹进行有危险性的操作时，系统会要求用户进行交互确认。

quiet: 用户对文件/文件夹进行除清空回收站之外的其他操作时，系统均不要求用户进行确认。

【使用指导】

如果将文件/文件夹操作的提示方式设置为 **quiet**，则系统对除清空回收站之外的文件/文件夹操作均不要求用户进行确认，这样可能会导致一些因误操作而发生的、不可恢复的、对系统造成破坏的操作产生。

【举例】

设置用户对文件进行有危险性的操作时，要求进行交互确认。

```
<Sysname> system-view  
[Sysname] file prompt alert
```

1.1.7 fixdisk

fixdisk 命令用来恢复文件系统的空间。

【命令】

fixdisk *filesystem*

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

filesystem: 文件系统的名称。

【使用指导】

本命令仅缺省 Context 支持。

由于异常操作等原因，文件系统的某些空间可能不可用，或者某些空间已经不再需要使用但是没有释放，用户可以通过 **fixdisk** 命令来恢复文件系统的空间。

用户对文件系统执行 **fixdisk** 操作时，如果同时还有其他用户在访问该文件系统，系统会提示 **fixdisk** 操作失败。

【举例】

恢复文件系统 Flash 的空间。

```
<Sysname> fixdisk flash:  
Restoring flash: may take some time...  
Restoring flash:...Done.
```

1.1.8 format

format 命令用来格式化文件系统。

【命令】

```
format filesystem [ ext4 | vfat ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

filesystem: 文件系统的名称。

ext4: 将文件系统格式化为 EXT4 类型。

vfat: 将文件系统格式化为 VFAT 类型。

【使用指导】

本命令仅缺省 Context 支持。

Flash 文件系统不支持 VFAT 和 EXT4 类型，格式化 Flash 时，请不要指定 **ext4** 和 **vfat** 参数。设备会将 Flash 格式化为缺省的文件系统类型。

对于其它类型的存储介质（如 U 盘、CF 卡、硬盘），设备仅支持 VFAT 或 EXT4 类型的文件系统。如果不是 VFAT 或 EXT4 类型的文件系统，需要先格式化成 VFAT 或 EXT4 类型才能读写。



说明

可以使用 **dir** 命令查看文件系统的类型。

格式化操作将导致文件系统中的所有文件丢失，并且不可恢复；尤其需要注意的是，如果文件系统中存在启动配置文件，格式化该文件系统，将丢失启动配置文件。

用户对文件系统执行格式化操作时，如果同时还有其他用户在访问该文件系统，系统会提示格式化操作失败。

如果待格式化的文件系统中存有安全日志文件，则不能进行格式化操作，请根据实际需要，将安全日志从文件系统里移出或删除。安全日志需要安全日志管理员对其进行操作，有关安全日志管理员的详细介绍请参见“基础配置指导”中的“RBAC”。

【举例】

格式化 flash:。

```
<Sysname> format flash:
```

```
All data on flash: will be lost, continue? [Y/N]:y
```

```
Formatting flash:... Done.
```

格式化 CF 卡上的第三个分区。

```
<Sysname> format cfa2:
```

```
All data on cfa2: will be lost, continue? [Y/N]:y
```

```
Formatting cfa2:... Done.
```


1.1.9 fuser

fuser 命令用来显示正在使用文件系统、文件夹或文件的进程信息。

【命令】

```
fuser { directory | file | filesystem }
```

【视图】

用户视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

- directory*: 文件夹名。
- file*: 文件名。
- filesystem*: 文件系统的名称。

【使用指导】

当用户对文件系统、文件夹或文件执行操作失败时（例如执行 **rmdir**、**rename**、**delete**、**copy**、**format**、**fdisk**、**fixdisk**、**umount** 等命令失败），可以使用本命令查看是否有进程正在使用文件系统、文件夹或文件。

进程名称为 **comsh** 的进程为 CLI 登录用户对应的进程（用户通过 CLI 登录设备时，系统自动运行一个用户登录进程来监控用户的操作），这样的进程会占用文件系统、文件夹或文件，但不会影响用户操作文件系统、文件夹或文件。

【举例】

显示正在使用文件系统 **flash:**的进程信息。

```
<Sysname> fuser flash:
Job ID      PID    Process name
198         198    comsh
223         223    ttymgrd
332         332    ntopd
```

表1-3 fuser 命令显示信息描述表

字段	描述
Job ID	任务编号，用于唯一标识一个进程，该编号不会随着进程的重启而改变
PID	进程编号，用于标识一个进程，但该编号可能会随着进程的重启而改变
Process name	进程名称

1.1.10 gunzip

gunzip 命令用来解压缩文件。

【命令】

gunzip *file*

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

file: 需要被解压缩的文件名，以.gz 为后缀。

【使用指导】

该命令将解压缩并替换当前指定文件。

【举例】

解压缩 system.bin.gz 文件。

- 解压缩前查看文件的相关信息。

<Sysname> dir system.*

Directory of flash:

1	-rw-	20 Jun 14 2012 10:18:53	system.bin.gz

252164 KB total (251820 KB free)

- 执行解压缩操作。

<Sysname> gunzip system.bin.gz

Decompressing file flash:/system.bin.gz..... Done.

- 解压缩后验证执行效果。

<Sysname> dir system.*

Directory of flash:

1	-rw-	0 May 30 2012 11:42:25	system.bin

252164 KB total (251820 KB free)

1.1.11 gzip

gzip 命令用来压缩文件。

【命令】

gzip *file*

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

file: 需要被压缩的文件名。

【使用指导】

执行本命令后，原文件将被压缩并命名为 *file.gz*，并删除原文件。

【举例】

压缩 system.bin 文件。

- 压缩前查看文件的相关信息。

```
<Sysname> dir system.*
```

```
Directory of flash:
```

```
1 -rw-          0 May 30 2012 11:42:24   system.bin
```

```
252164 KB total (251820 KB free)
```

- 执行压缩操作。

```
<Sysname> gzip system.bin
```

```
Compressing file flash:/system.bin..... Done.
```

- 压缩后验证执行效果。

```
<Sysname> dir system.*
```

```
Directory of flash:
```

```
1 -rw-          20 Jun 14 2012 10:18:53   system.bin.gz
```

```
252164 KB total (251820 KB free)
```

1.1.12 md5sum

md5sum 命令用来使用 MD5 摘要算法计算文件的摘要值。

【命令】

```
md5sum file
```

【视图】

用户视图

【缺省用户角色】

network-admin
network-operator

【参数】

file: 文件名。

【使用指导】

使用摘要算法对文件计算摘要值，通常用于验证文件的正确性和完整性。

【举例】

```
# 计算 system.bin 文件的 MD5 摘要值。
<Sysname> md5sum system.bin
MD5 digest:
4f22b6190d151a167105df61c35f0917
```

1.1.13 mkdir

mkdir 命令用来创建文件夹。

【命令】

mkdir *directory*

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

directory: 文件夹。

【使用指导】

如果创建的文件夹与指定文件夹下的文件或者其它文件夹重名，则创建操作失败。

在使用该命令创建文件夹之前，指定的文件夹必须已经存在。例如：创建文件夹 **flash:/test/mytest**，这时，**test** 文件夹必须已经存在，否则，创建失败。

【举例】

```
# 在当前路径创建文件夹 test。
<Sysname> mkdir test
Creating directory flash:/test... Done.
# 在当前路径创建文件夹 test/subtest。
<Sysname>mkdir test/subtest
Creating directory flash:/test/subtest... Done.
```

1.1.14 more

more 命令用来显示文本文件的内容。

【命令】

more *file*

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

file: 文件名。

【举例】

```
# 显示文件 test.txt 的内容。
<Sysname> more test.txt
Have a nice day.
# 显示文件 testcfg.cfg 的内容。
<Sysname> more testcfg.cfg

#
version 7.1.070, Release 1201
#
sysname Sysname
#
vlan 2
#
return
<Sysname>
```

1.1.15 mount

mount *filesystem* 命令用来挂载文件系统。

【命令】

mount *filesystem*

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

filesystem: 文件系统的名称。

【使用指导】

本命令仅缺省 Context 支持。

存储介质连接到设备后，文件系统自动被挂载。如果系统未能自动识别，则必须手动进行挂载操作后，才能对该文件系统执行读写操作。

在执行挂载操作过程中，禁止对存储介质进行如下操作，以免造成文件系统的损坏：

- 禁止对存储介质进行插拔操作。
- 禁止重新启动设备、或对设备断电。
- 禁止进行主备倒换操作。

处于挂载状态的存储介质在拔出系统前，请先执行卸载操作，以免损坏文件系统。

【举例】

```
# 挂载 CF 卡文件系统。  
<Sysname> mount cfa0:
```

【相关命令】

- **umount**

1.1.16 move

move 命令用来移动文件。

【命令】

```
move source-file { dest-file | dest-directory }
```

【视图】

用户视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

source-file: 源文件名。
dest-file: 目标文件名。
dest-directory: 目标文件夹。

【使用指导】

如果指定 *dest-directory*，则系统会将文件移到指定文件夹，文件名保持不变。

【举例】

```
# 将文件 flash:/test/sample.txt 移动到 flash:/，并更名为 1.txt。  
<Sysname> move test/sample.txt 1.txt  
Move flash:/test/sample.txt to flash:/1.txt? [Y/N]:y  
Moving file flash:/test/sample.txt to flash:/1.txt ...Done.  
# 将文件 b.cfg 移动到文件夹 test2 下。  
<Sysname> move b.cfg test2  
Move flash:/b.cfg to flash:/test2/b.cfg? [Y/N]:y  
Moving file flash:/b.cfg to flash:/test2/b.cfg... Done.
```

1.1.17 pwd

pwd 命令用来显示当前工作路径。

【命令】

```
pwd
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 显示当前路径。  
<Sysname> pwd  
flash:
```

1.1.18 rename

rename 命令用来重命名文件或文件夹。

【命令】

```
rename { source-file | source-directory } { dest-file | dest-directory }
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

source-file: 源文件名。
source-directory: 源文件夹名。
dest-file: 目标文件名。
dest-directory: 目标文件夹名。

【使用指导】

若目标文件名或目标文件夹与当前路径下已经存在的文件或目标文件夹重名（不区分大小写，只要字母相同就认为同名），则该操作不执行。

【举例】

```
# 将文件 copy.cfg 重命名为 test.cfg。  
<Sysname> rename copy.cfg test.cfg  
Rename flash:/copy.cfg as flash:/test.cfg? [Y/N]:y  
Renaming flash:/copy.cfg as flash:/test.cfg... Done.
```

1.1.19 reset recycle-bin

reset recycle-bin 命令用来清除回收站中的文件。

【命令】

```
reset recycle-bin [ /force ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

/force: 表示直接清空回收站，不需要用户对清空操作进行确认。如果不指定该参数，执行回收站清除操作时，系统将对每一个即将清除的文件进行确认。

【使用指导】

用 **delete file** 命令删除文件是将文件放在回收站中，但仍然占用存储空间，如果想要把回收站中的该文件删除，必须执行 **reset recycle-bin** 命令。

【举例】

回收站中有文件 a.cfg 和 b.cfg，清空回收站。

```
<Sysname> reset recycle-bin  
Clear flash:/a.cfg? [Y/N]:y  
Clearing file flash:/a.cfg... Done.  
Clear flash:/b.cfg? [Y/N]:y  
Clearing file flash:/b.cfg... Done.
```

回收站中有文件 a.cfg 和 b.cfg，删除 b.cfg。

```
<Sysname> reset recycle-bin  
Clear flash:/a.cfg? [Y/N]:n  
Clear flash:/b.cfg? [Y/N]:y  
Clearing file flash:/b.cfg... Done.
```

【相关命令】

- **delete**

1.1.20 rmdir

rmdir 命令用来删除文件夹。

【命令】

rmdir *directory*

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

directory: 文件夹名称。

【使用指导】

在删除文件夹前，必须先永久删除或者暂时删除文件夹中的所有文件和子文件夹。如果文件只是暂时删除，那么执行 **rmdir** 会导致这些文件从回收站中彻底删除。

【举例】

```
# 删除文件夹 subtest。
<Sysname> rmdir subtest/
Remove directory flash:/test/subtest and the files in the recycle-bin under this directory
will be deleted permanently. Continue? [Y/N]:y
Removing directory flash:/test/subtest... Done.
```

1.1.21 sha256sum

sha256sum 命令用来使用 SHA-256 摘要算法计算文件的摘要值。

【命令】

```
sha256sum file
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

file: 文件名。

【使用指导】

使用摘要算法对文件计算摘要值，通常用于验证文件的正确性和完整性。

【举例】

```
# 计算 system.bin 文件的 SHA-256 摘要值。
<Sysname> sha256sum system.bin
SHA256 digest:
0851e0139f2770e87d01ee8c2995ca9e59a8f5f4062e99af14b141b1a36ca152
```

1.1.22 tar create

tar create 命令用来将多个文件/文件夹打包成一个新文件。

【命令】

```
tar create [ gz ] archive-file dest-file [ verbose ] source { source-file
| source-directory }&<1-5>
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

gz: 表示打包后，再使用 **gzip** 格式压缩该打包文件。不指定该参数时，表示只打包，不压缩。

archive-file dest-file: 打包后生成的新文件的名称。当不指定 **gz** 参数时, *dest-file* 的后缀必须为 “.tar”; 当指定 **gz** 参数时, *dest-file* 的后缀必须为 “.tar.gz”。

verbose: 表示在打包过程中逐个显示已经打包的文件和文件夹的名称。不指定该参数时, 则不会显示。

source { source-file | source-directory }&<1-5>: 表示需要打包的原文件/文件夹列表。当包括文件夹时, 则表示打包该文件夹下的所有文件和子文件夹。&<1-5>表示前面的参数最多可以输入 5 次。

【使用指导】

执行该命令后, 设备会先拷贝原文件/文件夹, 再将它们打包成一个新文件后保存。

【举例】

将文件 1.cfg、2.cfg 和文件夹 test 打包后保存到新文件 a.tar。

```
<Sysname> tar create archive-file a.tar source 1.cfg 2.cfg test
Creating archive flash:/a.tar Done.
```

将文件 1.cfg、2.cfg 和文件夹 test 打包压缩后保存到新文件 b.tar.gz。

```
<Sysname> tar create gz archive-file b.tar.gz source 1.cfg 2.cfg test
Creating archive flash:/b.tar.gz Done.
```

将文件 1.cfg、2.cfg 和文件夹 test 打包压缩后保存到新文件 c.tar.gz, 并在打包过程中逐个显示已经打包的文件和文件夹的名称。

```
<Sysname> tar create gz archive-file c.tar.gz verbose source 1.cfg 2.cfg test
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

【相关命令】

- **tar extract**
- **tar list**

1.1.23 tar extract

tar extract 命令用来解包文件。

【命令】

```
tar extract archive-file file [ verbose ] [ screen | to directory ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

archive-file file: 需要解包的文件的名称, 后缀为.tar 或.tar.gz。

verbose: 在命令行执行过程中，显示 *file* 中包含的所有文件/文件夹的名称。

screen: 不解包，仅将 *file* 中包含的原文件的内容输出至登录终端，建议仅包含文本文件时使用该参数。

to directory: 解包至目标路径。*directory* 表示解包后文件的保存路径。

【使用指导】

使用 **screen** 参数前，请通过 **tar list** 命令确认压缩包内文件的类型，建议仅包含文本文件时使用该参数。如果压缩包中包含非文本文件，且非文本文件中包含终端控制字符，指定 **screen** 参数执行本命令，可能导致当前登录终端的显示信息出现乱码甚至当前登录终端不可用。通常情况下，断开当前连接重新登录设备后可将登录终端恢复到正常状态。

不指定 **screen** 和 **to directory** 参数时，目标路径为用户的当前路径。

执行该命令后，设备会将 *file* 中包含的文件/文件夹解包后保存到目标路径，名称保持不变。保存时会自动覆盖目标路径中已存在的同名文件/文件夹。

【举例】

将 a.tar 解包。

```
<Sysname> tar extract archive-file a.tar  
Extracting archive flash:/a.tar Done.
```

将 b.tar.gz 解包，并在解包过程中，显示 b.tar.gz 中包含的所有文件/文件夹的名称。

```
<Sysname> tar extract archive-file b.tar.gz verbose  
1.cfg  
2.cfg  
test/  
test/a.log  
test/subtest/  
test/subtest/aa.log
```

将 c.tar.gz 中包含的原文件的内容直接输出到登录终端。

```
<Sysname> tar extract archive-file c.tar.gz screen  
#  
version 7.1.070, Release 1201  
#  
sysname Sysname  
#
```

执行以上操作会不解包，直接显示文件内容，剩余的文件内容此处省略。

【相关命令】

- **tar create**
- **tar list**

1.1.24 tar list

tar list 命令用来显示打包文件中包含的文件/文件夹的名称。

【命令】

```
tar list archive-file file
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

archive-file file: 需要显示的打包文件的名称，后缀为.tar 或.tar.gz。

【举例】

显示 a.tar 中包含的文件/文件夹的名称。

```
<Sysname> tar list archive-file a.tar
```

```
1.cfg
```

```
2.cfg
```

```
test/
```

```
test/a.log
```

```
test/subtest/
```

```
test/subtest/aa.log
```

【相关命令】

- **tar create**
- **tar extrac**

1.1.25 umount

umount 命令用来卸载文件系统。

【命令】

umount *filesystem*

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

filesystem: 文件系统的名称。

【使用指导】

本命令仅缺省 Context 支持。

存储介质连接到设备后，文件系统自动被挂载，处于挂载状态。卸载存储介质中所有的文件系统后用户才可以安全的拔出存储介质，否则，可能引起文件损坏甚至存储介质损坏。

在执行卸载操作过程中，禁止对存储介质进行如下操作，以免造成文件系统的损坏：

- 禁止对存储介质进行插拔操作。
- 禁止重新启动设备、或对设备断电。
- 禁止进行主备倒换操作。

- 禁止访问存储介质或存储介质进行读写操作，如果此时有其他用户在访问该文件系统，系统会提示 **umount** 操作失败。

【举例】

```
# 卸载 CF 卡文件系统。
<Sysname> umount cfa0:
```

【相关命令】

- **mount**

1.1.26 undelete

undelete 命令用来恢复未被彻底删除（即存放在回收站里）的文件。

【命令】

```
undelete file
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

file: 要恢复的文件名。

【使用指导】

如果恢复的文件名与当前存在的文件重名，系统将提示操作者是否覆盖原有文件。如果输入<Y>，则覆盖源文件；如果输入<N>，则不再执行恢复操作。

【举例】

```
# 恢复 flash:下删除的文件 copy.cfg。
<Sysname> undelete copy.cfg
Undelete flash:/copy.cfg? [Y/N]:y
Undeleting file flash:/copy.cfg... Done.
# 恢复 flash:/seclog 下删除的文件 startup.cfg。
• 方法一
<Sysname> undelete seclog/startup.cfg
Undelete flash:/seclog/startup.cfg? [Y/N]:y
Undeleting file flash:/seclog/startup.cfg... Done.
• 方法二
<Sysname> cd seclog
<Sysname> undelete startup.cfg
Undelete flash:/seclog/startup.cfg? [Y/N]:y
Undeleting file flash:/seclog/startup.cfg... Done.
```

目 录

1 配置文件管理	1-1
1.1 配置文件管理命令	1-1
1.1.1 archive configuration	1-1
1.1.2 archive configuration interval	1-2
1.1.3 archive configuration location	1-3
1.1.4 archive configuration max	1-4
1.1.5 archive configuration server	1-5
1.1.6 archive configuration server password	1-6
1.1.7 archive configuration server user	1-7
1.1.8 backup startup-configuration	1-8
1.1.9 configuration encrypt	1-9
1.1.10 configuration replace file	1-9
1.1.11 configuration replace server	1-10
1.1.12 configuration replace server file	1-11
1.1.13 configuration replace server password	1-13
1.1.14 configuration replace server user	1-13
1.1.15 display archive configuration	1-14
1.1.16 display configuration replace server	1-16
1.1.17 display current-configuration	1-17
1.1.18 display current-configuration diff	1-18
1.1.19 display default-configuration	1-20
1.1.20 display diff	1-20
1.1.21 display saved-configuration	1-22
1.1.22 display startup	1-23
1.1.23 display this	1-24
1.1.24 reset saved-configuration	1-24
1.1.25 restore startup-configuration	1-25
1.1.26 save	1-26
1.1.27 startup saved-configuration	1-29

1 配置文件管理



说明

下次启动文件/缺省配置文件请勿放在硬盘中。

1.1 配置文件管理命令

1.1.1 archive configuration

archive configuration 命令用来手工备份当前配置。

【命令】

archive configuration

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

设备支持手工和自动两种方式备份当前配置。执行该命令后，系统会将当前的配置以指定的文件名保存到指定的路径。

执行 **archive configuration** 命令前必须先执行 **archive configuration location** 命令来设置备份配置文件的保存路径和文件名前缀，或者先执行 **archive configuration server** 命令进行相关设置以将配置文件备份到远程服务器上。

若使用 **archive configuration location** 命令指定了配置文件的本地备份路径，执行该命令后，只有主设备会备份当前配置，从设备不进行备份操作。

【举例】

手工备份当前配置。

```
<Sysname> archive configuration
```

```
Save the running configuration to an archive file. Continue? [Y/N]: Y
```

```
The archive configuration file myarchive_1.cfg is saved.
```

【相关命令】

- **archive configuration interval**
- **archive configuration location**
- **archive configuration max**
- **archive configuration server**
- **archive configuration server password**

- **archive configuration server user**
- **display archive configuration**

1.1.2 archive configuration interval

archive configuration interval 命令用来开启自动备份当前配置功能，并设置自动备份的时间间隔。

undo archive configuration interval 用来关闭自动备份当前配置功能。

【命令】

```
archive configuration interval interval
undo archive configuration interval
```

【缺省情况】

自动备份当前配置功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interval: 表示自动备份当前配置的时间间隔，取值范围为 10~525600，单位为分钟。

【使用指导】

设备支持手工和自动两种方式来备份当前配置。成功执行本命令后，每隔指定时间（由 *interval* 值决定）系统会把当前配置以指定文件名自动保存到指定路径，保存完毕后，重新开始计时，进入下一个周期。

执行 **archive configuration interval** 命令前必须先执行 **archive configuration location** 命令来设置备份文件的前缀和保存路径。

执行该命令后，只有主设备会备份当前配置，从设备不进行备份操作。

【举例】

```
# 设置每隔一小时自动备份当前配置。
<Sysname> system-view
[Sysname] archive configuration interval 60
Archive file will be saved every 60 minutes.
```

【相关命令】

- **archive configuration**
- **archive configuration location**
- **archive configuration max**
- **display archive configuration**

1.1.3 archive configuration location

archive configuration location 命令用来设置备份配置文件的保存路径和文件名前缀。

undo archive configuration location 命令用来恢复缺省情况。

【命令】

archive configuration location *directory* filename-prefix *filename-prefix*
undo archive configuration location

【缺省情况】

未设置备份配置文件的保存路径和文件名前缀。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

directory: 表示保存备份配置文件的文件夹的路径，为 1~63 个字符的字符串，不区分大小写，格式为存储介质名:[文件夹名]/子文件夹名。**directory** 必须是主设备上已存在的路径，且参数中不能包含成员编号。

filename-prefix: 表示备份配置文件的文件名前缀，为 1~30 个字符的字符串，不区分大小写，只能包含字母、数字、“_”和“-”。

【使用指导】

自动或手动备份当前配置前请使用本命令设置备份配置文件的本地保存路径和文件名前缀。

配置该命令后，设备备份当前运行配置时，将当前的配置以前缀_序号.cfg 格式（例如 archive_1.cfg）保存到该命令指定路径下的配置文件中。序号自动从 1 开始编号，依次加 1，累加至 1000 后重新从 1 开始编号。修改备份文件的保存路径、文件名前缀，备份序号也会从 1 开始重新自动编号。

执行 **undo archive configuration location** 命令后：

- 用户将不能手工备份当前配置，系统也不再自动备份当前配置。
- **archive configuration interval** 和 **archive configuration max** 配置恢复到缺省情况。
- **display archive configuration** 的显示信息被清除。

【举例】

在 flash:/archive/目录下备份配置文件，文件名前缀为 my_archive。

```
<Sysname> mkdir flash:/archive
```

```
Creating directory flash:/archive... Done.
```

```
<Sysname> system-view
```

```
[Sysname] archive configuration location flash:/archive filename-prefix my_archive
```

【相关命令】

- **archive configuration**
- **archive configuration interval**

- **archive configuration max**
- **display archive configuration**

1.1.4 archive configuration max

archive configuration max 命令用来设置保存备份配置文件的最大数。

undo archive configuration max 用来恢复缺省情况。

【命令】

```
archive configuration max file-number  
undo archive configuration max
```

【缺省情况】

保存备份配置文件的最大数为 5。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

file-number: 表示可保存的备份配置文件数目上限，取值范围为 1~10。该参数的具体数值应根据设备存储介质的空间大小来决定。对于存储空间较小的设备，建议设置 **file-number** 为较小值。

【使用指导】

备份配置文件数目过多会占用系统内存空间，通过本命令可以控制备份配置文件的数目。当备份配置文件数目到达上限后，下次备份配置文件（包括自动和手动两种触发方式）时，将删除保存时间最早的备份文件，以保存新的备份配置文件。修改备份配置文件数上限时并不删除多余文件，如果当前已有的备份配置文件数大于或等于新设置的上限值，则在备份新的配置时，系统将自动删除生成时间最早的 n ($n = \text{当前已有备份配置文件数} - \text{新设置的上限值} + 1$) 个备份配置文件。例如，当前已有备份配置文件数为 7，新设置的上限值为 4，当有配置需要备份时，系统会先删除 “ $7 - 4 + 1 = 4$ ” 个生成时间最早的备份配置文件。

在使用本命令前，必须先执行 **archive configuration location** 命令设置保存路径和文件名前缀，否则，本命令执行失败。

执行 **undo archive configuration location**，备份配置文件的最大数目也会恢复到缺省情况。

【举例】

```
# 设置备份配置文件的最大数为 10。  
<Sysname> system-view  
[Sysname] archive configuration max 10
```

【相关命令】

- **archive configuration**

- **archive configuration location**
- **archive configuration interval**
- **display archive configuration**

1.1.5 archive configuration server

archive configuration server 命令用来指定配置文件备份到远程服务器时使用的参数。

undo archive configuration server 命令用来恢复缺省情况。

【命令】

```
archive configuration server { ftp | tftp } { ipv4-address | ipv6
ipv6-address } [ port port-number ] [ vpn-instance vpn-instance-name ]
[ directory directory ] filename-prefix filename-prefix [ interval
interval ]
undo archive configuration server
```

【缺省情况】

未指定配置文件备份到远程服务器时使用的参数。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ftp: 将配置文件备份到远程 FTP 服务器。

tftp: 将配置文件备份到远程 TFTP 服务器。

ipv4-address: 指定远程服务器的 IPv4 地址。

ipv6 ipv6-address: 指定远程服务器的 IPv6 地址。

port port-number: 指定远程服务器提供服务的 TCP 端口号，取值范围为 1~65535。FTP 服务的缺省端口号为 21，TFTP 服务的缺省端口号为 69。

vpn-instance vpn-instance-name: 指定远程服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示远程服务器位于公网中。

directory directory: 指定配置文件在远程服务器上的备份目录，缺省为服务器的根目录，不区分大小写。

filename-prefix filename-prefix: 指定配置文件的文件名前缀，**filename-prefix** 为 1~30 个字符的字符串，只能包含字母、数字、“_”和“-”，不区分大小写。

interval interval: 开启自动将配置文件备份到远程服务器功能，并设置自动备份的时间间隔。取值范围为 10~525600，单位为分钟。

【使用指导】

如果将配置文件备份到远程 FTP 服务器，请保证本地配置和服务器端配置一致。如果 FTP 服务器端设置了登录用户的用户名和密码，请使用 **archive configuration server user** 命令配置登录 FTP 服务器的用户名、使用 **archive configuration server password** 命令配置登录 FTP 服务器的密码。

设备支持本地和远程两种备份方式，本命令用来配置远程备份参数，**archive configuration location** 命令用来配置本地备份参数。设备只支持将配置文件备份到一个目的地。所以，配置远程备份前需要先取消本地备份配置，配置本地备份配置前需要先取消远程备份配置。如果多次配置备份参数，最新的配置生效。

指定本地备份或远程备份参数后，可以使用 **archive configuration** 命令手动备份配置文件，缺省情况下，自动将配置文件备份到远程服务器功能处于关闭状态。如果在指定远程备份参数时，开启了自动将配置文件备份到远程服务器功能，则设备会自动将配置文件备份到远程服务器。远程备份成功后，会在远程服务器指定的路径下生成以“前缀_YYYYMMDD_HHMMSS.cfg”命名的配置文件，例如 **archive_20170526_203430.cfg**。执行 **undo archive configuration server** 命令后，设备将不再自动将配置文件备份到远程服务器。

【举例】

指定配置文件的存储路径为 FTP 服务器（IPv4 地址为 192.168.1.1）的 archive/目录，且文件名前缀为 my_archive。

```
<Sysname> system-view
[Sysname] archive configuration server ftp 192.168.1.1 port 22 directory /archive/
filename-prefix my_archive
```

【相关命令】

- **archive configuration**
- **archive configuration location**
- **archive configuration server password**
- **archive configuration server user**
- **display archive configuration**

1.1.6 archive configuration server password

archive configuration server password 命令用来配置向远程 FTP 服务器备份配置时使用的密码。

undo archive configuration server password 命令用来恢复缺省情况。

【命令】

```
archive configuration server password { cipher | simple } string
undo archive configuration server password
```

【缺省情况】

未配置向远程 FTP 服务器备份配置时使用的密码。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

cipher: 表示以密文方式设置密码。

simple: 表示以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 33~117 个字符的字符串。

【举例】

```
# 配置向远程 FTP 服务器备份配置时使用的密码为 admin。  
<Sysname> system-view  
[Sysname] archive configuration server password simple admin
```

【相关命令】

- **archive configuration server**
- **archive configuration server user**
- **display archive configuration**

1.1.7 archive configuration server user

archive configuration server user 命令用来配置向远程 FTP 服务器备份配置时使用的用户名。

undo archive configuration server user 命令用来恢复缺省情况。

【命令】

```
archive configuration server user username  
undo archive configuration server user
```

【缺省情况】

未配置向远程 FTP 服务器备份配置时使用的用户名。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

username: 向远程 FTP 服务器备份配置时使用的用户名，为 1~63 个字符的字符串，区分大小写。

【使用指导】

如果没有配置向远程 FTP 服务器备份配置时使用的用户名，则使用匿名用户“anonymous”。

【举例】

```
# 配置登录远程 FTP 配置备份服务器的用户名为 admin。
```

```
<Sysname> system-view
[Sysname] archive configuration server user admin
```

【相关命令】

- **archive configuration server**
- **archive configuration server password**
- **display archive configuration**

1.1.8 backup startup-configuration

backup startup-configuration 命令用于将设备的主用下次启动配置文件备份到 TFTP 服务器。

【命令】

```
backup startup-configuration to { ipv4-server | ipv6 ipv6-server }
[ dest-filename ] [ vpn-instance vpn-instance-name ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ipv4-server: TFTP 服务器的 IPv4 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

ipv6 ipv6-server: TFTP 服务器的 IPv6 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

dest-filename: 目的文件名，为不超过 255 个字符的字符串，不区分大小写，后缀必须为“.cfg”。在服务器上将以该文件名保存设备的启动配置文件。不指定该参数时，使用原文件名备份。

vpn-instance vpn-instance-name: 指定 TFTP 服务器所在的 VPN 实例。**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 TFTP 服务器位于公网中。

【举例】

将设备的下次启动配置文件备份到 IP 地址为 2.2.2.2 的 TFTP 服务器上，文件名为 192-168-1-26.cfg。

```
<Sysname> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg
Backing up the main startup configuration file to 2.2.2.2...
Done.
```

将设备的下次启动配置文件备份到 IP 地址为 2.2.2.2 的 TFTP 服务器上，TFTP 服务器位于 VPN 实例（名称为 VPN1）中，文件名为 192-168-1-26.cfg。

```
<Sysname> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg vpn-instance VPN1
Backing up the main startup configuration file to 2.2.2.2 in VPN VPN1...
Done.
```

将设备的下次启动配置文件备份到 IPv6 地址为 2001::2 的 TFTP 服务器上，文件名为 192-168-1-26.cfg。

```
<Sysname> backup startup-configuration to ipv6 2001::2 192-168-1-26.cfg
Backing up the main startup configuration file to 2001::2...
Done.
```

【相关命令】

- **restore startup-configuration**

1.1.9 configuration encrypt

configuration encrypt 命令用来开启配置文件加密功能。

undo configuration encrypt 命令用来关闭配置文件加密功能。

【命令】

```
configuration encrypt { private-key | public-key }
undo configuration encrypt
```

【缺省情况】

配置文件加密功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

private-key: 使用私钥进行加密。所有运行 Uniware V7 平台软件的设备拥有相同的私钥。

public-key: 使用公钥进行加密。所有运行 Uniware V7 平台软件的设备拥有相同的公钥。

【使用指导】

开启该功能后，每次执行 **save** 操作，都会先将当前生效的配置进行加密，再保存。

加密后的文件能被所有运行 Uniware V7 平台软件的设备识别和解析。因此，为了防止非法用户对加密后配置文件的解析，需确保只有合法用户才能获取加密后的配置文件。运行其它平台软件的设备不能识别和解析。

【举例】

```
# 设置保存配置文件时使用公钥进行加密。
<Sysname> system-view
[Sysname] configuration encrypt public-key
```

1.1.10 configuration replace file

configuration replace file 命令用来执行配置回滚操作。

【命令】

```
configuration replace file filename
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

filename: 指定用来回滚配置的配置文件路径以及文件名，其长度不能超过 194 个字符，文件路径必须是本地路径，该配置文件必须是有效的.cfg 文件。

【使用指导】

配置回滚是在不重启设备的情况下，将当前的配置回退到指定配置文件中的配置状态。

配置文件可以使用手工/自动备份功能或者 **save** 命令生成，也可以是其他设备的可兼容配置文件，推荐使用手工/自动备份功能生成。

如果使用的配置文件不是由 **save** 命令、自动备份或手工备份生成的完整文件，或是不同类型设备的配置文件，配置回滚可能不能完全恢复至配置文件中的配置状态。因此，需要用户确保回滚配置文件中配置的正确性和与当前设备的兼容性。

本命令中配置文件只能是明文配置文件，设备不能对加密后的配置文件进行回滚。

【举例】

将当前配置回滚到配置文件 my_archive_1.cfg 中的配置状态。

```
<Sysname> system-view
```

```
[Sysname] configuration replace file my_archive_1.cfg
```

```
Current configuration will be lost, save current configuration? [Y/N]:n
```

```
Now replacing the current configuration. Please wait...
```

```
Succeeded in replacing current configuration with the file my_archive_1.cfg.
```

1.1.11 configuration replace server

configuration replace server 命令用来指定从远程服务器下载配置文件时使用的参数。

undo configuration replace server 命令用来恢复缺省情况。

【命令】

```
configuration replace server { ftp | tftp } { ipv4-address | ipv6  
ipv6-address } [ port port-number ] [ vpn-instance vpn-instance-name ]  
[ directory directory ] file filename
```

```
undo configuration replace server
```

【缺省情况】

未指定从远程配置回滚服务器下载配置文件时使用的参数。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ftp: 从远程 FTP 服务器下载配置文件。

tftp: 从远程 TFTP 服务器下载配置文件。

ipv4-address: 指定远程回滚服务器的 IPv4 地址。

ipv6 ipv6-address: 指定远程服务器的 IPv6 地址。

port port-number: 指定远程服务器提供服务的 TCP 端口号，取值范围为 1~65535。FTP 服务的缺省端口号为 21，TFTP 服务的缺省端口号为 69。

vpn-instance vpn-instance-name: 指定远程服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示远程服务器位于公网中。

directory directory: 指定配置文件在远程服务器上的目录，缺省为服务器的根目录，不区分大小写。

file filename: 指定用于远程配置回滚功能的缺省配置文件，不区分大小写，文件名后缀必须是“.cfg”。

【使用指导】

如果指定从远程 FTP 服务器下载配置文件并进行配置回滚，请保证本地配置和服务器端配置一致。如果 FTP 服务器端设置了登录用户的用户名和密码，请使用 **configuration replace server user** 命令配置登录 FTP 服务器的用户名、使用 **configuration replace server password** 命令配置登录 FTP 服务器的密码。

【举例】

```
# 指定配置文件的下载路径为 FTP 服务器（IPv4 地址为 192.168.1.1）的 archive/目录。  
<Sysname> system-view  
[Sysname] configuration replace server ftp 192.168.1.1 port 22 directory /archive/
```

【相关命令】

- **configuration replace server file**
- **configuration replace server password**
- **configuration replace server user**
- **display configuration replace server**

1.1.12 configuration replace server file

configuration replace server file 命令用来开启远程配置回滚功能。

undo configuration replace server file 命令用来关闭远程配置回滚功能。

【命令】

```
configuration replace server file [ filename ] [ at time [ date ] ]  
undo configuration replace server file
```

【缺省情况】

远程配置回滚功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

filename: 指定配置文件的文件名，其长度不能超过 255 个字符，文件名后缀必须是 “.cfg”。如果没有指定本参数，则使用 **configuration replace server** 命令指定的用于远程配置回滚功能的缺省配置文件。

at time: 指定下载配置文件并执行配置回滚的时间，格式为 HH:MM。HH 代表小时，取值范围为 0~23，MM 代表分钟，取值范围为 0~59。

date: 指定下载配置文件并执行配置回滚的日期，格式为 MM/DD/YYYY（月/日/年）或者 YYYY/MM/DD（年/月/日）。YYYY 的取值范围为 2000~2035，MM 的取值范围为 1~12，DD 的取值范围为 1~N，N 为当月的实际天数。

【使用指导】

如果没有指定开启远程配置回滚功能的时间，则立即开启本功能。如果开启定时远程配置回滚功能，在时间到达前，可以取消；如果开启立即远程配置回滚功能，则无法取消。

该命令会使设备立即或者在将来的某个时间点从配置回滚服务器上下载配置文件并执行配置回滚，可能导致业务中断，请谨慎使用。

指定的时间不能早于当前系统时间。如果修改了系统时间，且晚于所配置的开启远程配置回滚功能的时间，则配置失效。

如果没有指定 **date** 参数：

- 配置的时间点在当前系统时间之后，则设备将在当天的该时间点从远程配置回滚服务器下载配置文件并进行配置回滚。
- 配置的时间点在当前系统时间之前，则设备将在第二天的该时间点从远程配置回滚服务器下载配置文件并进行配置回滚。

使用 **configuration replace server** 命令指定从远程服务器下载配置文件时使用的参数后，执行本命令，会从远程服务器下载指定的配置文件，在本地保存为临时文件，并进行配置回滚。配置回滚完成后，删除该临时文件。

多次执行本命令，最后一次配置生效。

【举例】

手动从远程配置回滚服务器下载配置文件并进行配置回滚。

```
<Sysname> system-view
```

```
[Sysname] configuration replace server file my_archive_2017-05-09_14:20:18.cfg
```

```
The running configuration will be lost. Do you want to save the running configuration? [Y/N]:
```

```
N
```

```
Now replacing the running configuration...
```

```
Successfully replaced running configuration with file my_archive_2017-05-09_14:20:18.cfg.
```

【相关命令】

- **configuration replace server**

- **configuration replace server password**
- **configuration replace server user**

1.1.13 configuration replace server password

configuration replace server password 命令用来配置从远程 FTP 服务器下载配置文件时使用的密码。

undo configuration replace server password 命令用来恢复缺省情况。

【命令】

```
configuration replace server password { cipher | simple } string
undo configuration replace server password
```

【缺省情况】

未配置从远程 FTP 服务器下载配置文件时使用的密码。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

cipher: 表示以密文方式设置密码。

simple: 表示以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 33~117 个字符的字符串。

【举例】

配置从远程 FTP 服务器下载配置文件时使用的密码为 admin。

```
<Sysname> system-view
```

```
[Sysname] configuration replace server password simple admin
```

【相关命令】

- **configuration replace server**
- **configuration replace server file**
- **configuration replace server user**

1.1.14 configuration replace server user

configuration replace server user 命令用来配置从远程 FTP 服务器下载配置文件时使用的用户名。

undo configuration replace server user 命令用来恢复缺省情况。

【命令】

```
configuration replace server user user-name
```

undo configuration replace server user

【缺省情况】

未配置从远程 FTP 服务器下载配置文件时使用的用户名。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-name: 从远程 FTP 服务器下载配置文件时使用的用户名，为 1~63 个字符的字符串，区分大小写。

【使用指导】

如果没有配置从远程 FTP 服务器下载配置文件时使用的用户名，则使用匿名用户名“anonymous”。

【举例】

配置从远程 FTP 服务器下载配置文件时使用的用户名为 admin。

```
<Sysname> system-view
```

```
[Sysname] configuration replace server user admin
```

【相关命令】

- **configuration replace server**
- **configuration replace server file**
- **configuration replace server password**
- **display configuration replace server**

1.1.15 display archive configuration

display archive configuration 命令用来显示备份配置文件的相关信息。

【命令】

display archive configuration

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【使用指导】

如果当前配置为将配置文件备份到远程服务器，则显示远程备份的相关信息；如果当前配置为将配置文件备份到本地，则显示本地备份的相关信息。

【举例】

设置配置文件保存路径为本地，显示备份配置文件的相关信息。

```
<Sysname> display archive configuration
```

```
Location: flash:/archive
```

```
Filename prefix: my_archive
```

```
Archive interval in minutes: 120
```

```
Maximum number of archive files: 10
```

```
Archive history:
```

```
    No. TimeStamp          FileName
      1  Sat Oct 20 22:50:26 2018 my_archive_1.cfg
      2  Sat Oct 20 22:50:31 2018 my_archive_2.cfg
# 3  Sat Oct 20 22:50:35 2018 my_archive_3.cfg
```

The pound sign (#) indicates the most recent archive file.

```
Next archive file to be saved: my_archive_4.cfg
```

设置配置文件保存路径为远程服务器，显示备份配置文件的相关信息。

```
<Sysname> display archive configuration
```

```
Username: test
```

```
Location: ftp://192.168.21.21:21/archive
```

```
VPN instance: VPN1
```

```
Filename prefix: my_archive
```

```
Archive interval in minutes: 120
```

```
Archive history:
```

```
    No. TimeStamp          FileName
    ! 1  Thu Oct 18 14:23:51 2018 my_archive_20181018_142351.cfg
    ! 2  Sat Oct 20 22:46:44 2018 my_archive_20181020_224644.cfg
#! 3  Sat Oct 20 22:46:49 2018 my_archive_20181020_224649.cfg
```

The exclamation mark (!) indicates that the remote archiving attempt failed.

The pound sign (#) indicates the most recent archive file.

表1-1 display archive configuration 命令显示信息描述表

字段	描述
Username	登录远程FTP服务器的用户名，如果是TFTP服务器，则不显示此项
Location	保存备份配置文件的绝对路径
VPN instance	远程服务器所属的VPN实例
Filename prefix	保存备份配置文件的文件名前缀
Archive interval in minutes	自动备份配置文件的时间间隔，以分钟为单位 若不自动备份配置文件，不显示此项
Maximum number of archive files	设备可保存的最大备份配置文件数目
Archive history	配置文件的历史备份信息
No.	备份文件序号
TimeStamp	备份配置文件的保存时间
FileName	备份配置文件名，不包含路径

【相关命令】

- archive configuration
- archive configuration interval
- archive configuration location
- archive configuration max
- archive configuration server

1.1.16 display configuration replace server

display configuration replace server 命令用来显示远程配置回滚功能的相关信息。

【命令】

display configuration replace server

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

设备最多保存最近 10 次的远程配置回滚记录。

【举例】

显示远程配置回滚功能的相关信息。

```
<Sysname> display configuration replace server
```

```
Username: test
```

```
Location: ftp://192.168.21.21:22/test/
```

```
VPN instance: VPN1
```

```
Next replacement file: my_archive_20180509_143018.cfg
```

```
Next replacement time: 22:00 2018/6/12
```

```
Replacement history:
```

No.	Time	FileName
! 1	20:21:09 2018/10/18	my_archive_20180509_142018.cfg
! 2	20:25:00 2018/10/18	my_archive_20180509_143018.cfg
#! 3	22:52:23 2018/10/20	my_archive_20180509_144018.cfg

The exclamation mark (!) indicates that the remote replacing attempt failed.

The pound sign (#) indicates the most recent replacement file.

表1-2 display configuration replace server 命令显示信息描述表

字段	描述
Username	登录远程配置回滚服务器的用户名

字段	描述
Location	配置文件所在目录的绝对路径
VPN instance	远程服务器所属的VPN实例
Next replacement file	下一次执行远程配置回滚时使用的配置文件
Next replacement time	下一次执行远程配置回滚的时间，若没有指定远程配置回滚的时间，不显示此项
Replacement history	远程配置回滚的历史回滚信息
No.	远程配置回滚序号
Time	远程配置回滚的时间
Filename	执行远程配置回滚使用的配置文件的文件名，不包含路径

【相关命令】

- **configuration replace server**
- **configuration replace server file**
- **configuration replace server password**
- **configuration replace server user**

1.1.17 display current-configuration

display current-configuration 命令用来显示设备生效的配置。

【命令】

display current-configuration [**configuration** [*module-name*] | **interface** [*interface-type* [*interface-number*]] | **vpn-instance** [*vpn-instance-name*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

configuration [*module-name*]: 显示具体功能模块的配置信息，如果未指定 *module-name*，则显示所有功能模块的配置信息。

interface [*interface-type* [*interface-number*]]: 显示接口的配置。
interface-type 表示接口类型，*interface-number* 表示接口编号。如果未指定接口类型和接口编号，则显示所有接口的配置信息；如果仅指定接口类型，则显示所有该类型接口的配置信息。

vpn-instance [*vpn-instance-name*]: 显示与 VPN 实例相关的配置信息。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定 *vpn-instance-name*，则显示与所有 VPN 实例相关的配置信息。

【使用指导】

当用户完成一组配置之后，需要验证是否配置正确，则可以执行 **display current-configuration** 命令来查看当前生效的配置。对于某些参数，由于硬件或者规格限制，实际生效值和用户配置值不一致，则显示实际生效值。对于某些当前配置的参数，如果与缺省参数相同，则不显示。

执行 **display current-configuration vpn-instance [vpn-instance-name]** 命令，仅会显示 VPN 配置、绑定 VPN 的接口和路由协议配置等信息，如果要查看所有与 VPN 实例相关的配置信息，可以通过在 **display current-configuration** 命令中输入 **| include regular-expression** 参数的方式来过滤显示。

【举例】

查看设备上本地用户的相关配置。

```
<Sysname> display current-configuration configuration local-user
#
local-user ftp
  password simple 123
  service-type ftp
  authorization-attribute user-role network-operator
#
local-user root
  password simple admin
  service-type ssh telnet terminal
  authorization-attribute user-role network-admin
#
return
```

查看当前设备上以太网接口的相关配置。

```
<Sysname> display current-configuration interface gigabitethernet
#
interface GigabitEthernet1/0/1
  port link-mode route
#
return
```

1.1.18 display current-configuration diff

display current-configuration diff 命令用来显示下次启动配置文件与运行配置之间的差异。

【命令】

display current-configuration diff

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

context-admin
context-operator

【使用指导】

将下次启动配置文件和其他配置文件进行比较时：

- 优先使用主用下次启动配置文件。
- 如果主用下次启动配置文件不可用，则使用备用下次启动配置文件。
- 如果主用下次启动配置文件和备用下次启动配置文件都不可用，系统会给出相应的错误提示信息。

【举例】

显示下次启动配置文件与运行配置之间的差异。

```
<Sysname>display current-configuration diff
--- Startup configuration
+++ Current configuration
@@ -5,7 +5,7 @@
#
sysname Sysname
#
-alias dhc display history-command
+alias dh display hotkey
<Sysname>
```

表1-3 display current-configuration diff 和 display diff 命令显示信息描述表

字段	描述
--- A +++ B	• A 表示参与比较的源配置文件，可以是 Startup configuration、Current configuration 或者配置文件的名称。 • B 表示参与比较的目标配置文件，可以是 Startup configuration、Current configuration 或者配置文件的名称。 在这个例子中，Startup configuration表示参与比较的源配置文件，Current configuration表示参与比较的目标配置文件。
@@ -linenumber1,number1 +linenumber2,number2 @@	• -linenumber1,number1：表示从 A 中、行号为 linenumber1 的配置开始显示，共显示 number1 条 • +linenumber2,number2：表示从 B 中、行号为 linenumber2 的配置开始显示，共显示 number2 条
cmd1 - cmd2 + cmd3 cmd4	• cmd1、cmd4 表示 A 和 B 中都存在的配置，差异配置的上下文，用于定位差异配置 • - cmd2 表示该配置是 A 中的配置，B 中没有 • + cmd3 表示该配置是 B 中的配置，A 中没有 在这个例子中，从显示信息中可以看出，alias dhc display history-command 只存在于源配置文件中，alias dh display hotkey只存在于目标配置文件中，这是它们之间的差异。

【相关命令】

- display current-configuration

- **display diff**
- **display saved-configuration**

1.1.19 display default-configuration

display default-configuration 命令用来显示设备的出厂配置。

【命令】

display default-configuration

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

出厂配置可能与命令行的缺省情况不一致，设备会根据需要定制各自的出厂配置。

设备在出厂时，通常会带有一些基本的配置，称为出厂配置。它用来保证设备在没有配置文件或者配置文件损坏的情况下，能够正常启动、运行。

【举例】

```
# 显示设备的出厂配置。
<Sysname> display default-configuration
```

1.1.20 display diff

display diff 命令用来查看两份配置之间的差异。

【命令】

```
display diff configfile file-name-s { configfile file-name-d |
current-configuration | startup-configuration }
display diff current-configuration { configfile file-name-d |
startup-configuration }
display diff startup-configuration { configfile file-name-d |
current-configuration }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin

context-operator

【参数】

configfile file-name-s: 指定用于比较的源配置文件。*file-name-s* 为配置文件的名称。

configfile file-name-d: 指定用于比较的目标配置文件。*file-name-d* 为配置文件的名称。

current-configuration: 表示当前运行配置。在 **display diff current-configuration** 命令中, 本关键字表示当前运行配置为参与比较的源配置。在 **display diff configfile file-name-s** 命令和 **display diff startup-configuration** 命令中, 本关键字表示当前运行配置为参与比较的目标配置。

startup-configuration: 表示下次启动配置文件。在 **display diff startup-configuration** 命令中, 本关键字表示下次启动配置文件为参与比较的源配置文件。在 **display diff configfile file-name-s** 命令和 **display diff current-configuration** 命令中, 本关键字表示下次启动配置文件为参与比较的目标配置文件。

【使用指导】

将下次启动配置文件和其他配置文件进行比较时:

- 优先使用主用下次启动配置文件。
- 如果主用下次启动配置文件不可用, 则使用备用下次启动配置文件。
- 如果主用下次启动配置文件和备用下次启动配置文件都不可用, 系统会给出相应的错误提示信息。

【举例】

显示配置文件 startup.cfg 与 test.cfg 之间的差异。

```
<Sysname> display diff configfile startup.cfg configfile test.cfg
--- flash:/startup.cfg
+++ flash:/test.cfg
@@ -5,7 +5,7 @@
#
sysname Sysname
#
-alias dhc display history-command
+alias dh display hotkey
<Sysname>
```

以上显示信息表明: startup.cfg 文件中有配置 alias dhc display history-command, test.cfg 文件中有配置 alias dh display hotkey, 这就是它们之间的差异。

显示运行配置与下次启动配置文件之间的差异。

```
<Sysname> display diff current-configuration startup-configuration
--- Current configuration
+++ Startup configuration
@@ -5,7 +5,7 @@
#
sysname Sysname
#
-alias dhc display history-command
+alias dh display hotkey
<Sysname>
```

以上显示信息表明：运行配置中有 `alias dhc display history-command`，下次启动配置文件中配置 `alias dh display hotkey`，这就是它们之间的差异。

本命令显示信息的描述请参见 [表 1-3](#)。

【相关命令】

- `display current-configuration`
- `display current-configuration diff`
- `display saved-configuration`

1.1.21 display saved-configuration

`display saved-configuration` 命令用来查看下次启动配置文件的内容。

【命令】

`display saved-configuration`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

在管理/维护设备时可以使用该命令确认重要的配置是否已经保存到下次启动配置文件。

查看下次启动配置文件的内容时：

- 如果主用下次启动配置文件存在，执行该命令会显示主用下次启动配置文件的内容；
- 如果主用下次启动配置文件不存在，但备用下次启动配置文件存在，执行该命令会显示备用下次启动配置文件的内容；
- 如果主用和备用下次启动配置文件均不存在，执行该命令，则不显示任何信息。

【举例】

```
# 显示主用下次启动配置文件的内容。
<Sysname> display saved-configuration
#
version 7.1.070, Release 1201
#
sysname Sysname
#
ftp server enable
#
telnet server enable
#
domain default enable system
#
```

```
vlan 1
#
domain system
#
.....略.....
```

【相关命令】

- save
- reset saved-configuration

1.1.22 display startup

display startup 命令用来显示用于本次及下次启动的配置文件的名称。

【命令】

```
display startup
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【使用指导】

因为从设备是根据主设备的当前配置启动和运行的，所以 IRF 中所有成员设备显示的当前启动配置文件始终是相同的。

当主设备角色变更后，新的主设备没有从配置文件重启而是沿用当前的配置继续运行，使用 **display startup** 查看时，所有成员设备的当前启动配置文件均会显示为 NULL。

【举例】

```
# 显示本次及下次启动的配置文件名。
<Sysname> display startup
Current startup saved-configuration file: flash:/startup.cfg(*)
Next main startup saved-configuration file: flash:/startup.cfg
Next backup startup saved-configuration file: NULL
```

表1-4 display startup 命令显示信息描述表

字段	描述
Current startup saved-configuration file	当前启动使用的配置文件
Next main startup saved-configuration file	下一次启动时使用的主用配置文件
Next backup startup saved-configuration file	下一次启动时使用的备用配置文件

【相关命令】

- **startup saved-configuration**

1.1.23 display this

display this 命令用来显示当前视图下生效的配置。

【命令】

display this

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

当用户在某一视图下完成一组配置之后，需要验证是否配置成功，则可以执行 **display this** 命令来查看当前生效的配置。

有些已经生效的配置如果与缺省情况相同，则不显示。

对于某些参数，虽然用户已经配置，但如果这些参数所在的功能没有生效，则不显示。

在任意一个用户界面视图下执行此命令，将会显示所有用户线下生效的配置。

【举例】

```
# 显示接口 GigabitEthernet1/0/1 下生效的配置。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
#
return
```

1.1.24 reset saved-configuration

reset saved-configuration 命令用来删除设备存储介质中保存的下次启动配置文件。

【命令】

reset saved-configuration [backup | main]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

backup: 删除备用下次启动配置文件。

main: 删除主用下次启动配置文件。

【使用指导】

执行该命令会将配置文件从所有成员设备上彻底删除，所以请慎用该命令。

当用户不再使用当前系统指定的下次启动配置文件启动设备时，使用该功能可将下次启动配置文件从设备上删除。

如果设备的主备用下次启动配置文件相同，仅执行一次删除操作（例如指定了 **backup** 参数），系统只将相应的下次启动配置文件设置为 NULL，不删除该文件，需要再次执行删除操作（指定 **main** 参数），才能将该配置文件彻底删除。

不指定 **backup** 和 **main** 参数时，缺省使用 **main**。

【举例】

删除主用下次启动配置文件。

```
<Sysname> reset saved-configuration
```

```
The saved configuration file will be erased. Are you sure? [Y/N]:y
```

```
Configuration file in flash: is being cleared.
```

```
Please wait .....
```

```
Configuration file is cleared.
```

【相关命令】

- **display saved-configuration**

1.1.25 restore startup-configuration

restore startup-configuration 命令用于从 TFTP 服务器上下载配置文件并设置为设备的主用下次启动配置文件。

【命令】

```
restore startup-configuration from { ipv4-server | ipv6 ipv6-server }  
src-filename [ vpn-instance vpn-instance-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-server: TFTP 服务器的 IPv4 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

ipv6 ipv6-server: TFTP 服务器的 IPv6 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

src-filename: TFTP 服务器上将要下载的文件的文件名，其长度不能超过 255 个字符。

vpn-instance vpn-instance-name : 指定 TFTP 服务器所在的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 TFTP 服务器位于公网中。

【使用指导】

在执行该命令前，请保证设备与服务器之间的路由可达，服务器端开启了 TFTP 服务。

多台设备组成 IRF 环境下，执行该命令会将配置文件下载到所有成员设备存储介质的根目录下（对存储设备分区后，配置文件下载到存储设备的第一个分区），并设置为所有成员设备的主用下次启动配置文件。如果成员设备使用不同存储介质的情况（例如：主设备使用 Flash，从设备使用 U 盘），备份操作失败。

【举例】

从 IP 地址为 2.2.2.2 的 TFTP 服务器上下载 test.cfg 文件作为设备的下次启动配置文件。

```
<Sysname> restore startup-configuration from 2.2.2.2 test.cfg
Restoring the next startup-configuration file from 2.2.2.2...
Done.
```

从 IP 地址为 2.2.2.2 的 TFTP 服务器上下载 test.cfg 文件作为设备的下次启动配置文件，TFTP 服务器位于 VPN 实例（名称为 VPN1）中。

```
<Sysname> restore startup-configuration from 2.2.2.2 test.cfg vpn-instance VPN1
Restoring the next startup-configuration file from 2.2.2.2...
Done.
```

从 IPv6 地址为 2001::2 的 TFTP 服务器上下载 test.cfg 文件作为设备的下次启动配置文件。

```
<Sysname> restore startup-configuration from ipv6 2001::2 test.cfg
Restoring the next startup-configuration file from 2001::2...
Done.
```

【相关命令】

- **backup startup-configuration**

1.1.26 save

save file-url [all | slot slot-number] 命令用来将设备的当前配置保存到文件，但不会将该文件设置为下次启动配置文件。

save [safely] [backup | main] [force] [context-all | changed] 命令用来将当前配置保存到存储介质的根目录，并将该文件设置为下次启动配置文件。

【命令】

```
save file-url [ all | slot slot-number ]
```

```
save [ safely ] [ backup | main ] [ force ] [ context-all | changed ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

context-admin

【参数】

file-url: 文件路径, 必须以“.cfg”为后缀, 文件路径的总长度不能超过 255 个字符。当本参数和关键字 **all** 或者 **slot** 一起使用时, 本参数不能包含成员编号, 如果路径中包含了文件夹, 则必须先相应的成员设备上创建该文件夹, 否则本成员设备上的保存操作将失败。

all: 将当前配置以指定的名称保存到所有成员设备。不指定 **all** 和 **slot** 参数, 则保存到 Master 上。

slot slot-number: 将当前配置以指定的名称保存到指定从设备。**slot-number** 表示设备在 IRF 中的成员编号。不指定 **all** 和 **slot** 参数, 则保存到 Master 上。

safely: 以安全模式保存配置文件。如果不指定该参数, 表示以快速保存方式保存配置文件。

backup: 将该文件设置为备用下次启动配置文件。当不指定 **backup** 和 **main** 时, 系统缺省使用 **main**。

main: 将该文件设置为主用下次启动配置文件。当不指定 **backup** 和 **main** 时, 系统缺省使用 **main**。

force: 表示直接将当前配置保存到主用下次启动配置文件, 系统不再输出交互信息。缺省情况下, 用户执行 **save** 命令, 系统要求用户输入<Y>或<N>等参数来确认本次操作, 如果在 30 秒内没有确认, 系统会自动退出本次操作。如果在执行 **save** 操作时使用了 **force** 参数, 则系统会直接保存当前配置, 不再需要用户输入任何信息。

context-all: 将设备上所有 **context** 内的配置保存到插卡的文件系统中。不指定该参数时, 只保存用户当前登录的 **context** 的当前配置。

changed: 如果当前运行配置与目标配置文件相比较有修改, 则保存当前配置到设备目标配置文件中, 否则不执行保存配置操作。不指定该参数时, 无论配置是否修改都执行保存配置操作。

【使用指导】

当执行 **save** 命令时, 如果指定的文件名不存在, 则系统会先创建该文件, 再执行保存操作。如果指定的文件名存在, 则会提示用户是否覆盖该文件, 如果用户选择不覆盖, 则不会继续执行 **save** 命令。

执行 **save** 命令时, 如果不指定 **file-url** 参数, 设备将当前配置保存到存储介质的根目录, 并将该文件设置为下次启动配置文件; 如果指定 **file-url** 参数, 则设备仅将当前配置保存到指定文件。用户执行 **save** 命令保存配置时, 系统会自动生成一个文本类型的配置文件 (后缀名为“.cfg”, 可以通过 **more** 命令查看该文件的内容) 和一个二进制类型的配置文件 (后缀为“.mdb”, 仅软件能够解析该类配置文件, 而用户不能读取和编辑文件内容), 两个文件的内容完全相同, 设备启动时, 优先使用二进制类型的配置文件, 以便提高加载配置的速度。如果无二进制类型的配置文件, 则使用文本类型的配置文件。

当执行 **save [safely] [backup | main] [force] [context-all | changed]** 命令输入的文件名和设备上已存在的文件同名时:

- 如果使用了 **safely** 参数, 则系统会先将当前配置保存到一个临时文件, 保存成功后, 再用这个临时文件替换原同名文件。因此, 即使在保存过程中出现设备重启、断电等问题导致配置保存失败, 仍然能够以原同名的配置文件启动设备。
- 如果没有使用 **safely** 参数, 则会直接覆盖原同名文件。在保存过程中如果出现设备重启、断电、内存不足、设备存储空间不足等问题, 结果是当前配置保存失败, 原同名文件已删除, 下次启动文件为空。

因此, 为了安全起见, 在需要将当前配置保存到下次启动配置文件的时候, 建议选用 **safely** 参数。

【举例】

将当前配置文件保存到配置文件 **backup.cfg**，但不将该文件设置为下次启动配置文件。

```
<Sysname> save backup.cfg
The current configuration will be saved to flash:/backup.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration flash:/backup.cfg. Please wait...
Configuration is saved to device successfully.
```

直接将当前配置保存到主用下次启动配置文件，不再进行信息确认。

```
<Sysname> save force
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

将当前配置保存到存储介质的根目录，并将该文件设置为下次启动配置文件。

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/backup.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
Validating file. Please wait.....
Saved the current configuration to mainboard device successfully.
```

将当前配置保存到存储介质的根目录，并将该文件设置为下次启动配置文件。

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/backup.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
Validating file. Please wait.....
The current configuration adds 5 commands and deletes 2 commands.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
```

保存所有 **Context** 内的配置，并将该文件设置为下次启动配置文件。

```
<Sysname >save context-all
Save current configuration in all context? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration of context Admin to mainboard device successfully.
```

保存所有 **Context** 内的配置，并将该文件设置为下次启动配置文件。

```
<Sysname >save context-all
Save current configuration in all context? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The current configuration adds 5 commands and deletes 2 commands.
The startup.cfg file already exists. The save operation will overwrite the file.
Are you sure you want to continue the save operation? [Y/N]:y
Saved the current configuration of context Admin to mainboard device successfully.
```

【相关命令】

- **display current-configuration**
- **display saved-configuration**

1.1.27 startup saved-configuration

startup saved-configuration 命令用来配置下次启动配置文件（系统下次启动时使用的配置文件）。

undo startup saved-configuration 命令用来设置设备以出厂配置启动。

【命令】

startup saved-configuration *cfgfile* [**backup** | **main**]
undo startup saved-configuration

【缺省情况】

未配置下次启动配置文件。

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

cfgfile: 配置文件的路径、以及文件名，该文件必须是存储介质根目录下、后缀为.cfg 的文件，其长度不能超过 194 个字符。该参数只能为配置文件名称、或存储介质名称+配置文件名称。

backup: 将配置文件设置为备用下次启动配置文件。

main: 将配置文件设置为主用下次启动配置文件。设备优先使用主用下次启动配置文件，如果主用下次启动配置文件不存在或损坏，则使用备用下次启动配置文件。

【使用指导】

执行 **undo startup saved-configuration** 命令并重启 IRF 或 IRF 中的成员设备时，会导致 IRF 分裂，请谨慎使用。

所有成员设备的下次启动配置文件必须是相同的文件，因此，使用本命令前，请确保指定的配置文件已经保存在所有成员设备相同类型存储介质的根目录下，否则，操作失败。

不指定 **main** 和 **backup** 参数时，缺省使用 **main**。

主用下次启动配置文件和备用下次启动配置文件可以设置为同一文件，但为了更可靠，建议设置为不同的文件，或者将一份配置保存在两个不同名的文件中，一个设置为主用，一个设置为备用。

在执行 **undo startup saved-configuration** 命令之后，系统会将主用/备用下次启动配置文件均设置为 NULL，但不会删除该文件。

执行 **save** 命令将当前配置保存到存储介质的同时，可将该文件设置为下次启动时使用的主用、或备用配置文件。

【举例】

配置下次启动配置文件。

```
<Sysname> startup saved-configuration testcfg.cfg  
Please wait ..... Done.
```

【相关命令】

- **display startup**

目 录

1 软件升级	1-1
1.1 软件升级配置命令	1-1
1.1.1 boot-loader file	1-1
1.1.2 boot-loader update	1-3
1.1.3 bootrom backup	1-4
1.1.4 bootrom read	1-5
1.1.5 bootrom restore	1-6
1.1.6 bootrom update	1-6
1.1.7 bootrom-update security-check enable	1-7
1.1.8 display boot-loader	1-8

1 软件升级

如果将可插拔存储介质内的软件包指定为设备下次启动时使用的软件包，重启设备时不要将可插拔存储介质从设备上拔出，否则可能导致设备无法正常启动。建议将设备出厂时的缺省介质作为设备下次启动时使用软件包的存储位置。

1.1 软件升级配置命令

1.1.1 boot-loader file

boot-loader file 命令用来配置设备下次启动时使用的软件包。

【命令】

```
boot-loader file boot filename system filename [ feature filename<1-30> ]  
{ all | slot slot-number } { backup | main }  
boot-loader file ipe-filename { all | slot slot-number } { backup | main }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

boot: Boot 包。

system: System 包。

feature: Feature 包。

filename<1-30>: 软件包的名称，形如 *filesystemname/filename.bin*。该文件必须保存在设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，从存储介质名称开始最多可输入 63 个字符。**<1-30>**表示前面的参数最多可以输入 30 次。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

ipe-filename: IPE（Image Package Envelope，复合软件包套件）文件的名称，形如 *filesystemname/filename.ipe*。该文件必须保存在设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，从存储介质名称开始最多可输入 63 个字符。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

all: 指定系统中软件包适用的所有的硬件。

slot slot-number: 表示待升级的成员设备的编号。

backup: 指定该软件包为备用启动软件包。备用启动软件包用于主用启动软件包不可用或异常情况时，引导设备启动。

main: 指定该软件包为主用启动软件包。主用启动软件包用于引导设备启动。

【使用指导】

成功执行该命令后，系统会用命令中指定的软件包替换现有的软件包列表。如果命令行中没有指定 **Feature** 包，则更新后的软件包列表中不会有 **Feature** 包。

请先查看软件包版本发布说明书，如果软件包需要 **License** 才能运行，且设备当前没有对应的有效的 **License** 时，需安装对应的 **License**，再执行该命令。否则：

- 当使用软件包配置该命令时，只要指定某个的软件包当前没有有效的 **License**，就会导致整条命令配置失败。
- 当使用 **IPE** 文件配置该命令时，只有当前没有有效的 **License** 的软件包配置失败，其它软件包会配置成功。

需要重启系统来完成指定下次启动软件包的加载。

系统会自动检查指定 **slot** 上对应路径下是否存在同名文件，如果不存在，则直接从指定路径拷贝一份并设置为下次启动软件包；如果存在，则提示用户是否从指定路径拷贝一份并设置为下次启动软件包。

本命令不支持安装叠加补丁。

【举例】

配置指定 **slot** 下次启动时所用的主用启动文件为 **flash:/all.ipe**。

```
<Sysname> boot-loader file flash:/all.ipe slot 1 main
Verifying the file flash:/all.ipe on slot 1.....Done.
UNIS T1000-G20 images in IPE:
    boot.bin
    system.bin
This command will set the main startup software images. Continue? [Y/N]:Y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:Y
Decompressing file boot.bin to flash:/boot.bin.....Done.
Decompressing file system.bin to flash:/system.bin.....Done.
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1.....Done.
The images that have passed all examinations will be used as the main startup software images
at the next reboot on slot 1.
```

配置 **IRF** 的主用下次启动软件为 **flash:/all.ipe**。

```
<Sysname> boot-loader file slot1#flash:/all.ipe all main
Verifying the file flash:/all.ipe on slot 1.....Done.
UNIS T1000-G20 images in IPE:
    Boot.bin
    System.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
File flash:/Boot.bin already exists on slot 1.
File flash:/System.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:y
Decompressing file Boot.bin to flash:/Boot.bin.....Done.
Decompressing file System.bin to flash:/System.bin.....Done.
```

```

The images that have passed all examinations will be used as the main startup software images
at the next reboot on slot 1.
File flash:/Boot.bin already exists on slot 2.
Do you want to overwrite the file?
Y: Overwrite the file.
N: Not overwrite the file.
A: From now on, overwrite or not overwrite without prompt.
Please make a choice. [Y/N/A]:a
What type of overwrite operation do you want to perform?
Y: Overwrite without prompt.
N: Not overwrite or display prompt.
Q: Return to the previous step.
Please make a choice. [Y/N/Q]:y
An existing file will be overwritten without prompt if it has the same name as any upgrade
file.
Loading.....Done.
Loading.....Done.
Loading.....Done.
Loading.....Done.
Loading.....Done.
Loading.....Done.
The images that have passed all examinations will be used as the main startup software images
at the next reboot on slot 2.
The images that have passed all examinations will be used as the main startup software images
at the next reboot on slot 3.
Decompression completed.
Do you want to delete flash:/all.ipe now? [Y/N]:n

```

【相关命令】

- **display boot-loader**

1.1.2 boot-loader update

boot-loader update 命令用来实现当前软件版本的自动同步。

【命令】

```
boot-loader update { all | slot slot-number }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

all: 表示同步升级所有备设备。

slot slot-number: 表示待升级的成员设备的编号。

【使用指导】

对于新增的 IRF 成员设备，可以使用本命令同步启动软件包。

请先查看软件包版本发布说明书，如果软件包需要 License 才能运行，且设备当前没有对应的有效的 License 时，需安装对应的 License，再执行该命令。否则，会导致命令执行失败。

通过该命令指定从设备的下次启动软件包时，系统会进行如下处理：

- 如果主设备当前是使用主用启动软件包列表启动的，则将其主用下次启动软件包列表中的软件包拷贝到从设备的对应目录下，并设置为从设备的主用下次启动软件包。如果这些软件包中有任一软件包不存在或者不可用，则命令执行失败。
- 如果主设备当前是使用备用启动软件包列表启动的，则将其备用下次启动软件包列表中的软件包拷贝到从设备的对应目录下，并设置为从设备的主用下次启动软件包。如果这些软件包中有任一软件包不存在或者不可用，则命令执行失败。

如果主设备刚安装了补丁或者进行了 ISSU 升级，在执行本命令前，请执行 **install commit** 命令刷新主设备的下次启动软件包列表。否则，可能导致从设备升级后与主设备的版本不一致。

执行本命令时，请不要重启任何成员设备，以免设备不能正常启动。

【举例】

同步指定 slot 的软件版本。

```
<Sysname> boot-loader update slot 1
```

```
This command will update the specified standby MPU. Please do not reboot any MPU during the upgrade. Continue? [Y/N]:y
```

```
Updating. Please wait...
```

```
Verifying the file flash:/BOOT.bin on slot 1.....Done.
```

```
Verifying the file flash:/SYSTEM.bin on slot 1.....Done.
```

```
Successfully updated the startup software images of all the standby MPU.
```

【相关命令】

- **display boot-loader**
- **install commit**（基础配置命令参考/ISSU）

1.1.3 bootrom backup

bootrom backup 命令用来将 BootWare 程序从 BootWare 的 Normal 区备份到 Backup 区。

【命令】

```
bootrom backup slot slot-number-list [ all | part ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number-list：成员编号列表，表示同时备份多个成员设备的 BootWare 程序。表示方式为 **slot-number-list = { slot-number [to slot-number] }&<1-7>**。其中，**slot-number** 表示需要备份的设备在 IRF 中的成员编号。

all：操作 BootWare 程序的全部内容。不指定 **all** 和 **part** 参数时，默认使用 **all**。

part: 只操作 BootWare 程序的扩展段（BootWare 程序分为两部分：基本段和扩展段，基本段提供 BootWare 菜单的基本操作项，扩展段提供更多的 BootWare 菜单操作项）。不指定 **all** 和 **part** 参数时，默认使用 **all**。

【使用指导】

BootWare 分为 Normal 区和 Backup 区：

- Normal 区用于存放 BootWare 程序。设备启动时，会自动读取 Normal 区的 BootWare 程序。如果 Normal 区的 BootWare 程序不可用，再自动读取 Backup 区的 BootWare 程序。
- Backup 区用于存放 BootWare 程序的副本。如果在设备运行过程中，Normal 区的 BootWare 程序被损坏或者需要版本回退，可以使用 **bootrom restore** 命令将 BootWare 程序从 Backup 区恢复到 Normal 区。

【举例】

将 BootWare 程序从 BootWare 的 Normal 区备份到 Backup 区。

```
<Sysname> bootrom backup slot 1
Now backing up the Boot ROM, please wait...
.....Done.
```

【相关命令】

- **bootrom restore**

1.1.4 bootrom read

bootrom read 命令用来将 BootWare 程序从 BootWare 的 Normal 区读取到缺省文件系统中。

【命令】

bootrom read slot slot-number-list [all | part]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number-list: 成员编号列表，表示同时读取多个成员设备的 BootWare 程序。表示方式为 *slot-number-list* = { *slot-number* [**to** *slot-number*] }&<1-7>。其中，*slot-number* 表示需要读取的设备在 IRF 中的成员编号。

all: 操作 BootWare 程序的全部内容。不指定 **all** 和 **part** 参数时，默认使用 **all**。

part: 只操作 BootWare 程序的扩展段。不指定 **all** 和 **part** 参数时，默认使用 **all**。

【使用指导】

成功执行本命令后，系统会自动生成 **basicbtm.bin** 和 **extendbtm.bin** 文件并保存到缺省文件系统中。其中，**basicbtm.bin** 存储了 BootWare 程序的基本段，**extendbtm.bin** 存储了 BootWare 程序的扩展段。

【举例】

读取 BootWare 程序。

```
<Sysname> bootrom read slot 1
Now reading the Boot ROM, please wait...
.....Done.
```

【相关命令】

- **bootrom update**

1.1.5 bootrom restore

bootrom restore 命令用来将 BootWare 程序从 BootWare 的 Backup 区恢复到 Normal 区。

【命令】

```
bootrom restore slot slot-number-list [ all | part ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number-list: 成员编号列表，表示同时恢复多个成员设备的 BootWare 程序。表示方式为 *slot-number-list* = { *slot-number* [**to** *slot-number*] }&<1-7>。其中，*slot-number* 表示需要恢复的设备在 IRF 中的成员编号。

all: 操作 BootWare 程序的全部内容。不指定 **all** 和 **part** 参数时，默认使用 **all**。

part: 只操作 BootWare 程序的扩展段。不指定 **all** 和 **part** 参数时，默认使用 **all**。

【举例】

恢复 BootWare 程序。

```
<Sysname> bootrom restore slot 1
This command will restore the Boot ROM file on the specified board(s), Continue? [Y/N]:y
Now restoring the Boot ROM, please wait...
.....Done.
```

【相关命令】

- **bootrom backup**

1.1.6 bootrom update

bootrom update 命令用来将文件系统中的 BootWare 程序加载到 BootWare 的 Normal 区。

【命令】

```
bootrom update file file slot slot-number-list [ all | part ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

file file: 文件系统中包含 BootWare 程序的文件，*file* 表示用于 BootWare 程序升级的文件名称，为 1~63 个字符的字符串。

slot slot-number-list: 成员编号列表，表示同时升级多个成员设备的 BootWare 程序。表示方式为 *slot-number-list* = { *slot-number* [**to** *slot-number*] }&<1-7>。其中，*slot-number* 表示需要升级的设备在 IRF 中的成员编号。

all: 操作 BootWare 程序的全部内容。不指定 **all** 和 **part** 参数时，默认使用 **all**。

part: 只操作 BootWare 程序的扩展段。不指定 **all** 和 **part** 参数时，默认使用 **all**。

【使用指导】

BootWare 程序通过 *.btw 文件发布，产品会将需要升级的设备的 BootWare 程序集成到 Boot 包中。此时可以使用本命令将升级文件指定为 Boot 包，系统会根据设备的型号自动将相应的 BootWare 程序加载到 BootWare 中；也可以在升级 Boot 包的同时完成 BootWare 程序的加载。

执行该命令后，设备会将文件系统中的 BootWare 程序加载到 BootWare 的 Normal 区。设备启动时，会直接使用 Normal 区的 BootWare 程序。因此，如果文件系统空间不足，BootWare 程序加载完成之后，BootWare 文件可以删除。

加载后，要使新的 BootWare 程序生效，需要重启设备。

【举例】

使用 Flash 根目录下的 a.bin 文件升级设备的 BootWare 程序。

```
<Sysname> bootrom update file flash:/a.bin slot 1
```

```
This command will update the Boot ROM file on the specified board(s), Continue? [Y/N]:y  
Now updating the Boot ROM, please wait.....Done.
```

【相关命令】

- **boot-loader file**

1.1.7 bootrom-update security-check enable

bootrom-update security-check enable 命令用来开启 BootWare 程序合法性检查功能。

undo bootrom-update security-check enable 命令用来关闭 BootWare 程序合法性检查功能。

【命令】

bootrom-update security-check enable

undo bootrom-update security-check enable

【缺省情况】

BootWare 程序合法性检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

如果开启了本功能，则在升级 BootWare 程序时，设备会先检查 BootWare 文件的合法性：包括 BootWare 文件是否有效以及是否和硬件匹配等。检查通过后，才会升级。

【举例】

```
# 启动 BootWare 升级时的合法性检查功能。
<Sysname> system-view
[Sysname] bootrom-update security-check enable
```

1.1.8 display boot-loader

display boot-loader 命令用来显示本次启动和下次启动所采用的启动软件包的名称。

【命令】

```
display boot-loader [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

slot slot-number：表示成员设备的编号。不指定该参数时，表示 IRF 中的所有成员设备。

【举例】

```
# 显示本次启动和下次启动所采用的启动软件包的名称。
<Sysname> display boot-loader
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
  flash:/boot.bin
  flash:/system.bin
```

表1-1 display boot-loader 命令显示信息描述表

字段	描述
Software images	启动软件包的相关信息
Current software images	最近一次启动使用的启动软件包列表
Main startup software images	主用下次启动软件包列表

字段	描述
Backup startup software images	备用下次启动软件包列表

【相关命令】

- **boot-loader file**

目 录

1 ISSU	1-1
1.1 ISSU配置命令	1-1
1.1.1 display install active	1-1
1.1.2 display install backup	1-3
1.1.3 display install committed	1-4
1.1.4 display install inactive	1-6
1.1.5 display install ipe-info	1-7
1.1.6 display install job	1-7
1.1.7 display install log	1-8
1.1.8 display install package	1-9
1.1.9 display install rollback	1-10
1.1.10 display install which	1-11
1.1.11 display issu rollback-timer	1-13
1.1.12 display issu state	1-14
1.1.13 display version comp-matrix	1-16
1.1.14 install abort	1-18
1.1.15 install activate	1-18
1.1.16 install add	1-21
1.1.17 install commit	1-22
1.1.18 install deactivate	1-23
1.1.19 install remove	1-24
1.1.20 install rollback to	1-24
1.1.21 install verify	1-26
1.1.22 issu accept	1-27
1.1.23 issu commit	1-27
1.1.24 issu load	1-29
1.1.25 issu rollback	1-32
1.1.26 issu rollback-timer	1-33
1.1.27 issu run switchover	1-34
1.1.28 reset install log-history oldest	1-35
1.1.29 reset install rollback oldest	1-36

1 ISSU

1.1 ISSU配置命令

1.1.1 display install active

display install active 命令用来显示当前系统中处于激活状态的软件包的相关信息。

【命令】

display install active [*slot slot-number*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示 IRF 中的所有成员设备。

verbose: 显示处于激活状态的软件包的详细信息，包括软件包的名称、基本信息和所包含的组件。不指定该参数时，仅显示软件包的名称。

【举例】

显示设备上处于激活状态的软件包的简要信息。

```
<Sysname> display install active
```

```
Active packages on slot 1:
```

```
flash:/boot.bin  
flash:/system.bin  
flash:/feature1.bin
```

显示设备上处于激活状态的软件包的详细信息。

```
<Sysname> display install active verbose
```

```
Active packages on slot 1:
```

```
flash:/boot.bin  
[Package]  
Vendor: UNIS  
Product: xxxx  
Service name: boot  
Platform version: 7.1.070  
Product version: Test 0001015  
Supported board: mpu  
[Component]  
Component: boot  
Description: boot package
```


flash:/system.bin
[Package]
Vendor: UNIS
Product: xxxx
Service name: system
Platform version: 7.1.070
Product version: Test 0001015
Supported board: mpu
[Component]
Component: system
Description: system package

flash:/feature1.bin
[Package]
Vendor: UNIS
Product: xxxx
Service name: test
Platform version: 7.1.070
Product version: Test 0001015
Supported board: mpu
[Component]
Component: test
Description: test package

表1-1 display install active 命令显示信息描述表

字段	描述
Active packages on the device	处于激活状态的软件包的相关信息
flash:/boot.bin	软件包的名称
[Package]	软件包的信息
Vendor	生产厂商
Product	产品名称
Service name	软件包所包含的服务名称： - 如果显示为 boot，表示该软件包为 Boot 包 - 如果显示为 system，表示该软件包为 System 包 - 如果显示为 boot patch，表示该软件包为 Boot 包的补丁包；如果显示为 system patch，表示该软件包为 System 包的补丁包 - 如果显示为其它值，则表示该软件包为提供某项功能的 Feature 包
Platform version	平台软件版本号
Product version	产品软件版本号
Supported board	软件包支持的硬件类型： mpu 表示成员设备
[Component]	组件信息，表示软件包的组成部分

字段	描述
Component	组件的名称
Description	组件的描述信息

【相关命令】

- **install active**

1.1.2 display install backup

display install backup 命令用来显示设备下次启动时使用的备用软件包的相关信息。

【命令】

display install backup [*slot slot-number*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示 IRF 中的所有成员设备。

verbose: 显示详细信息，包括软件包的名称、基本信息和所包含的组件。不指定该参数时，仅显示软件包的名称。

【使用指导】

当主用启动软件包列表中的 **Boot** 包或 **System** 包不存在或者损坏时，使用备用启动软件包列表中的软件包。有关设备下次启动时使用的软件包的详细介绍请参见“基础配置指导”中的“软件升级”。

执行 **boot-loader file** 命令可以修改设备下次启动时使用的备用软件包列表。

【举例】

显示设备下次启动时使用的备用软件包的相关信息。

```
<Sysname> display install backup
Backup startup software images on slot 1:
  flash:/boot.bin
  flash:/system.bin
```

显示设备下次启动时使用的备用软件包的详细信息。

```
<Sysname> display install backup verbose
Backup startup software images on slot 1:
  flash:/boot.bin
  [Package]
  Vendor: UNIS
  Product: xxxx
  Service name: boot
```

```
Platform version: 7.1.070
Product version: Test 0001015
Supported board: mpu
[Component]
Component: boot
Description: boot package
```

```
flash:/system.bin
[Package]
Vendor: UNIS
Product: xxxx
Service name: system
Platform version: 7.1.070
Product version: Test 0001015
Supported board: mpu
[Component]
Component: system
Description: system package
```

本命令显示信息的描述请参见 [表 1-1](#)。

【相关命令】

- **boot-loader file**（基础配置命令参考/软件升级）
- **display install committed**

1.1.3 display install committed

display install committed 命令用来显示设备下次启动时使用的主用软件包的相关信息。

【命令】

```
display install committed [ slot slot-number ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示 IRF 中的所有成员设备。

verbose: 显示详细信息，包括软件包的名称、基本信息和所包含的组件。不指定该参数时，仅显示软件包的名称。

【使用指导】

某些 **install** 命令可以修改设备的软件包列表，但需要执行 **install commit** 命令来确认运行当前的软件包，这些软件包才会被列入主用下次启动软件包，使得设备重启后，这些软件包能够继续生效。可以使用本命令查看已被确认为下次启动的软件包。

执行 **install commit** 和 **boot-loader file** 命令都可以修改设备下次启动时使用的主用软件包列表。

【举例】

显示设备下次启动时使用的主用软件包的相关信息。

```
<Sysname> display install committed
```

```
Committed packages on slot 1:
```

```
flash:/boot.bin
```

```
flash:/system.bin
```

```
flash:/feature1.bin
```

显示设备下次启动时使用的主用软件包的详细信息。

```
<Sysname> display install committed verbose
```

```
Committed packages on slot 1:
```

```
flash:/boot.bin
```

```
[Package]
```

```
Vendor: UNIS
```

```
Product: xxxx
```

```
Service name: boot
```

```
Platform version: 7.1.070
```

```
Product version: Test 0001015
```

```
Supported board: mpu
```

```
[Component]
```

```
Component: boot
```

```
Description: boot package
```

```
flash:/system.bin
```

```
[Package]
```

```
Vendor: UNIS
```

```
Product: xxxx
```

```
Service name: system
```

```
Platform version: 7.1.070
```

```
Product version: Test 0001015
```

```
Supported board: mpu
```

```
[Component]
```

```
Component: system
```

```
Description: system package
```

```
flash:/feature1.bin
```

```
[Package]
```

```
Vendor: UNIS
```

```
Product: xxxx
```

```
Service name: feature1
```

```
Platform version: 7.1.070
```

```
Product version: Test 0001015
```

```
Supported board: mpu
```

```
[Component]
```

```
Component: feature1
```

```
Description: feature1 package
```

本命令显示信息的描述请参见 [表 1-1](#)。

【相关命令】

- **boot-loader file**（基础配置命令参考/软件升级）
- **display install backup**
- **install commit**

1.1.4 display install inactive

display install inactive 命令用来显示文件系统根目录下没有被激活的所有软件包的相关信息。

【命令】

display install inactive [*slot slot-number*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示 IRF 中的所有成员设备。

verbose: 显示详细信息，包括软件包的名称、基本信息和所包含的组件。不指定该参数时，仅显示软件包的名称。

【举例】

显示文件系统根目录下没有被激活的所有软件包的简要信息。

```
<Sysname> display install inactive
Inactive packages on slot 1:
  flash:/feature1.bin
```

显示文件系统根目录下没有被激活的所有软件包的详细信息。

```
<Sysname> display install inactive verbose
Inactive packages on slot 1:
flash:/feature1.bin
[Package]
Vendor: UNIS
Product: xxxx
Service name: feature1
Platform version: 7.1.070
Product version: Test 0001015
Supported board: mpu
[Component]
Component: feature1
Description: feature1 package
```

本命令显示信息的描述请参见 [表 1-1](#)。

【相关命令】

- **install deactivate**

1.1.5 display install ipe-info

display install ipe-info 命令用来显示 IPE 文件包含的软件包列表。

【命令】

display install ipe-info *ipe-filename*

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ipe-filename: 表示 IPE 文件的名称，形如 *filesystemname/filename.ipe*。该文件必须保存在设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，从存储介质名称开始最多可输入 63 个字符。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

【使用指导】

IPE 文件是一个或多个软件包的集合。用户获得 IPE 文件后，可以选择其中的软件包进行升级。

【举例】

```
# 显示 flash:/test.ipe 的 IPE 信息。
<Sysname> display install ipe-info flash:/test.ipe
Verifying the file flash:/test.ipe on slot 1.....Done.
XX images in IPE:
    boot.bin
    system.bin
```

【相关命令】

- **display install package**

1.1.6 display install job

display install job 命令用来显示系统中正在执行的激活、卸载或回滚操作。

【命令】

display install job

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示系统中正在执行的激活、卸载、回滚操作。

```
<Sysname> display install job
```

```
JobID:5
```

```
Action:install activate flash:/feature1.bin on slot 1
```

以上显示信息表明：设备正在执行 **install activate flash:/feature1.bin slot 1** 操作。

1.1.7 display install log

display install log 命令用来显示与 ISSU 升级相关的日志。

【命令】

```
display install log [ log-id ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

log-id：显示指定升级日志的信息。*log-id* 表示升级日志的编号，不指定该参数时，则显示所有 ISSU 升级日志的信息。

verbose：显示日志的详细信息。不指定该参数时，仅显示日志的摘要信息。

【使用指导】

ISSU 日志记录了软件包历史操作信息，每当用户执行一次安装、升级、卸载、删除、取消或回滚操作时，都会自动产生一条日志信息，记录下该操作的过程，以及操作结果是成功还是失败。每条日志均分配一个全局唯一的 ID。

设备最多可保存 50 条 ISSU 日志，达到该规格时新日志会覆盖最老的日志。

【举例】

显示所有显示与软件包升级相关的日志。

```
<Sysname> display install log
```

```
Install job 1 started by user root at 04/28/2001 08:39:29.
```

```
Job 1 completed successfully at 04/28/2001 08:39:30.
```

```
Install job 1 started by user root at 04/28/2001 08:39:29.
```

```
Install activate flash:/feature1.bin on slot 1
```

```
Job 1 completed successfully at 04/28/2001 08:39:30.
```

```
Install job 1 started by user root at 04/28/2001 08:39:29.
```

```
Job 1 completed successfully at 04/28/2001 08:39:30.
```

```
-----
```

```
Install job 2 started by user root at 04/28/2001 08:40:29.
```

```
Job 2 completed successfully at 04/28/2001 08:40:30.
```

```
Install job 2 started by user root at 04/28/2001 08:40:29.
```

```

Install activate flash:/route.bin on slot 1
Job 2 completed successfully at 04/28/2001 08:40:30.
Install job 2 started by user root at 04/28/2001 08:40:29.
Job 2 completed successfully at 04/28/2001 08:40:30.
# 显示系统中编号为 1 的软件包升级日志的详细信息。
<Sysname> display install log 1 verbose
Install job 1 started by user root at 04/28/2001 08:39:29.
Job 1 completed successfully at 04/28/2001 08:39:30.
Install job 1 started by user root at 04/28/2001 08:39:29.
Install activate flash:/feature1.bin on slot 1
Job 1 completed successfully at 04/28/2001 08:39:30.
Install job 1 started by user root at 04/28/2001 08:39:29.
Job 1 completed successfully at 04/28/2001 08:39:30.

```

```

Detail of activating packages on slot 1.
Get upgrade policy successfully.

```

```

Detail of activating packages on slot 1.
Uncompress package to system successfully.
Remove files from system successfully.

```

表1-2 display install log 命令显示信息描述表

字段	描述
Install job 1 started by user root at 04/28/2001 08:39:29.	ISSU动作的执行者和执行时间
Job 1 completed successfully at 04/28/2001 08:39:30.	ISSU动作的完成时间
Install activate flash:/feature1.bin	执行的ISSU动作
Detail of activating packages	激活包动作的详细信息
Get upgrade policy successfully	表示升级决策处理成功
Uncompress package to system successfully	解压软件包文件到系统成功
Remove files from system successfully	从系统中删除文件成功

【相关命令】

- **reset install log-history oldest**

1.1.8 display install package

display install package 命令用来显示软件包的相关信息。

【命令】

display install package { filename | all } [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

filename: 软件包的名称，形如 *filesystemname/filename.bin*。该文件必须保存在设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，从存储介质名称开始最多可输入 63 个字符。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

all: 表示主设备上各文件系统根目录下的所有软件包。

verbose: 显示软件包的基本信息和软件包所包含的组件。不指定该参数时，仅显示软件包的基本信息。

【举例】

显示软件包 **system.bin** 的相关信息。

```
<Sysname> display install package flash:/system.bin
flash:/system.bin
[Package]
Vendor: UNIS
Product: xxxx
Service name: system
Platform version: 7.1.070
Product version: Test 0001015
Supported board: mpu
Software image signature: HPE
```

显示软件包 **system.bin** 的详细信息。

```
<Sysname> display install package flash:/system.bin verbose
flash:/system.bin
[Package]
Vendor: UNIS
Product: xxxx
Service name: system
Platform version: 7.1.070
Product version: Test 0001015
Supported board: mpu
[Component]
Component: system
Description: system package
Software image signature: HPE
```

本命令显示信息的描述请参见 [表 1-1](#)。

1.1.9 display install rollback

display install rollback 命令用来显示回滚点的相关信息。

【命令】

display install rollback [*point-id*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

point-id: 回滚点的编号。如果未指定 *point-id*，则显示所有回滚点的相关信息。

【使用指导】

可以通过这个命令查看回滚点信息，以便进行相应的回滚操作。
issu 命令升级过程中不会记录回滚点，因此，在 issu 命令升级过程中执行该命令，没有信息可显示。

【举例】

显示所有回滚点的相关信息。

```
<Sysname> display install rollback
Install rollback information 1 on slot 1:
  Updating from flash:/route-1.bin
    to flash:/route-2.bin.

Install rollback information 2 on slot 1:
  Deactivating flash:/route-2.bin
```

以上显示信息表明：设备上共有两个回滚点，回滚点 1 是将 flash:/route-1.bin 升级至 flash:/route-2.bin，回滚点 2 是卸载 flash:/route-2.bin。

表1-3 display install rollback 命令显示信息描述表

字段	描述
Install rollback information <i>n</i>	回滚点信息， <i>n</i> 为回滚点编号
Updating from <i>A</i> to <i>B</i>	从软件包 <i>A</i> 升级到软件包 <i>B</i> ， <i>A</i> 和 <i>B</i> 为软件包的名称
Deactivating <i>A</i>	卸载软件包 <i>A</i> ， <i>A</i> 为软件包的名称

【相关命令】

- install rollback
- reset install rollback oldest

1.1.10 display install which

display install which 命令用来显示一个组件或文件的所属软件包，以及该软件包的相关信息。

【命令】

display install which { component *name* | file *filename* } [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

component name: 软件包所包含的组件的名称。
file filename: 软件包所包含的文件的名称，为 1~63 个字符的字符串，不区分大小写。必须为纯文件名的形式。
slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示 IRF 中的所有成员设备。

【使用指导】

组件是特性的集合，组件中的特性是同时安装/卸载的。
当软件包运行错误，系统提示 xx 组件或者 xx 文件运行错误的时候，可以根据组件名/文件名使用该命令查找它属于哪个软件包，从而帮助进一步定位是否是软件包本身有缺陷。通过检验该软件包，定位是否为软件包的问题。使用 **install verify** 命令可以对软件包进行检验。
执行该命令后，系统会扫描指定位置的所有文件系统根目录下的所有软件包，将包含该组件/文件的软件包都依次显示。

【举例】

```
# 显示文件 pkg_ctr 属于哪个软件包以及该软件包的相关信息。  
<Sysname> display install which file pkg_ctr  
Verifying the file flash:/system-t0001015.bin on slot 1.....Done.  
Found pkg_ctr in flash:/system-t0001015.bin on slot 1.  
  flash:/system-t0001015.bin  
  [Package]  
  Vendor: UNIS  
  Product: xxxx  
  Service name: system  
  Platform version: 7.1.070  
  Product version: Test 0001015  
  Supported board: mpu  
  
Verifying the file flash:/boot-d2601007.bin on slot 1.....Done.
```

表1-4 display install which 命令显示信息描述表

字段	描述
Verifying the file	验证文件是否合法
Found pkg_ctr	找到文件
[Package]	软件包的信息
Vendor	生产厂商

字段	描述
Product	产品名称
Service name	软件包所包含的服务名称： • 如果显示为 boot，表示该软件包为 Boot 包 • 如果显示为 system，表示该软件包为 System 包 • 如果显示为 patch，表示该软件包为补丁包 • 如果显示为其它值，则表示该软件包为提供某项功能的 Feature 包
Platform version	平台软件版本号
Product version	产品软件版本号
Supported board	软件包支持的硬件类型： • mpu 表示成员设备
File xxx was not found in the image packages under the root directory of the storage medium	在存储介质根目录下的所有包中都没有找到指定文件

1.1.11 display issu rollback-timer

display issu rollback-timer 命令用来显示回滚定时器的相关信息。

【命令】

display issu rollback-timer

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

因为新设置的回滚定时器时长会在下次 ISSU 升级中生效，因此，可能出现剩余时间大于定时器时长的情况。

【举例】

执行 **issu run switchover** 命令后，显示回滚定时器的相关信息。

```
<Sysname> display issu rollback-timer
Rollback timer: Working
Rollback interval: 45 minutes
Rollback time remaining : 40 minutes
```

执行 **issu accept** 命令后，显示回滚定时器的相关信息。

```
<Sysname> display issu rollback-timer
Rollback timer: Not working
Rollback interval: 30 minutes
```

当前没有进行 ISSU 升级，显示回滚定时器的相关信息。

```
<Sysname> display issu rollback-timer
Rollback timer: Not working
Rollback interval: 45 minutes
```

表1-5 display issu rollback-timer 命令显示信息描述表

字段	描述
Rollback timer	回滚定时器是否处于工作状态： - Working: 回滚定时器已经启动 - Not working: 回滚定时器没有启动或者已经超时
Rollback interval	用户配置的回滚定时器的时间，单位为分钟
Rollback time remaining	距离回滚定时器超时的时间，单位为分钟

【相关命令】

- **issu rollback-timer**

1.1.12 display issu state

display issu state 命令用来显示当前 ISSU 升级所处的状态，以及 ISSU 升级的相关信息。

【命令】

```
display issu state
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

issu 命令升级需要经过一系列的操作步骤，升级过程中有严格的步骤要求，执行升级步骤会导致 ISSU 状态的变化，通过该命令的显示信息可以帮助管理员确定下一步需执行的操作。

该命令不能显示 **install** 命令升级过程中设备所处的状态，因为 **install** 命令升级过程没有用到状态机。

【举例】

当前设备没有 ISSU 升级，显示 ISSU 状态。

```
<Sysname> display issu state
ISSU state: Init
Compatibility: Unknown
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot: None
```

```
Current version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
  feature1: 7.1.070, Test 0001015
Current software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
# issu load 命令执行过程中，显示 ISSU 状态。
<Sysname> display issu state
ISSU state: Loading
Compatibility: Incompatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot:
  slot 1
Previous version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
  feature1: 7.1.070, Test 0001015
Previous software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
Upgrade version list:
  boot: 7.1.070, Test 0001016
  system: 7.1.070, Test 0001016
  feature1: 7.1.070, Test 0001016
Upgrade software images:
  flash:/boot-t0001016.bin
  flash:/system-t0001016.bin
  flash:/feature1-t0001016.bin
```

表1-6 display issu state 命令显示信息描述表

字段	描述
ISSU state	ISSU升级状态，取值可能为： Init: 表示还没有开始ISSU升级或者ISSU升级已经完成 Loading: 表示正在执行 issu load 操作 Loaded: 表示 issu load 操作完成 Switching: 表示正在执行 issu run switchover 操作 Switchover: 表示 issu run switchover 操作完成 Accepted: 表示 issu accept 操作完成 Committing: 表示正在执行 issu commit 操作 Rollbacking: 表示系统正在回滚中 Unknown: 在非原主成员设备上查看，表示设备正在升级过程中

字段	描述
Compatibility	版本兼容性检查结果，取值可能为： Compatible: 表示兼容升级 Incompatible: 表示不兼容升级 Unknown: 没有升级
Work state	设备的工作模式，取值可能为： Normal: 表示正常模式 Independent active: 表示独立成员模式。当升级到不兼容版本时，先升级的从设备就会进入独立成员模式。该模式使得同一设备上的不同成员设备可以运行不同的软件版本
Upgrade method	升级方式，取值为： Card by card: 表示以堆叠成员设备为单位进行升级，升级完一个成员设备再升级另一个成员设备
Upgraded slot	完成升级的成员设备。取值为Unknown时，表示设备处于回滚过程中
Current upgrading slot	正在升级的成员设备。取值为Unknown时，表示设备处于回滚过程中
Current version list	设备没有升级，表示当前系统软件版本
Current software images	设备没有升级，表示当前运行软件包的名称
Previous version list	进行ISSU升级前的系统软件版本 Unknown: 不兼容升级的时候，在非原主成员设备上查看，表示设备正在升级过程中
Previous software images	进行ISSU升级前版本文件 Unknown: 不兼容升级的时候，在非原主成员设备上查看，表示设备正在升级过程中
Upgrade version list	正在ISSU升级的目标版本 Unknown: 不兼容升级的时候，在非原主成员设备上查看，表示设备正在升级过程中
Upgrade software images	正在ISSU升级中用到的目标文件 Unknown: 不兼容升级的时候，在非原主成员设备上查看，表示设备正在升级过程中

【相关命令】

- **issu accept**
- **issu commit**
- **issu load**
- **issu rollback**
- **issu run switchover**

1.1.13 display version comp-matrix

display version comp-matrix 显示设备将采用的 ISSU 升级策略。

【命令】

```
display version comp-matrix file { boot filename | system filename | feature filename&<1-30> | patch filename&<1-16> } *
```

display version comp-matrix file ipe ipe-filename[patch filename<1-16>]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

boot: Boot 包。
system: System 包。
feature: Feature 包。最多可指定 30 个。
patch: 补丁包。最多可指定 16 个。
filename<1-30>: 软件包的名称，形如 *filesystemname/filename.bin*。该文件必须保存在设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，从存储介质名称开始最多可输入 63 个字符。**<1-30>**表示前面的参数最多可以输入 30 次。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。
ipe ipe-filename: IPE 文件名，*ipe-filename* 表示 IPE 文件的名称，形如 *filesystemname/filename.ipe*。该文件必须保存在设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，从存储介质名称开始最多可输入 63 个字符。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

【使用指导】

只要设备上有一个软件包不兼容，均判定为不兼容升级方式，需要重启整个系统。

【举例】

显示设备将采用的 ISSU 升级策略。（兼容版本显示信息举例）
<Sysname> display version comp-matrix file boot flash:/boot-t0001015.bin system
flash:/system-t0001015.bin feature flash:/feature1-t0001015.bin
Verifying the file flash:/boot-t0001015.bin on slot 1.....Done.
Verifying the file flash:/system-t0001015.bin on slot 1.....Done.
Verifying the file flash:/feature1-t0001015.bin on slot 1.....Done.

Slot Upgrade Way
1 File Upgrade

表1-7 display version comp-matrix 命令显示信息描述表

字段	描述
Verifying the file flash:/xx.bin.....Done.	验证文件是否合法
Influenced service according to following table	如果升级，受影响的功能模块。只有版本兼容时，才会显示该信息
Incompatible upgrade	如果升级指定的软件包，则升级的方式为不兼容升级

字段	描述
Upgrade Way	兼容升级策略。只有版本兼容时，才会显示该信息。取值可能为： • Service Upgrade: 表示服务级增量升级 • File Upgrade: 表示文件级增量升级 • ISSU Reboot: 表示通过软重启方式升级 • Reboot: 表示通过重启方式升级 有关兼容升级的具体介绍请参见“基础配置指导”中的“ISSU配置”

【相关命令】

- **issu load**

1.1.14 install abort

install abort 命令用来取消正在执行中的激活或卸载操作。

【命令】

install abort [*job-id*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

job-id: 任务 ID。不指定该参数时，则取消正在执行中的所有激活和卸载操作。

【使用指导】

当用户执行 **install activate**、**install add**、**install commit**、**install deactivate**、**install remove** 或 **install rollback to** 命令时，系统会创建相应的任务。为了管理和监控这些任务，系统会给每个任务分配一个任务 ID。一个任务 ID 代表一条命令。可以使用 **display install job** 命令来查看任务 ID。

使用本命令取消正在进行的激活或卸载操作后，系统回退到操作前的状态。

【举例】

取消正在执行中的所有激活和卸载操作。

```
<Sysname> install abort
```

【相关命令】

- **display install job**

1.1.15 install activate

install activate 命令用来激活或查看软件包。

【命令】

```
install activate { boot filename | system filename | feature filename<1-30> }  
* slot slot-number [ test ]  
install activate patch filename { all | slot slot-number }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

boot: Boot 包。

system: System 包。

feature: Feature 包。

patch: 补丁包。该参数一次只能指定一个补丁包，但是可以通过多次执行此命令为设备激活多个补丁包。

filename<1-30>: 软件包的名称，形如 *filesystemname/filename.bin*。该文件必须保存在设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，从存储介质名称开始最多可输入 63 个字符。**<1-30>**表示前面的参数最多可以输入 30 次。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

all: 升级补丁包对应的所有成员设备。

slot slot-number: 表示设备在 IRF 中的成员编号。

test: 查看指定软件包的升级策略。不带该参数时，表示直接执行升级操作。

【使用指导】

请先查看软件包版本发布说明书，如果某软件包需要 License 才能运行，且设备当前没有对应的有效的 License 时，需安装对应的 License，再执行该命令。否则，会导致命令执行失败。

使用本命令激活指定硬件上的软件包后，被激活的软件包只在本次运行的系统中生效。要使被激活的软件包在设备重启后继续生效，还需要执行 **install commit** 命令。激活补丁包时，若使用 **install activate patch filename all** 命令同时激活所有硬件上的补丁包，则无需执行 **install commit** 命令，所有补丁包在设备重启后继续生效。

执行该命令时，如果 **filename** 不是存放在待升级成员设备上的文件，则系统会先将该文件拷贝到待升级成员设备上，再执行升级动作。

从设备重启后，会自动批量备份主设备的配置和状态数据。请使用 **display system stable state** 命令查看设备是否处于稳定状态。只有 System State 处于 Stable 状态，才能执行该命令。否则，命令执行失败。关于 **display system stable state** 命令的详细介绍请参见“基础配置命令参考”中的“设备管理”。

【举例】

显示从设备 2 上的 Feature 包 feature1.bin 的升级策略

```
<Sysname> install activate feature flash:/feature1.bin slot 2 test  
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin.....Done.  
Verifying the file flash:/feature1.bin on slot 2.....Done.
```

Upgrade summary according to following table:

flash:/feature1.bin	
Running Version	New Version
Test 0001015	Test 0001016
Slot	Upgrade Way
2	Reboot

Influenced service according to following table:

flash:/feature1.bin	
Feature1	

以上显示信息表明，该软件将采用重启方式升级。

激活从设备 2 上的 System 包 system.bin 和 Feature 包 feature1.bin。

```
<Sysname> install activate system flash:/system.bin feature flash:/feature1.bin slot 2
Copying file flash:/system.bin to slot2#flash:/system.bin.....Done.
Verifying the file flash:/system.bin on slot 2.....Done.
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin.....Done.
Verifying the file flash:/feature1.bin on slot 2.....Done.
Upgrade summary according to following table:
```

flash:/system.bin	
Running Version	New Version
Test 0001015	Test 0001016

flash:/feature1.bin	
Running Version	New Version
None	Test 0001016

Slot	Upgrade Way
2	Service Upgrade

Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.

表1-8 install activate 命令显示信息描述表

字段	描述
Copying file A to B.....Done.	将文件从位置A拷贝到位置B。
Verifying the file flash:/xx.bin.....Done.	验证文件是否合法
Upgrade summary according to following table	升级摘要信息
Running Version	设备当前运行的相同类型软件包的产品版本号
New Version	目标软件包的产品版本号

字段	描述
Upgrade Way	兼容升级策略，取值可能为： • Service Upgrade: 表示服务级增量升级 • File Upgrade: 表示文件级增量升级 • ISSU Reboot: 表示通过软重启方式升级 • Reboot: 表示通过重启方式升级 有关兼容升级的具体介绍请参见“基础配置指导”中的“ISSU配置”
Influenced service according to following table	将受影响的功能模块
Upgrading software images to compatible versions. Continue? [Y/N]	询问用户是否执行兼容升级操作
This operation might take several minutes, please wait	升级操作需要花费一定时间，请等待
Done.	表示激活成功
Operation failed.	表示激活失败
Install command does not support incompatible upgrade.	不能使用 install 命令来升级不兼容版本

【相关命令】

- **display install active**
- **install commit**
- **install deactivate**

1.1.16 install add

install add 命令用来解压缩 IPE 文件。

【命令】

install add *ipe-filename filesystem*

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

ipe-filename: IPE 文件的名称，形如 **filesystemname/filename.ipe**。该文件必须保存在设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，从存储介质名称开始最多可输入 63 个字符。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

filesystem: 解压缩 IPE 文件保存的目的文件系统的名称。

【使用指导】

由于使用 **install** 命令激活的软件包只能是.bin 软件包, 所以在使用 **install** 命令激活软件包之前需要使用 **install add** 命令将 IPE 文件进行解压缩。

用户获取 IPE 文件后, 可以使用 **display install ipe-info** 命令查看该 IPE 文件中包含了哪些软件包, 可以通过 **install add** 命令将 IPE 文件解压生成软件包, 再利用生成的软件包更新设备软件。

【举例】

解压缩 all.ipe 文件到存储介质 flash 上。

```
<Sysname> install add flash:/all.ipe flash:
```

```
Verifying the file flash:/all.ipe on slot 1...Done.
```

```
Decompressing file boot.bin to flash:/boot.bin.....Done.
```

```
Decompressing file system.bin to flash:/system.bin.....Done.
```

1.1.17 install commit

install commit 命令用来确认软件包更改。

【命令】

install commit

【视图】

用户视图

【缺省用户角色】

network-admin

【使用指导】

请先查看软件包版本发布说明书, 如果某软件包需要 License 才能运行, 且设备当前没有对应的有效的 License 时, 需安装对应的 License, 再执行该命令。否则, 会导致命令执行失败。

该命令会将补丁包文件添加到系统当前使用的软件包列表中:

- 如果系统使用了主用软件包启动, 该命令会将补丁包文件添加到主用软件包列表中。
- 如果系统使用了备用软件包启动, 该命令会将补丁包文件添加到备用软件包列表中。

只有在进行如下情况的配置修改设备当前的软件包列表时才需要执行本命令用来确认软件包更改:

- 执行 **install activate** 命令, 且为增量升级方式时
- 执行 **install deactivate** 命令时
- 执行 **install rollback** 命令时

当执行 **install activate** 命令, 且为软重启或重启升级方式时, 因为用户在执行 **install activate** 命令时, 系统已经修改了下次启动软件列表, 所以, 即便不再执行 **install commit** 命令, 升级软件包也会在系统重启后继续生效。

boot-loader file 命令和 **install commit** 命令都可以变更主用下次启动软件包列表, 最新的配置生效。两条命令的不同之处在于, **install commit** 命令自动使用当前激活的软件包列表作为主用下次启动软件包列表。而 **boot-loader file** 命令还可以指定其它当前未激活的软件包, 可以配置为主用或者备用下次启动软件包列表。

有关主用/备用软件包的详细介绍请参见“基础配置指导”中的“软件升级”。

【举例】

```
# 确认软件包更改。
<Sysname> install commit
This operation will take several minutes, please wait.....Done.
```

【相关命令】

- **install activate**
- **install deactivate**
- **install rollback**

1.1.18 install deactivate

install deactivate 命令用来卸载 Feature 包或补丁包。

【命令】

```
install deactivate feature filename&<1-30> slot slot-number
install deactivate patch filename { all | slot slot-number }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

feature: Feature 包。

patch: 补丁包。该参数一次只能指定一个补丁包，若要卸载多个补丁包，则需要多次执行此命令。

filename&<1-30>: 软件包的名称，形如 *filesystemname/filename.bin*。该参数中必须且只能包含文件系统的名称，不能包含文件系统位置信息，从存储介质名称开始最多可输入 63 个字符。&<1-30>表示前面的参数最多可以输入 30 次。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

all: 表示安装了该补丁包的所有成员设备。

slot slot-number: 表示设备在 IRF 中的成员编号。

【使用指导】

从设备重启后，会自动批量备份主设备的配置和状态数据。请使用 **display system stable state** 命令查看设备是否处于稳定状态。只有 System State 处于 Stable 状态，才能执行该命令。否则，命令执行失败。关于 **display system stable state** 命令的详细介绍请参见“基础配置命令参考”中的“设备管理”。

该命令只能对已经激活的软件包进行卸载操作。使用本命令卸载指定 slot 上的软件包后，卸载的软件包的特性功能在本次系统运行中失效。如果要使卸载的软件包在设备重启后继续失效，请执行 **install commit** 命令对卸载操作进行确认。卸载补丁包时，若使用 **install deactivate patch filename all** 命令同时卸载所有 slot 上的补丁包，则无需执行 **install commit** 命令，所有补丁包在设备重启后继续失效。

【举例】

```
# 卸载指定 slot 上的 patch 包 route-patch.bin。
<Sysname> install deactivate patch flash:/route-patch.bin slot 1
This operation might take several minutes, please wait...Done.
```

【相关命令】

- **display install active**
- **display install inactive**

1.1.19 install remove

install remove 命令用来删除没有激活的软件包。

【命令】

```
install remove [ slot slot-number ] { filename | inactive }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

filename: 软件包的名称，形如 *filesystemname/filename.bin*。该文件必须保存在设备任一文件系统的根目录下，该参数中必须且只能包含文件系统的名称，不能包含文件系统位置信息，从存储介质名称开始最多可输入 63 个字符。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示 IRF 中的所有成员设备。

inactive: 表示将删除指定文件系统根目录下、没有被激活的所有软件包。

【使用指导】

执行该命令后，指定的软件包将从设备上被彻底删除，用户将不能使用该软件包进行回滚或回退操作。

【举例】

```
# 删除软件包 flash:/feature1.bin。
<Sysname> install remove flash:/feature1.bin
```

1.1.20 install rollback to

install rollback to 命令用来回滚到指定的回滚点，即按回滚点上记录的信息，进行回滚操作。

【命令】

```
install rollback to { point-id | original }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

point-id: 回滚点的编号，当系统中至少存在两个回滚点的时候，才能输入该参数。可以用 **display install rollback** 命令查看系统中存在的回滚点。

original: 回滚到 ISSU 升级初始状态。

【使用指导】

每次激活或者卸载软件包之后，系统将这些变化记录为回滚点。通过回滚功能，可将系统回滚到某个历史状态，或者恢复到 ISSU 升级初始状态。

当升级方式为增量升级时，软件包回滚只在设备本次运行过程中生效，用户只有通过 **install commit** 命令确认软件包的更改后，才能使此次的回滚操作在系统重启后生效。系统最多支持 50 个回滚点，当回滚点超过最大值时，旧的回滚点会被删除，新的回滚点会被保存。

当升级方式为软重启或重启升级时，系统不会保留任何回滚点，只支持回滚到系统升级初始状态。补丁包不支持回滚操作。

【举例】

回滚到回滚点 1。

```
<Sysname> install rollback to 1
```

This operation might take several minutes, please wait...Done.

回滚到 ISSU 升级的初始状态。可通过观察 **active** 列表和回滚点的变化看出执行的结果。

```
<Sysname> display install active
```

Active packages on slot 1:

flash:/boot-t0001015.bin

flash:/system-t0001015.bin

flash:/feature1-t0001015.bin

```
<Sysname> display install rollback
```

Install rollback information 1 on slot 1:

Updating from no package

to flash:/feature1-t0001015.bin.

以上显示信息表明，当前激活的包有三个，但是确认的只有两个，回滚点 1 是激活了 flash:/feature1-t0001015.bin。

```
<Sysname> install rollback to original
```

This operation might take several minutes, please wait...Done.

```
<Sysname> display install active
```

Active packages on slot 1:

flash:/boot-t0001015.bin

flash:/system-t0001015.bin

```
<Sysname> display install committed
```

Committed packages on slot 1:

flash:/boot-t0001015.bin

flash:/system-t0001015.bin

执行 **install rollback to original** 命令后，设备运行的软件集恢复到 ISSU 升级初始状态，flash:/feature1-t0001015.bin 被卸载。

【相关命令】

- **display install rollback**

1.1.21 install verify

install verify 命令用来执行对软件包状态、完整性和一致性的检验。

【命令】

install verify

【视图】

用户视图

【缺省用户角色】

network-admin

【使用指导】

为了保证设备进行 ISSU 升级之后能够正常运行，需要执行本命令对软件包进行如下检验：

完整性：检验 Boot 包、System 包和 Feature 包的完整性。

一致性：检验系统内各激活的软件包列表的差异，以方便用户知道系统内各软件包版本是否一致。

软件包状态：检查各设备上激活的软件包列表和确认的软件包列表之间的差异，以方便用户知道是否有未确认的软件包。

使用该命令，能帮助用户进行软件包检查：

- 当系统提示软件包不完整时，请重新下载并安装软件包。
- 当系统提示软件包不一致时，请使用 **install activate**、**install deactivate** 以及 **install commit** 命令来确保它们的一致。

【举例】

检验设备上软件包状态、完整性和一致性信息。

```
<Sysname> install verify
Active packages on slot 1 are the reference packages.
Packages will be compared with the reference packages.
This operation will take several minutes, please wait...
  Verifying packages on slot 1:
    Start to check active package completeness.
Verifying the file flash:/boot-t0001015.bin on slot 1.....Done.
  flash:/boot-t0001015.bin verification successful.
Verifying the file flash:/system-t0001015.bin on slot 1.....Done.
  flash:/system-t0001015.bin verification successful.
    Start to check active package consistency.
      Active packages are consistent with committed packages on their own board.
      Active packages are consistent with the reference packages.
  Verifying packages on slot 2:
    Start to check active package completeness.
Verifying the file flash:/boot-t0001015.bin on slot 2.....Done.
  flash:/boot-t0001015.bin verification successful.
Verifying the file flash:/system-t0001015.bin on slot 2.....Done.
```

```
flash:/system-t0001015.bin verification successful.  
Start to check active package consistency.  
Active packages are consistent with committed packages on their own board.  
Active packages are consistent with the reference packages.  
Verification is done.
```

1.1.22 issu accept

issu accept 命令用来确认 ISSU 兼容升级，接受已升级的软件版本，并删除回滚定时器。

【命令】

issu accept

【视图】

用户视图

【缺省用户角色】

network-admin

【使用指导】

执行本命令后，系统会删除回滚定时器，本次 ISSU 升级过程中不会再进行自动回滚，用户可以执行 **issu rollback** 命令进行手动回滚。

ISSU 不兼容升级时，不需要执行该命令。

【举例】

版本兼容情况下，确认升级步骤。

```
<Sysname> issu accept
```

【相关命令】

- **issu load**
- **issu run switchover**

1.1.23 issu commit

issu commit 命令用来对原主设备及未升级的从设备进行兼容版本升级。

【命令】

issu commit slot slot-number

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 待升级的原主设备以及其它从设备的成员编号。

【使用指导】

从设备重启后，会自动批量备份主设备的配置和状态数据。请使用 **display system stable state** 命令查看设备是否处于稳定状态。只有 System State 处于 Stable 状态，才能执行该命令。否则，命令执行失败。关于 **display system stable state** 命令的详细介绍请参见“基础配置命令参考”中的“设备管理”。

所有成员设备完成升级后，本次升级结束，ISSU 回到初始状态。执行此命令后，不能再通过 ISSU 回滚命令或者回滚定时器进行回滚操作。多个从设备的情况下应该在一个从设备启动完成并重新加入 IRF 后再对下一个从设备执行该命令，否则可能引起升级错误。

【举例】

版本兼容情况下，成员 2 已经升级完成成为新的主设备，升级原主设备（假设成员编号为 3）和其他成员（假设成员编号为 4 和 1）。

```
<Sysname> issu commit slot 3
```

Upgrade summary according to following table:

```
flash:/feature1.bin
```

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
3	Service Upgrade

Upgrading software images to compatible versions. Continue? [Y/N]:y

This operation might take several minutes, please wait...Done.

```
<Sysname> issu commit slot 4
```

Copying file flash:/feature1.bin to slot4#flash:/feature1.bin...Done.

Verifying the file flash:/feature1.bin on slot 4.....Done.

Upgrade summary according to following table:

```
flash:/feature1.bin
```

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
4	Service Upgrade

Upgrading software images to compatible versions. Continue? [Y/N]:y

This operation might take several minutes, please wait...Done.

```
<Sysname> issu commit slot 1
```

Copying file flash:/feature1.bin to slot1#flash:/feature1.bin...Done.

Verifying the file flash:/feature1.bin on slot 1.....Done.

Upgrade summary according to following table:

```
flash:/feature1.bin
```

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
1	Service Upgrade

Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
本命令显示信息的描述请参见 [表 1-9](#)。

【相关命令】

- **issu accept**
- **issu load**
- **issu run switchover**

1.1.24 issu load

issu load 命令用来升级从设备的启动软件包并将设备的主用下次启动软件包设置为指定的软件包。

【命令】

```
issu load file { boot filename | system filename | feature filename&<1-30> | patch filename&<1-16> } * slot slot-number&<1-9> [ reboot ]  
issu load file ipe ipe-filename slot slot-number&<1-9> [ patch filename&<1-16> ] [ reboot ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

boot: Boot 包。

system: System 包。

feature: Feature 包。最多可指定 30 个。

patch: 补丁包。最多可指定 16 个。该参数既可以指定叠加补丁也可以指定非叠加补丁。有关叠加补丁和非叠加补丁的详细解释请参见，“基础配置指导”的“软件升级”。

filename&<1-30>: 表软件包的名称，形如 *filesystemname/filename.bin*。该文件必须保存在主设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，从存储介质名称开始最多可输入 63 个字符。**&<1-30>**表示前面的参数最多可以输入 30 次。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

ipe ipe-filename: IPE 文件，*ipe-filename* 表示 IPE 文件的名称，形如 *filesystemname/filename.ipe*。该文件必须保存在主设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，从存储介质名称开始最多可输入 63 个字符。有关指定文件夹和文件详细介绍请参见“基础配置指导”中的“文件系统管理”。

slot slot-number: 表示从设备在 IRF 中的成员编号。**&<1-9>**表示前面的参数最多可以输入 9 次。

- 如果 IRF 中只有一个成员设备，则输入该成员设备的编号，用来完成整个 IRF 的升级。
- 如果 IRF 中有多个成员设备：

- 当要升级的软件包的版本和设备当前运行的软件包的版本兼容时，只允许输入一个 *slot-number*。
- 当要升级的软件包的版本和设备当前运行的软件包的版本不兼容时，可以输入多个 *slot-number*，一次升级多个从设备。
- 如果 IRF 为环形连接，建议一次升级一半数量的物理上邻接的成员设备（也称为对半升级）

reboot: 表示在版本兼容的情况下，如果决策出来的结果是文件级增量升级、服务级增量升级、ISSU 软重启升级则强制使用兼容重启升级重启成员设备以完成升级。不指定该参数时，系统会按照决策结果进行升级。

【使用指导】

当 **issu** 命令指定的软件包不能全部覆盖设备当前启动软件包时，除 **issu** 命令指定的软件包之外的其他软件包会被沿用，例如设备当前启动软件包中含有 **Feature** 包并且该 **Feature** 包有效，**issu** 命令指定新的软件包中不包含新的 **Feature** 包，那么当前版本的 **Feature** 包会被沿用。若沿用的软件包与 **issu** 命令指定的软件包不兼容，会导致设备升级失败。

输入该命令后，系统将自动执行以下操作：

- 进行版本兼容性检查。
- 确定升级策略。
- 按照升级策略进行升级，并将指定成员设备的主用下次启动软件包设置为 **issu load** 命令中指定的包。

从设备重启后，会自动批量备份主设备的配置和状态数据。请使用 **display system stable state** 命令查看设备是否处于稳定状态。只有 **System State** 处于 **Stable** 状态，才能执行该命令。否则，命令执行失败。关于 **display system stable state** 命令的详细介绍请参见“基础配置命令参考”中的“设备管理”。

【举例】

版本兼容情况下，使用 **flash:/feature1.bin** 升级从设备 2 上的 **Feature** 包。

```
<Sysname> issu load file feature flash:/feature1.bin slot 2
```

```
This operation will delete the rollback point information for the previous upgrade and maybe get unsaved configuration lost. Continue? [Y/N]:Y
```

```
Verifying the file flash:/feature1.bin on slot 1...Done.
```

```
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin.....Done.
```

```
Verifying the file flash:/feature1.bin on slot 2...Done.
```

```
Identifying the upgrade methods...Done.
```

```
Upgrade summary according to following table:
```

```
flash:/feature1.bin
```

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
2	Service Upgrade

```
Upgrading software images to compatible versions. Continue? [Y/N]:y
```

```
This operation might take several minutes, please wait...Done.
```

增量升级情况下，使用 **flash:/feature1.bin** 升级从设备 2 上的 **Feature** 包，带 **reboot** 参数。

```
<Sysname> issu load file feature flash:/feature1.bin slot 2 reboot
```

This operation will delete the rollback point information for the previous upgrade and maybe get unsaved configuration lost. Continue? [Y/N]:Y
Verifying the file flash:/feature1.bin on slot 1...Done.
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin.....Done.
Verifying the file flash:/feature1.bin on slot 2...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/feature1.bin

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
2	Reboot

Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
版本不兼容情况下，使用 flash:/feature1.bin 升级从设备 3 和 4 上的 Feature 包。

<Sysname> issu load file feature flash:/feature1.bin slot 3 4
This operation will delete the rollback point information for the previous upgrade and maybe get unsaved configuration lost. Continue? [Y/N]:Y
Verifying the file flash:/feature1.bin on slot 1...Done.
Copying file flash:/feature1.bin to slot3#flash:/feature1.bin.....Done.
Verifying the file flash:/feature1.bin on slot 3...Done.
Copying file flash:/feature1.bin to slot4#flash:/feature1.bin.....Done.
Verifying the file flash:/feature1.bin on slot 4...Done.
Identifying the upgrade methods...Done.
Upgrade summary according to following table:

flash:/feature1.bin

Running Version	New Version
Test 0001015	Test 0001016

Slot	Upgrade Way
3	Reboot
4	Reboot

Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.

表1-9 issu load 命令显示信息描述表

字段	描述
This operation will delete the rollback point information for the previous upgrade and maybe get unsaved configuration lost. Continue? [Y/N]	当前操作会删除上一次ISSU升级的日志信息和回滚点，并且未保存的配置可能会丢失，询问用户是否继续执行升级操作
Verifying the file flash:/xx.bin.....Done.	验证文件是否合法
Decompressing file A to B.....Done.	将文件从位置A解压缩到位置B。只有使用IPE文件升级时，才显示该信息

字段	描述
Copying file B to C.....Done.	将文件从位置B拷贝到位置C。当配置从设备时才有该提示信息
Identifying the upgrade methods.....Done.	获取升级策略
Upgrade summary according to following table	升级信息摘要
Running Version	设备当前运行的相同类型软件包的产品版本号
New Version	将要升级的软件包的产品版本号
Upgrade Way	升级策略，取值可能为： • Service Upgrade: 表示服务级增量升级 • File Upgrade: 表示文件级增量升级。 • ISSU Reboot: 表示通过软重启方式升级 • Reboot: 表示通过重启方式升级 有关兼容升级的具体介绍请参见“基础配置指导”中的“ISSU配置”
Upgrading software images to compatible versions. Continue? [Y/N]	询问用户是否执行兼容升级操作
Upgrading software images to incompatible versions. Continue? [Y/N]	询问用户是否执行不兼容升级操作
This operation might take several minutes, please wait	升级操作需要花费一定时间，请等待
Done.	表示激活成功
Operation failed.	表示激活失败

1.1.25 issu rollback

issu rollback 命令用来回滚到升级前的版本。

【命令】

issu rollback

【视图】

用户视图

【缺省用户角色】

network-admin

【使用指导】

设备支持自动回滚和手动回滚，自动回滚定时器的时长由 **issu rollback-timer** 命令配置；手工回滚由 **issu rollback** 命令触发。

当 ISSU 升级状态为如下几种情况时，支持手工回滚：

- Loaded
- Switching（兼容升级）

- Switchover（兼容升级）
- Accepted

在重启升级的 **Switching** 状态下如果进行手工回滚或者发生自动回滚和在不兼容升级的 **Switching** 状态下发生自动回滚，将会导致如下现象：

- 已升级的从设备重启，此时主用主设备可能因正在进行主备倒换重启而导致断流。
- 回滚只保证版本回到升级前，但不能保证主备状态和升级前一致。

建议不要在 **Switching** 状态下进行手工回滚，并且设置足够长的自动回滚定时器时长。

【举例】

回滚到升级之前的版本。

```
<Sysname> issu rollback
```

```
This command will quit the ISSU process and roll back to the previous version. Continue?
[Y/N]:y
```

【相关命令】

- **issu accept**
- **issu commit**
- **issu load**
- **issu run switchover**

1.1.26 issu rollback-timer

issu rollback-timer 命令用来设置回滚定时器时长。

undo issu rollback-timer 命令用来恢复缺省情况。

【命令】

```
issu rollback-timer minutes
```

```
undo issu rollback-timer
```

【缺省情况】

回滚定时器的时长为 45 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

minutes：回滚定时器的时长，取值范围为 0~120，单位为分钟。如果时长设置为 0，则表示关闭自动回滚功能。

【使用指导】

设备只有在兼容版本升级且存在多个成员设备的 IRF 系统情况下才能启动回滚定时器。

兼容版本升级的情况下，执行 **issu run switchover** 命令后系统会自动启动回滚定时器。如果在指定的时间内（回滚定时器超时前）未执行 **issu accept** 或者 **issu commit** 命令，则系统会自动回滚到升级前的版本。

新设置的时长会在下次 ISSU 升级中生效。

【举例】

```
# 设置回滚定时器时长为 50 分钟。
<Sysname> system-view
[Sysname] issu rollback-timer 50
```

【相关命令】

- **issu rollback**

1.1.27 issu run switchover

issu run switchover 命令用来进行 ISSU 倒换。

【命令】

issu run switchover

【视图】

用户视图

【缺省用户角色】

network-admin

【使用指导】

当设备上只有一个成员并需要升级时，不需要使用此命令。

输入该命令后，系统在不同情况下将自动执行不同的操作：

- 兼容升级：增量升级时系统会对升级的进程进行了进程级主备倒换；软重启或者重启升级时系统会将当前主设备使用原版本重新启动，将刚使用 **issu load** 命令升级的从设备选举为新主设备。
- 不兼容版本升级：执行 **issu load** 后 IRF 分裂，生成两个的 IRF。执行 **issu run switchover** 重启并升级原 IRF，原 IRF 组重启后加入新的 IRF 即完成升级过程，系统选择新 IRF 的主设备为合并后 IRF 的主设备。

从设备重启后，会自动批量备份主设备的配置和状态数据。请使用 **display system stable state** 命令查看设备是否处于稳定状态。只有 System State 处于 Stable 状态，才能执行该命令。否则，命令执行失败。关于 **display system stable state** 命令的详细介绍请参见“基础配置命令参考”中的“设备管理”。

兼容版本升级时，如果在回滚定时器超时时仍未执行 **issu accept** 或者 **issu commit** 命令，则系统会自动回滚到升级前的版本。

不兼容版本升级执行 **issu run switchover** 之后，即完成升级过程。

【举例】

```
# 版本兼容情况下，进行主备倒换。
<Sysname> issu run switchover
Upgrade summary according to following table:
```

```
flash:/feature1.bin
Running Version      New Version
```

```

Test 0001015                                Test 0001016

Slot                                          Switchover Way
1                                             Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
# 版本不兼容情况下，进行主备倒换，同时升级成员设备 1（主设备）和成员设备 2（从设备）。
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1.bin
Running Version          New Version
Test 0001015            Test 0001016

Slot                    Upgrade Way
1                       Reboot
2                       Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.

```

表1-10 issu run switchover 命令显示信息描述表

字段	描述
Switchover Way	倒换方式，取值可能为： - Active standby process switchover：表示主备进程的倒换 - Master subordinate switchover：表示主设备和从设备之间的倒换
其它字段	请参见 表1-9

【相关命令】

- **issu load**

1.1.28 reset install log-history oldest

reset install log-history oldest 命令用来清除 ISSU 日志。

【命令】

reset install log-history oldest *log-number*

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

log-number：ISSU 日志的数量。

【使用指导】

执行本命令后，系统将按创建时间由早到晚的顺序清除指定数量的 ISSU 日志。

【举例】

清除 2 条最早的 ISSU 日志。

```
<Sysname> reset install log-history oldest 2
```

【相关命令】

- **display install log**

1.1.29 reset install rollback oldest

reset install rollback oldest 命令用来清除 ISSU 回滚点。

【命令】

```
reset install rollback oldest point-id
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

point-id: 系统存储的回滚点的编号。

【使用指导】

使用本命令，清除指定回滚点以及在此回滚点之前创建的所有回滚点。

【举例】

清除编号为 2 以及在此回滚点之前创建的所有回滚点。

```
<Sysname> reset install rollback oldest 2
```

【相关命令】

- **display install rollback**

目 录

1 应急Shell	1-1
1.1 应急Shell配置命令	1-1
1.1.1 copy	1-1
1.1.2 delete	1-2
1.1.3 dir	1-2
1.1.4 display copyright	1-4
1.1.5 display install package	1-4
1.1.6 display interface m-eth0	1-5
1.1.7 display ip routing-table	1-6
1.1.8 display ipv6 routing-table	1-7
1.1.9 display version	1-8
1.1.10 format	1-9
1.1.11 ftp	1-9
1.1.12 install load	1-10
1.1.13 interface m-eth0	1-10
1.1.14 ip address	1-11
1.1.15 ip gateway	1-12
1.1.16 ipv6 address	1-12
1.1.17 ipv6 gateway	1-13
1.1.18 mkdir	1-13
1.1.19 more	1-14
1.1.20 move	1-14
1.1.21 ping	1-15
1.1.22 ping ipv6	1-16
1.1.23 pwd	1-17
1.1.24 quit	1-17
1.1.25 reboot	1-18
1.1.26 reset ssh public-key	1-18
1.1.27 rmdir	1-19
1.1.28 shutdown	1-19
1.1.29 ssh2	1-20
1.1.30 system-view	1-21
1.1.31 telnet	1-21

1.1.32 tftp 1-22

1 应急Shell

本命令手册中文件名参数的输入规则请参见“基础配置分册”中的“文件系统管理”。

如无特殊说明，本文中的文件名或目录参数，遵循如下规格：必须带存储介质名称，不能携带存储介质位置信息，全路径长度为 1~511 个字符，支持多级目录，每级目录以及纯文件名长度均为 1~255 个字符，不区分大小写。

如果设备同时支持 CF 卡和 Flash 两种存储介质，则在应急 Shell 环境下，可以操作这两种存储介质，只需在文件/文件夹路径处指定正确的存储介质名称即可。本文以 Flash 为例。

1.1 应急Shell配置命令

1.1.1 copy

copy 命令用来复制文件。

【命令】

copy *source-file* { *dest-file* | *dest-directory* }

【视图】

用户视图

【参数】

source-file: 源文件的名称。

dest-file: 目标文件的名称。

dest-directory: 为目标文件夹的名称。系统会将文件复制到指定文件夹，使用源文件名作为目标文件名。

【使用指导】

执行该命令时，如果指定的目标文件不存在，则系统会先创建该文件，再复制内容；如果指定的目标文件已存在，则系统会提示是否覆盖该文件，如果选择“Y”，系统会将目标文件的内容替换成源文件的内容，如果选择“N”，则不做任何处理。

【举例】

将文件 test.cfg 复制一份，并命名为 testbackup.cfg。

```
<boot> copy flash:/test.cfg flash:/testbackup.cfg
Copy flash:/test.cfg to flash:/testbackup.cfg?[Y/N]:y
Start to copy flash:/test.cfg to flash:/testbackup.cfg...Done.
```

将文件 test.cfg 复制到已存在的文件 testbackup.cfg。

```
<boot> copy flash:/test.cfg flash:/testbackup.cfg
Copy flash:/test.cfg to flash:/testbackup.cfg?[Y/N]:y
flash:/testbackup.cfg already exists. Overwrite it?[Y/N]:y
Start to copy flash:/test.cfg to flash:/testbackup.cfg...Done.
```

1.1.2 delete

delete 命令用来彻底删除指定文件。

【命令】

delete *file*

【视图】

用户视图

【参数】

file: 要彻底删除的文件的名称。

【举例】

```
# 彻底删除文件 tt.cfg。
<boot> delete flash:/tt.cfg
Delete flash:/tt.cfg? [Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Start to delete flash:/tt.cfg...Done.
```

1.1.3 dir

dir 命令用来显示目录或文件信息。

【命令】

dir [*/all*] [*file* | *directory*]

【视图】

用户视图

【参数】

/all: 显示当前目录下所有的文件及子文件夹信息，显示内容包括隐藏文件和文件夹。不指定该参数时，显示当前目录下所有非隐藏的文件及子文件夹信息。

file: 显示指定的文件或文件夹的信息。不指定该参数时，显示当前目录下的文件及子文件夹信息。

directory: 显示指定的文件夹的信息。

【举例】

显示系统中所有的文件及文件夹信息。

```
<boot> dir /all
Directory of flash:
 0      drw-          - Jan 01 2012 00:06:09      01
 1      drw-          - Sep 15 2012 04:03:14      pki
 2      drw-          - Jan 01 2012 00:04:07      test
 4      drw-          - Nov 05 2012 06:45:07      logfile
 5      -rwh          20 Oct 20 2012 09:09:52      .snmpboots
 6      drw-          - Nov 05 2012 05:56:22      diagfile
 7      drwh          - Aug 20 2012 09:23:48      .trash
 8      -rw-          816 Aug 20 2012 06:15:00      ifindex.dat
 9      -rw-          3231 Aug 31 2012 09:01:41      startup.cfg
```

```

10      -rw-          60620 Aug 31 2012 09:01:43  startup.mdb
11      drw-          - Sep 30 2012 04:43:24    versionInfo
12      drw-          - Nov 05 2012 05:56:22    seclog
13      -rwh          18 Aug 20 2012 09:09:34    .pathfile
14      -rw-      11238400 Aug 30 2012 11:06:53    boot-t2301001.bin
15      -rw-          0 Aug 31 2012 05:04:40    lauth.dat
16      -rw-          4383 Oct 20 2012 06:15:00    test.cfg

```

61440 KB total (11108 KB free)

显示系统中所有的非隐藏文件及文件夹信息。

<boot> dir

Directory of flash:

```

 0      drw-          - Jan 01 2012 00:06:09    01
 1      drw-          - Sep 15 2012 04:03:14    pki
 2      drw-          - Jan 01 2012 00:04:07    test
 4      drw-          - Nov 05 2012 06:45:07    logfile
 5      drw-          - Nov 05 2012 05:56:22    diagfile
 6      -rw-          816 Aug 20 2012 06:15:00    ifindex.dat
 7      -rw-          3231 Aug 31 2012 09:01:41    startup.cfg
 8      -rw-          60620 Aug 31 2012 09:01:43    startup.mdb
 9      drw-          - Sep 30 2012 04:43:24    versionInfo
10      drw-          - Nov 05 2012 05:56:22    seclog
11      -rw-      11238400 Aug 30 2012 11:06:53    boot-t2301001.bin
12      -rw-          0 Aug 31 2012 05:04:40    lauth.dat
13      -rw-          4383 Aug 20 2012 06:15:00    test.cfg

```

61440 KB total (11108 KB free)

显示文件 config.cfg 的相关信息。

<boot> dir flash:/config.cfg

Directory of flash:

```

 0      -rw-          3231 Aug 31 2012 09:01:41    startup.cfg

```

61440 KB total (11108 KB free)

表1-1 dir 命令显示信息描述表

字段	说明
Directory of	当前显示的目录
7 -rw- 3231 Aug 31 2012 09:01:41 startup.cfg	文件或文件夹的信息： 7 表示编号，由系统自动分配 -rw-表示属性。第一个字符如果是 d 表示文件夹，如果显示为“-”，则表示它是文件；第二个字符是 r，表示本文件或文件夹是可读的；第三个字符是 w，表示本文件或文件夹是可写的；第四个字符如果是 h，表示本文件或文件夹是隐藏的，如果显示为“-”，则表示它是可见的 3231 表示文件大小，单位为字节。如果显示为“-”，则表示它是文件夹 - Aug 31 2012 09:01:41 表示最近一次修改的时间 - startup.cfg 表示文件或文件夹的名称

字段	说明
61440 KB total (11108 KB free)	存储介质存储空间的大小，单位为千字节（存储介质中空闲存储空间的大小，单位为千字节）

1.1.4 display copyright

display copyright 命令用来显示版权信息。

【命令】

display copyright

【视图】

任意视图

【举例】

```
# 显示版权信息。
<boot> display copyright
.....显示信息略.....
```

1.1.5 display install package

display install package 命令用来显示指定软件包的信息。

【命令】

display install package package

【视图】

任意视图

【参数】

package：软件包的名称，形如 *filesystemname/filename.bin*，比如 *flash:/startup-system.bin*。该文件必须保存在本成员设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，不能包含文件系统位置信息，从存储介质名称开始最多可输入 63 个字符。

【举例】

```
# 显示软件包 system.bin 的信息。
<boot> display install package flash:/system-t6101010.bin
Verifying the file flash:/system-t6101010.bin .....Done.
flash:/system-t6101010.bin
[Package]
Vendor: UNIS
Product: xxxx
Service name: system
Platform version: 7.1.070
Product version: Test 0001010
Supported board: mpu
```

[Component]
Component: system
Description: system package

表1-2 display install package 命令显示信息描述表

字段	描述
[Package]	软件包的信息
Vendor	厂商
Product	产品名称
Service name	软件包所包含的服务名称 - 如果显示为 boot，表示该软件包为 Boot 包 - 如果显示为 system，表示该软件包为 System 包 - 如果显示为 patch，表示该软件包为补丁包 - 如果显示为其它值，则表示该软件包为提供某项功能的 Feature 包
Platform version	平台版本号
Product version	产品版本号，通过该信息可以判断System包和Boot包版本是否一致
Supported board	软件包支持的设备类型： mpu 表示成员设备
[Component]	组件信息，表示软件包的组成部分
Component	组件信息名称
Description	软件包的描述信息

1.1.6 display interface m-eth0

display interface m-eth0 命令用来显示管理以太网接口的相关信息。

【命令】

display interface m-eth0

【视图】

任意视图

【举例】

```
# 显示管理以太网接口的相关信息。
<boot> display interface m-eth0
m-eth0 current state: UP
Line protocol current state: UP
The Maximum transmit unit is 1500
Inet4 Address is 192.168.20.189/24
Inet6 Address is 1::1:1:1/64 Scope:Global
Inet6 Address is FE80::202:3FF:FE04:506/10 Scope:Link
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: c4ca-d94c-e201
```

IPv6 Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: c4ca-d94c-e201
Input: 8983 packets, 0 errors, 0 dropped, 0 overruns, 2 frame
Output: 431 packets, 0 errors, 0 dropped, 0 overruns, 0 carrier,
0 collisions, 1000 txqueuelen
Input bytes:804168
Output bytes:30367

表1-3 display interface m-eth0 命令显示信息描述表

字段	描述
m-eth0 current state	接口的物理状态，状态可能为： - Administratively DOWN: 表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 - DOWN: 表示该接口的管理状态为开启，但物理状态为关闭（可能因为没有物理连线或者线路故障） - UP: 该端口的管理状态和物理状态均为开启
Line protocol current state	接口的链路层状态，其值直接取用接口的物理状态的当前值
The Maximum transmit unit	接口的MTU
Inet4 Address	接口的IPv4地址，给接口配置IPv4地址后才显示该信息
Inet6 Address	接口的IPv6地址，给接口配置IPv6地址后才显示该信息。Scope:Global表示该地址为全球单播地址
Inet6 Address is FE80::202:3FF:FE04:506/10 Scope:Link	接口的IPv6链路本地地址，该地址在接口物理状态变为UP时，由系统自动生成
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address	IPv4报文发送帧格式，以及硬件地址
IPv6 Packet Frame Type, Hardware Address	IPv6报文发送帧格式，以及硬件地址
Input: 8983 packets, 0 errors, 0 dropped, 0 overruns, 2 frame	接口接收的报文的统计信息：报文总数，错误报文数，丢弃报文数，队列溢出报文数，帧队列错误报文数
Output: 431 packets, 0 errors, 0 dropped, 0 overruns, 0 carrier, 0 collisions, 1000 txqueuelen	接口发送的报文的统计信息：报文总数，错误报文数，丢弃报文数，队列溢出报文数，载波出错报文数，冲突的报文数，每个队列允许的最大帧数
Input bytes	接口接收的报文的总字节数
Output bytes	接口发送的报文的总字节数

1.1.7 display ip routing-table

display ip routing-table 命令用来显示 IPv4 路由信息表。

【命令】

display ip routing-table

【视图】

任意视图

【举例】

```
# 显示 IPv4 路由信息表。
<boot> display ip routing-table
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
192.168.116.0    *                255.255.255.0    U        0      0      0 m-eth0
default          192.168.116.1   0.0.0.0          UG       0      0      0 m-eth0
```

表1-4 display ip routing-table 命令显示信息描述表

字段	描述
Kernel IP routing table	IPv4路由表信息
Destination	目的地址（取值为default时表示缺省路由）
Gateway	网关（如果不需要使用网关，则该字段显示为“*”）
Genmask	掩码（取值为0.0.0.0时表示缺省路由的掩码）
Flags	标志位： • G：网关路由 • H：主机路由 • D：通过邻居发现学习到的缺省路由 • A：通过路由发布学习到的路由 • C：缓存表项，用于快速转发去往某目的地的报文 • U：可用路由
Metric	路由开销
Ref	表示路由表项被其它表项引用的次数，即和其它表项间的依赖关系
Use	表示这条表项被使用过的次数，即该路由被匹配到的次数
Iface	出接口

1.1.8 display ipv6 routing-table

display ipv6 routing-table 命令用来显示 IPv6 路由信息表。

【命令】

display ipv6 routing-table

【视图】

任意视图

【举例】

```
# 显示 IPv6 路由信息表。
<boot> display ipv6 routing-table
```

```
Kernel IPv6 routing table
Destination                                     Next Hop
  Flags Metric Ref    Use Iface
::1/128                                         ::
  U      0      0      1 lo
FE80::201:2FF:FE03:406/128                    ::
  U      0      0      1 lo
FE80::/64                                       ::
  U    256      0      0 m-eth0
FF02::1:2/128                                FF02::1:2
  UC     0    2888      0 m-eth0
FF00::/8                                       ::
  U    256      0      0 m-eth0
```

表1-5 display ipv6 routing-table 命令显示信息描述表

字段	描述
Kernel IPv6 routing table	IPv6路由表信息
Destination	目的地址
Next Hop	下一跳
Flags	标志位： • G: 网关路由 • H: 主机路由 • D: 通过邻居发现学习到的缺省路由 • A: 通过路由发布学习到的路由 • C: 缓存表项，用于快速转发去往某目的地的报文 • U: 可用路由
Metric	路由开销
Ref	表示路由表项被其它表项引用的次数，即和其它表项间的依赖关系
Use	表示这条表项被使用过的次数，即该路由被匹配到的次数
Iface	出接口，lo表示环回口

1.1.9 display version

display version 命令用来显示 Boot 包的版本信息。

【命令】

display version

【视图】

任意视图

【举例】

查看 Boot 包的版本信息。

```
<boot> display version
.....显示信息略.....
```

1.1.10 format

format 命令用来格式化文件系统。

【命令】

format *filesystem*

【视图】

用户视图

【参数】

filesystem: 文件系统的名称。

【使用指导】

格式化操作将导致文件系统上的所有文件丢失，并且不可恢复。如果文件系统上有启动配置文件和启动文件，格式化该文件系统，将丢失启动配置文件和启动文件，导致设备重启后无法启动，请谨慎操作。

【举例】

```
# 格式化 Flash 文件系统。
<boot> format flash:
All data on flash: will be lost, continue?[Y/N]:y
Formatting flash:... Done.
```

1.1.11 ftp

ftp 命令用来访问 FTP 服务器。

【命令】

ftp { *server-ipv4-address* | **ipv6** *server-ipv6-address* } { **get** *remote-file* *local-file* | **put** *local-file* *remote-file* }

【视图】

用户视图

【参数】

server-ipv4-address: FTP 服务器的 IPv4 地址。

server-ipv6-address: FTP 服务器的 IPv6 地址。

get *remote-file* *local-file*: 表示从 FTP 服务器上下载一个文件到本地，*remote-file* 表示 FTP 服务器上的文件的名称，*local-file* 表示本地的文件的名称。

put *local-file* *remote-file*: 表示从本地上传一个文件到 FTP 服务器，*local-file* 表示本地的文件的名称，*remote-file* 表示 FTP 服务器上的文件的名称。

【使用指导】

当网络拥塞，文件传输速度很慢的时候，用户可以使用<Ctrl+C>组合键中断本次 FTP 操作，稍后再试。

【举例】

```
# 到 FTP 服务器 192.168.1.100 上下载文件 111.txt，保存到本地时使用名称 222.txt。
<boot> ftp 192.168.1.100 get 111.txt flash:/222.txt
User: test
Password: ***
```

1.1.12 install load

install load 命令用来加载 System 包，并引导设备进入 Uniware 系统。

【命令】

```
install load system-package
```

【视图】

用户视图

【参数】

system-package：System 包的名称，形如 *filesystemname/filename.bin*，比如 *flash:/startup-system.bin*。该文件必须保存在本成员设备任一文件系统的根目录下，该参数中必须包含文件系统的名称，不能包含文件系统位置信息，从存储介质名称开始最多可输入 63 个字符。

【使用指导】

执行该命令，系统会同时更新主用下次启动软件包列表，新列表中只包含 Boot 包和 System 包，以保证设备下次能够正常启动。

如需运行 Feature 包和补丁包，须重新下载、安装，具体配置步骤请参见“基础配置指导”中的“软件升级”和“ISSU”。

【举例】

```
# 加载 System 包，进入 Uniware 系统。
<boot> install load flash:/system.bin
Check package flash:/system.bin ...
Verifying the file flash:/system.bin .....Done.
Extracting package ...

Loading...
Cryptographic algorithms tests passed.
Line con1 is available.

Press ENTER to get started.
```

1.1.13 interface m-eth0

interface m-eth0 命令用来进入管理以太网接口视图。

【命令】

interface m-eth0

【视图】

系统视图

【使用指导】

进入管理以太网接口视图后，可以为管理以太网接口配置 IP 地址和网关。

【举例】

进入管理以太网接口视图。

```
<boot> system-view
[boot] interface m-eth0
[boot-m-eth0]
```

【相关命令】

- **quit**

1.1.14 ip address

ip address 命令用来配置管理以太网接口的 IPv4 地址。

undo ip address 命令用来恢复缺省情况。

【命令】

ip address ip-address { mask-length | mask }
undo ip address

【缺省情况】

未配置管理以太网接口的 IPv4 地址。

【视图】

管理以太网接口视图

【参数】

ip-address: IPv4 地址，为点分十进制格式。

mask-length: 子网掩码长度，取值范围为 1~31。

mask: 子网掩码，为点分十进制格式。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

在手工关闭的管理以太网接口下配置或删除 IP 地址时，系统会同时自动激活该接口。

请确保配置的 IP 地址没有和网络上其它设备的 IP 地址冲突。

【举例】

将管理以太网接口的 IP 地址配置为 192.168.1.1/24。

```
<boot> system-view
[boot] interface m-eth0
[boot-m-eth0] ip address 192.168.1.1 24
```


1.1.15 ip gateway

ip gateway 命令用来配置管理以太网接口的 IPv4 网关。

undo ip gateway 命令用来恢复缺省情况。

【命令】

ip gateway *ip-address*

undo ip gateway

【缺省情况】

未配置管理以太网接口的 IPv4 网关。

【视图】

管理以太网接口视图

【参数】

ip-address: IPv4 网关的地址，为点分十进制格式。

【使用指导】

在 IPv4 网络中,当本设备需要和不在同一网段的远程设备通信时,需要配置 IPv4 网关来转发报文。

多次执行本命令，最后一次执行的命令生效。

修改或者删除管理以太网接口的 IP 地址，会导致网关配置被删除。

【举例】

将管理以太网接口的 IPv4 网关配置为 192.168.1.5。

```
<boot> system-view
```

```
[boot] interface m-eth0
```

```
[boot-m-eth0] ip gateway 192.168.1.5
```

1.1.16 ipv6 address

ipv6 address 命令用来配置管理以太网接口的 IPv6 地址。

undo ipv6 address 命令用来恢复缺省情况。

【命令】

ipv6 address *ipv6-address prefix-length*

undo ipv6 address

【缺省情况】

未配置管理以太网接口的 IPv6 地址。

【视图】

管理以太网接口视图

【参数】

ipv6-address: IPv6 地址。

prefix-length: 前缀的长度，取值范围为 1~127。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

在手工关闭的管理以太网接口下配置或删除 IPv6 地址时，系统会同时自动激活该接口。

【举例】

将管理以太网接口的 IPv6 地址配置为 2001::1/64。

```
<boot> system-view
[boot] interface m-eth0
[boot-m-eth0] ipv6 address 2001::1 64
```

1.1.17 ipv6 gateway

ipv6 gateway 命令用来配置管理以太网接口的 IPv6 网关。

undo ipv6 gateway 命令用来恢复缺省情况。

【命令】

```
ipv6 gateway link-local
undo ipv6 gateway
```

【缺省情况】

未配置管理以太网接口的 IPv6 网关。

【视图】

管理以太网接口视图

【参数】

link-local: IPv6 网关的链路本地地址。

【使用指导】

在 IPv6 网络中，当本设备需要和不在同一网段的远程设备通信时，需要配置 IPv6 网关来转发报文。

多次执行本命令，最后一次执行的命令生效。

修改或者删除管理以太网接口的 IPv6 地址，会导致 IPv6 网关配置被删除。

【举例】

将管理以太网接口的 IPv6 网关配置为 FE80::BAAF:67FF:FE27:DCD0。

```
<boot> system-view
[boot] interface m-eth0
[boot-m-eth0] ipv6 gateway FE80::BAAF:67FF:FE27:DCD0
```

1.1.18 mkdir

mkdir 命令用来在指定路径下创建文件夹。

【命令】

```
mkdir directory
```

【视图】

用户视图

【参数】

directory: 文件夹的名称。

【使用指导】

在使用该命令创建文件夹之前，指定的路径必须已经存在。比如：创建文件夹 `flash:/test/mytest` 时，`test` 文件夹必须已经存在，否则 `mytest` 文件夹创建失败。

如果创建的文件夹与指定路径下的其它文件或文件夹重名，则创建操作失败。

【举例】

```
# 创建文件夹 test。
<boot> mkdir flash:/test
Directory flash:/test created.
# 在路径 flash:/test/下创建文件夹 subtest。
<boot> mkdir flash:/test/subtest
Directory flash:/test/subtest created.
```

【相关命令】

- `dir`
- `rmdir`

1.1.19 more

`more` 命令用来显示指定文本文件的内容。

【命令】

`more file`

【视图】

用户视图

【参数】

file: 要显示的文件的名称。

【举例】

```
# 显示文件 test.txt 的内容。
<boot> more flash:/test.txt
Have a nice day.
```

1.1.20 move

`move` 命令用来移动文件。

【命令】

`move source-file { dest-file | dest-directory }`

【视图】

用户视图

【参数】

source-file: 源文件的名称。为 1~63 个字符的字符串，不区分大小写。

dest-file: 目标文件的名称。为 1~63 个字符的字符串，不区分大小写。

dest-directory: 为目标文件夹的名称。系统会将文件复制到指定文件夹，使用源文件名作为目标文件名。为 1~63 个字符的字符串，不区分大小写。

【使用指导】

如果指定的目标文件已存在，则系统会提示是否覆盖该文件，如果选择“Y”，系统会执行文件移动操作，如果选择“N”，则不做任何处理。

【举例】

移动文件 config.cfg 到目录 flash:/test 下。

```
<boot>move flash:/config.cfg flash:/test/
```

```
Move flash:/config.cfg to flash:/test/config.cfg?[Y/N]:y
```

```
<boot> dir flash:/test
```

```
Directory of flash:/test
```

```
0      -rw-      77065  Oct 20 1939 06:15:02      config.cfg
```

```
61440 KB total (11108 KB free)
```

1.1.21 ping

ping 命令用来检查指定目的端是否可达。

【命令】

```
ping [ -c count | -s size ] * ip-address
```

【视图】

任意视图

【参数】

-c count: 指定发送的 ICMP 回显请求报文的数目，取值范围为 1~2147483647，缺省值为 5。

-s size: 指定发送的 ICMP 回显请求报文的长度，取值范围为 20~8100，单位为字节，缺省值为 56。

ip-address: 目的端的 IPv4 地址，为点分十进制格式。

【使用指导】

执行 **ping** 命令后，源端会给目的端发送 ICMP 回显请求报文。在执行命令过程中，键入<Ctrl+C>可终止 **ping** 操作。

【举例】

检查到目的端 1.2.1.1 是否可达。

```
<boot> ping 1.2.1.1
```

```
PING 1.2.1.1 (1.2.1.1): 56 data bytes
```

```
56 bytes from 1.2.1.1: seq=0 ttl=128 time=2.243 ms
```

```
56 bytes from 1.2.1.1: seq=1 ttl=128 time=0.717 ms
```

```
56 bytes from 1.2.1.1: seq=2 ttl=128 time=0.891 ms
```

```
56 bytes from 1.2.1.1: seq=3 ttl=128 time=0.745 ms
56 bytes from 1.2.1.1: seq=4 ttl=128 time=0.911 ms

--- 1.2.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.717/1.101/2.243 ms
```

表1-6 ping 命令显示信息描述表

字段	描述
PING 1.2.1.1 (1.2.1.1)	检查IP地址为1.2.1.1的设备是否可达
56 data bytes	每个ICMP回显请求报文中的数据字节数
56 bytes from 1.2.1.1: seq=0 ttl=128 time=2.243 ms	收到IP地址为1.2.1.1的设备回复的ICMP响应报文 - bytes 表示 ICMP 响应报文中数据的字节数 - seq 表示报文序号，用来判断报文是否有分组丢失、失序或重复 - ttl 表示 ICMP 响应报文中的 TTL 值 - time 表示响应时间
--- 1.2.1.1 ping statistics ---	Ping操作中收发数据的统计结果
5 packets transmitted	发送的ICMP回显请求报文数
5 packets received	收到的ICMP响应报文数
0% packet loss	未响应请求报文占发送的总请求报文的百分比
round-trip min/avg/max = 0.717/1.101/2.243 ms	响应时间的最小值、平均值和最大值，单位为毫秒

1.1.22 ping ipv6

ping ipv6 命令用来检查指定 IPv6 地址是否可达。

【命令】

```
ping ipv6 [ -c count | -s size ] * ipv6-address
```

【视图】

任意视图

【参数】

- c count: 指定发送的 ICMPv6 回显请求报文的数目，取值范围为 1~2147483647，缺省值为 5。
- s size: 指定发送的 ICMPv6 回显请求报文的长度，取值范围为 20~8100，单位为字节，缺省值为 56。
- ipv6-address: 目的主机的 IPv6 地址。

【使用指导】

执行 ping ipv6 命令后，源端会给目的端发送 ICMPv6 回显请求报文。在执行命令过程中，键入 <Ctrl+C>可终止 ping ipv6 操作。

【举例】

```
# 检查到目的端 2001::2 是否可达。
<boot> ping ipv6 2001::2
ping ipv6 2001::2
PING 2001::2 (2001::2): 56 data bytes
56 bytes from 2001::2: seq=0 ttl=64 time=5.420 ms
56 bytes from 2001::2: seq=1 ttl=64 time=1.140 ms
56 bytes from 2001::2: seq=2 ttl=64 time=2.027 ms
56 bytes from 2001::2: seq=3 ttl=64 time=0.887 ms
56 bytes from 2001::2: seq=4 ttl=64 time=0.791 ms

--- 2001::2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.791/2.053/5.420 ms
该命令的显示信息描述表请参见 表 1-6。
```

1.1.23 pwd

pwd 命令用来显示当前工作路径。

【命令】

pwd

【视图】

用户视图

【举例】

```
# 显示当前工作路径。
<boot> pwd
flash:
```

1.1.24 quit

quit 命令用来从当前视图退回到上一级视图。

【命令】

quit

【视图】

系统视图

管理以太网接口视图

【举例】

```
# 从管理以太网接口视图退回到用户视图。
[boot-m-eth0] quit
[boot] quit
<boot>
```

1.1.25 reboot

reboot 命令用来重启当前登录的成员设备。

【命令】

reboot

【视图】

用户视图

【举例】

重启当前登录的成员设备。

```
<boot> reboot
```

1.1.26 reset ssh public-key

reset ssh public-key 命令用来清除保存在本设备的所有 SSH 服务器的公钥。

【命令】

reset ssh public-key

【视图】

用户视图

【使用指导】

在设备上使用 **ssh2** 命令首次登录 SSH 服务器时，设备会将该服务器的公钥保存到本地，以便下次登录进行身份认证时使用。如果 SSH 服务器的公钥变更，因为新旧公钥不一致，会导致设备再次 SSH 登录该服务器失败。此时可使用 **reset ssh public-key** 命令来清除原公钥，重新执行 **ssh2** 命令触发新的 SSH 协商。

【举例】

清除保存在本设备的所有 SSH 服务器的公钥。

```
<boot> ssh2 192.168.1.59
login as:client001
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@      WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!      @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
83:2d:b6:90:4a:1b:0e:c1:ea:af:09:3a:65:09:8a:b3.
Please contact your system administrator.
RSA host key for 192.168.1.59 has changed and you have requested strict checking
.
Host key verification failed.
<boot> reset ssh public-key
<boot> ssh2 192.168.1.59
login as:client001
```

```
The authenticity of host '192.168.1.59 (192.168.1.59)' can't be established.  
RSA key fingerprint is 83:2d:b6:90:4a:1b:0e:c1:ea:af:09:3a:65:09:8a:b3.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.1.59' (RSA) to the list of known hosts.  
client001@192.168.1.59's password:
```

```
*****  
* Copyright (c) 2015-2019 Beijing UNIS Hengyue Technologies Co., Ltd.      *  
* Without the owner's prior written consent,                             *  
* no decompiling or reverse-engineering shall be allowed.                 *  
*****
```

```
<Sysname.59>
```

1.1.27 rmdir

rmdir 命令用来删除已有目录。

【命令】

```
rmdir directory
```

【视图】

用户视图

【参数】

directory: 待删除的目录名。

【使用指导】

被删除的目录必须为空目录。即删除目录前，必须先删除该目录下的所有文件及子目录，文件的删除请参见 **delete** 命令。

【举例】

```
# 删除目录 mydir。  
<boot> rmdir flash:/mydir  
Remove directory flash:/mydir?[Y/N]:y  
Directory flash:/1 removed.
```

【相关命令】

- **delete**
- **dir**
- **mkdir**

1.1.28 shutdown

shutdown 命令用来关闭管理以太网接口。

undo shutdown 命令用来打开管理以太网接口。

【命令】

```
shutdown
```


undo shutdown

【缺省情况】

管理以太网接口处于打开状态。

【视图】

管理以太网接口视图

【使用指导】

当管理以太网接口异常时，可通过 **shutdown** 命令关闭此接口，然后再通过 **undo shutdown** 命令重新打开。

【举例】

```
# 关闭管理以太网接口。
<boot> system-view
[boot] interface m-eth0
[boot-m-eth0] shutdown
# 打开管理以太网接口。
[boot-m-eth0] undo shutdown
```

1.1.29 ssh2

ssh2 命令用来使用 SSH 协议登录到 SSH 服务器。

【命令】

```
ssh2 { server-ipv4-address | ipv6 server-ipv6-address }
```

【视图】

用户视图

【参数】

server-ipv4-address: SSH 服务器的 IPv4 地址，为点分十进制格式。

ipv6 server-ipv6-address: SSH 服务器的 IPv6 地址。

【使用指导】

如果在登录过程中，SSH 服务器长时间没有响应，用户可以使用<Ctrl+C>组合键中断本次 SSH 登录，稍后再试。

【举例】

```
# 使用 SSH 协议第一次登录到 SSH 服务器 192.168.1.59。
<boot> ssh2 192.168.1.59
login as:client001
The authenticity of host '192.168.1.59 (192.168.1.59)' can't be established.
RSA key fingerprint is 3d:ee:1f:f9:81:be:4f:aa:42:88:1c:ab:81:4e:95:6f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.59' (RSA) to the list of known hosts.
client001@192.168.1.59's password:

*****
```

```

* Copyright (c) 2015-2019 Beijing UNIS Hengyue Technologies Co., Ltd.      *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                  *
*****

```

```

<Sysname.59> quit
<boot>
# 使用 SSH 协议再次登录到 SSH 服务器 192.168.1.59。
<boot> ssh2 192.168.1.59
login as:client001
client001@192.168.1.59's password:

```

```

*****
* Copyright (c) 2015-2019 Beijing UNIS Hengyue Technologies Co., Ltd.      *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                  *
*****

```

```

<Sysname.59>

```

1.1.30 system-view

system-view 命令用来从用户视图进入系统视图。

【命令】

system-view

【视图】

用户视图

【举例】

```

# 从用户视图进入系统视图。
<boot> system-view
[boot]

```

【相关命令】

- **quit**

1.1.31 telnet

telnet 命令用来使用 Telnet 协议登录到 Telnet 服务器。

【命令】

telnet { server-ipv4-address | ipv6 server-ipv6-address }

【视图】

用户视图

【参数】

server-ipv4-address: Telnet 服务器的 IPv4 地址，为点分十进制格式。

server-ipv6-address: Telnet 服务器的 IPv6 地址。

【使用指导】

如果在登录过程中，Telnet 服务器长时间没有响应，用户可以使用<Ctrl+K>组合键中断本次 Telnet 登录，稍后再试。

【举例】

使用 Telnet 协议登录到 Telnet 服务器 192.168.100.1。

```
<boot> telnet 192.168.100.1
```

1.1.32 tftp

tftp 命令用来访问 TFTP 服务器。

【命令】

```
tftp server-ipv4-address { get remote-file local-file | put local-file remote-file }
```

```
tftp ipv6 server-ipv6-address { get remote-file local-file | put local-file remote-file }
```

【视图】

用户视图

【参数】

server-ipv4-address: TFTP 服务器的 IPv4 地址，点分十进制格式。

server-ipv6-address: TFTP 服务器的 IPv6 地址。

get *remote-file* *local-file*: 表示从 TFTP 服务器上下载一个文件到本地，*remote-file* 表示 TFTP 服务器上的文件的名称，*local-file* 表示本地的文件的名称。

put *local-file* *remote-file*: 表示从本地上传一个文件到 TFTP 服务器，*local-file* 表示本地的文件的名称，*remote-file* 表示 TFTP 服务器上的文件的名称。

【使用指导】

当网络拥塞，文件传输速度很慢的时候，用户可以使用<Ctrl+C>组合键中断本次 TFTP 操作，稍后再试。

【举例】

从 TFTP 服务器 192.168.1.100 上下载文件 111.txt，保存到本地时使用的文件名为 222.txt。

```
<boot> tftp 192.168.1.100 get 111.txt flash:/222.txt
```

将设备的启动配置文件 startup.cfg 上传到 TFTP 服务器 192.168.1.100。

```
<boot> tftp 192.168.1.100 put flash:/startup.cfg startup.cfg
```

目 录

1 设备管理.....	1-1
1.1 设备管理配置命令.....	1-1
1.1.1 clock datetime.....	1-1
1.1.2 clock protocol.....	1-2
1.1.3 clock summer-time.....	1-3
1.1.4 clock timezone.....	1-4
1.1.5 command.....	1-5
1.1.6 copyright-info enable.....	1-6
1.1.7 display alarm.....	1-7
1.1.8 display clock.....	1-7
1.1.9 display copyright.....	1-8
1.1.10 display cpu-usage.....	1-9
1.1.11 display cpu-usage configuration.....	1-10
1.1.12 display cpu-usage history.....	1-11
1.1.13 display device.....	1-13
1.1.14 display device manuinfo.....	1-15
1.1.15 display device manuinfo power.....	1-16
1.1.16 display diagnostic-information.....	1-17
1.1.17 display environment.....	1-19
1.1.18 display fan.....	1-20
1.1.19 display memory.....	1-21
1.1.20 display memory-threshold.....	1-22
1.1.21 display power.....	1-24
1.1.22 display scheduler job.....	1-25
1.1.23 display scheduler logfile.....	1-26
1.1.24 display scheduler reboot.....	1-27
1.1.25 display scheduler schedule.....	1-27
1.1.26 display system stable state.....	1-28
1.1.27 display transceiver alarm.....	1-30
1.1.28 display transceiver diagnosis.....	1-32
1.1.29 display transceiver interface.....	1-33
1.1.30 display transceiver manuinfo.....	1-34
1.1.31 display version.....	1-35

1.1.32 display version-update-record	1-36
1.1.33 header	1-37
1.1.34 job	1-38
1.1.35 locator blink	1-39
1.1.36 memory-threshold	1-39
1.1.37 memory-threshold usage	1-40
1.1.38 monitor cpu-usage enable	1-41
1.1.39 monitor cpu-usage interval	1-42
1.1.40 monitor cpu-usage statistics-interval core	1-43
1.1.41 monitor cpu-usage threshold	1-44
1.1.42 monitor disk-usage interval	1-45
1.1.43 monitor resend cpu-usage core-interval	1-45
1.1.44 monitor resource-usage { bridge-aggregation route-aggregation } threshold	1-46
1.1.45 monitor resource-usage bandwidth inbound threshold	1-47
1.1.46 monitor resource-usage context threshold	1-48
1.1.47 monitor resource-usage security-policy threshold	1-48
1.1.48 monitor resource-usage session-count threshold	1-49
1.1.49 monitor resource-usage session-rate threshold	1-50
1.1.50 monitor sample-interval	1-51
1.1.51 monitor statistics-interval	1-51
1.1.52 password-recovery enable	1-52
1.1.53 reboot	1-53
1.1.54 reset scheduler logfile	1-54
1.1.55 reset version-update-record	1-55
1.1.56 restore factory-default	1-55
1.1.57 scheduler job	1-56
1.1.58 scheduler logfile size	1-57
1.1.59 scheduler reboot at	1-57
1.1.60 scheduler reboot delay	1-58
1.1.61 scheduler schedule	1-59
1.1.62 shutdown-interval	1-60
1.1.63 sysid	1-61
1.1.64 sysname	1-61
1.1.65 temperature-limit	1-62
1.1.66 time at	1-64
1.1.67 time once	1-64

1.1.68 time repeating	1-66
1.1.69 usb disable	1-67
1.1.70 user-role	1-68

1 设备管理

1.1 设备管理配置命令

1.1.1 clock datetime

clock datetime 命令用来配置设备的系统时间。

【命令】

clock datetime *time date*

【缺省情况】

设备的系统时间为 UTC 时间 2011 年 1 月 1 日零点。

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

time: 配置的时间，格式为 HH:MM:SS（小时:分钟:秒），HH 取值范围为 0~23，MM 和 SS 取值范围为 0~59。如果要配置成整分，则可以不输入秒；如果要配置成整点，则可以不输入分和秒。比如将 **time** 参数配置为 0 表示零点。

date: 配置的日期，格式为 MM/DD/YYYY（月/日/年）或者 YYYY/MM/DD（年/月/日），MM 的取值范围为 1~12，DD 的取值范围与月份有关，YYYY 的取值范围为 2000~2035。

【使用指导】

仅缺省 Context 支持本命令。

为了保证与其它设备协调工作，为了更好的监控和维护设备，请确保设备的系统时间是准确的。

请先配置 **clock protocol none** 命令，再执行本命令。**clock datetime** 命令中指定的时间会立即生效，作为当前的系统时间。后续，设备使用内部晶体震荡器产生的时钟信号计时。

【举例】

配置设备的系统时间为 2015 年 1 月 1 日 8 时 8 分 8 秒。

```
<Sysname> clock datetime 8:8:8 1/1/2015
```

配置设备的系统时间为 2015 年 1 月 1 日 8 时 10 分。

```
<Sysname> clock datetime 8:10 2015/1/1
```

【相关命令】

- **clock protocol**
- **clock summer-time**
- **clock timezone**
- **display clock**

1.1.2 clock protocol

clock protocol 命令用来配置系统时间的获取方式。

undo clock protocol 命令用来恢复缺省情况。

【命令】

```
clock protocol { none | ntp context context-id }  
undo clock protocol
```

【缺省情况】

通过命令行配置系统时间。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

none: 表示通过命令行配置系统时间。

ntp: 表示通过 NTP（Network Time Protocol，网络时间协议）协议获取时间。关于 NTP 的详细介绍和配置，请参见“网络管理和监控配置指导”中的“NTP”。

context context-id: 表示从指定 Context 获取时间。**context-id** 表示 Context 的编号，关于 **context** 的取值范围及相关介绍，请参见“虚拟化技术命令参考”中的“Context”。

【使用指导】

仅缺省 Context 支持本命令。

为了保证与其它设备协调工作，为了更好的监控和维护设备，请确保设备的系统时间是准确的。系统时间的获取方式有：

- 配置 **clock protocol none** 命令后，通过 **clock datetime** 命令直接配置。**clock datetime** 命令中指定的时间即为当前的系统时间。后续，设备使用内部晶体震荡器产生的时钟信号计时。
- 配置 **clock protocol ntp** 命令后，通过 NTP 协议从网络中获取时间。该方式下，设备会周期性的同步服务器的 UTC（Coordinated Universal Time，国际协调时间）时间，并用同步得到的 UTC 时间和设备上配置的本地时区、夏令时参数运算，得出当前的系统时间。该方式获取的时间比命令行配置的时间更精准，推荐使用。

多次执行本命令，最后一次执行的命令生效。

所有 Context 的系统时间相同。当设备从某个 Context 获取时钟后，会同步给其它 Context。

【举例】

配置获取 UTC 时间的方式为通过命令行配置。

```
<Sysname> system-view  
[Sysname] clock protocol none
```


1.1.3 clock summer-time

clock summer-time 命令用来配置夏令时。

undo clock summer-time 命令用来恢复缺省情况。

【命令】

clock summer-time *name start-time start-date end-time end-date add-time*
undo clock summer-time

【缺省情况】

未配置夏令时。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

name: 夏令时的名称，为 1~32 个字符的字符串，区分大小写。

start-time: 开始时间，格式为 HH:MM:SS，HH 取值范围为 0~23，MM 和 SS 取值范围为 0~59。如果要配置成整分，则可以不输入秒；如果要配置成整点，则可以不输入分和秒。

start-date: 开始日期，有两种输入方式：

- 直接一次性输入月和日，参数格式为 MM/DD，MM 取值范围为 1~12，DD 的取值范围与月份有关。
- 分次输入月、日，各参数之间以<空格>键隔开。首先输入开始的月份，取值如下：January、February、March、April、May、June、July、August、September、October、November 或 December；然后输入开始的星期，用当月的第几个星期表示，取值如下：first、second、third、fourth、fifth 或 last；最后输入起始日，取值为 Sunday、Monday、Tuesday、Wednesday、Thursday、Friday 或 Saturday。

end-time: 结束时间，格式为 HH:MM:SS，HH 取值范围为 0~23，MM 和 SS 取值范围为 0~59。如果要配置成整分，则可以不输入秒；如果要配置成整点，则可以不输入分和秒。

end-date: 结束日期，有两种输入方式：

- 直接一次性输入月日，参数格式为 MM/DD，MM 取值范围为 1~12，DD 的取值范围与月份有关。
- 分次输入月、日，各参数之间以<空格>键隔开。首先输入开始的月份，取值如下：January、February、March、April、May、June、July、August、September、October、November 或 December；然后输入开始的星期，用当月的第几个星期表示，取值如下：first、second、third、fourth、fifth 或 last；最后输入起始日，取值为 Sunday、Monday、Tuesday、Wednesday、Thursday、Friday 或 Saturday。

add-time: 偏移时间，格式为 HH:MM:SS，HH 取值范围为 0~23，MM 和 SS 取值范围为 0~59。如果要配置成整分，则可以不输入秒；如果要配置成整点，则可以不输入分和秒。

【使用指导】

仅缺省 Context 支持本命令。

为了保证与其它设备协调工作，为了更好的监控和维护设备，请确保设备的系统时间是准确的。

配置该命令后，设备会自动重新计算当前的系统时间，计算后得到的系统时间可通过 **display clock** 命令查看。

请将所有网络设备的夏令时和当地夏令时保持一致。

【举例】

配置夏令时 PDT，从每年的 8 月 1 日的 06:00:00 开始，到 9 月 1 日的 06:00:00 结束，比当前设备标准时间增加 1 小时。

```
<Sysname> system-view
```

```
[Sysname] clock summer-time PDT 6 08/01 6 09/01 1
```

【相关命令】

- **clock datetime**
- **clock timezone**
- **display clock**

1.1.4 clock timezone

clock timezone 命令用来配置系统所在的时区。

undo clock timezone 命令用来恢复缺省情况。

【命令】

```
clock timezone zone-name { add | minus } zone-offset
```

```
undo clock timezone
```

【缺省情况】

系统所在的时区为零时区，即设备采用 UTC 时间。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

zone-name：时区名称，为 1~32 个字符的字符串，区分大小写。

add：在 UTC 时间的基础上增加指定时间。

minus：在 UTC 时间的基础上减少指定时间。

zone-offset：与 UTC 的时间差，格式为 HH:MM:SS，HH 取值范围为 0~23，MM 和 SS 取值范围为 0~59，如果要配置成整分，则可以不输入秒；如果要配置成整点，则可以不输入分和秒。

【使用指导】

仅缺省 Context 支持本命令。

为了保证与其它设备协调工作，为了更好的监控和维护设备，请确保设备的系统时间是准确的。

配置该命令后，设备会自动重新计算当前的系统时间，计算后得到的系统时间可通过 **display clock** 命令查看。

请将所有网络设备的时区和当地地理时区保持一致。

【举例】

配置本地时区名称为 Z5，比 UTC 标准时间增加 5 小时。

```
<Sysname> system-view
```

```
[Sysname] clock timezone Z5 add 5
```

【相关命令】

- **clock datetime**
- **clock summer-time**
- **display clock**

1.1.5 command

command 命令用来为 Job 分配命令。

undo command 命令用来取消为 Job 分配的命令。

【命令】

```
command id command
```

```
undo command id
```

【缺省情况】

没有为 Job 分配命令。

【视图】

Job 视图

【缺省用户角色】

network-admin

context-admin

【参数】

id: 命令编号，取值范围为 0~4294967295。该编号表示命令在 Job 中的执行顺序，编号小的命令优先执行。

command: 为 Job 分配的命令。

【使用指导】

多次输入 **command** 命令可以为当前 Job 分配多条命令，不同命令用编号来唯一区别。如果新分配命令的编号和已分配的某命令的编号相同，则新分配的命令会覆盖已分配的命令。

通过 **command** 分配的命令行必须是设备上可成功执行的命令行，不包括 **telnet**、**ftp**、**ssh2** 和 **monitor process**。由用户保证配置的正确性，否则，命令行不能自动被执行。

如果需要分配的命令（假设为 A）是用户视图下的命令，则直接使用 **command** 命令分配即可；如果需要分配的命令（假设为 A）是非用户视图下的命令，则必须先分配进入 A 所在视图的命令（指定较小的 **id** 值），再分配 A。

定时执行任务时,设备不会与用户交互信息。当需要用户交互确认时,系统将自动输入“Y”或“Yes”;当需要用户交互输入字符信息时,系统将自动输入缺省字符串,没有缺省字符串的将自动输入空字符串。

【举例】

为名称为 backupconfig 的 Job 分配命令,以便将配置文件 startup.cfg 备份到 TFTP 服务器 192.168.100.11。

```
<Sysname> system-view
[Sysname] scheduler job backupconfig
[Sysname-job-backupconfig] command 2 tftp 192.168.100.11 put flash:/startup.cfg backup.cfg
```

为 Job (假设名称为 shutdownGE) 分配命令,以便将接口 GigabitEthernet1/0/1 关闭。

```
<Sysname> system-view
[Sysname] scheduler job shutdownGE
[Sysname-job-shutdownGE] command 1 system-view
[Sysname-job-shutdownGE] command 2 interface gigabitethernet 1/0/1
[Sysname-job-shutdownGE] command 3 shutdown
```

【相关命令】

- scheduler job

1.1.6 copyright-info enable

copyright-info enable 命令用来开启版权信息显示功能。

undo copyright-info enable 命令用来关闭版权信息显示功能。

【命令】

```
copyright-info enable
undo copyright-info enable
```

【缺省情况】

版权信息显示功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

开启版权信息显示功能。

```
<Sysname> system-view
[Sysname] copyright-info enable
```

重新登录设备后,会显示如下信息:

```
*****
* Copyright (c) 2015-2019 Beijing UNIS Hengyue Technologies Co., Ltd.      *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
```

1.1.7 display alarm

display alarm 命令用来显示设备的告警信息。

【命令】

display alarm [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot *slot-number*: 显示指定成员设备的告警信息。*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，则表示所有成员设备。

【使用指导】

仅缺省 Context 支持本命令。

【举例】

显示设备的告警信息。
<Sysname> display alarm
Slot CPU Level Info
1 0 ERROR faulty

表1-1 display alarm 命令显示信息描述表

字段	描述
Slot	产生告警的slot，显示为“-”，表示产生告警的元件位于机框上
CPU	告警CPU的编号
Level	告警的级别，级别由高到低依次为ERROR、WARNING、NOTICE、INFO
Info	告警的详细信息。取值为： - faulty: 表示该 slot 处于 faulty 状态（该 slot 可能正在启动，或者当前处于故障状态） - Fan <i>n</i> is absent: 风扇 <i>n</i> 当前不在位 - Power <i>n</i> is absent: 电源 <i>n</i> 当前不在位 - Power <i>n</i> is faulty: 电源 <i>n</i> 处于异常状态 - The temperature of sensor <i>n</i> exceeds the lower limit: 传感器 <i>n</i> 的温度低于低温门限 - The temperature of sensor <i>n</i> exceeds the upper limit: 传感器 <i>n</i> 的温度高于高温门限

1.1.8 display clock

display clock 命令用来显示系统当前的时间、日期、本地时区以及夏令时配置。

【命令】

display clock

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

显示信息中，时间的格式采用“时:分:秒.毫秒”的格式。

【举例】

```
# 未配置本地时区时，显示系统当前日期和时间。
<Sysname> display clock
10:09:00.258 UTC Fri 03/16/2015
# 配置了本地时区 Z5 后，显示系统当前日期和时间。
<Sysname> display clock
15:10:00.152 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
# 配置了本地时区 Z5 和夏令时 PDT 后，显示系统当前日期和时间。
<Sysname> display clock
15:11:00.211 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
Summer Time : PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
```

【相关命令】

- **clock datetime**
- **clock timezone**
- **clock summer-time**

1.1.9 display copyright

display copyright 命令用来显示设备的版权信息。

【命令】

display copyright

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

context-admin
context-operator

【举例】

显示设备的版权信息。
<Sysname> display copyright
显示信息略……。

1.1.10 display cpu-usage

display cpu-usage 命令用来显示 CPU 利用率的统计信息。

【命令】

```
display cpu-usage [ summary ] [ slot slot-number [ cpu cpu-number [ core  
{ core-number | all } ] ] ]  
display cpu-usage [ control-plane | data-plane ] [ summary ] [ slot  
slot-number [ cpu cpu-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

control-plane: 显示控制平面 CPU 利用率的统计信息。不指定 **control-plane** 和 **data-plane** 参数时，显示整个 CPU 利用率的统计信息。

data-plane: 显示数据平面 CPU 利用率的统计信息。不指定 **control-plane** 和 **data-plane** 参数时，显示整个 CPU 利用率的统计信息。

summary: 以列表形式显示 CPU 利用率的统计信息。不指定该参数时，以区段形式显示 CPU 利用率的统计信息。

slot *slot-number*: 显示指定成员设备的 CPU 利用率的统计信息。*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，显示的是所有成员设备的相应信息。

cpu *cpu-number*: 显示指定 CPU 的利用率统计信息。*cpu-number* 表示 CPU 的编号。

core { *core-number* | **all** }: 显示 CPU 核利用率的统计信息。其中，**all** 表示显示所有 CPU 核利用率的统计信息；*core-number* 表示 CPU 核的编号，显示指定 CPU 核利用率的统计信息。不指定该参数时，显示所有 CPU 核的平均利用率。

【使用指导】

登录 Context 后执行该命令，会显示该 Context 可使用的 CPU 的利用率统计信息。

【举例】

```
# 以段的形式显示当前 CPU 利用率统计信息。
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
    1% in last 5 seconds
    1% in last 1 minute
    1% in last 5 minutes

# 以表的形式显示当前 CPU 利用率统计信息。
<Sysname> display cpu-usage summary
Slot CPU      Last 5 sec      Last 1 min      Last 5 min
1    0          17%          29%            28%
```

表1-2 display cpu-usage 命令显示信息描述表

字段	描述
1% in last 5 seconds	设备启动后，会以5秒为周期计算并记录一次该5秒内的CPU的平均利用率。该字段显示的是最近一个5秒统计周期内CPU的平均利用率
Last 5 sec	设备启动后，会以5秒为周期计算并记录一次该5秒内的CPU的平均利用率。该字段显示的是最近一个5秒统计周期内CPU的平均利用率
1% in last 1 minute	设备启动后，会以1分钟为周期计算并记录一次该1分钟内的CPU的平均利用率。该字段显示的是最近一个1分钟统计周期内CPU的平均利用率
Last 1 min	设备启动后，会以1分钟为周期计算并记录一次该1分钟内的CPU的平均利用率。该字段显示的是最近一个1分钟统计周期内CPU的平均利用率
1% in last 5 minutes	设备启动后，会以5分钟为周期计算并记录一次该5分钟内的CPU的平均利用率。该字段显示的是最近一个5分钟统计周期内CPU的平均利用率
Last 5 min	设备启动后，会以5分钟为周期计算并记录一次该5分钟内的CPU的平均利用率。该字段显示的是最近一个5分钟统计周期内CPU的平均利用率

1.1.11 display cpu-usage configuration

display cpu-usage configuration 命令用来显示 CPU 利用率监控功能的相关配置。

【命令】

```
display cpu-usage configuration [ slot slot-number [ cpu cpu-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number：表示设备在 IRF 中的成员编号。不指定该参数时，显示的是主设备上的相应信息。

cpu cpu-number：表示 CPU 的编号。

【使用指导】

登录 Context 后执行该命令，会显示该 Context 可使用的 CPU 的对应信息。

【举例】

```
# 显示 CPU 利用率监控功能的相关配置。
<Sysname> display cpu-usage configuration
CPU usage monitor is enabled.
Current monitor interval is 60 seconds.
Current monitor threshold is 90%.
Current monitor recovery threshold is 40%.
Current statistics-interval is 90 seconds for the following cores: 0 to 31.
```

表1-3 display cpu-usage configuration 命令显示信息描述表

字段	描述
CPU usage monitor is enabled.	CPU利用率历史记录功能处于开启状态
Current monitor interval is 60 seconds.	CPU利用率历史记录的采样周期为60秒
Current monitor threshold is 90%.	CPU利用率阈值
Current monitor recovery threshold is 40%.	CPU利用率的恢复阈值
Current statistics-interval is 90 seconds for the following cores: xx to xx.	CPU核利用率的统计周期

【相关命令】

- **monitor cpu-usage enable**
- **monitor cpu-usage interval**
- **monitor cpu-usage threshold**

1.1.12 display cpu-usage history

display cpu-usage history 命令用来以图表方式显示 CPU 利用率的历史信息。

【命令】

```
display cpu-usage history [ job job-id ] [ slot slot-number [ cpu  
cpu-number ] ]
```

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

job job-id: 显示指定进程的 CPU 利用率的历史信息。*job-id* 表示进程的编号, 取值范围为 1~2147483647。不指定该参数时, 显示的是整个系统的相应信息 (整个系统的 CPU 利用率等于所有进程 CPU 利用率之和)。可以使用 **display process** 命令可以查看当前运行的进程的编号和名称, **display process** 命令的详细介绍请参见“网络管理与监控”中的“系统维护与调试”。

slot slot-number: 显示指定成员设备的 CPU 利用率的历史信息。*slot-number* 表示设备在 IRF 中的成员编号。当不指定 **job** 和该参数时, 显示的是所有成员设备上所有进程的相应信息; 当指定 **job** 参数, 但不指定该参数时, 显示的是主设备上指定进程的相应信息。

cpu cpu-number: 显示指定 CPU 的利用率的历史信息。*cpu-number* 表示 CPU 的编号。当不指定 **job** 和该参数时, 表示所有 CPU。当指定 **job** 参数, 但不指定该参数时, 表示默认 CPU。

【使用指导】

开启 CPU 利用率历史记录功能后, 系统每隔一定时间 (可通过 **monitor cpu-usage interval** 命令配置) 会对 CPU 的利用率进行采样, 并把采样结果保存到历史记录区。通过 **display cpu-usage history** 命令可以查看到最近 60 个采样点的值。结果以坐标的形式进行显示, 显示信息中:

- 纵坐标表示利用率, 采用就近显示的原则。比如, 利用率的间隔为 5%, 则实际统计值 53% 将被显示成 55%, 实际统计值 52% 将被显示成 50%。
- 横坐标表示时间, 时间越靠左表示距离当前时间越近。
- 用连续的 # 号表示该时刻的利用率, 某个时间点上最高处的 # 号对应的纵坐标值即为该时刻 CPU 的利用率。

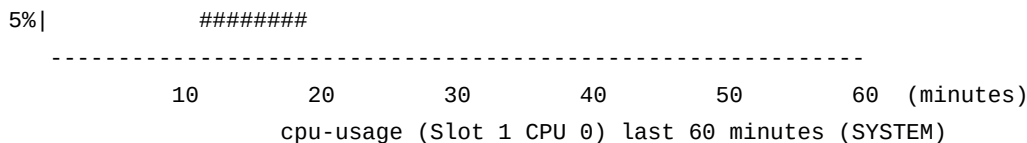
登录 Context 后执行该命令, 会显示该 Context 可使用的 CPU 的对应信息。

【举例】

以图表方式显示 CPU 利用率的历史记录。

```
<Sysname> display cpu-usage history
```

```
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|          #
 10%|        #### #
```



以上显示信息表明系统（用“SYSTEM”表示，运行在 Slot 1 CPU 0 上）在最近 60 分钟内 CPU 的利用率情况：12 分钟前大约为 5%，13 分钟前大约为 10%，14 分钟前大约为 15%，15 分钟前大约为 10%，16、17 分钟前大约为 5%，18 分钟前大约为 10%，19 分钟前大约为 5%，其它时间均小于或等于 2%。

【相关命令】

- **monitor cpu-usage enable**
- **monitor cpu-usage interval**

1.1.13 display device

display device 命令用来显示设备信息。

【命令】

display device [**cf-card** | **harddisk** | **usb**] [**slot** *slot-number* [**subslot** *subslot-number*] | **verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

cf-card: 显示 CF 卡的信息。

本参数的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	支持
T5000-G30	不支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	不支持
T1000-CN60/T1000-CN80	不支持

harddisk: 显示硬盘的信息。

本参数的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	不支持

型号	说明
T5000-G30	支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	支持
T1000-CN60/T1000-CN80	支持

usb: 显示 USB 接口的信息。
 本参数的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	不支持
T5000-G30	支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	支持
T1000-CN60/T1000-CN80	支持

slot slot-number: 显示指定成员设备的信息。*slot-number* 表示设备在 IRF 中的成员编号。
 不指定该参数时，表示所有成员设备。

subslot subslot-number: 显示指定子卡的信息。*subslot-number* 表示子卡所在的子槽位号。
 不指定该参数时，不会显示子卡的信息。

verbose: 显示设备的详细信息。不指定该参数时，显示设备的简要信息。

【使用指导】

不指定 **cf-card**、**harddisk** 和 **usb** 参数时，显示成员设备的信息。
 在缺省 Context 和非缺省 Context 下执行该命令，显示信息相同，且均显示物理设备的对应信息。

【举例】

```
# 显示设备信息。
<Sysname> display device
Slot.No   Cpu.Id   Brd Type   Brd Status   Subslot   Sft Ver   Patch Ver
1         0       T5000-G20   Normal       0         8524P08   None
1         0       NONE       Absent       1         None      None
```

表1-4 display device 命令显示信息描述表

字段	描述
Slot.No	成员编号
Cpu.Id	CPU编号
Brd Type	设备类型
Brd Status	成员设备的状态，取值为： - Normal: 表示该成员设备处于正常工作状态 - Absent: 表示该成员设备不存在 - Fault: 表示该成员设备不能正常工作

字段	描述
Soft Ver	设备上运行的软件版本
Patch Ver	当前设备上运行的、最新发布的热补丁版本。取值为None时表示没有安装热补丁 若同时安装了叠加补丁和非叠加补丁，则显示最新发布的叠加补丁。关于叠加补丁和非叠加补丁的介绍请参见“基础配置指导”中的“软件升级”

1.1.14 display device manuinfo

display device manuinfo 命令用来显示设备的电子标签信息。

【命令】

display device manuinfo [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot *slot-number*: 显示指定成员设备的电子标签信息。*slot-number* 表示设备在 IRF 中的成员编号。不输入该参数时，显示所有成员设备的相应信息。

【使用指导】

电子标签信息也可以称为永久配置数据或档案信息等，在硬件的调测（调试、测试）过程中被写入到设备的存储器件中，包括硬件的名称、生产序列号、MAC 地址、制造商等信息。

本命令仅缺省 Context 支持。

【举例】

```
# 显示设备的电子标签信息。
<Sysname> display device manuinfo
Slot 1 CPU 0:
DEVICE_NAME           : T5000-G20
DEVICE_SERIAL_NUMBER  : 210235A1RSH163000006
MAC_ADDRESS           : 50DA-00F2-1772
MANUFACTURING_DATE    : 2016-03-22
VENDOR_NAME           : UNIS
```

表1-5 display device manuinfo 命令信息显示描述表

字段	描述
Slot 1 CPU 0:	表示设备的电子标签信息，包括： • DEVICE_NAME: 表示设备的名称 • DEVICE_SERIAL_NUMBER: 表示设备的序列号 • MAC_ADDRESS: 表示设备出厂 MAC 地址 • MANUFACTURING_DATE: 表示设备的调测日期 • VENDOR_NAME: 表示设备制造商的名称 • PRODUCT ID: 表示产品代码
Subslot 1:	表示子卡的电子标签信息
Fan 1:	表示风扇的电子标签信息
Power 1:	表示电源的电子标签信息

1.1.15 display device manuinfo power

display device manuinfo power 命令用来显示电源的电子标签信息。

【命令】

display device manuinfo slot *slot-number* power *power-id*

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot *slot-number*: 表示设备在 IRF 中的成员编号。

power-id: 表示设备上电源的 ID 编号。

【使用指导】

本命令仅缺省 Context 支持。

【举例】

```
# 显示指定电源的电子标签信息。
<Sysname> display device manuinfo slot 1 power 1
Power 1:
DEVICE_NAME           : XXXX
DEVICE_SERIAL_NUMBER  : XXXXXXXXXXXXXXXXXXXX
MANUFACTURING_DATE    : XXXX-XX-XX
```

VENDOR_NAME : UNIS

本命令的显示信息描述请参见 [表 1-5](#)。

1.1.16 display diagnostic-information

display diagnostic-information 命令用来收集诊断信息。

【命令】

```
display diagnostic-information [ hardware | infrastructure | l2 | l3 |  
service ] [ context context-name ] [ key-info ] [ filename ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

hardware: 收集硬件相关的诊断信息。

infrastructure: 收集基础模块的诊断信息。

l2: 收集二层特性相关诊断信息。

l3: 收集三层特性相关诊断信息。

service: 收集上层业务模块相关诊断信息。

context context-name: 收集指定 Context 的诊断信息。*context-name* 表示 Context 的名称，为 1~15 个字符的字符串，区分大小写。不指定该参数时，收集缺省 Context 的诊断信息。

key-info: 收集关键诊断信息。当设备异常或者运行时间较长时，可能会产生较多诊断信息，此时，使用该关键字，即可以收集到关键的诊断信息，又可以缩短诊断信息的收集时间。不指定该参数时，收集当前全部诊断信息。

filename: 表示将收集到的诊断信息保存到指定文件。*filename* 表示文件的名称，后缀必须为“.tar.gz”。不指定该参数时，用户可根据提示信息选择将诊断信息保存到指定文件或者是直接显示诊断信息。

【使用指导】

在日常维护或系统出现故障时，为了便于问题定位，用户需要查看各个模块的诊断信息。因为各个功能模块都有其对应的运行信息，所以一般情况下，用户需要逐条运行相应的 **display** 命令。为便于一次性收集更多信息，用户可以在任意视图下执行 **display diagnostic-information** 命令，收集多个模块的诊断信息。

使用该命令，用户可以直接显示指定的诊断信息或者将诊断信息直接保存到指定文件，因为诊断信息较多，系统会自动将该文件压缩后保存，文件名后缀为“.tar.gz”。如果要在设备上查看该文件的内容，请执行以下操作：

(1) 使用 **tar extract** 命令将文件 XXXX.tar.gz 解包成文件 XXXX.gz。

(2) 使用 **gunzip** 命令将文件 **XXXX.gz** 解包成文件 **XXXX**。

(3) 使用 **more** 命令查看文件 **XXXX** 的内容。

如果收集诊断文件过程半途中止，可能导致 **gunzip** 命令无法正常解压，但诊断文件中仍包括已经生成的诊断信息，可以将诊断文件传输到 PC 上使用 Linux 系统下的 **gunzip -c** 命令解压查看。

不指定 **filename** 参数执行 **display diagnostic-information** 命令时，系统会要求用户选择显示诊断信息还是将诊断信息保存到文件中。如果用户选择保存诊断信息，且当系统提示用户输入文件名时直接回车，设备会自动将当前诊断信息保存到一个新文件，并使用设备名称和当前系统时间为该文件命名，以免和现有文件重名，导致现有文件被覆盖。如果设备名称中包含“/”、“\”、“:”、“*”、“?”、“<”、“>”、“|”、“”等特殊字符，在给诊断文件命名时，这些特殊字符会被转换为下划线“_”。比如设备的名称为 **A/B**，设备会使用形如 **flash:/diag_A_B_20160101-000438.tar.gz** 的字符串为新生成的诊断文件命名。

未指定 **hardware**、**infrastructure**、**l2**、**l3** 和 **service** 参数时，将收集设备产生的所有诊断信息。

该命令不支持“|”、“>”和“>>”参数。

执行本命令收集诊断信息时，请不要配置设备，以免影响收集结果。

【举例】

收集系统当前各个功能模块运行的统计信息。

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:n
=====
=====display clock=====
14:03:55 UTC Thu 01/05/2015
=====
=====display version=====
```

显示信息略……。

将收集到的诊断信息保存到缺省诊断文件。

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag_Sysname_20160101-024601.tar.gz]:
Diagnostic information is outputting to flash:/diag_Sysname_20160101-024601.tar.gz.
Please wait...
Save successfully.
```

请在“Please input the file name”提示信息处，直接回车。

将收集到的诊断信息保存到文件 **test.tar.gz**。

```
<Sysname> display diagnostic-information test.tar.gz
Diagnostic information is outputting to flash:/test.tar.gz.
Please wait...
Save successfully.
```

【相关命令】

- **gunzip**（基础配置命令参考/文件系统管理）
- **more**（基础配置命令参考/文件系统管理）
- **tar extract**（基础配置命令参考/文件系统管理）

1.1.17 display environment

display environment 命令用来显示设备上温度传感器的温度信息。

【命令】

display environment [slot slot-number]

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

slot slot-number: 显示 IRF 中指定成员设备上的温度传感器的温度信息。*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，显示的是 IRF 中所有温度传感器的温度信息。不指定该参数时，显示所有成员设备的对应信息。
本命令仅缺省 Context 支持。

【举例】

```
# 显示设备上所有温度传感器的温度信息。
<Sysname> display environment
System Temperature information (degree centigrade):
-----
-
Slot      Sensor  Temperature LowerLimit Warning-UpperLimit Alarm-UpperLimit Shutdown-UpperLimit
1         inflow 1      39           0             60             70              NA
1         outflow 1      64           0             80             92              NA
```

表1-6 display environment 命令显示信息描述表

字段	描述
System Temperature information (degree centigrade)	系统温度信息，单位为摄氏度
sensor	温度传感器 - hotspot: 表示热点温度传感器 - inflow: 表示入风口温度传感器 - outflow: 表示出风口温度传感器
Slot	当显示数字时表示指定slot上温度传感器的温度信息
Temperature	当前温度
LowerLimit	低温告警门限。当显示为NA时，表示不支持该门限

字段	描述
Warning-UpperLimit	一般级（Warning）高温告警门限。当显示为NA时，表示不支持该门限
Alarm-UpperLimit	严重级（Alarm）高温告警门限。当显示为NA时，表示不支持该门限
Shutdown-UpperLimit	关断级（Shutdown）高温告警门限，当温度传感器的温度大于该门限时，设备会自动关闭。当显示为NA时，表示不支持该门限

1.1.18 display fan

display fan 命令用来显示风扇的工作状态。

【命令】

display fan [slot slot-number [fan-id]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示所有风扇。

fan-id: 表示设备内置风扇的编号。不指定该参数时，表示指定位置的所有风扇。

本参数的取值范围与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	取值范围为0~3
T5000-G30	取值范围为0~3
T1000-G20/T1000-G50/T1000-G60/T1000-G80	取值范围为0~2
T1000-CN60/T1000-CN80	取值范围为0~2

verbose: 显示设备内置风扇的详细信息。不指定该参数时，显示设备内置风扇的简要信息。

【使用指导】

本命令仅缺省 Context 支持。

【举例】

显示设备上所有风扇的工作状态。

```
<Sysname> display fan
SLOT 1 Fan 0      Status: Normal  Speed:9500
SLOT 1 Fan 1      Status: Normal  Speed:9500
```

SLOT 1 Fan 2 Status: Normal Speed:9500

表1-7 display fan 命令显示信息描述表

字段	描述
SLOT 1	设备的成员编号
Fan 0	设备上风扇的编号
Status	风扇状态: • Absent: 风扇不在位 • Normal: 风扇正常工作 • Fault: 风扇故障 • FanDirectionFault: 用户期望的风道方向与风扇框的实际风道方向不一致
Speed	风扇速率

1.1.19 display memory

display memory 命令用来显示内存使用情况。

【命令】

display memory [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

summary: 显示内存使用情况的简要信息。不指定该参数时，显示内存使用情况的详细信息。

slot *slot-number*: 表示设备在 IRF 中的成员编号。不指定该参数时，表示所有成员设备。

cpu *cpu-number*: 表示 CPU 编号。

【使用指导】

登录 Context 后执行该命令，会显示该 Context 可使用的内存的使用情况。

【举例】

显示设备的内存使用情况的详细信息。

```
<Sysname> display memory
```

Memory statistics are measured in KB:

Slot 1:

	Total	Used	Free	Shared	Buffers	Cached	FreeRatio
Mem:	984560	456128	528432	0	4	45616	53.7%

```

-/+ Buffers/Cache:      410508      574052
Swap:                   0           0           0
# 显示设备的内存使用情况的简要信息。
<Sysname> display memory summary
Memory statistics are measured in KB:
Slot CPU      Total      Used      Free  Buffers    Caches FreeRatio
  1    0      984560    456128    528432      4     45616     53.7%

```

表1-8 display memory 命令显示信息描述表

字段	描述
Memory statistics are measured in KB:	系统内存使用情况，以下统计信息均以KB为单位
Mem	内存使用信息
Total	系统可分配的物理内存的大小 设备总物理内存分为不可分配物理内存和可分配物理内存。其中，不可分配物理内存用于内核代码段存储、内核管理开销以及ISSU功能运行等；可分配物理内存用于支撑业务模块的运行、文件存储等操作。不可分配内存的大小由设备根据系统运行需要自动计算划分，可分配物理内存的大小等于设备总物理内存减去不可分配内存的大小
Used	整个系统已用的物理内存大小
Free	整个系统可用的物理内存大小
Shared	多个进程共享的物理内存总额。取值为“--”时，表示不支持统计该参数的值
Buffers	已使用的文件缓冲区的大小。取值为“--”时，表示不支持统计该参数的值
Cached	高速缓冲寄存器已使用的内存大小。取值为“--”时，表示不支持统计该参数的值
Caches	高速缓冲寄存器已使用的内存大小
FreeRatio	整个系统物理内存的空闲率
-/+ buffers/cache	-/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached，表示应用程序已用的物理内存大小 -/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached，表示应用程序可用的物理内存大小
Swap	交换分区的使用信息

1.1.20 display memory-threshold

display memory-threshold 命令用来显示内存告警门限相关信息。

【命令】

display memory-threshold [slot slot-number [cpu cpu-number]]

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 编号。

【使用指导】

仅缺省 Context 支持本命令。

当设备已经使用的物理内存大小超过内存某个告警门限阈值时，系统会认为发生了一次该类型内存异常，并记录第一次、最近一次发生异常的时间，以及这段时间内发生的该类异常的次数。如果想了解该类异常的详细情况，请查看日志信息，可按日志摘要关键字“MEM_EXCEED_THRESHOLD”或“MEM_BELOW_THRESHOLD”进行搜索。

【举例】

显示内存告警门限相关信息。

```
<Sysname> display memory-threshold
Memory usage threshold: 100%
Free memory threshold:
    Minor: 224M
    Severe: 128M
    Critical: 96M
    Normal: 256M
Current memory state: Normal
Event statistics:
[Back to normal state]
    First notification: 0.0
    Latest notification: 0.0
    Total number of notifications sent: 0
[Enter minor low-memory state]
    First notification at: 0.0
    Latest notification at: 0.0
    Total number of notifications sent: 0
[Back to minor low-memory state]
    First notification at: 0.0
    Latest notification at: 0.0
    Total number of notifications sent: 0
[Enter severe low-memory state]
    First notification at: 0.0
    Latest notification at: 0.0
    Total number of notifications sent: 0
[Back to severe low-memory state]
    First notification at: 0.0
    Latest notification at: 0.0
    Total number of notifications sent: 0
[Enter critical low-memory state]
    First notification at: 0.0
    Latest notification at: 0.0
    Total number of notifications sent: 0
```

表1-9 display memory-threshold 命令显示信息描述表

字段	描述
Memory usage threshold	内存利用率阈值
Free-memory thresholds Minor Severe Critical Normal	剩余内存门限阈值： - Minor: 一级告警门限，单位为 MB - Severe: 二级告警门限，单位为 MB - Critical: 三级告警门限，单位为 MB - Normal: 恢复到正常状态的阈值，单位为 MB
Current free-memory state	系统当前内存使用状态： - Normal: 正常状态 - Minor: 一级告警门限状态 - Severe: 二级告警门限状态 - Critical: 三级告警门限状态
Free-memory event statistics:	门限事件统计信息，事件分为： - Back to normal state: 内存恢复到正常状态 - Entered minor alarm state: 进入一级告警门限状态 - Back to minor alarm state: 恢复到一级告警前的状态 - Entered severe alarm state: 进入二级告警门限状态 - Back to severe alarm state: 恢复到二级告警前的状态 - Entered critical alarm state: 进入三级告警门限状态
First notification at	事件第一次发生的时间，格式yyyy-mm-dd hh:mm:ss.msec
Latest notification at	事件最近一次发生的时间，格式yyyy-mm-dd hh:mm:ss.msec
Total number of notification send	事件发生的总次数

1.1.21 display power

display power 命令用来显示设备电源的信息。

【命令】

display power [slot slot-number [power-id]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示所有电源。
power-id: 表示电源模块的编号。不指定该参数时，表示指定位置的所有电源。

【使用指导】

本命令仅缺省 Context 支持。

【举例】

显示设备电源的简要信息。

```
<Sysname> display power
Slot 1 Power 0      Status: Absent
Slot 1 Power 1      Status: Normal
```

表1-10 display power 命令显示信息描述表

字段	描述
Power	设备上的电源模块编号
Status	电源模块的状态 - Absent: 电源不在位 - Normal: 电源正常工作 - Fault: 电源故障

1.1.22 display scheduler job

display scheduler job 命令用来显示 Job 的配置信息。

【命令】

display scheduler job [*job-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

job-name: Job 的名称，为 1~47 个字符的字符串，区分大小写。不指定该参数时，则显示所有 Job 的配置信息。

【举例】

查看所有 Job 的配置信息。

```
<Sysname> display scheduler job
```

```
Job name: saveconfig
copy startup.cfg backup.cfg
```

```
Job name: backupconfig
```

```
Job name: creat-VLAN100
system-view
vlan 100
```

以上显示信息表明，设备当前配置了 3 个 Job，分别显示了 Job 的名称，以及为 Job 分配的命令（如果没有为 Job 分配命令，则只显示 Job 的名称），不同 Job 间用空行分隔。

1.1.23 display scheduler logfile

display scheduler logfile 命令用来显示 Job 的执行日志信息。

【命令】

```
display scheduler logfile
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【举例】

```
# 显示 Schedule 日志文件的相关信息。
<Sysname> display scheduler logfile
Logfile Size: 1902 Bytes.

Job name      : shutdown
Schedule name : shutdown
Execution time : Tue Dec 27 10:44:42 2015
Completion time : Tue Dec 27 10:44:47 2015
----- Job output -----
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface rang gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[Sysname-if-range]shutdown
```

表1-11 display scheduler logfile 命令显示信息描述表

字段	描述
Logfile Size	Schedule日志文件的大小，单位为字节
Job name	Job的名称
Schedule name	Schedule的名称

字段	描述
Execution time	开始执行Job的时间
Completion time	Job执行结束的时间（没有调度的或者没有分配命令的Job，均不会显示该信息）
Job output	Job中的命令执行时的输出信息

【相关命令】

- **reset scheduler logfile**

1.1.24 display scheduler reboot

display scheduler reboot 命令用来显示定时重启功能的相关配置。

【命令】

display scheduler reboot

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 显示定时重启功能的相关配置。
<Sysname> display scheduler reboot
System will reboot at 16:32:00 05/23/2015 (in 1 hours and 39 minutes).
```

【相关命令】

- **scheduler reboot at**
- **scheduler reboot delay**

1.1.25 display scheduler schedule

display scheduler schedule 命令用来显示 Schedule 的相关信息。

【命令】

display scheduler schedule [*schedule-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

context-admin
context-operator

【参数】

schedule-name: Schedule 的名称, 为 1~47 个字符的字符串, 区分大小写。如果不指定该参数, 则显示所有 Schedule 的信息。

【举例】

显示所有 Schedule 的信息。

```
<Sysname> display scheduler schedule
Schedule name       : shutdown
Schedule type       : Run once after 0 hours 2 minutes
Start time          : Tue Dec 27 10:44:42 2015
Last execution time : Tue Dec 27 10:44:42 2015
Last completion time : Tue Dec 27 10:44:47 2015
Execution counts    : 1
-----
Job name                Last execution status
shutdown                Successful
```

表1-12 display scheduler schedule 命令显示信息描述表

字段	描述
Schedule name	Schedule的名称
Schedule type	Schedule的执行时间配置。如果没有为Schedule配置执行时间, 则不会显示该信息
Start time	Schedule第一次开始执行的时间。如果没有为Schedule配置执行时间, 则不会显示该信息
Last execution time	Schedule上一开始执行的时间 - 如果没有为 Schedule 配置执行时间, 则不会显示该信息 - 如果还没有执行, 则显示 Yet to be executed
Last completion time	Schedule上一次执行完成的时间。如果没有为Schedule配置执行时间, 则不会显示该信息
Execution counts	Schedule已经执行的次数。如果Schedule还没有执行, 则不会显示该信息
Job name	Schedule下关联的Job的名称
Last execution status	Job上一次被执行的状态 (Job下分配的命令是否执行以及执行结果, 请通过 display scheduler logfile 命令查看) - Successful: 表示执行成功 - Failed: 表示执行失败 - Waiting: 表示正在等待被执行 - In process: 表示正在执行 -NA-: 表示还没有到执行时间

1.1.26 display system stable state

display system stable state 命令用来显示系统的稳定状态。

【命令】

display system stable state [context { context-id | all }]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

context { context-id | all }: 显示指定或所有 Context 的系统稳定状态。*context-id* 表示 Context 的编号，关于 **context** 的取值范围及相关介绍，请参见“虚拟化技术命令参考”中的“Context”。

【使用指导】

不指定 **context** 参数时，显示系统的稳定状态。

在进行 ISSU 升级或主备倒换前，请先执行该命令，检查设备是否处于稳定状态。如果 System State 未处于 Stable 状态，不能进行 ISSU 升级；如果 Redundancy Stable 未处于 Stable 状态，不能进行主备倒换。

设备/Context 启动需要一定的时间，才能达到 Stable 状态。如果设备/Context 长时间未能进入 Stable 状态，可通过该命令的显示信息找出未稳定的设备/Context，根据其具体状态，采取进一步措施。

系统处于不稳定状态时，需要结合相关命令查看设备的具体情况。例如：

- 通过 **display device** 命令查看设备是否处于故障状态。
- 通过 **display ha service-group** 命令查看 HA 服务组的状态，以找出未批复完成的模块。
- 通过 Probe 视图下的 **display system internal process state** 命令查看服务启动状态。

操作时，建议多次执行命令，以确认稳定状态的连续性。

【举例】

显示系统的稳定状态。

```
<Sysname> display system stable state
System state      : Stable
Redundancy state: No redundancy
  Slot   CPU   Role     State
  ----   ---   ---     ---
   1      0   Active   Stable
```

表1-13 display system stable state 命令显示信息描述表

字段	描述
System state	系统状态： - Stable: 稳定运行 - Not ready: 未稳定，此时不能进行 ISSU 升级
Redundancy state	主备状态： - Stable: 主备状态稳定，可以倒换 - No redundancy: 系统无冗余，不能倒换 - Not ready: 未稳定，不可以倒换
Role	成员设备在系统中的身份： - Active: 主设备 - Standby: 备设备，提供冗余备份
State	成员设备状态： - Stable: 成员设备稳定运行 - Board inserted: 成员设备加入 - Kernel initiating: 成员设备内核初始化 - Service starting: 成员设备上的服务正在启动 - Service stopping: 成员设备上的服务正在关闭 - HA Batch backup: HA 批量备份中 - Interface data batch backup: 接口管理批量备份未完成 - Context starting: Context 正在启动 - Context stopping: Context 正在关闭
*	当前对象处于未稳定状态

【相关命令】

- display context（虚拟化技术命令参考/Context）
- display device
- display ha service-group（可靠性命令参考/进程分布优化）

1.1.27 display transceiver alarm

display transceiver alarm 命令用来显示可插拔接口模块的当前故障告警信息。

【命令】

display transceiver alarm interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

interface [*interface-type interface-number*]: 显示接口上插入的可插拔接口模块的当前故障告警信息。*interface-type interface-number* 表示接口类型和接口编号，如果不指定该参数，表示所有接口。

【使用指导】

目前，使用的可插拔接口模块可能出现的故障告警信息见“**display transceiver alarm** 命令输出信息描述表”。如果没有故障，则显示为 None。

表1-14 SFP/SFP+的 display transceiver alarm 命令输出信息描述表

字段	描述
RX loss of signal	接收信号丢失
RX power high	接收光功率高
RX power low	接收光功率低
TX fault	发送错误
TX bias high	偏置电流高
TX bias low	偏置电流低
TX power high	发送光功率高
TX power low	发送光功率低
Temp high	温度高
Temp low	温度低
Voltage high	电压高
Voltage low	电压低
Transceiver info I/O error	模块信息读写错误
Transceiver info checksum error	模块信息校验和错误
Transceiver type and port configuration mismatch	模块类型和端口配置不匹配
Transceiver type not supported by port hardware	端口不支持该模块类型

【举例】

显示接口 GigabitEthernet1/0/1 上插入的可插拔接口模块的当前故障告警信息。

```
<Sysname> display transceiver alarm interface gigabitethernet 1/0/1
```

GigabitEthernet1/0/1 transceiver current alarm information:

RX loss of signal

RX power low

表1-15 display transceiver alarm 显示信息描述表

字段	描述
transceiver current alarm information	接口光模块当前故障告警信息
RX loss of signal	接收信号丢失
RX power low	接收光功率低告警

1.1.28 display transceiver diagnosis

display transceiver diagnosis 命令用来显示可插拔光模块的数字诊断参数的当前测量值。

【命令】

display transceiver diagnosis interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface [*interface-type interface-number*]：显示接口上插入的可插拔光模块的数字诊断参数的当前测量值。*interface-type interface-number* 表示接口类型和接口编号，如果不指定该参数，表示所有接口。

【举例】

显示接口 GigabitEthernet1/0/1 上插入的可插拔光模块的数字诊断参数的当前测量值。

```
<Sysname> display transceiver diagnosis interface gigabitethernet 1/0/1
```

```
GigabitEthernet1/0/1 transceiver diagnostic information:
```

```
Current diagnostic parameters:
```

Temp(°C)	Voltage(V)	Bias(mA)	RX power(dBm)	TX power(dBm)
36	3.31	6.13	-35.64	-5.19

```
Alarm thresholds:
```

	Temp(°C)	Voltage(V)	Bias(mA)	RX power(dBm)	TX power(dBm)
High	50	3.55	1.44	-10.00	5.00
Low	30	3.01	1.01	-30.00	0.00

表1-16 display transceiver diagnosis 显示信息描述表

字段	描述
transceiver diagnostic information	接口插入的光模块的数字诊断信息
Current diagnostic parameters	当前的诊断参数

字段	描述
Temp.(°C)	数字诊断参数——温度，单位为°C，精确到1°C
Voltage(V)	数字诊断参数——电压，单位为V，精确到0.01V
Bias(mA)	数字诊断参数——偏置电流，单位为mA，精确到0.01mA
RX power(dBm)	数字诊断参数——接收光功率，单位为dBm，精确到0.01dBm
TX power(dBm)	数字诊断参数——发送光功率，单位为dBm，精确到0.01dBm
Alarm thresholds	告警门限
High	高告警门限
Low	低告警门限

1.1.29 display transceiver interface

display transceiver interface 命令用来显示可插拔接口模块的主要特征参数。

【命令】

display transceiver interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-type interface-number: 显示接口上插入的可插拔接口模块的主要特征参数。
interface-type interface-number 表示接口类型和接口编号，如果不指定该参数，表示所有接口。

【举例】

显示接口 GigabitEthernet1/0/1 上插入的可插拔接口模块的主要特征参数。

```
<Sysname> display transceiver interface gigabitethernet 1/0/1
```

```
GigabitEthernet1/0/1 transceiver information:
```

```
Transceiver Type       : 1000_BASE_SX_SFP
Connector Type         : LC
Wavelength(nm)         : 850
Transfer Distance(m)    : 550(50um),270(62.5um)
Digital Diagnostic Monitoring : YES
Vendor Name            : UNIS
Ordering Name          : SFP-GE-SX-MM850
```

表1-17 display transceiver interface 显示信息中光学参数统计信息描述表

字段	描述
Transceiver Type	光模块的类型
Connector Type	光连接器的类型
Wavelength(nm)	- 对于光模块：显示发送激光中心波长，单位 nm；对于支持多条不同波长光路的模块（例如 10GBASE-LX4 模块），各个波长值之间用逗号分隔 - 对于电模块：显示为 “N/A”
Transfer Distance(m)	传输距离，对于单模模块，xx显示为km，其他模块xx显示为m。当模块支持多种传输介质时，各个传输距离值之间用逗号分隔。距离值后面括号里包含对应的“传输介质”。下面是各个介质的名称： 9um：表示 9/125um 单模光纤 50um：表示 50/125um 多模光纤 62.5um：表示 62.5/125um 多模光纤 - TP：表示双绞线 - CX4：表示 CX4 电缆
Digital Diagnostic Monitoring	对数字诊断功能的支持情况，其中： - YES：表示支持数字诊断 - NO：表示不支持数字诊断
Vendor Name	模块生产或定制厂商名称
Ordering Name	可插拔接口模块的对外型号

1.1.30 display transceiver manuinfo

display transceiver manuinfo 命令用于显示可插拔接口模块的电子标签信息。

【命令】

display transceiver manuinfo interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface [*interface-type interface-number*]：显示接口上插入的可插拔接口模块的部分电子标签信息。*interface-type interface-number* 表示接口类型和接口编号，如果不指定该参数，表示所有接口。

【举例】

```
# 显示接口 GigabitEthernet1/0/1 上插入的可插拔接口模块的电子标签信息。
<Sysname> display transceiver manuinfo interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver manufacture information:
  Manu. Serial Number   : 213410A0000054000251
  Manufacturing Date    : 2017-09-01
  Vendor Name           : UNIS
```

表1-18 display transceiver manuinfo 显示信息中光学参数统计信息描述表

字段	描述
Manu. Serial Number	光模块的序列号
Manufacturing Date	光模块的生产日期
Vendor Name	光模块定制厂商的名称

1.1.31 display version

display version 命令用来显示系统版本信息。

【命令】

display version

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 查看系统版本信息。
<Sysname> display version
UNIS Uniware Software, Version 7.1.064, Ess 8524P08
Copyright (c) 2015-2019 Beijing UNIS Hengyue Technologies Co., Ltd.
UNIS T5000-G20 uptime is 0 weeks, 0 days, 5 hours, 11 minutes
Last reboot reason: User reboot

Boot image: cfa0:/main-unw710-boot-E8524P08.bin
Boot image version: 7.1.064, Ess 8524P08
  Compiled Jun 11 2018 16:00:00
System image: cfa0:/main-unw710-system-E8524P08.bin
System image version: 7.1.064, Ess 8524P08
  Compiled Jun 11 2018 16:00:00
```

显示信息略……。

表1-19 display version 命令显示信息描述表

字段	描述
UNIS Uniware Software, Version 7.1.064, Ess 8524P08	表示设备使用的软件版本
Copyright (c) 2015-2019 Beijing UNIS Hengyue Technologies Co., Ltd.	表示设备的版权申明
UNIS T5000-G20 uptime is 0 weeks, 0 days, 5 hours, 11 minutes	表示设备的型号以及本次启动后的持续运行时间
Last reboot reason	表示设备上上次重启的原因，主要取值有： • User reboot: 表示用户通过命令行、SNMP 等方式重启设备 • Cold reboot: 表示断电导致的重启 • Kernel abnormality reboot: 表示内核异常导致的重启 • DeadLoop reboot: 表示内核死循环导致的重启 • DEV HandShake reboot: 表示设备管理握手失败导致的重启 • SlaveSwitch reboot: 表示主备倒换导致的重启 • IRF Merge reboot: 表示 IRF 合并重启本设备 • Auto Update reboot: 表示版本自动升级导致的重启
Boot image: cfa0:/main-unw710-boot-E8524P08.bin Boot image version: 7.1.064, Ess 8524P08 Compiled Jun 11 2018 16:00:00	表示设备当前运行过程中使用的Boot包以及该软件包的版本、编译时间

1.1.32 display version-update-record

display version-update-record 命令用来显示启动软件包版本更新操作的记录。

【命令】

display version-update-record

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

仅缺省 Context 支持本命令。

设备启动时会记录当前使用的启动软件包版本信息，如果在运行过程中进行启动软件包版本更新操作，系统会记录该次更新的简要信息，包括升级时间和版本，以便管理员了解相关信息。设备重启这些记录也不会被删除。

【举例】

```
# 显示设备启动软件包版本更新操作的记录。
<Sysname> display version-update-record
Record 1 (updated on Apr 18 2015 at 06:23:54):
  *Name      : simware-unw710-boot.bin
  Version    : 7.1.070 Test 0001
  Compile time: Mar 25 2015 15:52:43

  *Name      : simware-unw710-system.bin
  Version    : 7.1.070 Test 0001
  Compile time: Mar 25 2015 15:52:43
```

表1-20 display version-update-record 命令显示信息描述表

字段	描述
Record <i>n</i> (updated on Apr 18 2014 at 06:23:54)	最近的第 <i>n</i> 次更新的时间，Record 1为最新的一次更新
*Name	软件包的名称。带*符号，表示软件包的版本和升级前的版本有变化；不带*符号，表示版本没有变化
Version	软件包的版本号
Compile time	版本编译时间

【相关命令】

- **reset version-update-record**

1.1.33 header

header 命令用来配置欢迎信息。

undo header 命令用来取消配置的欢迎信息。

【命令】

```
header { legal | login | motd | shell } text
undo header { legal | login | motd | shell }
```

【缺省情况】

未配置欢迎信息。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

legal: 配置登录终端界面前的授权信息，在输入认证用户名和密码前输出。

login: 配置登录验证时的欢迎信息。

motd: 配置登录终端界面前的欢迎信息。

shell: 配置用户登录进入用户视图时的欢迎信息。

text: 欢迎信息的内容。内容的输入支持单行和多行两种方式，具体输入规则请参见“基础配置指导”中的“设备管理”。

【举例】

```
# 配置 legal 欢迎信息。
<Sysname> system-view
[Sysname] header legal
Please input banner content, and quit with the character '%'.
Welcome to use the legal banner%
```

1.1.34 job

job 命令用来为 Schedule 分配 Job。

undo job 命令用来将 Job 从 Schedule 中删除。

【命令】

```
job job-name
undo job job-name
```

【缺省情况】

未为 Schedule 分配 Job。

【视图】

Schedule 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

job-name: Job 的名称，为 1~47 个字符的字符串，区分大小写。

【使用指导】

多次执行该命令，可以为 Schedule 分配多个 Job。多个 Job 在 Schedule 指定的时间同时执行，没有先后顺序。

分配的 Job 必须是设备上已经创建的 Job，否则不能分配。Job 可以通过 **scheduler job** 命令来创建。

【举例】

```
# 为 Schedule 分配一个名称为 save-job 的 Job。
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] job save-job
```

【相关命令】

- **scheduler job**
- **scheduler schedule**

1.1.35 locator blink

locator blink *blink-time* 命令用来定位设备的位置。

locator blink stop 命令用来停止定位。

【命令】

locator [**slot** *slot-number*] **blink** *blink-time*

locator [**slot** *slot-number*] **blink stop**

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number*: 表示设备在 IRF 中的成员编号。不指定该参数时，表示对所有设备进行操作。

blink-time: 闪烁的持续时间，取值范围为 5~120，单位为秒。

stop: 停止闪烁。

【使用指导】

仅缺省 Context 支持本命令。

配置 **locator blink blink-time** 命令后，指定设备上用于定位的 LED 灯会以间隔快闪的方式闪烁，并持续指定的时间。用户可根据 LED 灯的指示来定位设备所在的位置。

blink-time 时间到或者执行 **locator blink stop** 命令，则定位闪烁的 LED 灯会恢复正常点亮状态。

【举例】

开始定位。

```
<Sysname> locator blink 30
```

结束定位。

```
<Sysname> locator blink stop
```

1.1.36 memory-threshold

memory-threshold 命令用来配置空闲内存告警的门限值。

undo memory-threshold 命令用来恢复缺省情况。

【命令】

memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] **minor** *minor-value*
severe *severe-value* **critical** *critical-value* **normal** *normal-value*

undo memory-threshold [slot slot-number [cpu cpu-number]]

【缺省情况】

不同设备空闲内存告警的门限值可能不同，请先使用 **undo memory-threshold** 命令恢复缺省情况后，再通过 **display memory-threshold** 命令查看设备的缺省温度告警门限。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

minor minor-value: 一级告警门限。输入该参数的值时可通过输入？，来获取该参数的取值范围。取值为 0 时，表示关闭该级门限告警功能。

severe severe-value: 二级告警门限。输入该参数的值时可通过输入？，来获取该参数的取值范围。取值为 0 时，表示关闭该级门限告警功能。

critical critical-value: 三级告警门限。输入该参数的值时可通过输入？，来获取该参数的取值范围。取值为 0 时，表示关闭该级门限告警功能。

normal normal-value: 系统内存恢复正常状态时的内存大小。输入该参数的值时可通过输入？，来获取该参数的取值范围。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 编号。

【使用指导】

仅缺省 Context 支持本命令。

系统实时监控系统剩余空闲内存大小，当条件达到一级、二级、三级告警门限或者恢复正常状态门限时，就产生相应的告警/告警解除通知，通知关联的业务模块/进程采取相应的措施，以便最大限度的利用内存，又能保证设备的正常运行。

当设备出现内存告警时，可删除暂时不用的配置或关闭部分功能来释放内存。但因为内存不足，部分配置可能删除失败。

关于告警门限的详细介绍请参见“基础配置指导”中的“设备管理”。

【举例】

配置一级、二级、三级告警门限分别为 64MB、48MB、32MB，当系统剩余空闲内存大于 96MB 时，恢复到正常状态。

```
<Sysname> system-view
```

```
[Sysname] memory-threshold minor 64 severe 48 critical 32 normal 96
```

【相关命令】

- **display memory-threshold**

1.1.37 memory-threshold usage

memory-threshold usage 命令用来配置内存利用率阈值。

undo memory-threshold usage 命令用来恢复缺省情况。

【命令】

```
memory-threshold [ slot slot-number [ cpu cpu-number ] ] usage  
memory-threshold  
undo memory-threshold [ slot slot-number [ cpu cpu-number ] ] usage
```

【缺省情况】

内存利用率阈值为 100%。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

memory-threshold: 内存利用率阈值百分比，取值范围为 0~100。

【使用指导】

仅缺省 Context 支持本命令。

系统每隔 1 分钟会对内存利用率进行采样，当采样值大于或等于用户配置的内存利用率阈值时，则认为内存利用率过高，设备会发送 Trap 报文。

【举例】

```
# 配置内存利用率阈值为 80%。  
<Sysname> system-view  
[Sysname] memory-threshold usage 80
```

【相关命令】

- **display memory-threshold**

1.1.38 monitor cpu-usage enable

monitor cpu-usage enable 命令用来开启 CPU 利用率历史记录功能。

undo monitor cpu-usage enable 命令用来关闭 CPU 利用率历史记录功能。

【命令】

```
monitor cpu-usage enable [ slot slot-number [ cpu cpu-number ] ]  
undo monitor cpu-usage enable [ slot slot-number [ cpu cpu-number ] ]
```

【缺省情况】

CPU 利用率历史记录功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号，不指定表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

开启 CPU 利用率历史记录功能后，系统会每隔一定时间（可通过 **monitor cpu-usage interval** 命令配置）对 CPU 的利用率进行采样，并把采样结果保存到历史记录区。这些记录可通过 **display cpu-usage history** 命令查看，以使用户监控设备近期的运行情况。

【举例】

```
# 打开 CPU 利用率历史记录功能。  
<Sysname> system-view  
[Sysname] monitor cpu-usage enable
```

【相关命令】

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage interval**

1.1.39 monitor cpu-usage interval

monitor cpu-usage interval 命令用来配置 CPU 利用率历史记录的采样周期。

【命令】

monitor cpu-usage interval interval [slot slot-number [cpu cpu-number]]

【缺省情况】

CPU 利用率历史记录采样周期为 1 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval: CPU 利用率历史记录采用周期，取值为 5Sec、1Min 或者 5Min，不区分大小写。输入该参数时，请完整输入，否则，系统会提示参数错误。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

开启 CPU 利用率历史记录功能后，系统会每隔一定时间（可通过 **monitor cpu-usage interval** 命令配置）对 CPU 的利用率进行采样，并把采样结果保存到历史记录区。这些记录可通过 **display cpu-usage history** 命令查看，以便用户监控设备近期的运行情况。

【举例】

```
# 配置 CPU 利用率历史记录采样周期为 5 秒。  
<Sysname> system-view  
[Sysname] monitor cpu-usage interval 5Sec
```

【相关命令】

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage enable**

1.1.40 monitor cpu-usage statistics-interval core

monitor cpu-usage statistics-interval core 命令用来配置 CPU 核利用率的统计周期。
undo monitor cpu-usage statistics-interval core 命令用来恢复缺省情况。

【命令】

```
monitor cpu-usage statistics-interval interval slot slot-number cpu  
cpu-number core core-id-list  
undo monitor cpu-usage statistics-interval slot slot-number cpu cpu-number  
core core-id-list
```

【缺省情况】

CPU 核利用率的统计周期为 60 秒。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

interval: CPU 核利用率信息的统计周期，取值范围为 10~3600，单位为秒。配置的统计周期建议是采样周期的整数倍，采样周期是 5 秒，不是整数倍时，实际生效统计周期为最接近配置值、但小于配置值的、采样周期整数倍。例如，采样周期是 5 秒，配置统计周期为 12 秒，则实际生效的统计周期是 10 秒。

slot slot-number: 表示设备在 IRF 中的成员编号。

cpu cpu-number: 表示 CPU 的编号。

core-id-list: 表示 CPU 核的编号列表。表示方式为 **core-id-list = { core-id1 [to core-id2] }&<1-10>**，**core-id2** 的值要大于或等于 **core-id1** 的值，&<1-10>表示前面的参数最多可以重复输入 10 次。

【使用指导】

系统按 5 秒周期对 CPU 核的利用率进行采样，然后对统计周期内的采样值进行计算，并将计算值 and 用户配置的 CPU 核利用率的阈值比较。当计算值大时，则认为 CPU 核利用率过高，设备会发送告警信息并记录日志。

【举例】

```
# 配置产生告警的 CPU 利用率指定 core 平均时长为 60 秒。
<Sysname> system-view
[Sysname] monitor cpu-usage statistics-interval 60 slot 1 cpu 0 core 0
```

【相关命令】

- **monitor cpu-usage threshold core**
- **monitor resend cpu-usage core-interval**

1.1.41 monitor cpu-usage threshold

monitor cpu-usage threshold 命令用来配置 CPU 利用率告警门限。

undo monitor cpu-usage threshold 命令用来恢复缺省情况。

【命令】

```
monitor cpu-usage threshold severe-threshold recovery-threshold  
recovery-threshold [ slot slot-number [ cpu cpu-number ] ]  
undo monitor cpu-usage threshold recovery-threshold [ slot slot-number [ cpu  
cpu-number ] ]
```

【缺省情况】

CPU 利用率告警门限为 70%，CPU 利用率恢复门限为 30%。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

severe-threshold: CPU 利用率高级别告警门限，取值范围为 2~100，单位为百分比。

recovery-threshold recovery-threshold: CPU 利用率恢复门限，取值范围为 0~“*minor-threshold* 的配置值减 1”，单位为百分比。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

系统每隔 1 分钟会对 CPU 的利用率进行采样，并将采样值和用户配置的告警门限比较。当采样值大时，则认为利用率过高，设备会进行相应的处理。

【举例】

```
# 配置 CPU 利用率高级别告警门限为 90%，恢复门限为 70%。  
<Sysname> system-view  
[Sysname] monitor cpu-usage threshold 90 recovery-threshold 70
```

【相关命令】

- **display cpu-usage configuration**

1.1.42 monitor disk-usage interval

monitor disk-usage interval 命令用来配置磁盘利用率的采样周期。

undo monitor disk-usage interval 命令用来恢复缺省情况。

【命令】

```
monitor disk-usage interval interval  
undo monitor disk-usage interval
```

【缺省情况】

磁盘利用率的采样周期为 300 秒。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

interval：磁盘利用率的采样周期，取值范围为 5~1800，且必须为 5 的倍数，单位为秒。

【使用指导】

配置本命令后，系统会按照指定周期对磁盘利用率进行采样。

【举例】

```
# 配置磁盘利用率的采样周期为 120 秒。  
<Sysname> system-view  
[Sysname] monitor disk-usage interval 120
```

【相关命令】

- **monitor disk-usage disk**

1.1.43 monitor resend cpu-usage core-interval

monitor resend cpu-usage core-interval 命令用来配置发送 CPU 核告警的间隔。

undo monitor resend cpu-usage core-interval 命令用来恢复缺省情况。

【命令】

```
monitor resend cpu-usage core-interval core-interval [ slot slot-number
[ cpu cpu-number ] ]
undo monitor resend cpu-usage core-interval [ slot slot-number [ cpu
cpu-number ] ]
```

【缺省情况】

发送 CPU 核告警的间隔为 300。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

core-interval: CPU 核告警事件周期发送的间隔，取值范围为 10~3600，且只能是 5 的倍数，单位为秒。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【举例】

```
# 配置设备上所有 CPU 核发送告警事件的间隔为 60 秒。
<Sysname> system-view
[Sysname] monitor resend cpu-usage core-interval 60
```

1.1.44 monitor resource-usage { bridge-aggregation | route-aggregation } threshold

monitor resource-usage { bridge-aggregation | route-aggregation } threshold
命令用来配置聚合接口数的告警阈值。

undo monitor resource-usage { bridge-aggregation | route-aggregation } threshold 命令用来恢复缺省情况。

【命令】

```
monitor resource-usage { bridge-aggregation | route-aggregation } threshold
threshold-value
undo monitor resource-usage { bridge-aggregation | route-aggregation }
threshold
```

【缺省情况】

未配置聚合接口的告警阈值，不会触发告警。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

bridge-aggregation: 表示对可创建的二层聚合接口数设置告警阈值。

route-aggregation: 表示对可创建的三层聚合接口数设置告警阈值。

threshold-value: 表示可创建聚合接口数的告警阈值，取值范围为 1~4294967295。

【使用指导】

配置此功能后，当设备上创建的二层聚合接口或三层聚合接口的数量达到告警阈值时，则输出告警信息。之后每 3 小时输出一次告警，直到设备上创建的二层聚合接口或三层聚合接口的数量低于告警阈值后，才停止输出告警。

【举例】

配置二层聚合接口数的告警阈值为 100。

```
<Sysname> system-view
```

```
[Sysname] monitor resource-usage bridge-aggregation threshold 100
```

配置三层聚合接口数的告警阈值为 150。

```
<Sysname> system-view
```

```
[Sysname] monitor resource-usage route-aggregation threshold 150
```

1.1.45 monitor resource-usage bandwidth inbound threshold

monitor resource-usage bandwidth inbound threshold 命令用来配置整机入方向带宽的告警阈值。

undo monitor resource-usage bandwidth inbound threshold 命令用来恢复缺省情况。

【命令】

```
monitor resource-usage bandwidth inbound threshold threshold-value  
[ duration duration-value ]
```

```
undo monitor resource-usage bandwidth inbound threshold
```

【缺省情况】

未配置整机入方向带宽的告警阈值，不会触发告警。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

threshold-value: 表示整机入方向带宽的告警阈值，取值范围为 1~4294967295，单位为 Mbps。

duration *duration-value*: 表示整机入方向流量超过告警阈值的持续时间。***duration-value*** 是持续时间，取值范围为 5~300，必须是 5 的倍数，单位为秒，缺省值为 300 秒。

【使用指导】

当入方向流量在持续时间内一直大于或等于带宽告警阈值，则输出告警，且之后会每 5 秒输出一次告警；直到入方向流量低于带宽告警阈值后，才停止输出告警。

此命令仅缺省 Context 支持，非缺省 Context 不支持。

【举例】

配置整机入方向带宽告警的阈值为 1024Mbps，持续时间为 60 秒。

```
<Sysname> system-view
```

```
[Sysname] monitor resource-usage bandwidth inbound threshold 1024 duration 60
```

1.1.46 monitor resource-usage context threshold

monitor resource-usage context threshold 命令用来配置 Context 个数的告警阈值。

undo monitor resource-usage context threshold 命令用来恢复缺省情况。

【命令】

monitor resource-usage context threshold *threshold-value*

undo monitor resource-usage context threshold

【缺省情况】

未配置 Context 个数的告警阈值，不会触发告警。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

threshold-value：表示可创建的 Context 个数的告警阈值，取值范围为 1~4294967295。

【使用指导】

配置此功能后，当设备上新建 Context 的数量达到告警阈值时，则输出告警信息。之后每 6 小时输出一告警，直到设备上新建 Context 的数量低于告警阈值后，才停止输出告警。

此命令仅缺省 Context 支持，非缺省 Context 不支持。

【举例】

配置 Context 数的告警阈值为 16。

```
<Sysname> system-view
```

```
[Sysname] monitor resource-usage context threshold 16
```

1.1.47 monitor resource-usage security-policy threshold

monitor resource-usage security-policy { ip | ipv6 } threshold 命令用来配置安全策略规则数的告警阈值。

undo monitor resource-usage security-policy { ip | ipv6 } threshold 命令用来恢复缺省情况。

【命令】

monitor resource-usage security-policy { ip | ipv6 } threshold threshold-value

undo monitor resource-usage security-policy { ip | ipv6 } threshold

本命令的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	支持
T5000-G30	不支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	支持
T1000-CN60/T1000-CN80	支持

【缺省情况】

未配置安全策略规则数的告警阈值，不会触发告警。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip: 表示对可创建的 IPv4 类型安全策略规则设置告警阈值。

ipv6: 表示对可创建的 IPv6 类型安全策略规则设置告警阈值。

threshold-value: 表示可创建安全策略规则数的告警阈值，取值范围为 1~4294967295。

【使用指导】

配置此功能后，当设备上创建的安全策略规则的数量达到告警阈值时，则输出告警信息。之后每 6 小时输出一次告警，直到设备上创建的安全策略规则的数量低于告警阈值后，才停止输出告警。

【举例】

配置 IPv4 类型安全策略规则数的告警阈值为 500。

<Sysname> system-view

[Sysname] monitor resource-usage security-policy ip threshold 500

配置 IPv6 类型安全策略规则数的告警阈值为 500。

<Sysname> system-view

[Sysname] monitor resource-usage security-policy ipv6 threshold 500

1.1.48 monitor resource-usage session-count threshold

monitor resource-usage session-count threshold 命令用来配置会话连接数的告警阈值。

undo monitor resource-usage session-count threshold 命令用来恢复缺省情况。

【命令】

```
monitor resource-usage session-count [ slot slot-number ] threshold  
threshold-value  
undo monitor resource-usage session-count [ slot slot-number ] threshold
```

【缺省情况】

未配置会话连接数的告警阈值，不会触发告警。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。
threshold-value: 表示会话连接数的告警阈值，取值范围为 1~4294967295。

【使用指导】

配置此功能后，当设备上的会话连接数达到告警阈值时，则输出告警信息。之后每 10 分钟输出一次告警，直到会话连接数低于告警阈值后，才停止输出告警。

【举例】

```
# 配置整机会话连接数的告警阈值为 100000。  
<Sysname> system-view  
[Sysname] monitor resource-usage session-count threshold 100000
```

1.1.49 monitor resource-usage session-rate threshold

monitor resource-usage session-rate threshold 命令用来配置会话新建速率的告警阈值。

undo monitor resource-usage session-rate threshold 命令用来恢复缺省情况。

【命令】

```
monitor resource-usage session-rate [ slot slot-number ] threshold  
threshold-value  
undo monitor resource-usage session-rate [ slot slot-number ] threshold
```

【缺省情况】

未配置会话新建速率的告警阈值，不会触发告警。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```


【参数】

threshold-value: 表示会话新建速率的告警阈值，取值范围为 1~4294967295。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

【使用指导】

配置此功能后，当设备上的会话新建速率达到告警阈值时，则输出告警信息。之后每 10 分钟输出一次告警，直到会话新建速率低于告警阈值后，才停止输出告警。

多次执行此命令，可以为不同的成员设备或单板配置会话新建速率的告警阈值。

【举例】

配置会话新建速率的告警阈值为 500。

```
<Sysname> system-view
```

```
[Sysname] monitor resource-usage session-rate threshold 500
```

1.1.50 monitor sample-interval

monitor sample-interval 命令用来配置 CPU 利用率、内存利用率的采样周期。

undo monitor sample-interval 命令用来恢复缺省情况。

【命令】

```
monitor sample-interval interval
```

```
undo monitor sample-interval
```

【缺省情况】

CPU 利用率、内存利用率的采样周期为 0 秒，表示不采样。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval: 表示 CPU 利用率、内存利用率的采样周期，取值范围为 0~300，单位为秒。建议配置成大于 5 的数。

【举例】

配置 CPU 利用率、内存利用率的采样周期为 30 秒。

```
<Sysname> system-view
```

```
[Sysname] monitor sample-interval 30
```

【相关命令】

- **monitor statistics-interval**

1.1.51 monitor statistics-interval

monitor statistics-interval 命令用来配置 CPU 利用率、内存利用率的统计周期。

undo monitor statistics-interval 命令用来恢复缺省情况。

【命令】

```
monitor statistics-interval interval
undo monitor statistics-interval
```

【缺省情况】

CPU 利用率、内存利用率的统计周期为 0 秒，表示不统计。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interval: 利用率信息的统计周期，取值范围为 0~900，单位为秒。配置的统计周期建议是采样周期的整数倍，不是整数倍时，实际生效统计周期为最接近配置值、但小于配置值的、采样周期整数倍。例如，采样周期是 15 秒，配置统计周期为 40 秒，则实际生效的统计周期是 30 秒。

【使用指导】

配置 **monitor sample-interval** 和 **monitor statistics-interval** 命令后，设备会按周期获取 CPU 利用率、内存利用率的值，并对统计周期内获取到的采样值进行计算，以便获取统计周期内 CPU 利用率、内存利用率的平均值。

如果仅配置了 **monitor sample-interval** 或 **monitor statistics-interval** 命令，设备不会进行采样和统计。

【举例】

```
# 配置 CPU 利用率、内存利用率的统计周期为 90 秒。
<Sysname> system-view
[Sysname] monitor statistics-interval 90
```

【相关命令】

- **monitor sample-interval**

1.1.52 password-recovery enable

password-recovery enable 命令用来开启密码恢复功能。

undo password-recovery enable 命令用来关闭密码恢复功能。

【命令】

```
password-recovery enable
undo password-recovery enable
```

【缺省情况】

密码恢复功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

仅缺省 Context 支持本命令。

配置密码恢复功能后，当用户忘记 Console 口认证密码或者登录认证失败，导致无法使用命令行操作设备时，可通过 BootWare 菜单清除该认证密码，再继续使用设备；关闭密码恢复功能后，设备将处于一个安全性更高的状态，即当出现上述情况时，若想继续使用 Console 口对设备进行命令行操作，只能通过 BootWare 菜单选择将设备恢复为出厂配置之后方可继续操作，这样可以有效地防止非法用户获取启动配置文件。

清除认证密码的操作必须在主设备的启动过程中进入 BootWare 菜单进行。

BootWare 菜单中支持配置的选项与密码恢复功能的配置有关，详见设备的版本说明书。

【举例】

```
# 关闭密码恢复功能。
<Sysname> system-view
[Sysname] undo password-recovery enable
```

1.1.53 reboot

reboot 命令用来重启设备。

【命令】

reboot [*slot slot-number*] [*force*]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，会重启整个 IRF。

cpu cpu-number: CPU 的编号。不指定该参数时，会重启 slot。

force: 强制重启：

- 不指定该参数时，重启设备，系统会做一些保护性检查（如启动文件是否存在，是否正在写磁盘等），若检查不通过则退出处理，不会重启设备；
- 指定该参数时，系统将不进行任何检查，直接执行重启操作。

【使用指导】



注意

- 重新启动可能会导致业务中断，请谨慎使用该命令。
- 使用 **force** 参数时，系统在重启时不会做任何保护性措施。重启后，可能导致文件系统损坏，请谨慎使用该参数。建议在系统故障或无法正常重启时，才使用该参数。

如果主用启动文件损坏或者不存在，则不能通过 **reboot** 命令重启设备。此时，可以通过指定新的主用启动文件再重启。

如果设备在准备重启时，用户正在进行文件操作，为了安全起见，系统将不会执行此次重启操作。

重启主设备时，如果备设备不存在，会重启整个 IRF；如果备设备存在并稳定运行，会引起主备倒换。当系统中有成员设备处于非稳定状态时，请不要使用 **reboot** 命令来触发主备倒换，以免影响 IRF 和成员设备的运行。可使用 **display system stable state** 命令来显示 IRF 的稳定状态。

【举例】

重启设备，并保存配置文件。

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait.....DONE!
Current configuration will be lost after the reboot, save current configuration? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

强制重启设备。

```
<Sysname> reboot force
A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:y
Now rebooting, please wait...
```

【相关命令】

- **display system stable state**

1.1.54 reset scheduler logfile

reset scheduler logfile 命令用来清除 Schedule 日志文件的相关信息。

【命令】

reset scheduler logfile

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

```
# 清除 Schedule 日志文件的相关信息。  
<Sysname> reset scheduler logfile
```

【相关命令】

- **display scheduler logfile**

1.1.55 reset version-update-record

reset version-update-record 命令用来清除启动软件包版本更新操作的记录。

【命令】

```
reset version-update-record
```

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

仅缺省 Context 支持本命令。

【举例】

```
# 清除设备启动软件包版本更新操作的记录。  
<Sysname> system-view  
[Sysname] reset version-update-record  
This command will delete all records of version update. Continue? [Y/N]:y
```

【相关命令】

- **display version-update-record**

1.1.56 restore factory-default

restore factory-default 命令用来将设备恢复到出厂状态。

【命令】

```
restore factory-default
```

【视图】

用户视图

【缺省用户角色】

network-admin

【使用指导】

仅缺省 Context 支持本命令。

配置本命令，设备会自动强制重启并恢复到出厂状态，请谨慎使用该命令。

当设备使用场景更改，或者设备出现故障时，可以使用本命令来将设备恢复到出厂状态。

【举例】

将设备恢复到出厂状态。

```
<Sysname> restore factory-default
```

This command will restore the system to the factory default configuration and clear the operation data, and forcibly reboot the system. Continue [Y/N]:y

Restoring the factory default configuration. This process might take a few minutes. Please wait....Done.

The system is rebooting...

【相关命令】

- **reboot**

1.1.57 scheduler job

scheduler job 命令用来创建 Job，并进入 Job 视图。如果指定的 Job 已存在，则直接进入 Job 视图。

undo scheduler job 命令用来删除已创建的 Job。

【命令】

```
scheduler job job-name
```

```
undo scheduler job job-name
```

【缺省情况】

不存在 Job。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

job-name: Job 的名称，为 1~47 个字符的字符串，区分大小写。

【使用指导】

一个 Job 可以被多个 Schedule 引用。Job 视图下用户可以通过 **command** 命令为 Job 分配命令。

【举例】

创建名称为 backupconfig 的 Job 并进入 Job 视图。

```
<Sysname> system-view
```

```
[Sysname] scheduler job backupconfig
```

```
[Sysname-job-backupconfig]
```

【相关命令】

- **command**
- **scheduler schedule**

1.1.58 scheduler logfile size

scheduler logfile size 命令用来配置 Schedule 日志文件的大小。

【命令】

scheduler logfile size *value*

【缺省情况】

Schedule 日志文件的大小为 16KB。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

value: Schedule 日志文件的大小，取值范围为 16~1024，单位是 KB。

【使用指导】

Schedule 日志文件用来记录 Job 下命令行的执行结果。如果该文件的大小超过了用户配置值，则系统会把老的记录删除，用来记录新的记录。如果要记录的日志信息超长，超过了日志文件的大小，则该日志超出的部分不会记录。

【举例】

```
# 配置 Schedule 日志文件的大小为 32KB。  
<Sysname> system-view  
[Sysname] scheduler logfile size 32
```

【相关命令】

- **display scheduler logfile**

1.1.59 scheduler reboot at

scheduler reboot at 命令用来配置设备重启的具体时间和日期。

undo scheduler reboot 命令用来取消定时重启配置。

【命令】

scheduler reboot at *time* [*date*]
undo scheduler reboot

【缺省情况】

未配置设备重启的具体时间和日期。

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

time: 设备重启的时间，格式为 *HH:MM*。*HH* 代表小时，取值范围为 0~23，*MM* 代表分钟，取值范围为 0~59。

date: 设备重启的日期，格式为 *MM/DD/YYYY*（月/日/年）或者 *YYYY/MM/DD*（年/月/日）。

- *YYYY* 的取值范围为 2000~2035;
- *MM* 的取值范围为 1~12;
- *DD* 的取值范围与具体月份有关。

【使用指导】

该命令会使设备在将来的某个时间点重新启动，从而导致业务中断，请谨慎使用。

如果没有指定 **date** 参数，并且：

- 配置的时间点在当前时间之后，则设备将在当天的该时间点重启；
- 配置的时间点在当前时间之前，则设备将在第二天的该时间点重启。

多次配置 **scheduler reboot at**、**scheduler reboot delay** 命令，最后一次执行的命令生效。

如果设备在准备重启时，用户正在进行文件操作，为了安全起见，系统将不会执行此次重启操作。

【举例】

假设系统的当前时间为 2015 年 6 月 6 日 11:43，配置设备在当天中午 12:00 重启。

```
<Sysname> scheduler reboot at 12:00
```

```
Reboot system at 12:00:00 06/06/2015 (in 0 hours and 16 minutes). Confirm? [Y/N]:
```

【相关命令】

- **scheduler reboot delay**

1.1.60 scheduler reboot delay

scheduler reboot delay 命令用来配置重启设备的延迟时间。

undo scheduler reboot 命令用来取消定时重启配置。

【命令】

```
scheduler reboot delay time
```

```
undo scheduler reboot
```

【缺省情况】

未配置重启设备的延迟时间。

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

time: 设备重启的等待时延, 格式为 **HH:MM** (小时:分钟) 或 **MM** (分钟)。

- 使用 **HH:MM** 格式时, **MM** 的取值范围为 0~59, **HH:MM** 的最大长度为 6 个字符。
- 使用 **MM** 格式时, 最大长度为 6 个字符。

【使用指导】

该命令会使设备在将来的某个时间点重新启动, 从而导致业务中断, 请谨慎使用。

多次配置 **scheduler reboot at**、**scheduler reboot delay** 命令, 最后一次执行的命令生效。

如果设备在准备重启时, 用户正在进行文件操作, 为了安全起见, 系统将不会执行此次重启操作。

【举例】

假设系统的当前时间为 2015 年 6 月 6 日 11:48, 配置设备在 88 分钟后重启。

```
<Sysname> scheduler reboot delay 88
```

```
Reboot system at 13:16 06/06/2015(in 1 hours and 28 minutes). Confirm? [Y/N]:
```

1.1.61 scheduler schedule

scheduler schedule 命令用来创建 Schedule, 并进入相应的 Schedule 视图。如果指定的 Schedule 已存在, 则直接进入 Schedule 视图。

undo scheduler schedule 命令用来删除指定 Schedule。

【命令】

scheduler schedule *schedule-name*

undo scheduler schedule *schedule-name*

【缺省情况】

不存在 Schedule。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

schedule-name: Schedule 的名称, 为 1~47 个字符的字符串, 区分大小写。

【使用指导】

使用 **scheduler schedule** 命令可以配置定时执行任务, 让设备在指定时间执行指定命令。

配置步骤如下:

- (1) 使用 **scheduler job** 命令创建 Job。
- (2) 在 Job 视图下, 使用 **command** 命令配置需要执行的命令。
- (3) 使用 **scheduler schedule** 命令创建 Schedule。

- (4) 在 Schedule 视图下，使用 **job** 命令为 Schedule 分配 Job。一个 Schedule 下可以分配多个 Job，但必须是已创建的 Job，否则分配失败。
- (5) 在 Schedule 视图下，使用 **user-role** 命令为 Schedule 配置用户角色。一个 Schedule 下最多可以分配 64 个角色。
- (6) 在 Schedule 视图下，使用 **time at**、**time once** 或者 **time repeating** 命令来配置任务执行的时间。一个 Schedule 下只能配置一个执行时间。

【举例】

```
# 创建名为 saveconfig 的 Schedule。  
<Sysname> system-view  
[Sysname] scheduler schedule saveconfig
```

【相关命令】

- **job**
- **time at**
- **time once**

1.1.62 shutdown-interval

shutdown-interval 命令用来配置端口状态检测定时器的时长。

undo shutdown-interval 命令用来恢复缺省情况。

【命令】

```
shutdown-interval interval  
undo shutdown-interval
```

【缺省情况】

端口状态检测定时器的时长为 30 秒。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

interval: 端口状态检测定时器的时长，取值范围为 0~300，单位为秒。取值为 0 时，表示不进行定时检测。

【使用指导】

某些协议模块在特定情况下会自动关闭某个端口，比如当开启了 BPDU 保护功能的端口收到配置消息时，MSTP 协议模块将自动关闭该端口。同时，系统会启动一个检测定时器，如果直到定时器超时（即经过 **time** 秒之后），该端口仍处于关闭状态，协议模块则自动激活该端口，令其恢复到真实的物理状态。

如果用户在端口定时检测过程中将检测时间间隔修改为 **T1**，修改时刻距协议关闭端口时间间隔为 **T**。

- 若 $T < T1$ ，则被关闭的端口会再经过 $T1 - T$ 时间后被恢复。
- 若 $T \geq T1$ ，则被关闭的端口会立即恢复。

例如当前 *time* 配置为 30，当端口被协议模块关闭 2 秒 ($T=2$) 后，修改 *time* 为 10 ($T1=10$)，则该接口会再经过 8 秒后被恢复；如果当前 *time* 为 30，端口被协议模块关闭 10 秒后，修改 *time* 为 2，则该端口会立即恢复。

【举例】

配置端口状态检测定时器的时长为 100 秒。

```
<Sysname> system-view
[Sysname] shutdown-interval 100
```

1.1.63 sysid

sysid 命令用来配置设备的网元信息。

undo sysid 命令用来恢复缺省情况。

【命令】

```
sysid system-id
undo sysid
```

【缺省情况】

未配置设备的网元信息。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

system-id：表示设备的网元信息，可用于表示设备的位置信息、功能信息、用户自定义的名字标记等。

【举例】

配置网元信息为 position-hall，表明设备位置在大厅。

```
<Sysname> system-view
[Sysname] sysid positon-hall
```

1.1.64 sysname

sysname 命令用来配置设备的名称。

undo sysname 用来恢复缺省情况。

【命令】

```
sysname sysname
undo sysname
```

【缺省情况】

设备的名称为 UNIS。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

sysname: 设备名称，为 1~64 个字符的字符串。

【使用指导】

设备的名称对应于命令行接口的提示符，如设备的名称为 Sysname，则用户视图的提示符为 <Sysname>。

【举例】

配置设备的名称为 R2000。

```
<Sysname> system-view
[Sysname] sysname R2000
[R2000]
```

1.1.65 temperature-limit

temperature-limit 命令用于配置设备的温度告警门限。

undo temperature-limit 命令用来恢复缺省情况。

【命令】

```
temperature-limit slot slot-number { hotspot | inflow | outflow }
sensor-number lowlimit warninglimit [ alarmlimit ]
undo temperature-limit slot slot-number { hotspot | inflow | outflow }
sensor-number
```

【缺省情况】

不同温度传感器的温度门限可能不同，请先使用 **undo temperature-limit** 命令恢复缺省情况后，再通过 **display environment** 命令查看设备的缺省温度告警门限。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot slot-number: 配置指定成员设备上温度传感器的温度门限。*slot-number* 表示设备在 IRF 中的成员编号。

hotspot: 配置热点传感器的温度门限。热点传感器一般置于发热量较大的芯片附近，监测芯片温度。

本参数的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	不支持
T5000-G30	支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	不支持
T1000-CN60/T1000-CN80	不支持

inflow: 配置入风传感器的温度门限。入风传感器一般置于入风口附近，监测环境温度。

outflow: 配置出风传感器的温度门限。出风传感器一般置于出风口附近，监测设备温度。

本参数的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	支持
T5000-G30	支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	不支持
T1000-CN60/T1000-CN80	支持

sensor-number: 温度传感器的编号，输入该参数的值时可通过输入？，来获取该参数的取值范围。

lowlimit: 低温告警门限，单位为摄氏度。不同温度传感器的低温告警门限取值范围不同，输入该参数的值时可通过输入？，来获取该参数的取值范围。

warninglimit: 一般级高温告警门限，单位为摄氏度，必须大于低温告警门限。输入该参数的值时可通过输入？，来获取该参数的取值范围。

alarmlimit: 严重级高温告警门限，单位为摄氏度，必须大于一般级高温告警门限。输入该参数的值时可通过输入？，来获取该参数的取值范围。

【使用指导】

如果温度低于低温告警门限、高于一般级或严重级高温门限，系统均会生成相应的日志信息和告警信息提示用户，并通过设备面板上的指示灯来告警，以便用户及时进行处理。

本命令仅缺省 Context 支持。

【举例】

配置指定 slot 上热点 1 号温度传感器，低温门限为-10 摄氏度，一般级高温门限为 50 摄氏度，严重级高温门限为 60 摄氏度。

```
<Sysname> system-view
```

```
[sysname] temperature-limit slot 1 hotspot 1 -10 50 60
```

【相关命令】

- **display environment**

1.1.66 time at

time at 命令用来配置在指定时刻执行 Schedule。

undo time 命令用来为 Schedule 取消执行时间配置。

【命令】

time at *time date*

undo time

【缺省情况】

未为 Schedule 配置执行时间。

【视图】

Schedule 视图

【缺省用户角色】

network-admin

context-admin

【参数】

time: Schedule 的执行时间，格式为 *HH:MM*（小时:分钟）。*HH* 取值范围为 0~23，*MM* 取值范围为 0~59。

date: Schedule 执行的日期，格式为 *MM/DD/YYYY*（月/日/年）或者 *YYYY/MM/DD*（年/月/日）。

- *YYYY* 的取值范围为 2000~2035;
- *MM* 的取值范围为 1~12;
- *DD* 的取值范围与具体月份有关。

【使用指导】

配置的时间点必须晚于系统当前时间点，否则配置失败。

一个 Schedule 只能配置一个执行时间。因此，同一 Schedule 视图下，多次执行 **time at**、**time once** 或 **time repeating** 命令时，最后一次执行的命令生效。

【举例】

配置 2015 年 5 月 11 日 1 点 1 分执行名称为 saveconfig 的 Schedule。

```
<Sysname> system-view
```

```
[Sysname] scheduler schedule saveconfig
```

```
[Sysname-schedule-saveconfig] time at 1:1 2015/05/11
```

【相关命令】

- **scheduler schedule**

1.1.67 time once

time once 命令用来为 Schedule 配置执行时间。

undo time 命令用来为 Schedule 取消执行时间配置。

【命令】

```
time once at time [ month-date month-day | week-day week-day<1-7> ]
time once delay time
undo time
```

【缺省情况】

未为 Schedule 配置执行时间。

【视图】

Schedule 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

at time: Schedule 的执行时间，格式为 *HH:MM*（小时:分钟）。*HH* 取值范围为 0~23，*MM* 取值范围为 0~59。

month-date month-day: Schedule 在一个月中的哪天被执行。*month-day* 表示日期，取值范围为 1~31。如果指定了一个本月不存在的日期，则实际生效的时间为下一个月的该日期，比如，二月没有 30 号，则实际生效的时间为三月的 30 号。

week-day week-day<1-7>: Schedule 在一周中的哪（些）天被执行。*week-day<1-7>* 表示一周中任一天或几天的组合，*week-day* 取值为: **Mon、Tue、Wed、Thu、Fri、Sat、Sun**，<1-7> 表示前面的参数最多可以输入 7 次。配置多天，字符串之间用空格分开。

delay time: 指定 Schedule 延迟执行的时间。格式为 *HH:MM*（小时:分钟）或 *MM*（分钟）。

- 使用 *HH:MM* 格式时，*MM* 的取值范围为 0~59，*HH:MM* 最大长度为 6 个字符。
- 使用 *MM* 格式时，最大长度为 6 个字符。

【使用指导】

配置该命令后，Schedule 在该设定时间点到达时执行，若当天/本月/本周该时间点已过去，则顺延到第二天/下月/下周。执行后下次再到达该时间点时 Schedule 不再执行。

一个 Schedule 只能配置一个执行时间。因此，同一 Schedule 视图下，多次执行 **time at**、**time once** 或 **time repeating** 命令时，最后一次执行的命令生效。

【举例】

当天的 15 点执行名称为 saveconfig 的 Schedule。

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 15:00
```

最近到达的 15 号的 15 点执行名称为 saveconfig 的 Schedule。

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 15:00 month-date 15
```

最近一个周一和周五的 12 点整执行名称为 saveconfig 的 Schedule。

```
<Sysname> system-view
```

```
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 12:00 week-day mon fri
# 延迟 10 分钟执行名称为 saveconfig 的 Schedule。
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once delay 10
```

【相关命令】

- **scheduler schedule**

1.1.68 time repeating

time repeating 命令用来配置重复执行 Schedule 的时间。

undo time 命令用来为 Schedule 取消执行时间配置。

【命令】

```
time repeating [ at time [ date ] ] interval interval
time repeating at time [ month-date [ month-day | last ] | week-day
week-day<1-7> ]
undo time
```

【缺省情况】

未配置重复执行 Schedule 的时间。

【视图】

Schedule 视图

【缺省用户角色】

network-admin

context-admin

【参数】

at time: 表示重复执行的时间，格式为 *HH:MM*（小时:分钟）。*HH* 取值范围为 0~23，*MM* 取值范围为 0~59。不指定该参数时，表示从现在开始。

date: 指定 Schedule 重复执行的开始日期，格式为 *MM/DD/YYYY*（月/日/年）或者 *YYYY/MM/DD*（年/月/日）。不指定该参数时，表示将来第一次到达 **time** 的时间点的日期。

- *YYYY* 的取值范围为 2000~2035;
- *MM* 的取值范围为 1~12;
- *DD* 的取值范围与具体月份有关。

interval interval: 指定重复执行的时间间隔。格式为 *HH:MM*（小时:分钟）或 *MM*（分钟）。

- 使用 *HH:MM* 格式时，*MM* 的取值范围为 0~59，最大长度为 6 个字符。
- 使用 *MM* 格式时，取值的最小值为 1，最大长度为 6 个字符。

month-date [month-day | last]: 表示每月中的某一天。其中，*month-day* 表示日期，取值范围为 1~31。如果指定了一个本月不存在的日期，则实际生效的时间为下一个月的该日期，比如，二月没有 30 号，则实际生效的时间为三月的 30 号。**last** 表示每月的最后一天。

week-day week-day<1-7>: 表示每周中的某（些）天。**week-day<1-7>**表示一周中任一天或几天的组合，**week-day** 取值为: **Mon**、**Tue**、**Wed**、**Thu**、**Fri**、**Sat**、**Sun**，&<1-7>表示前面的参数最多可以输入 7 次。配置多天时，字符串之间用空格分开。

【使用指导】

time repeating [at time [date]] interval interval 表示从指定时间开始，周期性执行 Schedule。

time repeating at time [month-date [month-day | last] | week-day week-day<1-7>]表示每月/每周的某（些）天重复执行 Schedule。

一个 Schedule 只能配置一个执行时间。因此，同一 Schedule 视图下，多次执行 **time at**、**time once** 或 **time repeating** 命令时，最后一次执行的命令生效。

【举例】

配置从早上八点开始，每隔 1 小时执行一次名称为 saveconfig 的 Schedule。

```
<Sysname> system-view
```

```
[Sysname] scheduler schedule saveconfig
```

```
[Sysname-schedule-saveconfig] time repeating at 8:00 interval 60
```

配置从现在开始每天的 12:00 执行名称为 saveconfig 的 Schedule。

```
<Sysname> system-view
```

```
[Sysname] scheduler schedule saveconfig
```

```
[Sysname-schedule-saveconfig] time repeating at 12:00
```

配置从现在开始每个月 5 号的上午 8 点执行名称为 saveconfig 的 Schedule。

```
<Sysname> system-view
```

```
[Sysname] scheduler schedule saveconfig
```

```
[Sysname-schedule-saveconfig] time repeating at 8:00 month-date 5
```

配置从现在开始每个月的最后一天 8 点执行名称为 saveconfig 的 Schedule。

```
<Sysname> system-view
```

```
[Sysname] scheduler schedule saveconfig
```

```
[Sysname-schedule-saveconfig] time repeating at 8:00 month-date last
```

配置从现在开始每个周五和周六的上午 8 点执行名称为 saveconfig 的 Schedule。

```
<Sysname> system-view
```

```
[Sysname] scheduler schedule saveconfig
```

```
[Sysname-schedule-saveconfig] time repeating at 8:00 week-day fri sat
```

【相关命令】

- **scheduler schedule**

1.1.69 usb disable

usb disable 命令用来关闭 USB 接口。

undo usb disable 命令用来开启 USB 接口。

【命令】

usb disable

undo usb disable

【缺省情况】

设备上所有的 USB 接口处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

仅缺省 Context 支持本命令。

用户可通过 USB 口进行文件的上传和下载。缺省状态下 USB 口处于开启状态，用户可根据需要关闭 USB 口。

在执行 **usb disable** 命令前，请先使用 **umount** 命令卸载所有 USB 分区，否则命令执行失败。有关 **umount** 命令的详细介绍，请参见“基础配置命令参考”中的“文件系统管理”。

【举例】

```
# 打开 USB 接口。  
<Sysname> system-view  
[Sysname] undo usb disable
```

1.1.70 user-role

user-role 命令用来配置执行 Schedule 时使用的用户角色。

undo user-role 命令用来将已经配置的用户角色从 Schedule 中删除。

【命令】

```
user-role role-name  
undo user-role role-name
```

【缺省情况】

执行 Schedule 时使用的用户角色，为创建该 Schedule 的用户的用户角色。

【视图】

Schedule 视图

【缺省用户角色】

network-admin
context-admin

【参数】

role-name: 用户角色的名称，为 1~63 个字符的字符串，区分大小写。可以是系统预定义的角色名称，包括 network-admin、network-operator、context-admin、context-operator、level-0~level-15，也可以是自定义的用户角色名称。

【使用指导】

设备支持的每条命令执行时都需要相应的用户角色。只有本命令中配置的用户角色具有权限，Schedule 中的 **command** 命令中指定的命令行才能执行。关于用户角色的详细描述请参见“基础配置指导”中的“RBAC”。

同一 Schedule 最多可配置 64 个用户角色，超过该上限后，新配置会执行失败。

【举例】

配置执行定时任务 test 时使用的用户角色为 rolename。

```
<sysname> system-view
```

```
[Sysname] scheduler schedule test
```

```
[Sysname-schedule-test] user-role rolename
```

【相关命令】

- **command**
- **scheduler schedule**

目 录

1 Tcl	1-1
1.1 Tcl配置命令	1-1
1.1.1 cli	1-1
1.1.2 tclquit	1-2
1.1.3 tclsh	1-2

1 Tcl

1.1 Tcl配置命令

1.1.1 cli

cli 命令用来在 Tcl 配置视图下优先执行 Uniware 命令。

【命令】

cli *command*

【视图】

Tcl 配置视图

【缺省用户角色】

network-admin
context-admin

【参数】

command: 需执行的 Uniware 命令。请按照 Uniware 命令形式输入完整的命令行。

【使用指导】

在 Tcl 配置视图下执行命令时，如果 Tcl 命令与 Uniware 命令的命令字冲突，则执行 Tcl 命令。如果需要在 Tcl 配置视图下优先执行 Uniware 命令，可以在 Uniware 命令前添加命令关键字 **cli**。

【举例】

在 Tcl 配置视图下，当 Tcl 命令与 Uniware 命令的命令字冲突时，若需要执行 Uniware 命令，可以通过如下方式配置：

- 在 Tcl 配置视图下执行与 Tcl 命令冲突的 Uniware 命令。

```
<Sysname> tclsh  
<Sysname-tcl> system-view  
[Sysname-tcl] route-policy 1 permit node 10  
[Sysname-tcl-route-policy-1-10] apply cost 10  
can't interpret "cost" as a lambda expression
```

- 在 Uniware 命令前添加 **cli** 关键字重新执行该命令。

```
[Sysname-tcl-route-policy-1-10] cli apply cost 10
```

在 Tcl 配置视图下一次执行多条 Uniware 命令，进入 OSPF 区域视图：

- 方式一：

```
[Sysname-tcl] cli "ospf 100 ; area 0"  
[Sysname-tcl-ospf-100-area-0.0.0.0]
```

- 方式二：

```
[Sysname-tcl] cli ospf 100 ; cli area 0  
[Sysname-tcl-ospf-100-area-0.0.0.0]
```

1.1.2 tclquit

tclquit 命令用来从 Tcl 配置视图退回到用户视图。

【命令】

tclquit

【视图】

Tcl 配置视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

执行该命令效果等同于在 Tcl 配置视图下执行 **quit** 命令。

如果在 Tcl 配置视图下使用了 Uniware 命令进入了子视图,则只能用 **quit** 命令退回到上一级视图,不能执行 **tclquit** 命令。

【举例】

从 Tcl 配置视图退回到用户视图。

```
<Sysname-tcl> tclquit  
<Sysname>
```

【相关命令】

- **tclsh**

1.1.3 tclsh

tclsh 命令用来从用户视图进入 Tcl 配置视图。

【命令】

tclsh

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

为兼容 Uniware 配置方式,在 Tcl 配置视图下,用户可以直接输入如下命令并直接回车即可执行:

- 所有 Tcl8.5 版本的命令。
- Uniware 系统的命令。Tcl 配置视图相当于用户视图,配置方式同用户视图下的配置。

【举例】

从用户视图进入 Tcl 配置视图。

```
<Sysname> tclsh
```

<Sysname-tcl>

【相关命令】

- **tclquit**

目 录

1 License管理	1-1
1.1 License管理命令	1-1
1.1.1 display license	1-1
1.1.2 display license device-id.....	1-3
1.1.3 display license feature	1-4
1.1.4 license activation-file install	1-5
1.1.5 license activation-file uninstall.....	1-6
1.1.6 license compress	1-6

1 License管理

1.1 License管理命令

非缺省 Context 不支持 License 管理命令。请在缺省 Context 上配置 License，授权给缺省 Context 的特性，会同步授权给非缺省 Context。有关 Context 的详细介绍，请参见“虚拟化技术配置指导”中的“Context”。

1.1.1 display license

display license 命令用来显示 License 的详细信息。

【命令】

display license [**activation-file**] [**slot slot-number**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

activation-file: 显示设备上激活文件对应的 License 的相关信息。目前设备仅支持通过激活文件来安装 License，所以，不管是否选择该参数，显示结果相同。

slot slot-number: 显示指定成员设备上安装的 License 信息。*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，显示所有成员设备上的 License 信息。

【使用指导】

目前设备仅支持通过激活文件来安装 License。

【举例】

```
# 显示设备上所有 License 的详细信息。
<Sysname> display license
Slot 1:
cfa0:/license/NGIPS2016122714015630234.ak
Feature: IPS
Product Description: Trial IPS License, 30 Days
Registered at: 2016-12-27 13:55:08
License Type: Trial (date restricted)
Trial Validity Period: 2016-12-27 to 2017-01-26
Current State: Expired
```

cfa0:/license/NGIPS2016122714015630234.ak
 Feature: AV
 Product Description: Trial AV License, 30 Days
 Registered at: 2016-12-27 13:55:08
 License Type: Trial (date restricted)
 Trial Validity Period: 2016-12-27 to 2017-01-26
 Current State: Expired

cfa0:/license/NGIPS2016122714015630234.ak
 Feature: ACG
 Product Description: Trial ACG License, 30 Days
 Registered at: 2016-12-27 13:55:08
 License Type: Trial (date restricted)
 Trial Validity Period: 2016-12-27 to 2017-01-26
 Current State: Expired

表1-1 display license 命令显示信息描述表

字段	描述
Feature	特性名称
Product Description	License的描述信息
Registered at	在设备上的安装时间
License Type	License的类型，取值为： • NA: 无法获取 License 的类型 • Permanent: 永久类型，表示该 License 永远有效，不会过期 • Days restricted: 相对时间类型，表示该 License 是正式发布的，且有效期是一个相对时间段，比如 30 天 • Date restricted: 绝对时间类型，表示该 License 是正式发布的，且有效期是一个绝对时间段，比如 2017 年 5 月 1 日到 2017 年 5 月 30 日 • Trial (days restricted): 相对时间类型的试用 License，表示该 License 是相对时间类型的、非正式发布的 License • Trial (date restricted): 绝对时间类型的试用 License，表示该 License 是绝对时间类型的、非正式发布的 License
Time Left (days)	正式授权相对时间类型剩余时间
Trial Time Left (days)	临时授权相对时间类型剩余时间
Validity Period	正式授权绝对时间类型过期日期。No limit表示不限制时间
Trial Validity Period	临时授权绝对时间类型过期日期。No limit表示不限制时间

字段	描述
Current State	License当前状态取值为： • In use: 当前 License 正在使用 • Usable: 当前 License 正在等待使用（当设备同时安装了多个相对时间 License，且多个 License 均支持某一特性时，则只有一个 License 中的该特性处于 In use 状态，其它 License 中的该特性会处于 Usable 状态。绝对时间 License，此状态表示未到启用时间） • Expired: 当前 License 已过期 • Uninstalled: 当前 License 已卸载 • Unusable: 当前 License 无法使用 • Invalid: 不合法的数据，无法使用
Uninstall Key	卸载码。卸载激活文件，会生成卸载文件，卸载文件中包含卸载码。卸载码用于授权迁移
Uninstall Date	卸载日期

1.1.2 display license device-id

display license device-id 命令用来显示 SN 和 DID 信息。

【命令】

display license device-id slot slot-number

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。

【使用指导】

生成 License 激活文件需要使用 DID 和 SN，用来表示激活文件和设备的绑定关系。

DID 在执行压缩命令的时候会发生变化。因此，请在申请激活文件前，查询设备的 DID 信息。

DID 为文件形式，在申请激活文件时，需通过申请页面上传该文件。

【举例】

显示指定 slot 的 SN 和 DID 信息。

```
<Sysname> display license device-id slot 1
SN: 210235A1FXH164000026
Device ID: flash:/license/210235A1FXH164000026.did
```

表1-2 display license device-id 命令显示信息描述表

字段	描述
SN	序列号信息，用于生成激活文件
Device ID	设备编号信息，用于生成激活文件

1.1.3 display license feature

display license feature 命令用来显示特性的 License 摘要信息。

【命令】

display license feature

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 License 摘要信息。

```
<Sysname> display license feature
```

```
Slot 1:
```

```
Slot 1:
```

```
Total: 32  Usage: 1
```

Feature	Licensed	State
ACG	Y	Formal
AV	Y	Formal
IPS	Y	Formal

表1-3 display license feature 命令显示信息描述表

字段	描述
Total	设备上一共可安装License的总数目
Usage	设备上已经安装的License总数
Feature	需要License授权才能使用的业务特性的名称
Licensed	是否已经授权 - N 表示未授权 - Y 表示已授权

字段	描述
State	License的当前状态： • Formal 表示当前已经为该特性安装了正式 License，License 处于有效状态 • Trial 表示当前已经为该特性安装了临时 License，License 处于有效状态 • -表示当前无有效 License，用户如需使用该特性，请安装对应的 License

1.1.4 license activation-file install

license activation-file install 命令用来安装激活文件。

【命令】

license activation-file install *license-file* **slot** *slot-number*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

license-file: 激活文件的全路径，为 1~127 个字符的字符串，区分大小写。激活文件必须合法、有效，并且保存在设备存储介质上。

slot slot-number: 表示给成员设备安装激活文件。**slot-number** 表示设备在 IRF 中的成员编号。

【使用指导】

用户需要为每台成员设备安装激活文件。

用户使用指定成员设备的 SN 和 DID 申请到的激活文件只能安装在这台成员设备上。

成员设备安装激活文件后，即便加入别的 IRF，也具有运行相应特性的授权。

【举例】

给指定 slot 安装激活文件 20170811.ak。

```
<Sysname> system-view
```

```
[Sysname] license activation-file install flash:/license/20170811.ak slot 1
```

```
This operation might take some time. Do not perform any other operations until the operation is completed or a failure message is displayed. Please wait...Done.
```

【相关命令】

- **display license activation-file**
- **display license device-id**
- **license activation-file uninstall**

1.1.5 license activation-file uninstall

license activation-file uninstall 命令用来卸载激活文件。

【命令】

license activation-file uninstall *license-file slot slot-number*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

license-file: 激活文件的全路径，为 1~127 个字符的字符串，区分大小写。

slot slot-number: 表示给成员设备卸载激活文件。**slot-number** 表示设备在 IRF 中的成员编号。

【使用指导】

当用户购买的正式激活文件还没有到期，并且当前设备不需要再使用时，可以卸载该激活文件，此时设备会产生一个卸载凭证——卸载文件。用户可以将该卸载凭证和其它设备绑定，获取一个新的激活文件，并在新设备上安装，从而将 License 从当前设备迁移到其它设备。

激活文件被卸载后，对应的特性将无法获得到被卸载的激活文件的信息，特性无法运行。

临时激活文件不能迁移，所以卸载临时激活文件，不会产生卸载文件。如果卸载的是正式激活文件，则会产生卸载文件。

【举例】

给指定 slot 卸载正式激活文件 flash:/license/20130811.ak。

```
<Sysname> system-view
```

```
[Sysname] license activation-file uninstall flash:/license/20130811.ak slot 1
```

```
This operation might take some time. Do not perform any other operations until the operation is completed or a failure message is displayed. Please wait...Done.
```

```
Uninstall file: flash:/license/20130813.uak
```

【相关命令】

- **display license activation-file**
- **license activation-file install**

1.1.6 license compress

license compress 命令用来压缩 License 存储区。

【命令】

license compress slot slot-number

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number: 表示对指定成员设备的 License 存储区进行压缩。*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

License 存储区空间是有限的。执行该命令后，系统会自动判断各 License 的状态，将过期和卸载的 License 及其相关数据删除。从而释放空间，以便用户安装新的 License。

用户卸载了 License 或者有 License 过期，且这个 License 是通过激活文件申请的，再执行压缩操作，系统会自动变更 DID。因此，在压缩 License 存储区前，请确保使用旧 DID 申请的 License 已经安装完毕，否则，License 存储区压缩后，使用旧 DID 申请的 License 将无法继续安装。

请在执行该命令前，保存各卸载 License 的卸载码。因为执行该命令后，卸载码会被删除。

【举例】

给指定 slot 压缩 License 存储区。

```
<Sysname> system-view
```

```
[Sysname] license compress slot 1
```

This command will delete all data relevant to uninstalled and expired keys/licenses, including Uninstall keys, and create a new device ID for activation keys/files. Make sure you have saved the Uninstall keys so you can apply for a new activation key/file for the unexpired licenses that were covered by the uninstalled activation keys/files.

Are you sure you want to continue? [Y/N]: Y

This operation might take some time. Do not perform any other operations until the operation is completed or a failure message is displayed. Please wait...Done.



UNIS 入侵检测系统

虚拟化技术命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《虚拟化技术命令参考》主要介绍 IRF 和 Context 相关的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用 “[]” 括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由 “#” 号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号 “< >” 表示按钮名，如 “单击<确定>按钮”。
[]	带方括号 “[]” 表示窗口名、菜单名和数据表，如 “弹出[新建用户]窗口”。
/	多级菜单用 “/” 隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下

格 式	意 义
	的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 IRF	1-1
1.1 IRF配置命令	1-1
1.1.1 display irf	1-1
1.1.2 display irf configuration	1-2
1.1.3 display irf link	1-3
1.1.4 display irf topology	1-4
1.1.5 display irf-port load-sharing mode	1-5
1.1.6 display mad	1-7
1.1.7 easy-irf	1-9
1.1.8 irf auto-update enable	1-11
1.1.9 irf domain	1-12
1.1.10 irf mac-address persistent	1-13
1.1.11 irf member description	1-14
1.1.12 irf member priority	1-14
1.1.13 irf member renumber	1-15
1.1.14 irf-port	1-16
1.1.15 irf-port global load-sharing mode	1-17
1.1.16 irf-port load-sharing mode	1-17
1.1.17 irf-port-configuration active	1-18
1.1.18 mad bfd enable	1-19
1.1.19 mad enable	1-22
1.1.20 mad exclude interface	1-23
1.1.21 mad ip address	1-24
1.1.22 mad restore	1-25
1.1.23 port group interface	1-25

1 IRF

1.1 IRF配置命令

1.1.1 display irf

display irf 命令用来显示 IRF 的相关信息。

【命令】

display irf

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

```
# 显示 IRF 的相关信息。
<Sysname> display irf
MemberID  Role      Priority  CPU-Mac      Description
   1       Loading  1        00e0-fcbe-3102  F1Num001
  *+2      Master   1        00e0-fcb1-ade2  F1Num002
-----

* indicates the device is the master.
+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is: 00e0-fc00-1000
Auto upgrade           : yes
Mac persistent         : always
Domain ID              : 30
```

表1-1 display irf 命令显示信息描述表

字段	描述
MemberID	成员设备的编号： - 如果编号前带“*”，表示该设备是主设备 - 如果编号前带“+”，表示该设备是用户当前登录的、正在操作的设备
Role	成员设备的角色，可能为： - Standby: 从设备 - Master: 主设备 - Loading: 正在自动加载系统启动文件

字段	描述
Priority	成员设备的优先级
CPU-MAC	设备的CPU MAC地址
Description	设备的描述信息： - 没有描述信息时，Description 字段显示为"-----" - 如果描述信息较多，无法在一行中完全显示，则以“...”结尾，省略后面的信息。此时可以使用 display current-configuration 来查询完整的描述信息
Bridge MAC of the IRF is	IRF的桥MAC
Auto upgrade	是否开启自动加载系统启动文件功能： - yes 表示开启 - no 表示未开启
MAC persistent	是否开启IRF桥MAC保留功能： 6 min 表示 IRF 的桥 MAC 保留时间为 6 分钟 - always 表示 IRF 的桥 MAC 永久保留不改变 - no 表示立即改变 IRF 的桥 MAC
Domain ID	IRF的域编号，当网络中存在多个IRF时，用来唯一标识一个IRF

【相关命令】

- display irf configuration**
- display irf topology**

1.1.2 display irf configuration

display irf configuration 命令用来显示 IRF 中所有成员设备的 IRF 配置。

【命令】

display irf configuration

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 IRF 中所有成员设备的 IRF 配置。

```
<Sysname> display irf configuration
```

MemberID	NewID	IRF-Port1	IRF-Port2
1	1	Ten-GigabitEthernet1/0/1	Ten-GigabitEthernet1/0/2
2	2	Ten-GigabitEthernet2/0/1	Ten-GigabitEthernet2/0/2

表1-2 display irf configuration 命令显示信息描述表

字段	描述
MemberID	设备当前的成员编号
NewID	配置的成员编号，设备重启后将会生效
IRF-Port1	IRF端口1的配置 - 如果显示信息中包含多个物理端口，则表示该 IRF 端口由多个 IRF 物理端口聚合而成 - 如果显示为 disable，则表示该 IRF 端口还没有和 IRF 物理端口绑定
IRF-Port2	IRF端口2的配置 - 如果显示信息中包含多个物理端口，则表示该 IRF 端口由多个 IRF 物理端口聚合而成 - 如果显示为 disable，则表示该 IRF 端口还没有和 IRF 物理端口绑定

【相关命令】

- **display irf**
- **display irf topology**

1.1.3 display irf link

display irf link 命令用来显示 IRF 链路信息。

【命令】

display irf link

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 IRF 链路信息。

```
<Sysname> display irf link
```

Member 1

IRF Port	Interface	Status
1	disable	--
2	Ten-GigabitEthernet1/0/1	UP
	Ten-GigabitEthernet1/0/2	ADM
	Ten-GigabitEthernet1/0/3	DOWN

Member 2

IRF Port	Interface	Status
1	Ten-GigabitEthernet2/0/1	UP


```

                Ten-GigabitEthernet2/0/2                DOWN
                Ten-GigabitEthernet2/0/3                ADM
2               disable                                  --

```

表1-3 display irf link 命令显示信息描述表

字段	描述
Member ID	成员编号
IRF Port	IRF端口号，其中： 1 表示 IRF 端口 1 2 表示 IRF 端口 2
Interface	对应的IRF物理端口的名称 - 如果显示信息中包含多个物理端口，则表示该 IRF 端口由多个 IRF 物理端口聚合而成 - 如果显示为 disable，则表示该 IRF 端口还没有和 IRF 物理端口绑定
Status	IRF物理端口的链路状态 - UP：链路 up - DOWN：链路 down - ADM：表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 - ABSENT：接口不存在，没有插入单板或接口模块扩展卡

1.1.4 display irf topology

display irf topology 命令用来查看 IRF 的拓扑信息。

【命令】

display irf topology

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【举例】

```

# 显示 IRF 的拓扑信息。
<Sysname> display irf topology
                        Topology Info
-----
                IRF-Port1                IRF-Port2
MemberID  Link    neighbor  Link    neighbor  Belong To
1          DOWN    ---      UP      2          000f-cbb8-1a82
2          UP      1        DIS     ---          000f-cbb8-1a82

```

表1-4 display irf topology 命令显示信息描述表

字段	描述
MemberID	成员编号
IRF-Port1	IRF-Port1的信息，包括Link和neighbor信息
IRF-Port2	IRF-Port2的信息，包括Link和neighbor信息
Link	IRF端口的链路状态，包括： • UP: 链路 up • DOWN: 链路 down，可能因为物理链路没有连通，或者没有执行 irf-port-configuration active 命令激活 IRF 端口 • DIS: 表示该 IRF 端口还没有和任何 IRF 物理端口绑定 • TIMEOUT: IRF 报文超时 • ISOLATE: 本设备处于隔离状态，原因可能为设备型号不符合加入 IRF 的要求，或当前 IRF 中成员设备已达到最大数量
neighbor	与该IRF端口直连的设备的成员编号（显示为“---”表示该端口没有连接其它成员设备）
Belong To	所属IRF，用IRF中当前主设备的CPU MAC地址表示

【相关命令】

- **display irf**
- **display irf configuration**

1.1.5 display irf-port load-sharing mode

display irf-port load-sharing mode 命令用来显示 IRF 链路的负载分担模式。

【命令】

display irf-port load-sharing mode [irf-port [*member-id*/*irf-port-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

irf-port: 显示指定 IRF 链路的负载分担模式。不指定该参数时，显示全局 IRF 链路的负载分担模式。

member-id*/*irf-port-number: 表示 IRF 端口编号。其中，*member-id* 表示设备在 IRF 中的成员编号；*irf-port-number* 表示 IRF 端口索引，取值为 1 或 2。不指定该参数时，显示所有连通的 IRF 链路的负载分担模式，如果当前没有连通的 IRF 链路，则显示 “No IRF link exists.”。

【使用指导】

未指定 **irf-port** 参数时，显示全局采用的 IRF 链路负载分担模式。

如果仅指定 **irf-port** 参数而未指定 IRF 端口编号，则显示所有 IRF 端口下分别采用的负载分担模式。

如果指定了 IRF 端口编号，则显示该 IRF 端口下采用的负载分担模式。

【举例】

显示缺省情况下全局采用的 IRF 链路负载分担模式。

```
<Sysname> display irf-port load-sharing mode
irf-port Load-Sharing Mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

显示非缺省情况下全局采用的 IRF 链路负载分担模式。

```
<Sysname> display irf-port load-sharing mode
irf-port Load-Sharing Mode:
destination-mac address, source-mac address
```

显示缺省情况下 IRF 端口 1/1 下采用的负载分担模式。

```
<Sysname> display irf-port load-sharing mode irf-port 1/1
irf-port1/1 Load-Sharing Mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

显示非缺省情况下 IRF 端口 1/1 下采用的负载分担模式。

```
<Sysname> display irf-port load-sharing mode irf-port 1/1
irf-port 1/1 Load-Sharing Mode:
destination-mac address, source-mac address
```

显示所有 IRF 端口下分别采用的负载分担模式。

```
<Sysname> display irf-port load-sharing mode irf-port
irf-port 1/2 Load-Sharing Mode:
destination-ip address, source-ip address
irf-port 2/1 Load-Sharing Mode:
Layer 2 traffic: destination-mac address, source-mac address
Layer 3 traffic: destination-ip address, source-ip address
```

表1-5 display irf-port load-sharing mode 命令显示信息描述表

字段	描述
irf-port Load-Sharing Mode	全局采用的IRF链路负载分担类型： - 缺省情况下，为设备缺省的 IRF 链路负载分担类型 - 非缺省情况下显示：用户配置后采用的 IRF 链路负载分担类型
irf-port1/1 Load-Sharing Mode	IRF端口1/1下采用的负载分担类型： - 缺省情况下显示：全局采用的负载分担类型 - 非缺省情况下显示：用户配置后采用的负载分担类型
Layer 2 traffic: destination-mac address, source-mac address	二层报文缺省采用的负载分担类型：按照源MAC地址和目的MAC地址进行负载分担

字段	描述
Layer 3 traffic: destination-ip address, source-ip address	三层报文缺省采用的负载分担类型：按照源IP地址和目的IP地址进行负载分担
destination-mac address, source-mac address	用户配置后采用的负载分担类型：按照源MAC地址和目的MAC地址进行负载分担（此字段的显示内容与用户的配置相关）

1.1.6 display mad

display mad 命令用来显示 MAD 配置信息。

【命令】

display mad [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

verbose：显示 MAD 详细配置信息。如果不指定该参数，则显示简要配置信息。

【举例】

显示 MAD 简要配置信息。

```
<Sysname> display mad
MAD ARP disabled.
MAD ND disabled.
MAD LACP enabled.
MAD BFD enabled.
```

显示 MAD 详细配置信息。

```
<Sysname> display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
  GigabitEthernet1/0/1
  GigabitEthernet2/0/1
Excluded ports (system-configured):
  GigabitEthernet1/0/2
  GigabitEthernet2/0/2
MAD ARP disabled.
MAD ND disabled.
MAD LACP enabled interface: Route-Aggregation2
MAD status                : Normal
Member ID      Port      MAD status
```

```

1          GigabitEthernet1/0/3          Normal
2          GigabitEthernet2/0/3          Normal
MAD BFD enabled interface: Route-Aggregation2
MAD status          : Normal
Member ID  MAD IP address      Neighbor  MAD status
1          192.168.1.1/24      2          Normal
2          192.168.1.2/24      1          Normal

```

表1-6 display mad 命令显示信息描述表

字段	描述
MAD ARP disabled.	ARP MAD检测功能未开启 如本功能已开启，则显示为MAD ARP enabled
MAD ND disabled.	ND MAD检测功能未开启 如本功能已开启，则显示为MAD ND enabled
MAD LACP enabled.	LACP MAD检测功能已开启 如本功能未开启，则显示为MAD LACP disabled
MAD BFD enabled.	BFD MAD检测功能已开启 如本功能未开启，则显示为MAD BFD disabled
Multi-active recovery state	当前IRF是否被MAD功能设置为Recovery状态： - Yes: IRF 处于 Recovery 状态，当一个 IRF 分裂为多个 IRF 后，将发生多 Active 冲突，选举失败的 IRF 进入 Recovery 状态，该状态下的 IRF 会自动关闭所有非保留的业务接口 - No: IRF 没有处于 Recovery 状态
Excluded ports (user-configured)	用户配置的保留接口
Excluded ports (system-configured)	系统默认保留的接口（不需要用户配置，自动保留），包括： - IRF 物理端口 - 系统自动保留的二层聚合接口的成员接口。当用户将二层聚合接口配置为保留接口时，其成员接口自动为系统保留接口 - 系统自动保留的三层聚合接口的成员接口。当用户将三层聚合接口配置为保留接口时，其成员接口自动为系统保留接口
MAD LACP enabled interface	开启了LACP MAD检测功能的接口 如LACP MAD检测功能未开启，则显示为MAD LACP disabled.
MAD status	LACP MAD的工作状态： - Normal: LACP MAD 工作状态正常 - Faulty: LACP MAD 工作状态不正常，需要检查接口状态、中间设备是否支持 LACP MAD、以及聚合接口的成员端口是否分布到所有成员设备上
Member ID Port MAD status	LACP MAD详细信息： - Member ID: IRF 中的成员设备编号 - Port: 开启了 LACP MAD 的聚合组中的成员端口 - MAD status: 该成员端口的 LACP MAD 工作状态，Normal 表示正常，Faulty 表示不正常

字段	描述
MAD BFD enabled interface:	开启了BFD MAD的三层接口 如BFD MAD检测功能未开启，则显示为MAD BFD disabled.
MAD status	BFD MAD的工作状态： - Normal: BFD MAD 工作状态正常 - Faulty: BFD MAD 工作状态不正常，需要检查 BFD MAD 链路的连通状态 - N/A: 无法判断 BFD MAD 工作状态，在使用管理用以太网口实现 BFD MAD 检测时可能出现此信息
Member ID MAD IP address Neighbor MAD status	BFD MAD详细信息： - Member ID: IRF 中的成员设备编号 - MAD IP address: 各成员设备对应的 MAD IP 地址 - Neighbor: 邻居设备的成员编号 - MAD status: IRF 设备成员到邻居成员的 BFD MAD 工作状态，Normal 表示正常，Faulty 表示不正常，N/A 表示无法判断 BFD MAD 工作状态（在使用管理用以太网口实现 BFD MAD 检测时可能出现此信息）

1.1.7 easy-irf

easy-irf 命令用于快速配置 IRF。

【命令】

```
easy-irf [ member member-id [ renumber new-member-id ] domain domain-id
[ priority priority ] [ irf-port1 interface-list1 ] [ irf-port2
interface-list2 ] ]
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

member *member-id*: 表示设备当前的成员编号，取值范围为 1~2。

renumber *new-member-id*: 表示新成员编号，取值范围为 1~2。如果给成员设备指定新的成员编号，该成员设备会立即自动重启，以使新的成员编号生效。如果不指定该参数，则表示不修改成员编号。

domain *domain-id*: 表示设备所属的 IRF 域编号，*domain-id* 的取值范围为 0~4294967295。同一 IRF 中的成员设备应配置相同的域编号。

priority *priority*: 表示 IRF 成员的优先级，*priority* 的取值范围为 1~32。优先级值越大表示优先级越高，优先级高的设备竞选时成为主设备的可能性越大。

irf-port1 *interface-list1*: 表示与 IRF 端口 1 绑定的 IRF 物理端口。表示方式为 *interface-list1* = { *interface-type* *interface-number* }&<1-n>。其中

interface-type interface-number 表示接口类型和接口编号。&<1-n>表示前面的参数最多可以输入 n 次。

irf-port2 interface-list2: 表示与 IRF 端口 2 绑定的 IRF 物理端口。表示方式为 *interface-list2 = { interface-type interface-number }&<1-n>*。其中 *interface-type interface-number* 表示接口类型和接口编号。&<1-n>表示前面的参数最多可以输入 n 次。一个物理端口只能与一个 IRF 端口绑定。

IRF 可绑定的最多物理端口数参数为 8 个。

【使用指导】

使用该功能，用户可以通过一条命令配置 IRF 的基本参数，包括新成员编号、域编号、绑定物理端口，简化了配置步骤，达到快速配置 IRF 的效果。

在配置该功能时，有两种方式：

- 交互模式：用户输入 **easy-irf**，回车，在交互过程中输入具体参数的值。
- 非交互模式，在输入命令行时直接指定所需参数的值。

两种方式的配置效果相同，如果用户对本功能不熟悉，建议使用交互模式。

多次执行本命令时，生效情况如下：

- 多次执行本命令来修改域编号或优先级时，最近一次执行的命令生效。
- 多次执行本命令来修改 IRF 物理端口时，本次配置的端口会与之前已配置的端口同时生效。

在交互模式下为 IRF 端口指定物理端口时，请注意：

- 接口类型和接口编号间不能有空格。
- 不同物理接口之间用英文逗号分隔，逗号前后不能有空格。

如需删除现有的 IRF 物理端口配置，需要在 IRF 端口视图下，执行 **undo port group interface** 命令。

更多配置要求，请参见“虚拟化技术配置指导”中的“IRF”。

【举例】

通过非交互模式配置成员设备 2 的新成员编号为 1，域编号为 10，优先级为 10，IRF 端口 1 和 Ten-GigabitEthernet2/0/1 和 Ten-GigabitEthernet2/0/2 绑定。

```
<Sysname> system-view
[Sysname] easy-irf member 2 renumber 1 domain 10 priority 10 irf-port1 ten-gigabitethernet
2/0/1 ten-gigabitethernet 2/0/2
*****
Configuration summary for member 2
IRF new member ID: 1
IRF domain ID      : 10
IRF priority       : 10
IRF-port 1         : Ten-GigabitEthernet2/0/1, Ten-GigabitEthernet2/0/2
IRF-port 2         : Disabled
*****
Are you sure to use these settings to set up IRF? [Y/N] y
Starting to configure IRF...
Configuration succeeded.
The device will reboot for the new member ID to take effect. Continue? [Y/N] y
```

通过交互模式配置成员设备 2 的新编号为 1，域编号为 10，优先级为 10，IRF 端口 1 和 Ten-GigabitEthernet2/0/1 和 Ten-GigabitEthernet2/0/2 绑定。

```
<Sysname> system-view
[Sysname] easy-irf
*****
Welcome to use easy IRF.
To skip the current step, enter a dot sign (.).
To return to the previous step, enter a minus sign (-).
To use the default value (enclosed in []) for each parameter, press Enter without entering a value.
To quit the setup procedure, press CTRL+C.
*****
Select a member by its ID <2> [2]:2
Specify a new member ID <1~10> [1]: 1
Specify a domain ID <0~4294967295> [0]: 10
Specify a priority <1~32> [1]: 10
Specify IRF-port 1 bindings (a physical interface or a comma-separated physical interface list)[Disabled]: ten-gigabitethernet2/0/1,ten-gigabitethernet2/0/2
Specify IRF-port 2 bindings (a physical interface or a comma-separated physical interface list)[Disabled]:
*****
Configuration summary for member 2
IRF new member ID: 3
IRF domain ID      : 10
IRF priority       : 10
IRF-port 1         : Ten-GigabitEthernet2/0/1, Ten-GigabitEthernet2/0/2
IRF-port 2         : Disabled
*****
Are you sure to use these settings to set up IRF? [Y/N] y
Starting to configure IRF...
Configuration succeeded.
The device will reboot for the new member ID to take effect. Continue? [Y/N] y
```

1.1.8 irf auto-update enable

irf auto-update enable 命令用来开启 IRF 启动文件自动加载功能。

undo irf auto-update enable 命令用来关闭 IRF 启动文件自动加载功能。

【命令】

irf auto-update enable

undo irf auto-update enable

【缺省情况】

IRF 启动文件的自动加载功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启启动文件自动加载功能后，当新加入 IRF 的设备和主设备的软件版本不同时，新加入的设备会自动同步主设备的软件版本，再重新加入 IRF。为了确保成功进行自动加载，请确保从设备存储介质上有足够的空闲空间用于存放 IRF 的启动文件。如果从设备存储介质上空闲空间不足，该设备将自动删除当前启动文件来再次尝试加载；如果空闲空间仍然不足，该从设备将无法进行自动加载。此时，需要管理员重启从设备并进入从设备的 BootWare 菜单，删除一些不重要的文件后，再将从设备重新加入 IRF。

【举例】

```
# 开启启动文件自动加载功能。  
<Sysname> system-view  
[Sysname] irf auto-update enable
```

1.1.9 irf domain

irf domain 命令用来配置 IRF 域编号。

undo irf domain 命令用来恢复缺省情况。

【命令】

```
irf domain domain-id  
undo irf domain
```

【缺省情况】

IRF 的域编号为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain-id: IRF 的域编号，取值范围为 0~4294967295。

【使用指导】

为了适应各种组网应用，同一个网络里可以部署多个 IRF。多个 IRF 之间使用不同的域编号以示区别。

如果 LACP MAD 组网的中间设备本身也是一个 IRF 系统，则必须配置该命令确保 IRF 和中间设备的 IRF 域编号不同，否则可能造成检测异常，甚至导致业务中断。

IRF 中的所有成员设备都共用这个 IRF 域编号。在 IRF 设备上使用 **irf domain**、**mad enable** 命令均可修改全局 IRF 域编号，最新的配置生效。请按照网络规划来修改 IRF 域编号，不要随意修改。

【举例】

```
# 配置 IRF 的域编号为 10。  
<Sysname> system-view  
[Sysname] irf domain 10
```

1.1.10 irf mac-address persistent

irf mac-address persistent 命令用来配置 IRF 桥 MAC 的保留时间。

undo irf mac-address persistent 命令用来配置 IRF 桥 MAC 不保留，立即变化。

【命令】

```
irf mac-address persistent { always | timer }  
undo irf mac-address persistent
```

【缺省情况】

IRF 桥 MAC 保留 6 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

always: 配置 IRF 桥 MAC 永久保留。如果配置了 MAC 地址永久保留，则无论 IRF 桥 MAC 拥有者是否离开 IRF，IRF 桥 MAC 始终保持不变。

timer: 配置 IRF 桥 MAC 的保留时间为 6 分钟。如果配置了桥 MAC 保留时间为 6 分钟，则当 IRF 桥 MAC 拥有者离开 IRF 时，IRF 桥 MAC 在 6 分钟内不变化。如果 IRF 桥 MAC 拥有者在 6 分钟内重新又加入 IRF，则 IRF 桥 MAC 不会变化。如果 6 分钟后 IRF 桥 MAC 拥有者没有回到 IRF，则会使用 IRF 当前主设备的桥 MAC 作为 IRF 桥 MAC。

【使用指导】

IRF 桥 MAC 保留时间是指在桥 MAC 拥有者离开 IRF 后，IRF 可以继续使用当前桥 MAC 的时间。如果配置了 MAC 地址不保留，立即变化，当 IRF 桥 MAC 拥有者离开 IRF 时，系统立即会使用 IRF 中当前主设备的桥 MAC 做 IRF 桥 MAC。

当使用链型拓扑搭建 IRF，且 IRF 与其他设备之间有聚合链路存在时，如果需要重启主设备，请不要使用 **undo irf mac-address persistent** 命令配置 IRF 的桥 MAC 立即变化，否则可能会导致数据传输的延时甚至丢包。

当 IRF 设备上存在跨成员设备的聚合链路时，请不要使用 **undo irf mac-address persistent** 命令配置 IRF 的桥 MAC 立即变化，否则可能会导致流量中断。

缺省情况下，IRF 的桥 MAC 为 IRF 中当前主设备的桥 MAC。

如果两台物理设备的桥 MAC 相同，则它们不能合并为一个 IRF。IRF 的桥 MAC 不受此限制，只要成员设备自身桥 MAC 唯一即可。

【举例】

```
# 配置 IRF 的桥 MAC 保留时间为永久保留。
```

```
<Sysname> system-view
[Sysname] irf mac-address persistent always
```

1.1.11 irf member description

irf member description 命令用来配置 IRF 中成员设备的描述信息。

undo irf member description 命令用来恢复缺省情况。

【命令】

```
irf member member-id description text
undo irf member member-id description
```

【缺省情况】

未配置成员设备的描述信息。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

member-id: 表示设备在 IRF 中的成员编号。

text: 设备的描述信息，为 1~127 个字符的字符串。

【举例】

配置成员设备 1 的描述信息为 F1Num001。

```
<Sysname> system-view
[Sysname] irf member 1 description F1Num001
```

1.1.12 irf member priority

irf member priority 命令用来配置 IRF 中成员设备的优先级。

undo irf member priority 命令用来恢复缺省情况。

【命令】

```
irf member member-id priority priority
undo irf member member-id priority
```

【缺省情况】

设备的成员优先级均为 1。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

member-id: 表示设备在 IRF 中的成员编号，取值范围是 1~2。

priority: 表示优先级，取值范围为 1~32。优先级值越大表示优先级越高，优先级高的设备竞选时成为主设备的可能性越大。

【使用指导】

本命令的配置会影响成员设备在下一次选举中的角色，但不会触发选举。

【举例】

配置 IRF 中成员编号为 2 的设备的优先级为 32。

```
<Sysname> system-view
```

```
[Sysname] irf member 2 priority 32
```

1.1.13 irf member renumber

irf member renumber 命令用来配置设备的成员编号。

undo irf member renumber 命令用来取消成员编号的设置。

【命令】

irf member *member-id* renumber *new-member-id*

undo irf member *member-id* renumber

【缺省情况】

设备的成员编号是 1。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

member-id: 表示设备在 IRF 中的成员编号，取值范围是 1~2。

new-member-id: 表示修改后的成员编号，取值范围 1~2。

【使用指导】



注意

在 IRF 中以设备编号标志设备，配置 IRF 端口和优先级也是根据设备编号来配置的，所以，修改设备成员编号可能导致设备配置发生变化或者丢失，请慎重处理。

当新加入的设备的编号和 IRF 中已有成员设备的编号相同时，设备不能加入 IRF。此时，请使用该命令修改设备的成员编号后，重新加入 IRF。

UNIS 建议您修改成员设备编号时勿配置两台成员设备编号互换。这样配置可能带来非预期的配置互换或数据丢失。例如配置成员设备 1 和 2 编号互换会引起对应接口下的配置也发生互换。

该配置需要重启 *member-id* 标识的设备才能生效。

undo irf member renumber 命令只能取消本次运行过程中配置的成员编号。设备重启后，设备的成员编号就变为 *new-member-id*，不能再取消，只能重新配置。

【举例】

配置 IRF 中设备（原成员编号为 1）的成员编号为 2。

```
<Sysname> system-view
```

```
[Sysname] irf member 1 renumber 2
```

```
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]y
```

如果要取消以上配置，使设备的成员编号仍然是 1，则可以执行以下命令：

```
[Sysname] undo irf member 1 renumber
```

```
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]y
```

如果配置 **irf member 1 renumber 2** 后，重启设备，则设备的成员编号会变为 2。此时，不能使用 **undo irf member 1 renumber** 恢复到编号 1，只能使用 **irf member 2 renumber 1** 重新配置。

1.1.14 irf-port

irf-port 命令用来进入 IRF 端口视图。

undo irf-port 用来取消 IRF 端口上的所有配置。

【命令】

irf-port *member-id/irf-port-number*

undo irf-port *member-id/irf-port-number*

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

member-id：表示设备在 IRF 中的成员编号。

irf-port-number 表示 IRF 端口索引，取值为 1 时表示 IRF-port1，为 2 时表示 IRF-port2。

【使用指导】

在组建 IRF 前，必须进入 IRF 端口视图，并绑定 IRF 物理端口才能开启该 IRF 端口，从而进行 IRF 连接。

【举例】

进入 IRF 端口 2/1。

```
<Sysname> system-view
```

```
[Sysname] irf-port 2/1
```

```
[Sysname-irf-port2/1]
```

【相关命令】

- **port group interface**

1.1.15 irf-port global load-sharing mode

irf-port global load-sharing mode 命令用来配置全局 IRF 链路的负载分担模式。

undo irf-port global load-sharing mode 命令用来恢复缺省情况。

【命令】

```
irf-port global load-sharing mode { destination-ip | destination-mac |  
source-ip | source-mac } *  
undo irf-port global load-sharing mode
```

【缺省情况】

IRF 链路基于源目的 IP 来进行负载分担。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

destination-ip: 表示按报文的目的 IP 地址进行负载分担。

destination-mac: 表示按报文的目的 MAC 地址进行负载分担。

source-ip: 表示按报文的源 IP 地址进行负载分担。

source-mac: 表示按报文的源 MAC 地址进行负载分担。

【使用指导】

用户可以通过本命令配置全局的 IRF 链路负载分担模式，也可以通过 **irf-port load-sharing mode** 命令配置指定 IRF 端口的负载分担模式：

- 在系统视图的配置对所有 IRF 链路生效；
- 在 IRF 端口视图下的配置只对当前 IRF 端口下的 IRF 链路生效；
- IRF 链路会优先采用端口下的配置。如果端口下没有配置，则采用全局配置。

多次执行本命令，最后一次执行的命令生效。

对于设备不支持的负载分担模式，系统将提示用户不支持。

【举例】

配置全局按照报文目的 MAC 地址进行负载分担。

```
<Sysname> system-view
```

```
[Sysname] irf-port global load-sharing mode destination-mac
```

【相关命令】

- **irf-port load-sharing mode**

1.1.16 irf-port load-sharing mode

irf-port load-sharing mode 命令用来配置端口下 IRF 链路的负载分担模式。

undo irf-port load-sharing mode 命令用来恢复缺省情况。

【命令】

```
irf-port load-sharing mode { destination-ip | destination-mac | source-ip |  
source-mac } *  
undo irf-port load-sharing mode
```

【缺省情况】

IRF 链路基于源目的 IP 来进行负载分担。

【视图】

IRF 端口视图

【缺省用户角色】

network-admin

【参数】

destination-ip: 表示按报文的目的 IP 地址进行负载分担。

destination-mac: 表示按报文的目的 MAC 地址进行负载分担。

source-ip: 表示按报文的源 IP 地址进行负载分担。

source-mac: 表示按报文的源 MAC 地址进行负载分担。

【使用指导】

在配置负载分担模式前，请先将 IRF 端口和 IRF 物理端口绑定。否则，负载分担模式将配置失败。用户可以通过本命令配置指定 IRF 端口的负载分担模式，也可以通过 **irf-port global load-sharing mode** 命令配置全局的 IRF 链路负载分担模式：

- 在系统视图的配置对所有 IRF 链路生效；
- 在 IRF 端口视图下的配置只对当前 IRF 端口下的 IRF 链路生效；
- IRF 链路会优先采用端口下的配置。如果端口下没有配置，则采用全局配置。

多次执行本命令，最后一次执行的命令生效。

对于设备不支持的负载分担模式，系统将提示用户不支持。

【举例】

配置按报文目的 MAC 地址实现 IRF 端口 1/1 下 IRF 链路的负载分担模式。

```
<Sysname> system-view  
[Sysname] irf-port 1/1  
[Sysname-irf-port1/1] irf-port load-sharing mode destination-mac
```

【相关命令】

- **irf-port global load-sharing mode**

1.1.17 irf-port-configuration active

irf-port-configuration active 命令用于来激活设备上所有 IRF 端口的配置。

【命令】

```
irf-port-configuration active
```

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

IRF 物理线缆连接好，并将 IRF 物理端口添加到 IRF 端口后，必须通过该命令手工激活 IRF 端口的配置才能形成 IRF。

系统启动，通过配置文件将 IRF 物理端口加入 IRF 端口，或者 IRF 形成后再加入新的 IRF 物理端口时，IRF 端口下的配置会自动激活不再需要使用该命令来激活。

【举例】

在 IRF 端口 1/2 状态为 DIS 的情况下，激活 IRF 端口的配置。

- IRF 端口状态为 DIS 表示 IRF 端口还没有与任何 IRF 物理端口绑定，所以，先配置绑定关系。绑定前需要先将 IRF 物理端口关闭，绑定后再将 IRF 物理端口激活。

```
<Sysname> system-view
[Sysname] interface ten-gigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] shutdown
[Sysname-Ten-GigabitEthernet1/0/1] quit
[Sysname] irf-port 1/2
[Sysname-irf-port1/2] port group interface Ten-GigabitEthernet 1/0/1
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[Sysname-irf-port1/2] quit
[Sysname] interface ten-gigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet1/0/1] quit
```

- 将当前配置保存到下次启动配置文件，以便 IRF 端口的配置在设备重启后能继续生效。

```
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait.....
Saved the current configuration to mainboard device successfully.
```

- 激活 IRF 端口的配置。

```
[Sysname] irf-port-configuration active
```

1.1.18 mad bfd enable

mad bfd enable 命令用来开启 BFD MAD 检测功能。

undo mad bfd enable 用来关闭 BFD MAD 检测功能。

【命令】

mad bfd enable

undo mad bfd enable

【缺省情况】

BFD MAD 检测功能处于关闭状态。

【视图】

三层聚合接口视图
管理用以太网口视图

【缺省用户角色】

network-admin

【使用指导】

BFD MAD 和 ARP MAD、ND MAD 冲突处理的原则不同，请不要同时配置。

使用VLAN接口进行BFD MAD检测时，请注意 表 1-7 所列配置注意事项。

表1-7 使用 VLAN 接口进行 BFD MAD 检测

注意事项类别	使用限制和注意事项
BFD MAD检测VLAN	• 不允许在 Vlan-interface1 接口上开启 BFD MAD 检测功能 • 如果使用中间设备，需要进行如下配置： ◦ 在 IRF 设备和中间设备上，创建专用于 BFD MAD 检测的 VLAN ◦ 在 IRF 设备和中间设备上，将用于 BFD MAD 检测的物理接口添加到 BFD MAD 检测专用 VLAN 中 ◦ 在 IRF 设备上，创建 BFD MAD 检测 VLAN 的 VLAN 接口 • 如果网络中存在多个 IRF，在配置 BFD MAD 时，各 IRF 必须使用不同的 VLAN 作为 BFD MAD 检测专用 VLAN • 用于 BFD MAD 检测的 VLAN 接口对应的 VLAN 中只能包含 BFD MAD 检测链路上的端口，请不要将其它端口加入该 VLAN。当某个业务端口需要使用 port trunk permit vlan all 命令允许所有 VLAN 通过时，请使用 undo port trunk permit 命令将用于 BFD MAD 的 VLAN 排除
BFD MAD检测VLAN的特性限制	开启BFD检测功能的VLAN接口及VLAN内的物理端口只能专用于BFD检测，不允许运行其它业务 • 开启 BFD 检测功能的 VLAN 接口只能配置 mad bfd enable 和 mad ip address 命令。如果用户配置了其它业务，可能会影响该业务以及 BFD 检测功能的运行
BFD MAD IP地址	• 在用于 BFD MAD 检测的接口下必须使用 mad ip address 命令配置 MAD IP 地址，而不要配置其它 IP 地址（包括使用 ip address 命令配置的普通 IP 地址），以免影响 MAD 检测功能 • 为不同成员设备配置同一网段内的不同 MAD IP 地址

使用管理用以太网口进行BFD MAD检测时，请注意 表 1-8 所列配置注意事项。

表1-8 使用管理用以太网口进行 BFD MAD 检测

注意事项类别	使用限制和注意事项
管理用以太网口	将IRF中所有成员设备的管理用以太网口连接到同一台中间设备的普通以太网端口上
BFD MAD检测VLAN	- 将中间设备上与 IRF 成员设备相连的端口配置在一个 VLAN 内（IRF 设备的管理以太网口不需要此配置） - 如果网络中存在多个 IRF，在配置 BFD MAD 时，各 IRF 必须使用不同的 VLAN 作为 BFD MAD 检测专用 VLAN - 请确保中间设备上 BFD MAD 检测 VLAN 中仅包含用于 BFD 检测的端口
MAD IP地址	- 在管理用以太网口使用 mad ip address 命令配置 MAD IP 地址，请勿使用 ip address 命令配置 - 为不同成员设备配置同一网段内的不同 MAD IP 地址

使用三层聚合接口进行BFD MAD检测时，请注意 表 1-9 所列配置注意事项。

表1-9 使用三层聚合接口进行 BFD MAD 检测

注意事项类别	使用限制和注意事项
三层聚合接口配置	- 必须使用静态聚合模式的三层聚合接口（聚合接口缺省工作在静态聚合模式） - 聚合成员端口的个数不能超过聚合组最大选中端口数。否则，由于超出聚合组最大选中端口数的成员端口无法成为选中端口，会使 BFD MAD 无法正常工作，工作状态显示为 Faulty
BFD MAD检测VLAN	- 如果使用中间设备，请将中间设备上用于 BFD MAD 检测的物理接口添加到同一个 VLAN 中，并允许 PVID 的报文不带 Tag 通过。中间设备上的端口不用加入聚合组 - 如果设备充当多个 IRF BFD MAD 检测的中间设备，请为各 IRF 分配不同的 VLAN - 中间设备上用于 BFD MAD 检测的 VLAN 必须专用，不允许运行其他业务。且该 VLAN 中只能包含 BFD MAD 检测链路上的端口，请不要将其它端口加入该 VLAN。当某个业务端口需要使用 port trunk permit vlan all 命令允许所有 VLAN 通过时，请使用 undo port trunk permit 命令将用于 BFD MAD 的 VLAN 排除
开启BFD MAD检测功能的三层聚合接口的特性限制	开启BFD检测功能的接口只能配置 bfd enable 和 mad ip address 命令。如果用户配置了其它业务，可能会影响该业务以及BFD检测功能的运行
MAD IP地址	- 在用于 BFD MAD 检测的接口下必须使用 mad ip address 命令配置 MAD IP 地址，而不要配置其它 IP 地址（包括使用 ip address 命令配置的普通 IP 地址），以免影响 MAD 检测功能 - 为不同成员设备配置同一网段内的不同 MAD IP 地址

【举例】

```
# 在三层聚合接口 3 上启用 BFD MAD 检测功能。
<Sysname> system-view
[Sysname] interface route-aggregation 3
[Sysname-Route-Aggregation 3] mad bfd enable
```

1.1.19 mad enable

mad enable 命令用来开启 LACP MAD 方式检测功能。

undo mad enable 用来关闭 LACP MAD 方式检测功能。

【命令】

```
mad enable
undo mad enable
```

【缺省情况】

LACP MAD 检测功能处于关闭状态。

【视图】

聚合接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

LACP MAD 检测方式需要使用 UNIS 设备作为中间设备，每个成员设备都需要连接到中间设备。请在动态聚合接口下开启 LACP MAD 方式检测功能。聚合接口创建后，可使用 **link-aggregation mode dynamic** 命令将该接口配置为动态接口。

在 LACP MAD 检测组网中，如果中间设备本身也是一个 IRF 系统，则必须通过配置确保其 IRF 域编号与被检测的 IRF 系统不同，否则可能造成检测异常，甚至导致业务中断。

为了防止 IRF 级联组网时，本 IRF 的 MAD 检测报文转发到邻居 IRF 中影响邻居 IRF 的 MAD 检测，执行 **mad enable** 命令时，系统会要求用户输入 IRF 域编号。如果继续使用当前编号，则直接按回车即可。

IRF 域编号是一个全局变量，在 IRF 设备上使用 **irf domain**、**mad enable** 命令均可修改全局 IRF 域编号，最新的配置生效。

【举例】

```
# 在二层动态聚合接口 1 下启用 LACP MAD 方式检测功能。
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation1] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
```

```
MAD LACP only enable on dynamic aggregation interface.  
# 在三层动态聚合接口 1 下启用 LACP MAD 方式检测功能。  
<Sysname> system-view  
[Sysname] interface route-aggregation 1  
[Sysname-Route-Aggregation1] link-aggregation mode dynamic  
[Sysname-Route-Aggregation1] mad enable  
You need to assign a domain ID (range: 0-4294967295)  
[Current domain is: 0]: 1  
The assigned domain ID is: 1  
MAD LACP only enable on dynamic aggregation interface.
```

【相关命令】

- **irf domain**

1.1.20 mad exclude interface

mad exclude interface 命令用来配置保留接口。

undo mad exclude interface 命令用来将接口配置为非保留接口。

【命令】

```
mad exclude interface interface-type interface-number  
undo mad exclude interface interface-type interface-number
```

【缺省情况】

缺省情况下，设备进入 Recovery 状态时会自动关闭本设备上除了系统保留接口以外的所有业务接口。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

interface-type interface-number：表示接口类型和接口编号。

【使用指导】

设备进入 Recovery 状态时会自动关闭本设备上除系统保留接口外的所有的业务接口。如果希望 Recovery 状态 IRF 上有特殊用途的接口（比如 Telnet 登录接口）保持 UP 状态，可以将其配置为保留接口。建议您仅将 Telnet 登录接口配置为保留接口。

当分裂的 IRF 恢复时，处于 Recovery 状态的设备重启后重新加入 IRF，被 MAD 关闭的接口会自动恢复到正常状态。

在 MAD 故障未修复，接口没有自动恢复时，如果需要让 Recovery 状态 IRF 中的成员设备及其接口恢复到正常状态（原因可能是 Active 状态的 IRF 出现故障），可以在 Recovery 状态 IRF 上执行 **mad restore** 命令。

【举例】

```
# 配置 GigabitEthernet1/0/1 为保留接口，即当设备进入 Recovery 状态时，该接口不会被关闭。
<Sysname> system-view
[Sysname] mad exclude interface gigabitethernet 1/0/1
```

【相关命令】

- **mad restore**

1.1.21 mad ip address

mad ip address 命令用来为成员设备配置 MAD IP 地址。

undo mad ip address 命令用来删除成员设备的 MAD IP 地址。

【命令】

```
mad ip address ip-address { mask | mask-length } member member-id
undo mad ip address ip-address { mask | mask-length } member member-id
```

【缺省情况】

没有为成员设备配置 MAD IP 地址。

【视图】

VLAN 接口视图
三层聚合接口视图
管理用以太网口视图

【缺省用户角色】

network-admin

【参数】

ip-address: 接口的 IP 地址，为点分十进制格式。
mask: 接口 IP 地址相应的子网掩码，为点分十进制格式。
mask-length: 子网掩码长度，即掩码中连续“1”的个数，取值范围为 0~32。
member member-id: 表示成员在 IRF 中的成员编号。

【使用指导】

当使用 BFD MAD 检测时，IRF 中的所有成员设备都需要配置 MAD IP 地址，这些 IP 地址与成员编号绑定，且必须为同一网段。只有主设备的 MAD IP 地址生效，从设备的 MAD IP 地址不生效。当 IRF 链路分裂时，IRF 中的原从设备变为主设备，配置的 MAD IP 地址生效，BFD 会话被激活，设备将认为在网络中检测到存在配置冲突的 IRF。

在用于 BFD MAD 检测的接口不要配置其它 IP 地址（包括使用 **ip address** 命令配置的普通 IP 地址），以免影响 MAD 检测功能。

【举例】

```
# 配置三层聚合接口 3 在成员设备 1 上的 MAD IP 地址。
<Sysname> system-view
[Sysname] interface route-aggregation 3
[Sysname- Route-Aggregation 3] mad ip address 192.168.0.1 255.255.255.0 member 1
```

配置三层聚合接口 3 在成员设备 2 上的 MAD IP 地址。

```
[Sysname-Route-Aggregation 3] mad ip address 192.168.0.2 255.255.255.0 member 2
```

【相关命令】

- **mad bfd enable**

1.1.22 mad restore

mad restore 命令用来将设备从 Recovery 状态恢复到正常状态。

【命令】

mad restore

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当 IRF 链路故障会导致多 Active 冲突，原 IRF 分裂为多个 IRF，为了防止网络中配置冲突，IRF 系统会通过多 Active 检测机制，让其中一个 IRF 继续正常工作，其它 IRF 的状态修改为 Recovery（处于该状态的 IRF 不能处理业务报文）。如果继续正常工作的 IRF 也发生故障不能工作，此时可以通过本命令将处于 Recovery 状态的 IRF 恢复到正常工作状态接替原 IRF 工作，以便保证业务尽量少受影响。

【举例】

将 IRF 从 Recovery 状态恢复到正常状态。

```
<Sysname> system-view
```

```
[Sysname] mad restore
```

```
This command will restore the device from multi-active conflict state. Continue? [Y/N]:Y
```

```
Restoring from multi-active conflict state, please wait...
```

1.1.23 port group interface

port group interface 命令用来绑定设备的 IRF 端口和 IRF 物理端口，在 IRF 端口上第一次绑定 IRF 物理端口的同时相当于开启了 IRF 端口的 IRF 功能。

undo port group interface 命令用来取消设备的 IRF 端口和 IRF 物理端口的绑定关系。

【命令】

port group interface *interface-type interface-number*

undo port group interface *interface-name*

【缺省情况】

IRF 端口创建后未与任何物理端口绑定。

【视图】

IRF 端口视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number: 表示 IRF 物理端口的类型和编号。

interface-name: IRF 物理端口的名称, 格式为 *interface-type+interface-number*, *interface-type* 与 *interface-number* 之间没有空格。

【使用指导】

多次执行该命令可以将同一 IRF 端口与多个 IRF 物理端口绑定, 最多可绑定的物理端口数为 8 个。需要先使用 **shutdown** 命令关闭相应的物理端口, 才能将 IRF 端口与物理端口绑定或解绑定。在绑定或解绑定的操作完成后, 需要执行 **undo shutdown** 命令开启物理端口。

配置本命令后, 即便热插拔接口板导致绑定的 IRF 物理端口不存在了, 但绑定关系仍然存在, 使用 **undo port group interface** 命令可以取消绑定关系。

有些接口板出厂时已将接口分组, 同一组内的接口只能都作为 IRF 物理端口, 或者都不作为 IRF 物理端口。当将某组中的一个接口和 IRF 端口绑定时, 系统要求先将该组中的所有接口都关闭, 否则, 绑定失败; 当绑定后, 将其中一个接口激活时, 系统会判断该组中的其它接口是否已经和 IRF 端口绑定 (可以绑定到同一 IRF 端口, 也可以绑定到不同 IRF 端口), 如果未绑定, 则不允许激活。

更多配置要求, 请参见“虚拟化技术配置指导”中的“IRF”。

【举例】

将成员设备 1 的 IRF 物理端口 Ten-GigabitEthernet1/0/1 和 IRF 端口 IRF-port1 绑定。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] shutdown
[Sysname-Ten-GigabitEthernet1/0/1] quit
[Sysname] irf-port 1/1
[Sysname-irf-port1/1] port group interface ten-gigabitethernet 1/0/1
[Sysname-irf-port1/1] quit
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] undo shutdown
```

【相关命令】

- **irf-port**

目 录

1 Context	1-1
1.1 Context命令	1-1
1.1.1 allocate interface	1-1
1.1.2 allocate vlan	1-2
1.1.3 capability security-policy-rule maximum	1-3
1.1.4 capability session maximum	1-4
1.1.5 capability session rate	1-4
1.1.6 capability throughput	1-5
1.1.7 context	1-6
1.1.8 context start	1-7
1.1.9 description	1-8
1.1.10 display context	1-9
1.1.11 display context capability	1-9
1.1.12 display context configuration	1-11
1.1.13 display context interface	1-12
1.1.14 display context resource	1-13
1.1.15 display context statistics	1-15
1.1.16 display context vlan	1-16
1.1.17 limit-resource cpu	1-17
1.1.18 limit-resource disk	1-18
1.1.19 limit-resource memory	1-19
1.1.20 switchto context	1-19
1.1.21 tar context log	1-20

1 Context

1.1 Context命令

对于本文列出的命令，缺省 Context 均支持，非缺省 Context 只支持 **display context interface** 命令。

1.1.1 allocate interface

allocate interface 命令用来为 Context 分配接口。

undo allocate interface 命令用来取消为 Context 分配的接口。

【命令】

```
allocate interface { interface-type interface-number }&<1-24> [ share ]  
undo allocate interface { interface-type interface-number }&<1-24>  
allocate interface interface-type interface-number1 to interface-type  
interface-number2 [ share ]  
undo allocate interface interface-type interface-number1 to interface-type  
interface-number2
```

【缺省情况】

设备上的所有接口都属于缺省 Context，不属于任何非缺省 Context。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

{ *interface-type interface-number* }&<1-24>: 表示给 Context 分配非连续的接口。
interface-type interface-number 表示接口类型和编号，&<1-24>表示前面的参数最多可以输入 24 次。

interface-type interface-number1 to interface-type interface-number2: 表示给 Context 分配一组连续的接口。其中，*interface-type* 表示接口类型，*interface-number1* 表示起始接口的编号，*interface-number2* 表示结束接口的编号。起始接口和结束接口的类型必须相同，并且处于同一接口板上，否则将配置失败。

share: 表示接口是否共享。不指定该参数表示独占。

【使用指导】

- 独占方式分配（不带 **share** 参数）。使用该方式分配的接口仅归该 Context 所有、使用。用户登录该 Context 后，能查看到该接口，并执行接口支持的所有命令。

- 共享方式分配（带 **share** 参数）。使用该方式分配的接口归多个 Context 所有、使用。在缺省 Context 内仍然存在该接口，可执行接口支持的所有命令；在分配给的非缺省 Context 内，会新建同名接口，用户登录这些 Context 后，能查看到该接口，但只能执行 **shutdown**、**description**、以及网络/安全相关的命令。



注意

- 当设备运行在 IRF 模式时，禁止将 IRF 物理端口分配给自定义 Context。
 - 当三层子接口作为冗余口的成员端口时，禁止把其主接口共享给自定义 Context。
 - 逻辑接口仅支持共享方式分配，物理接口支持独占和共享两种方式分配。
-

【举例】

```
# 将接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/3 以共享的方式分配给 context sub1。
<Sysname> system-view
[Sysname] context sub1
[Sysname-context-2-sub1] allocate interface gigabitethernet 1/0/1 gigabitethernet 1/0/3
share
```

1.1.2 allocate vlan

allocate vlan 命令用来为 Context 分配 VLAN。

undo allocate vlan 命令用来取消为 Context 分配的 VLAN。

【命令】

```
allocate vlan vlan-id<1-24>
undo allocate vlan vlan-id<1-24>
allocate vlan vlan-id1 to vlan-id2
undo allocate vlan vlan-id1 to vlan-id2
```

【缺省情况】

没有为 Context 分配 VLAN。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

vlan-id<1-24>：表示给 Context 分配非连续的 VLAN。*vlan-id* 表示 VLAN 的编号，<1-24> 表示前面的参数最多可以输入 24 次。

vlan-id1 to vlan-id2：表示给 Context 分配一组连续的 VLAN。其中，*vlan-id1* 表示起始 VLAN 的编号，*vlan-id2* 表示结束 VLAN 的编号。

【使用指导】

创建 Context 时，通过 **vlan-unshared** 参数可选择是否和其它 Context 共享 VLAN：

- 如果选择和其它 Context 共享 VLAN，可以通过本命令将设备上存在的除 VLAN 1 以外的静态 VLAN 分配给非缺省 Context。共享 VLAN 由多个 Context 共同所有。VLAN 被分配后，用户须在缺省 Context 内对该 VLAN 配置，非缺省 Context 内不能配置该 VLAN，只能查看该 VLAN 的相关信息。
- 如果选择不和其它 Context 共享 VLAN，请登录该 Context，并使用 **vlan** 命令创建 VLAN 2～VLAN 4094。VLAN 1 为缺省 VLAN，用户不能手工创建和删除。Context 各自使用和管理 VLAN，互不干扰。

【举例】

```
# 将 VLAN100 分配给 context sub1。
<Sysname> system-view
[Sysname] context sub1
[Sysname-context-2-sub1] allocate vlan 100
```

【相关命令】

- **display context vlan**

1.1.3 capability security-policy-rule maximum

capability security-policy-rule maximum 命令用来设置 Context 的安全策略规则总数限制。

undo capability security-policy-rule maximum 命令用来恢复缺省情况。

【命令】

```
capability security-policy-rule maximum max-number
undo capability security-policy-rule maximum
```

【缺省情况】

未对 Context 的安全策略规则总数进行限制。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

max-number：表示 Context 内可配置的安全策略规则最大数目，取值范围为 1～4294967295。

【使用指导】

一个 Context 内可以配置多个安全策略规则。如果不加限制，会出现大量规则占用过多的内存的情况，影响 Context 的其它功能正常运行。所以，请根据需要为 Context 设置安全策略规则总数限制。当规则总数达到限制值时，后续不能新增规则。

如果设置的最大值比当前存在的规则总数小，配置仍会成功，多出的规则不会删除，但不能新增规则。

【举例】

```
# 配置 Context 的安全策略规则数最多为 1000 条。
```

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability security-policy-rule maximum 1000
```

【相关命令】

- **display security-policy ip**（安全命令参考/安全策略）

1.1.4 capability session maximum

capability session maximum 命令用来设置 Context 的单播会话并发数限制。

undo capability session maximum 命令用来恢复缺省情况。

【命令】

```
capability session maximum max-number
undo capability session maximum
```

【缺省情况】

未对 Context 允许的单播会话并发数进行限制。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

max-number：允许同时存在的最大单播会话数目，取值范围为 1～4294967295。

【使用指导】

如果一个 Context 建立了太多会话会导致其他 Context 的会话由于内存不够而无法建立，为了防止这种情况，需要限制 Context 建立会话的数量，当会话总数达到限制值时，后续不能新建会话。

如果设置的最大值比当前存在的会话总数小，配置仍会成功，但不允许新建会话，且已经创建的会话不会被删除，直到已建立的会话通过老化机制使得会话总数低于配置的最大值后，系统才允许新建会话。

Context 会话并发数限制对本机流量不生效。

【举例】

配置 Context cnt2 上的单播会话并发数为 1000000。

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability session maximum 1000000
```

【相关命令】

- **context**
- **display session statistics**（安全命令参考/会话管理）

1.1.5 capability session rate

capability session rate 命令用来设置 Context 的会话新建速率限制。

undo capability session rate 命令用来恢复缺省情况。

【命令】

```
capability session rate max-value  
undo capability session rate
```

【缺省情况】

未对 Context 允许的会话新建速率进行限制。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

max-value: 允许的会话新建速率最大值，单位为每秒会话个数。

【使用指导】

如果一个 Context 的会话新建速率过快会导致其他 Context 由于 CPU 处理能力不够而无法建立会话，为了防止这种情况，需要限制 Context 的会话新建速率，当会话新建速率达到限制值时，后续不能新建会话。

Context 会话新建速率限制对本机流量不生效。

【举例】

```
# 配置 Context cnt2 上的会话新建速率最大值为每秒 20000 个会话数。  
<Sysname> system-view  
[Sysname] context cnt2  
[Sysname-context-2-cnt2] capability session rate 20000
```

【相关命令】

- **context**
- **display session statistics**（安全命令参考/会话管理）

1.1.6 capability throughput

capability throughput 命令用来设置 Context 的吞吐量限制。

undo capability throughput 命令用来恢复缺省情况。

【命令】

```
capability throughput { kbps | pps } value  
undo capability throughput
```

【缺省情况】

各 Context 不做吞吐量限制，按实际能力转发。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

kbps: 表示吞吐量按每秒千比特计算。
pps: 表示吞吐量按每秒报文数计算。
value: 表示吞吐量限制值，取值范围为 1000~100000000。

【举例】

```
# 配置 Context 的吞吐量为 100Mbps。
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability throughput kbps 100000
# 配置 Context 的吞吐量为 10000pps。
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability throughput pps 10000
```

1.1.7 context

context 命令用来创建 Context，并进入 Context 视图。如果指定的 Context 已经存在，则直接进入 Context 视图。

undo context 命令用来删除指定 Context。

【命令】

```
context context-name [ id context-id ] [ vlan-unshared ]
undo context context-name
```

【缺省情况】

存在缺省 Context，名称为 Admin，编号为 1。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

context-name: Context 的名称，为 1~15 个字符的字符串，区分大小写。
context-id: Context 的编号。不指定该参数时，系统会自动给 Context 分配一个当前空闲的最小编号。
本参数的取值范围与设备型号有关，请以设备实际情况为准。

型号	说明
T5000-G20	取值范围为1~257
T5000-G30	取值范围为1~257

型号	说明
T1000-G20/T1000-G50/T1000-G60/T1000-G80	• T1000-G50: 取值范围为 1~33 • T1000-G20/T1000-G80: 取值范围为 1~129 • T1000-G60: 取值范围为 1~65
T1000-CN60/T1000-CN80	取值范围为1~17

vlan-unshared: 不和其它 Context 共享 VLAN。不指定该参数时,表示和其它 Context 共享 VLAN。

【使用指导】

创建 Context 时, 通过 **vlan-unshared** 参数可选择是否和其它 Context 共享 VLAN:

- 如果选择和其它 Context 共享 VLAN, 需要在缺省 Context 内创建并配置 VLAN, 再分配给非缺省 Context。共享 VLAN 由多个 Context 共同所有。
- 如果选择不和其它 Context 共享 VLAN, 请登录该 Context, 并使用 **vlan** 命令创建 VLAN 1~VLAN 4094。Context 各自使用和管理 VLAN, 互不干扰。

【举例】

```
# 创建一个名称为 test 的 Context。
<Sysname> system-view
[Sysname] context test
[Sysname-context-2-test]

# 创建一个名称为 test, ID 为 2 的 Context。
<Sysname> system-view
[Sysname] context test id 2
[Sysname-context-2-test]
```

1.1.8 context start

context start 命令用来启动 Context。

undo context start 命令用来停止该 Context。

【命令】

```
context start [ force ]
undo context start [ force ]
```

【缺省情况】

未启动 Context。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

force: 强制启动/停止 Context。不指定该参数时, 表示按正常程序启动 Context。

【使用指导】



注意

停止 Context 会导致该 Context 的业务中断，以及登录该 Context 的用户自动退出，请谨慎使用。
为避免 Context 的当前配置丢失，停止 Context 前请保存 Context 的配置。

Context 创建后需要执行 **context start** 命令，才能完成新 Context 的初始化，相当于上电启动。
启动后，用户可以登录到该 Context 执行配置。

【举例】

```
# 启动 Context cnt2。  
<Sysname> system-view  
[Sysname] context cnt2  
[Sysname-context-2-cnt2] context start
```

1.1.9 description

description 命令用来配置 Context 的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text  
undo description
```

【缺省情况】

缺省 Context 描述信息为 DefaultContext。非缺省 Context 没有配置描述信息。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

text: Context 的描述信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

当设备上配置的 Context 较多时，用户可以为 Context 配置特定的描述信息，以便记忆和管理 Context。

【举例】

```
# 将 Context 的描述信息配置为 test。  
<Sysname> system-view  
[Sysname] context cnt2  
[Sysname-context-2-cnt2] description test
```


1.1.10 display context

display context 命令用来显示已经创建的 Context 的信息，包括编号和状态等。

【命令】

display context [*name context-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name: Context 的名称，为 1~15 个字符的字符串，区分大小写。

【使用指导】

在缺省 Context 中，可使用 **name context-name** 参数查看指定 Context 的信息。不指定 **name context-name** 参数时，则显示设备上创建的所有 Context 的信息。

【举例】

显示已经创建的 Context 的信息。
<Sysname> display context
ID Name Status Description
1 cnt1 active context1
2 cnt2 inactive context2
3 cnt3 inactive context3

表1-1 display context 命令显示信息描述表

字段	描述
ID	Context的编号
Name	Context的名称
Status	Context的状态： • active: 表示 Context 正常运行 • inactive: 表示 Context 处于未启动状态 • starting: 表示 Context 正在启动 • stopping: 表示 Context 正在停止
Description	Context描述信息

1.1.11 display context capability

display context capability 命令用来显示 Context 内可分配业务资源的使用情况。

【命令】

display context [*name context-name*] **capability** [*security-policy* | *session*] [*slot slot-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name: 显示指定 Context 内可分配业务资源的使用情况，*context-name* 是 Context 的名称，为 1~15 个字符的字符串，区分大小写。若不指定该参数，则表示显示所有 Context 内可分配业务资源的使用情况。

security-policy: 显示可分配安全策略规则资源的使用情况。

session: 显示可分配会话资源的使用情况。

slot slot-number: 显示指定成员设备上的 Context 内可分配会话资源的使用情况，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示显示所有成员设备上的 Context 内可分配会话资源的使用情况。

【使用指导】

此命令仅支持在缺省 Context 中使用。

【举例】

显示所有 Context 内可分配业务资源的使用情况。

```
<Sysname> display context capability
Session usage and establishment rate:
Slot 1 CPU 0:
  ID   Name      Maximum    Used    Free    Total(/s)  Rate(/s)  Usage(%)
  --   -
  1    Admin      NA         500     NA      NA         1000      NA
  2    conetxt1  10000     300     9700    1000       100       10
  3    context2   2000      1000    1000    2000       1000      50
Security policy rule usage:
  ID   Name      Maximum    Used    Free
  --   -
  1    Admin      NA         500     NA
  2    conetxt1  10000     300     9700
  3    context2   2000      1000    1000
```

表1-2 display context capability 命令显示信息描述表

字段	描述
Session usage	表示可分配会话连接数的使用情况
Session establishment rate	表示可分配会话新建速率的使用情况
Security policy rule usage	表示可分配安全策略规则资源的使用情况
ID	表示Context的ID

Name	表示Context的名称
Maximum	表示当前Context内可分配资源的最大值
Used	表示当前Context内可分配资源已被使用的数量
Free	表示当前Context内可分配资源未被使用的数量
Total	表示当前Context内会话新建速率的最大值，单位为每秒连接数
Rate	表示当前Context内会话的当前新建速率，单位为每秒连接数
Usage	表示当前Context内会话新建速率所占的百分比

【相关命令】

- **capability security-policy-rule maximum**
- **capability session maximum**
- **capability session rate**

1.1.12 display context configuration

display context configuration 命令用来显示各 Context 的配置信息。

【命令】

display context [name *context-name*] configuration [file *filename*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name *context-name*: 显示指定 Context 的配置信息，*context-name* 是 Context 的名称，为 1～15 个字符的字符串，区分大小写。若不指定该参数，则表示显示所有 Context 的配置信息。

file *filename*: 表示将显示的配置信息保存到指定文件。*filename* 表示文件的名称，为 1～255 个字符的字符串（含后缀），不区分大小写，文件名不能为 “.” 或 “..”，不能包含 “”、 “/”、 “:”、 “\”、 “?”、“\\”、“<”、“>”、“|”、“*”，首字符不能为 “-”，且后缀必须为 “.tar.gz”，后缀不区分大小写。不指定该参数时，用户可根据提示信息选择将配置信息保存到指定文件或直接将配置信息导出到终端显示。

【使用指导】

此命令仅支持在缺省 Context 中使用。

执行该命令，相当于在所有 Context 中一次性执行 **display current-configuration** 命令。

在缺省 Context 中，无法对处于未启动状态的自定义 Context 进行配置信息收集。

【举例】

显示所有 Context 的配置信息。

```

<Sysname> display context configuration
Save or display context configuration(Y=save, N=display)? [Y/N]:n
=====inner configuration of context Admin=====

=====
display current-configuration
#
  version 7.1.064, Feature 9321
#
sysname Sysname
#
context Admin id 1
#
context cnt1 id 2
#
return
<Sysname>

=====inner configuration of context cnt1=====

=====
display current-configuration
#
  version 7.1.064, Feature 9321
#
sysname Sysname
#
context Admin id 1
#
context cnt1 id 2
---- More ----
# 在交互信息时选择将配置信息保存到指定文件，并输入文件名为 test.tar.gz。
<Sysname> display context configuration
Save or display context configuration (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag.tar.gz]: test.tar.gz
Saving context configuration to flash:/test.tar.gz. Please wait...
# 在命令行中直接通过参数指定将配置信息保存到文件 test.tar.gz。
<Sysname> display context configuration file test.tar.gz
Saving context configuration to flash:/test.tar.gz. Please wait...

```

1.1.13 display context interface

display context interface 命令用来显示 Context 的接口列表。

【命令】

display context [name context-name] interface

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name: Context 的名称，为 1~15 个字符的字符串，区分大小写。

【使用指导】

在缺省 Context 中，可使用 **name context-name** 参数查看指定 Context 的接口列表；不指定 **name context-name** 参数时，则显示设备上创建的所有 Context 的接口列表。

【举例】

```
# 显示所有 Context 的接口列表。
<Sysname> display context interface
Context stub1's interfaces:
    GigabitEthernet1/0/2
Context stub2's interfaces:
    GigabitEthernet1/0/3
```

【相关命令】

- **allocate interface**

1.1.14 display context resource

display context resource 命令用来显示 Context 对 CPU/磁盘/内存资源的使用情况。

【命令】

```
display context [ name context-name ] resource [ cpu | disk | memory ] [ slot  
slot-number cpu cpu-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name: 显示指定 Context 对 CPU/磁盘/内存资源的使用情况。**context-name** 表示 Context 的名称，为 1~15 个字符的字符串，区分大小写。不指定该参数时，显示所有 Context 对 CPU/磁盘/内存资源的使用情况。

cpu: 显示 Context 对 CPU 的使用情况。

disk: 显示 Context 对磁盘的使用情况。

memory: 显示 Context 对内存的使用情况。

slot slot-number cpu cpu-number: 显示 Context 对指定成员设备上的 CPU/磁盘/内存资源的使用情况，*slot-number* 表示设备在 IRF 中的成员编号，*cpu-number* 表示 CPU 的编号。不指定该参数时，显示 Context 对所有成员设备的 CPU/磁盘/内存资源的使用情况。

【使用指导】

若不指定 **cpu**、**disk** 和 **memory** 参数，则显示 Context 对 CPU、磁盘和内存的使用情况。

【举例】

显示 Context 对所有成员设备上 CPU 资源的使用情况。

```
<Sysname> display context resource cpu
```

CPU usage:

Slot 1 CPU 0:

ID	Name	Weight	Usage(%)
1	cnt1	10	24
2	cnt2	10	0

Slot 2 CPU 0:

ID	Name	Weight	Usage(%)
1	cnt3	10	0
2	cnt4	10	0

表1-3 display context resource 命令显示信息描述表

字段	描述
Memory	表示下面显示的是内存的使用情况
CPU	表示下面显示的是CPU的使用情况
Disk	表示下面显示的是磁盘的使用情况
Used 238.1MB, Free 249.3MB, Total 487.4MB	内存的使用情况，Used表示内存已使用空间的大小（单位为MB），Free表示当前空闲内存的大小（单位为MB），Total表示整个内存大小（单位为MB）。如果Context没有启动，则Used会显示为0
Cfa0: Used 0MB, Free 61MB, Total 61MB	Cfa0表示磁盘的名称，Used表示整个磁盘已使用空间的大小（单位为MB），Free表示整个磁盘当前空闲空间的大小（单位为MB），Total表示整个磁盘空间大小（单位为MB）。如果Context没有启动，则Used会显示为0
ID	Context的编号
name	Context的名称
Weight	Context使用CPU的权重值
Usage(%)	Context对CPU的实际占用率，用百分比表示
Quota(MB)	Context使用磁盘/内存的限制值，单位为MB
Used(MB)	Context当前已使用的磁盘/内存空间的大小，单位为MB
Free(MB)	Context还可以使用的磁盘/内存空间的大小，单位为MB

【相关命令】

- **limit-resource cpu**

- **limit-resource disk**
- **limit-resource memory**

1.1.15 display context statistics

display context statistics 命令用来显示 Context 内资源的统计信息。

【命令】

display context [*name context-name*] **statistics** [*file filename*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name: 显示指定 Context 内资源的统计信息, *context-name* 是 Context 的名称, 为 1~15 个字符的字符串, 区分大小写。若不指定该参数, 则表示显示所有 Context 内资源的统计信息。

file filename: 表示将收集到的资源统计信息保存到指定文件。 *filename* 表示文件的名称, 为 1~255 个字符的字符串 (含后缀), 不区分大小写, 文件名不能为 “.” 或 “..”, 不能包含 “/”、“:”、“\”、“?”、“\\”、“<”、“>”、“|”、“*”, 首字符不能为 “-”, 且后缀必须为 “.tar.gz”, 后缀不区分大小写。不指定该参数时, 用户可根据提示信息选择将资源的统计信息保存到指定文件或直接将资源的统计信息导出到终端显示。

【使用指导】

此命令仅支持在缺省 Context 中使用。

执行该命令, 相当于一次性执行如下命令:

- **display context capability**
- **display counters inbound interface**
- **display counters outbound interface**
- **display counters rate inbound interface**
- **display counters rate outbound interface**
- **display interface**
- **display ip statistics**
- **display ipv6 statistics**
- **display session statistics**
- **display system internal aspf statistics zone-pair ipv4**
- **display system internal aspf statistics zone-pair ipv6**

有关此命令显示信息的详细介绍, 请参考各个命令显示信息的介绍。

【举例】

显示所有 Context 内资源的统计信息。

```
<Sysname> display context statistics
Save or display context statistics (Y=save, N=display)? [Y/N]:n
=====
===== display session statistics =====
Slot 1:
Current sessions: 0
      TCP sessions:          0
      UDP sessions:          0
      ICMP sessions:         0
      ICMPv6 sessions:       0
      UDP-Lite sessions:     0
      SCTP sessions:         0
      DCCP sessions:         0
      RAWIP sessions:        0
---- More ----
```

将资源统计信息保存到指定文件，并输入文件名为 test.tar.gz。

```
<Sysname> display context statistics
Save or display context statistics(Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag.tar.gz]: test.tar.gz
Saving context statistics to flash:/test.tar.gz. Please wait....
```

将资源统计信息保存到文件 test.tar.gz。

```
<Sysname> display context statistics file test.tar.gz
Saving context statistics to flash:/test.tar.gz. Please wait...
```

【相关命令】

- **display context capability**
- **display counters inbound interface**（接口管理命令参考/以太网接口）
- **display counters outbound interface**（接口管理命令参考/以太网接口）
- **display counters rate inbound interface**（接口管理命令参考/以太网接口）
- **display counters rate outbound interface**（接口管理命令参考/以太网接口）
- **display interface**（接口管理命令参考/以太网接口）
- **display ip statistics**（三层技术-IP 业务命令参考/IP 性能优化）
- **display ipv6 statistics**（三层技术-IP 业务命令参考/IPv6 基础）
- **display session statistics**（安全命令参考/会话管理）
- **display system internal aspf statistics zone-pair ipv4**（Probe 命令参考）
- **display system internal aspf statistics zone-pair ipv6**（Probe 命令参考）

1.1.16 display context vlan

display context vlan 命令用来显示 Context 的 VLAN 列表。

【命令】

display context [name context-name] vlan

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name: Context 的名称，为 1~15 个字符的字符串，区分大小写。

【使用指导】

在缺省 Context 中，可使用 **name context-name** 参数查看指定 Context 的 VLAN 列表；不指定 **name context-name** 参数时，则显示设备上创建的所有 Context 的 VLAN 列表。

【举例】

```
# 显示所有 Context 的 VLAN 列表。
<Sysname> display context vlan
Context stub1's VLAN(s):

Context stub2's VLAN(s):
    2,4094
Context stub3's VLAN(s):
    5,6,800-3000,3400
# 显示 Context sub1 的 VLAN 列表。
<Sysname> display context name sub1 vlan
Context stub1's VLAN(s):
    5,6,11-23,3400
```

【相关命令】

- **allocate vlan**

1.1.17 limit-resource cpu

limit-resource cpu 命令用来配置 Context 的 CPU 权重。

undo limit-resource cpu 命令用来恢复缺省情况。

【命令】

```
limit-resource cpu weight weight-value  
undo limit-resource cpu
```

【缺省情况】

各 Context 的 CPU 权重均为 10。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

weight weight-value: 配置指定 Context 的 CPU 权重，取值范围为 1~10。系统根据 Context 的权重为 Context 分配 CPU 时间。

【举例】

```
# 配置 Context 的 CPU 权重为 2。
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] limit-resource cpu weight 2
```

1.1.18 limit-resource disk

limit-resource disk 命令用来配置 Context 可使用的磁盘空间上限（用百分比表示）。

undo limit-resource disk 命令用来恢复缺省情况。

【命令】

```
limit-resource disk slot slot-number cpu cpu-number ratio limit-ratio
undo limit-resource disk slot slot-number cpu cpu-number
```

【缺省情况】

Context 可以使用物理设备上的所有空闲磁盘空间。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

slot slot-number cpu cpu-number: 配置 Context 在指定成员设备上可使用的磁盘空间上限。
slot-number 表示设备在 IRF 中的成员编号，*cpu-number* 表示 CPU 的编号。

ratio limit-ratio: 表示 Context 在设备上最多可使用的磁盘空间大小与该设备整个磁盘空间大小的百分比，取值范围为 1~100。

【使用指导】

为了防止单个 Context 过多的占用磁盘而影响其它 Context，特别是为防止异常情况下对磁盘的占用，可以为指定的 Context 配置磁盘上限，当 Context 占用磁盘空间达到限制值时，后续不能申请新的磁盘空间。

请在 Context 启动后配置磁盘上限。执行 **limit-resource disk** 命令前，请使用 **display context resource** 命令查看 Context 当前实际已经使用的磁盘空间大小。配置值应大于 Context 当前实际已经使用的磁盘空间大小，否则，会导致 Context 申请新的磁盘空间失败，从而无法进行文件夹创建、文件拷贝和保存等操作。

如果设备上有多块磁盘，该命令对所有磁盘生效。

【举例】

```
# 配置 Context cnt2 最多可使用 1 号成员设备上磁盘空间的 30%。
<Sysname> system-view
```

```
[Sysname] context cnt2
[Sysname-context-2-cnt2] limit-resource disk slot 1 cpu 0 ratio 30
```

1.1.19 limit-resource memory

limit-resource memory 命令用来配置 Context 可使用的内存空间上限（用百分比表示）。
undo limit-resource memory 命令用来恢复到缺省情况。

【命令】

```
limit-resource memory slot slot-number cpu cpu-number ratio limit-ratio
undo limit-resource memory slot slot-number cpu cpu-number
```

【缺省情况】

所有 Context 共享物理设备上的所有内存空间，每个 Context 可使用的内存空间上限为空闲内存空间值。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

slot slot-number cpu cpu-number: 配置 Context 在指定成员设备上可使用的内存空间上限。
slot-number 表示设备在 IRF 中的成员编号，*cpu-number* 表示 CPU 的编号。
ratio limit-ratio: 表示 Context 在设备上最多可使用的内存大小与该设备整个内存大小的百分比，取值范围为 1~100。

【使用指导】

为了防止单个 Context 过多的占用内存而影响其它 Context，特别是为防止异常情况下对内存的占用，可以为指定的 Context 配置内存上限，当 Context 占用内存达到限制值时，后续不能申请新的内存。

请在 Context 启动后再配置内存上限，并且配置的上限值不应过小，以免 Context 内业务申请不到内存而引起功能异常。

【举例】

```
# 配置 Context cnt2 最多可使用 1 号成员设备内存的 30%。
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] limit-resource memory slot 1 cpu 0 ratio 30
```

1.1.20 switchto context

switchto context 命令用来登录到指定的 Context。

【命令】

```
switchto context context-name
```

【视图】

系统视图

【缺省用户角色】

network-admin
network-operator

【参数】

context-name: 已启动的 Context 的名称。

【使用指导】

只要用户和物理设备之间路由可达，就能使用该命令，通过物理设备和 Context 的内联接口，登录 Context。

【举例】

```
# 切换到 Context test2。
<Sysname> system-view
[Sysname] switchto context test2
*****
* Copyright (c) 2015-2019 Beijing UNIS Hengyue Technologies Co., Ltd.      *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

<Context2>
```

1.1.21 tar context log

tar context log 命令用来收集各 Context 的日志信息。

【命令】

tar context [*name context-name*] **log file filename**

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

name context-name: 收集指定 Context 的日志信息，*context-name* 是 Context 的名称，为 1～15 个字符的字符串，区分大小写。若不指定该参数，则表示收集所有 Context 的日志信息。

file filename: 表示将收集到的日志信息保存到指定文件。*filename* 表示文件的名称，为 1～255 个字符的字符串（含后缀），不区分大小写，文件名不能为 “.” 或 “..”，不能包含 “”、“/”、“:”、“\”、“?”、“\\”、“<”、“>”、“|”、“*”，首字符不能为 “-”，且后缀必须为 “.tar.gz”，后缀不区分大小写。

【使用指导】

此命令仅支持在缺省 Context 中使用。

执行该命令会收集 logfile 文件夹和 diagfile 文件夹下的所有文件。

在缺省 Context 中，无法对从未启动过的自定义 Context 进行日志信息收集。

【举例】

收集各 Context 的日志信息，并指定保存文件的名称为 test.tar.gz。

```
<Sysname> tar context log file test.tar.gz
```



UNIS 入侵检测系统

安全命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《安全命令参考》主要介绍安全域、安全策略、对象组、AAA、用户身份识别和管理、Password Control、公钥管理、PKI、SSH、SSL、ASPF、APR、会话管理、连接数限制、攻击检测与防范、ARP 攻击防御、ND 攻击防御、uRPF、加密引擎相关和 IP-MAC 绑定等命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用 “[]” 括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由 “#” 号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号 “< >” 表示按钮名，如 “单击<确定>按钮”。

格 式	意 义
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 AAA	1-1
1.1 ISP域中实现AAA配置命令	1-1
1.1.1 aaa session-id mode	1-1
1.1.2 aaa session-limit	1-1
1.1.3 accounting command	1-2
1.1.4 accounting default	1-3
1.1.5 accounting ipoe	1-4
1.1.6 accounting lan-access	1-6
1.1.7 accounting login	1-7
1.1.8 accounting quota-out	1-9
1.1.9 accounting start-fail	1-9
1.1.10 accounting update-fail	1-10
1.1.11 authentication default	1-10
1.1.12 authentication ipoe	1-12
1.1.13 authentication lan-access	1-13
1.1.14 authentication login	1-14
1.1.15 authentication super	1-15
1.1.16 authorization command	1-16
1.1.17 authorization default	1-18
1.1.18 authorization ipoe	1-19
1.1.19 authorization lan-access	1-20
1.1.20 authorization login	1-21
1.1.21 authorization-attribute (ISP domain view)	1-23
1.1.22 display domain	1-24
1.1.23 domain	1-28
1.1.24 domain default enable	1-29
1.1.25 domain if-unknown	1-30
1.1.26 nas-id	1-31
1.1.27 nas-id bind vlan	1-31
1.1.28 session-time include-idle-time	1-32
1.1.29 state (ISP domain view)	1-33
1.1.30 user-address-type	1-34
1.2 本地用户配置命令	1-34

1.2.1 access-limit	1-34
1.2.2 access-user email authentication	1-35
1.2.3 access-user email format	1-36
1.2.4 access-user email sender	1-37
1.2.5 access-user email smtp-server	1-38
1.2.6 authorization-attribute (Local user view/user group view)	1-39
1.2.7 display local-user	1-41
1.2.8 display user-group	1-44
1.2.9 group	1-45
1.2.10 local-user	1-46
1.2.11 password	1-47
1.2.12 service-type (Local user view)	1-48
1.2.13 state (Local user view)	1-49
1.2.14 user-group	1-50
1.3 RADIUS配置命令	1-51
1.3.1 aaa device-id	1-51
1.3.2 accounting-on enable	1-51
1.3.3 attribute 15 check-mode	1-52
1.3.4 attribute 25 car	1-53
1.3.5 attribute 31 mac-format	1-54
1.3.6 attribute convert (RADIUS DAE server view)	1-55
1.3.7 attribute convert (RADIUS scheme view)	1-56
1.3.8 attribute reject (RADIUS DAE server view)	1-57
1.3.9 attribute reject (RADIUS scheme view)	1-58
1.3.10 attribute remanent-volume	1-59
1.3.11 attribute translate	1-60
1.3.12 attribute vendor-id 2011 version	1-61
1.3.13 client	1-62
1.3.14 data-flow-format (RADIUS scheme view)	1-63
1.3.15 display radius scheme	1-64
1.3.16 display radius statistics	1-67
1.3.17 key (RADIUS scheme view)	1-69
1.3.18 nas-ip (RADIUS scheme view)	1-69
1.3.19 port	1-71
1.3.20 primary accounting (RADIUS scheme view)	1-71
1.3.21 primary authentication (RADIUS scheme view)	1-73
1.3.22 radius attribute extended	1-74

1.3.23 radius dscp	1-75
1.3.24 radius dynamic-author server.....	1-76
1.3.25 radius nas-ip	1-77
1.3.26 radius scheme	1-78
1.3.27 radius session-control client	1-79
1.3.28 radius session-control enable	1-80
1.3.29 radius-server test-profile	1-80
1.3.30 reset radius statistics	1-81
1.3.31 retry	1-82
1.3.32 retry realtime-accounting	1-83
1.3.33 secondary accounting (RADIUS scheme view)	1-84
1.3.34 secondary authentication (RADIUS scheme view)	1-85
1.3.35 snmp-agent trap enable radius.....	1-87
1.3.36 state primary	1-88
1.3.37 state secondary	1-89
1.3.38 timer quiet (RADIUS scheme view)	1-90
1.3.39 timer realtime-accounting (RADIUS scheme view).....	1-91
1.3.40 timer response-timeout (RADIUS scheme view).....	1-92
1.3.41 user-name-format (RADIUS scheme view)	1-93
1.3.42 vpn-instance (RADIUS scheme view)	1-94
1.4 HWTACACS配置命令	1-95
1.4.1 data-flow-format (HWTACACS scheme view)	1-95
1.4.2 display hwtacacs scheme	1-96
1.4.3 hwtacacs nas-ip	1-101
1.4.4 hwtacacs scheme	1-102
1.4.5 key (HWTACACS scheme view)	1-103
1.4.6 nas-ip (HWTACACS scheme view).....	1-103
1.4.7 primary accounting (HWTACACS scheme view).....	1-105
1.4.8 primary authentication (HWTACACS scheme view).....	1-106
1.4.9 primary authorization	1-107
1.4.10 reset hwtacacs statistics	1-109
1.4.11 secondary accounting (HWTACACS scheme view)	1-109
1.4.12 secondary authentication (HWTACACS scheme view)	1-111
1.4.13 secondary authorization	1-112
1.4.14 server-block-action (HWTACACS scheme view)	1-114
1.4.15 timer quiet (HWTACACS scheme view)	1-115
1.4.16 timer realtime-accounting (HWTACACS scheme view).....	1-115

1.4.17 timer response-timeout (HWTACACS scheme view)	1-116
1.4.18 user-name-format (HWTACACS scheme view)	1-117
1.4.19 vpn-instance (HWTACACS scheme view)	1-118
1.5 LDAP配置命令	1-119
1.5.1 attribute-map	1-119
1.5.2 authentication-server	1-119
1.5.3 authorization-server	1-120
1.5.4 display ldap scheme	1-121
1.5.5 group-filter	1-123
1.5.6 ip	1-124
1.5.7 ipv6	1-125
1.5.8 ldap attribute-map	1-125
1.5.9 ldap scheme	1-126
1.5.10 ldap server	1-127
1.5.11 login-dn	1-128
1.5.12 login-password	1-128
1.5.13 map	1-129
1.5.14 protocol-version	1-130
1.5.15 search-base-dn	1-131
1.5.16 search-scope	1-132
1.5.17 server-timeout	1-132
1.5.18 user-parameters	1-133

1 AAA

1.1 ISP域中实现AAA配置命令

1.1.1 aaa session-id mode

aaa session-id mode 命令用来配置设备使用的 Acct-Session-Id 属性模式。

undo aaa session-id mode 命令用来恢复缺省情况。

【命令】

```
aaa session-id mode { common | simplified }  
undo aaa session-id mode
```

【缺省情况】

设备使用的 Acct-Session-Id 属性模式为普通模式。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

common: 普通模式。该模式下，Acct-Session-Id 属性的取值长度最小为 38 个字符，由前缀、日期时间、序列号、接入节点的 LIP 地址、设备 ID 以及进程的 Job ID 信息组成。

simplified: 精简模式。该模式下，Acct-Session-Id 属性的取值长度为 16 个字符，由前缀、月份值、序列号、设备 ID 以及接入节点的 LIP 地址信息组成。

【使用指导】

不同厂商的 RADIUS 服务器支持的 Acct-Session-Id 属性的格式可能有所不同，可通过本命令指定设备使用的 Acct-Session-Id 属性格式。

【举例】

```
# 配置设备使用的 Acct-Session-Id 属性模式为精简模式。  
<Sysname> system-view  
[Sysname] aaa session-id mode simplified
```

1.1.2 aaa session-limit

aaa session-limit 命令用来配置同时在线的最大用户连接数，即采用指定登录方式登录设备并同时在线的用户数。

undo aaa session-limit 命令用来将指定登录方式的同时在线的最大用户连接数恢复为缺省情况。

【命令】

```
aaa session-limit { ftp | http | https | ssh | telnet } max-sessions
undo aaa session-limit { ftp | http | https | ssh | telnet }
```

【缺省情况】

同时在线的各类型最大用户连接数均为 32。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ftp: 表示 FTP 用户。

http: 表示 HTTP 用户。

https: 表示 HTTPS 用户。

ssh: 表示 SSH 用户。

telnet: 表示 Telnet 用户。

max-sessions: 允许同时在线的最大用户连接数，SSH/Telnet 用户的取值范围为 1~32，FTP/HTTP/HTTPS 用户的取值范围为 1~64。

【使用指导】

配置本命令后，当指定类型的接入用户的用户数超过当前配置的最大连接数后，新的接入请求将被拒绝。

【举例】

```
# 设置同时在线的最大 FTP 用户连接数为 4。
<Sysname> system-view
[Sysname] aaa session-limit ftp 4
```

1.1.3 accounting command

accounting command 命令用来配置命令行计费方法。

undo accounting command 命令用来恢复缺省情况。

【命令】

```
accounting command hwtacacs-scheme hwtacacs-scheme-name
undo accounting command
```

【缺省情况】

命令行计费采用当前 ISP 域的缺省计费方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

命令行计费过程是指，用户执行过的合法命令会被发送给计费服务器进行记录。若未开启命令行授权功能，则计费服务器对用户执行过的所有合法命令进行记录；若开启了命令行授权功能，则计费服务器仅对授权通过的命令进行记录。

目前，仅支持使用远程 HWTACACS 服务器完成命令行计费功能。

【举例】

在 ISP 域 test 下，配置使用 HWTACACS 计费方案 hwtac 进行命令行计费。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] accounting command hwtacacs-scheme hwtac
```

【相关命令】

- **accounting default**
- **command accounting**（基础配置命令参考/登录设备）
- **hwtacacs scheme**

1.1.4 accounting default

accounting default 命令用来为当前 ISP 域配置缺省的计费方法。

undo accounting default 命令用来恢复缺省情况。

【命令】

```
accounting default { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme radius-scheme-name ] [ local ] [ none ] | local [ radius-scheme radius-scheme-name | hwtacacs-scheme hwtacacs-scheme-name ] * [ none ] | none | radius-scheme radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] [ none ] }  
undo accounting default
```

【缺省情况】

当前 ISP 域的缺省计费方法为 **local**。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中, *hwtacacs-scheme-name* 表示 HWTACACS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

local: 本地计费。

none: 不计费。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中, *radius-scheme-name* 表示 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

当前 ISP 域的缺省计费方法对于该域中未指定具体计费方法的所有接入用户都起作用, 但是如果某类型的用户不支持指定的计费方法, 则该计费方法对于这类用户不能生效。

本地计费只是为了支持本地用户的连接数管理, 没有实际的计费相关的统计功能。

可以指定多个备选的计费方法, 在当前的计费方法无效时按照配置顺序尝试使用备选的方法完成计费。例如, **radius-scheme radius-scheme-name local none** 表示, 先进行 RADIUS 计费, 若 RADIUS 计费无效则进行本地计费, 若本地计费也无效则不进行计费。

当采用本地计费方法为主计费方法, 且配置了备选计费方法时, 仅当 AAA 本地计费处理过程异常或者没有本地用户配置的情况下, 用户本地计费失败后才会尝试使用备选方法进行认证, 其它情况下不会转换计费方法, 直接认为计费失败。

【举例】

在 ISP 域 test 下, 配置缺省计费方法为使用 RADIUS 方案 rd 进行计费, 并且使用 **local** 作为备选计费方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting default radius-scheme rd local
```

【相关命令】

- **hwtacacs scheme**
- **local-user**
- **radius scheme**

1.1.5 accounting ipoe

accounting ipoe 命令用来为 IPoE 用户配置计费方法。

undo accounting ipoe 命令用来恢复缺省情况。

【命令】

```
accounting ipoe { broadcast radius-scheme radius-scheme-name1
radius-scheme radius-scheme-name2 [ local ] [ none ] | local [ radius-scheme
radius-scheme-name ] [ none ] | none | radius-scheme radius-scheme-name
[ local ] [ none ] }
undo accounting ipoe
```

【缺省情况】

IPoE 用户采用当前 ISP 域的缺省计费方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

broadcast: 指定广播 RADIUS 方案，即同时向指定的两个 RADIUS 方案中的计费服务器发送计费请求。

radius-scheme *radius-scheme-name1*: 表示主送计费 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写；

radius-scheme *radius-scheme-name2*: 表示抄送计费 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地计费。

none: 不计费。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

可以指定多个备选的计费方法。在当前的计费方法无效时按照配置顺序尝试使用备选的方法完成计费。例如，**radius-scheme** *radius-scheme-name* **local** **none** 表示，先进行 RADIUS 计费，若 RADIUS 计费无效则进行本地计费，若本地计费也无效则不进行计费。

当指定 **broadcast** 关键字时，将以主送 RADIUS 方案中的实时计费间隔同时向指定的两个 RADIUS 方案里的主计费服务器发送计费请求，若某 RADIUS 方案里的主计费服务器不可达，则按照配置顺序依次尝试向该 RADIUS 方案里的从计费服务器发送计费请求。主送计费方案计费成功时，表示用户计费成功；抄送计费方案的计费结果对用户无影响。

当采用本地计费方法为主计费方法，且配置了备选计费方法时，仅当 AAA 本地计费处理过程异常或者没有本地用户配置的情况下，用户本地计费失败后才会尝试使用备选方法进行认证，其它情况下不会转换计费方法，直接认为计费失败。

【举例】

在 ISP 域 test 下，为 IPoE 用户配置计费方法为 **local**。

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] accounting ipoe local
```

在 ISP 域 test 下，配置 IPoE 用户使用 RADIUS 方案 rd 进行计费，并且使用 **local** 作为备选计费方法。

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] accounting ipoe radius-scheme rd local
```

在 ISP 域 test 下, 配置 IPoE 用户使用 RADIUS 方案 rd1 和 rd2 进行广播计费, 并且使用 **local** 作为备选计费方法。

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] accounting ipoe broadcast radius-scheme rd1 radius-scheme rd2 local
```

【相关命令】

- **accounting default**
- **local-user**
- **radius scheme**
- **timer realtime-accounting**

1.1.6 accounting lan-access

accounting lan-access 命令用来为 lan-access 用户配置计费方法。

undo accounting lan-access 命令用来恢复缺省情况。

【命令】

```
accounting lan-access { broadcast radius-scheme radius-scheme-name1  
radius-scheme radius-scheme-name2 [ local ] [ none ] | local  
[ radius-scheme radius-scheme-name ] [ none ] | none | radius-scheme  
radius-scheme-name [ local ] [ none ] }  
undo accounting lan-access
```

【缺省情况】

lan-access 用户采用当前 ISP 域的缺省计费方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

broadcast: 指定广播 RADIUS 方案, 即同时向指定的两个 RADIUS 方案中的计费服务器发送计费请求。

radius-scheme radius-scheme-name1: 表示主送计费 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写;

radius-scheme radius-scheme-name2: 表示抄送计费 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

local: 本地计费。

none: 不计费。

radius-scheme radius-scheme-name: 指定 RADIUS 方案。其中, *radius-scheme-name* 表示 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

可以指定多个备选的计费方法。在当前的计费方法无效时按照配置顺序尝试使用备选的方法完成计费。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 计费，若 RADIUS 计费无效则进行本地计费，若本地计费也无效则不进行计费。

当指定 **broadcast** 关键字时，将以主送 RADIUS 方案中的实时计费间隔同时向指定的两个 RADIUS 方案里的主计费服务器发送计费请求，若某 RADIUS 方案里的主计费服务器不可达，则按照配置顺序依次尝试向该 RADIUS 方案里的从计费服务器发送计费请求。主送计费方案计费成功时，表示用户计费成功；抄送计费方案的计费结果对用户无影响。

当采用本地计费方法为主计费方法，且配置了备选计费方法时，仅当 AAA 本地计费处理过程异常或者没有本地用户配置的情况下，用户本地计费失败后才会尝试使用备选方法进行认证，其它情况下不会转换计费方法，直接认为计费失败。

【举例】

在 ISP 域 test 下，为 lan-access 用户配置计费方法为 **local**。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access local
```

在 ISP 域 test 下，配置 lan-access 用户使用 RADIUS 方案 rd 进行计费，并且使用 **local** 作为备选计费方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access radius-scheme rd local
```

在 ISP 域 test 下，配置 lan-access 用户使用 RADIUS 方案 rd1 和 rd2 进行广播计费，并且使用 **local** 作为备选计费方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access broadcast radius-scheme rd1 radius-scheme rd2
local
```

【相关命令】

- **accounting default**
- **local-user**
- **radius scheme**
- **timer realtime-accounting**

1.1.7 accounting login

accounting login 命令用来为 login 用户配置计费方法。

undo accounting login 命令用来恢复缺省情况。

【命令】

```
accounting login { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme  
radius-scheme-name ] [ local ] [ none ] | local [ radius-scheme  
radius-scheme-name | hwtacacs-scheme hwtacacs-scheme-name ] * [ none ] |
```

```
none | radius-scheme radius-scheme-name [ hwtacacs-scheme  
hwtacacs-scheme-name ] [ local ] [ none ] }  
undo accounting login
```

【缺省情况】

login 用户采用当前 ISP 域的缺省计费方法。

【视图】

ISP 域视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

local：本地计费。

none：不计费。

radius-scheme *radius-scheme-name*：指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

不支持对 FTP、SFTP 以及 SCP 类型的 login 用户进行计费。

可以指定多个备选的计费方法。在当前的计费方法无效时按照配置顺序尝试使用备选的方法完成计费。例如，**radius-scheme** *radius-scheme-name* **local** **none** 表示，先进行 RADIUS 计费，若 RADIUS 计费无效则进行本地计费，若本地计费也无效则不进行计费。

当采用本地计费方法为主计费方法，且配置了备选计费方法时，仅当 AAA 本地计费处理过程异常或者没有本地用户配置的情况下，用户本地计费失败后才会尝试使用备选方法进行认证，其它情况下不会转换计费方法，直接认为计费失败。

【举例】

在 ISP 域 test 下，为 login 用户配置计费方法为 **local**。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] accounting login local
```

在 ISP 域 test 下，配置 login 用户使用 RADIUS 方案 rd 进行计费，并且使用 **local** 作为备选计费方法。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] accounting login radius-scheme rd local
```

【相关命令】

- **accounting default**
- **hwtacacs scheme**

- **local-user**
- **radius scheme**

1.1.8 accounting quota-out

accounting quota-out 命令用来配置用户计费配额（流量或时长）耗尽策略。

undo accounting quota-out 命令用来恢复缺省情况。

【命令】

```
accounting quota-out { offline | online }
undo accounting quota-out
```

【缺省情况】

用户的计费配额耗尽后将被强制下线。

【视图】

ISP 域视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

offline: 当用户的整体配额耗尽后，强制用户下线。

online: 当用户的整体配额耗尽后，允许用户保持在线状态。

【举例】

在 ISP 域 test 下，配置用户计费配额耗尽策略为：当配额耗尽后用户仍能保持在线状态。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting quota-out online
```

1.1.9 accounting start-fail

accounting start-fail 命令用来配置用户计费开始失败策略，即设备向计费服务器发送计费开始请求失败后，是否允许用户接入网络。

undo accounting start-fail 命令用来恢复缺省情况。

【命令】

```
accounting start-fail { offline | online }
undo accounting start-fail
```

【缺省情况】

如果用户计费开始失败，允许用户保持在线状态。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

offline: 强制用户下线。

online: 允许用户保持在线状态。

【举例】

在 ISP 域 test 下，配置计费开始失败策略为：用户计费开始失败时允许用户保持在线状态。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] accounting start-fail online
```

1.1.10 accounting update-fail

accounting update-fail 命令用来配置用户计费更新失败策略，即设备向计费服务器发送用户的计费更新报文失败时，是否允许用户接入网络。

undo accounting update-fail 命令用来恢复缺省情况。

【命令】

```
accounting update-fail { [ max-times max-times ] offline | online }  
undo accounting update-fail
```

【缺省情况】

如果用户计费更新失败，允许用户保持在线状态。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

max-times max-times: 允许用户连续计费更新失败的次数，取值范围 1~255，缺省值为 1。

offline: 如果用户连续计费更新失败的次数达到了指定的次数，则强制用户下线。

online: 如果用户计费更新失败，允许用户保持在线状态。

【举例】

在 ISP 域 test 下，配置计费更新失败策略为：用户计费更新失败时允许用户保持在线状态。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] accounting update-fail online
```

1.1.11 authentication default

authentication default 命令用来为当前 ISP 域配置缺省的认证方法。

undo authentication default 命令用来为恢复缺省情况。

【命令】

```
authentication default { hwtacacs-scheme hwtacacs-scheme-name
[ radius-scheme radius-scheme-name ] [ local ] [ none ] | ldap-scheme
ldap-scheme-name [ local ] [ none ] | local [ radius-scheme
radius-scheme-name | hwtacacs-scheme hwtacacs-scheme-name ] * [ none ] |
local [ ldap-scheme ldap-scheme-name ] [ none ] | none | radius-scheme
radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ] [ local ]
[ none ] }
undo authentication default
```

【缺省情况】

当前 ISP 域的缺省认证方法为 **local**。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

hwtacacs-scheme hwtacacs-scheme-name：指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

ldap-scheme ldap-scheme-name：指定 LDAP 方案。其中 *ldap-scheme-name* 表示 LDAP 方案名，为 1~32 个字符的字符串，不区分大小写。

local：本地认证。

none：不进行认证。

radius-scheme radius-scheme-name：指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

当前 ISP 域的缺省的认证方法对于该域中未指定具体认证方法的所有接入用户都起作用，但是如果某类型的用户不支持指定的认证方法，则该认证方法对于这类用户不能生效。

可以指定多个备选的认证方法，在当前的认证方法无效时按照配置顺序尝试使用备选的方法完成认证。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 认证，若 RADIUS 认证无效则进行本地认证，若本地认证也无效则不进行认证。

当采用本地认证方案为主认证方法，且配置了备选认证方法时，仅当 AAA 本地认证处理过程异常或者没有本地用户配置的情况下，用户本地认证失败后才会尝试使用备选方法进行认证，其它情况下不会转换认证方法，直接认为认证失败。

【举例】

在 ISP 域 test 下，配置缺省认证方法为使用 RADIUS 方案 rd 进行认证，并且使用 **local** 作为备选认证方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication default radius-scheme rd local
```

【相关命令】

- **hwtaacacs scheme**
- **ldap scheme**
- **local-user**
- **radius scheme**

1.1.12 authentication ipoe

authentication ipoe 命令用来为 IPoE 用户配置认证方法。

undo authentication ipoe 命令用来恢复缺省情况。

【命令】

```
authentication ipoe { local [ radius-scheme radius-scheme-name ] [ none ]  
| none | radius-scheme radius-scheme-name [ local ] [ none ] }  
undo authentication ipoe
```

【缺省情况】

IPoE 用户采用当前 ISP 域的缺省认证方法。

【视图】

ISP 域视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

local: 本地认证。

none: 不认证。

radius-scheme radius-scheme-name: 指定 RADIUS 方案。其中, *radius-scheme-name* 表示 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

可以指定多个备选的认证方法, 在当前的认证方法无效时按照配置顺序尝试使用备选的方法完成认证。例如, **radius-scheme radius-scheme-name local none** 表示, 先进行 RADIUS 认证, 若 RADIUS 认证无效则进行本地认证, 若本地认证也无效则不进行认证。

当采用本地认证方案为主认证方法, 且配置了备选认证方法时, 仅当 AAA 本地认证处理过程异常或者没有本地用户配置的情况下, 用户本地认证失败后才会尝试使用备选方法进行认证, 其它情况下不会转换认证方法, 直接认为认证失败。

【举例】

在 ISP 域 test 下, 为 IPoE 用户配置认证方法为 **local**。

```
<Sysname> system-view
```

```
[Sysname] domain test
[Sysname-isp-test] authentication ipoe local
# 在 ISP 域 test 下，配置 IPoE 用户使用 RADIUS 方案 rd 进行认证，并且使用 local 作为备选
认证方法。
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication ipoe radius-scheme rd local
```

【相关命令】

- **authentication default**
- **local-user**
- **radius scheme**

1.1.13 authentication lan-access

authentication lan-access 命令用来为 lan-access 用户配置认证方法。

undo authentication lan-access 命令用来恢复缺省情况。

【命令】

```
authentication lan-access { ldap-scheme ldap-scheme-name [ local ] [ none ]  
| local [ ldap-scheme ldap-scheme-name | radius-scheme radius-scheme-name ]  
[ none ] | none | radius-scheme radius-scheme-name [ local ] [ none ] }  
undo authentication lan-access
```

【缺省情况】

lan-access 用户采用当前 ISP 域的缺省认证方法。

【视图】

ISP 域视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ldap-scheme *ldap-scheme-name*: 指定 LDAP 方案。其中 *ldap-scheme-name* 表示 LDAP 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地认证。

none: 不进行认证。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

可以指定多个备选的认证方法，在当前的认证方法无效时按照配置顺序尝试使用备选的方法完成认证。例如，**radius-scheme *radius-scheme-name* local none** 表示，先进行 RADIUS 认证，若 RADIUS 认证无效则进行本地认证，若本地认证也无效则不进行认证。

当采用本地认证方案为主认证方法，且配置了备选认证方法时，仅当 AAA 本地认证处理过程异常或者没有本地用户配置的情况下，用户本地认证失败后才会尝试使用备选方法进行认证，其它情况下不会转换认证方法，直接认为认证失败。

【举例】

在 ISP 域 test 下，为 lan-access 用户配置认证方法为 **local**。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication lan-access local
```

在 ISP 域 test 下，配置 lan-access 用户使用 RADIUS 方案 rd 进行认证，并且使用 **local** 作为备选认证方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication lan-access radius-scheme rd local
```

【相关命令】

- **authentication default**
- **hwtacacs scheme**
- **ldap scheme**
- **local-user**
- **radius scheme**

1.1.14 authentication login

authentication login 命令用来为 login 用户配置认证方法。

undo authentication login 命令用来恢复缺省情况。

【命令】

```
authentication login { hwtacacs-scheme hwtacacs-scheme-name  
[ radius-scheme radius-scheme-name ] [ local ] [ none ] | ldap-scheme  
ldap-scheme-name [ local ] [ none ] | local [ radius-scheme  
radius-scheme-name | hwtacacs-scheme hwtacacs-scheme-name ] * [ none ] |  
| local [ ldap-scheme ldap-scheme-name ] [ none ] | none | radius-scheme  
radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ] [ local ]  
[ none ] }  
undo authentication login
```

【缺省情况】

login 用户采用当前 ISP 域的缺省认证方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中, *hwtacacs-scheme-name* 表示 HWTACACS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

ldap-scheme *ldap-scheme-name*: 指定 LDAP 方案。其中 *ldap-scheme-name* 表示 LDAP 方案名, 为 1~32 个字符的字符串, 不区分大小写。

local: 本地认证。

none: 不进行认证。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中, *radius-scheme-name* 表示 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

可以指定多个备选的认证方法, 在当前的认证方法无效时按照配置顺序尝试使用备选的方法完成认证。例如, **radius-scheme radius-scheme-name local none** 表示, 先进行 RADIUS 认证, 若 RADIUS 认证无效则进行本地认证, 若本地认证也无效则不进行认证。

当采用本地认证方案为主认证方法, 且配置了备选认证方法时, 仅当 AAA 本地认证处理过程异常或者没有本地用户配置的情况下, 用户本地认证失败后才会尝试使用备选方法进行认证, 其它情况下不会转换认证方法, 直接认为认证失败。

【举例】

在 ISP 域 test 下, 为 login 用户配置认证方法为 **local**。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login local
```

在 ISP 域 test 下, 配置 login 用户使用 RADIUS 方案 rd 进行认证, 并且使用 **local** 作为备选认证方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login radius-scheme rd local
```

【相关命令】

- **authentication default**
- **hwtacacs scheme**
- **ldap scheme**
- **local-user**
- **radius scheme**

1.1.15 authentication super

authentication super 命令用来配置用户角色切换认证方法。

undo authentication super 命令用来恢复缺省情况。

【命令】

```
authentication super { hwtacacs-scheme hwtacacs-scheme-name |
radius-scheme radius-scheme-name } *
```

undo authentication super

【缺省情况】

用户角色切换认证采用当前 ISP 域的缺省认证方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

切换用户角色是指在不退出当前登录、不断开当前连接的前提下修改用户的用户角色，改变用户所拥有的命令行权限。为了保证切换操作的安全性，需要在用户执行用户角色切换时进行身份认证。设备支持本地和远程两种认证方式，关于用户角色切换的详细介绍请参见“基础配置指导”中的“RBAC”。

可以指定一个备选的认证方法，在当前的认证方法无效时尝试使用备选的方法完成认证。

【举例】

在 ISP 域 test 下，配置使用 HWTACACS 方案 tac 进行用户角色切换认证。

```
<Sysname> system-view
[Sysname] super authentication-mode scheme
[Sysname] domain test
[Sysname-isp-test] authentication super hwtacacs-scheme tac
```

【相关命令】

- **authentication default**
- **hwtacacs scheme**
- **radius scheme**

1.1.16 authorization command

authorization command 命令用来配置命令行授权方法。

undo authorization command 命令用来恢复缺省情况。

【命令】

```
authorization command { hwtacacs-scheme hwtacacs-scheme-name [ local ]  
[ none ] | local [ none ] | none }  
undo authorization command
```

【缺省情况】

命令行授权采用当前 ISP 域的缺省授权方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地授权。

none: 不授权。用户执行角色所允许的命令时，无须接受授权服务器的检查。

【使用指导】

命令行授权是指，用户执行的每一条命令都需要接受授权服务器的检查，只有授权成功的命令才被允许执行。用户登录后可以执行的命令受登录授权的用户角色和命令行授权的用户角色的双重限制，即，仅登录授权的用户角色和命令行授权的用户角色均允许执行的命令行，才能被执行。需要注意的是，命令行授权功能只利用角色中的权限规则对命令行执行权限检查，不进行其它方面的权限检查，例如资源控制策略等。

对用户采用本地命令行授权时，设备将根据用户登录设备时输入的用户名对应的本地用户配置来对用户输入的命令进行检查，只有本地用户中配置的授权用户角色所允许的命令才被允许执行。

可以指定多个备选的命令行授权方法，在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成命令授权。例如，**hwtacacs-scheme hwtacacs-scheme-name local none** 表示，先进行 HWTACACS 授权，若 HWTACACS 授权无效则进行本地授权，若本地授权也无效则不进行授权。

【举例】

在 ISP 域 test 下，配置命令行授权方法为 **local**。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] authorization command local
```

在 ISP 域 test 下，配置使用 HWTACACS 方案 hwtac 进行命令行授权，并且使用 **local** 作为备选授权方法。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] authorization command hwtacacs-scheme hwtac local
```

【相关命令】

- **command authorization**（基础配置命令参考/登录设备）
- **hwtacacs scheme**
- **local-user**

1.1.17 authorization default

authorization default 命令用来为当前 ISP 域配置缺省的授权方法。

undo authorization default 命令用来恢复缺省情况。

【命令】

```
authorization default { hwtacacs-scheme hwtacacs-scheme-name
[ radius-scheme radius-scheme-name ] [ local ] [ none ] | local
[ radius-scheme radius-scheme-name | hwtacacs-scheme
hwtacacs-scheme-name ] * [ none ] | none | radius-scheme radius-scheme-name
[ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] [ none ] }
undo authorization default
```

【缺省情况】

当前 ISP 域的缺省授权方法为 **local**。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

hwtacacs-scheme hwtacacs-scheme-name：指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

local：本地授权。

none：不授权。接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 Login 用户（通过 Console 口或者 Telnet、FTP/SFTP/SCP 访问设备的用户）只有系统给予的缺省用户角色 level-0，其中 FTP/SFTP/SCP 用户的工作目录是设备的根目录，但并无访问权限；认证通过的非 Login 用户可直接访问网络。关于用户角色 level-0 的详细介绍请参见“基础配置指导”中的“RBAC”。

radius-scheme radius-scheme-name：指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

当前 ISP 域的缺省的授权方法对于该域中未指定具体授权方法的所有接入用户都起作用，但是如果某类型的用户不支持指定的授权方法，则该授权方法对于这类用户不能生效。

在一个 ISP 域中，只有配置的认证和授权方法中引用了相同的 RADIUS 方案时，RADIUS 授权过程才能生效。

可以指定多个备选的授权方法，在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成授权。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 授权，若 RADIUS 授权无效则进行本地授权，若本地授权也无效则不进行授权。

当采用本地授权方案为主授权方法，且配置了备选授权方法时，仅当 AAA 本地授权处理过程异常或者没有本地用户配置的情况下，用户本地授权失败后才会尝试使用备选方法进行授权，其它情况下不会转换授权方法，直接认为授权失败。

【举例】

在 ISP 域 test 下，配置缺省授权方法为使用 RADIUS 方案 rd 进行授权，并且使用 **local** 作为备选授权方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization default radius-scheme rd local
```

【相关命令】

- **hwtacacs scheme**
- **local-user**
- **radius scheme**

1.1.18 authorization ipoe

authorization ipoe 命令用来为 IPoE 用户配置授权方法。

undo authorization ipoe 命令用来恢复缺省情况。

【命令】

```
authorization ipoe { local [ radius-scheme radius-scheme-name ] [ none ]  
| none | radius-scheme radius-scheme-name [ local ] [ none ] }  
undo authorization ipoe
```

【缺省情况】

IPoE 用户采用当前 ISP 域的缺省授权方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

local：本地授权。

none：不授权。

radius-scheme radius-scheme-name：指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

在一个 ISP 域中，只有配置的认证和授权方法中引用了相同的 RADIUS 方案时，RADIUS 授权过程才能生效。

可以指定多个备选的授权方法，在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成授权。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 授权，若 RADIUS 授权无效则进行本地授权，若本地授权也无效则不进行授权。

当采用本地授权方案为主授权方法，且配置了备选授权方法时，仅当 AAA 本地授权处理过程异常或者没有本地用户配置的情况下，用户本地授权失败后才会尝试使用备选方法进行授权，其它情况下不会转换授权方法，直接认为授权失败。

【举例】

在 ISP 域 test 下，为 IPoE 用户配置授权方法为 **local**。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ipoe local
```

在 ISP 域 test 下，配置 IPoE 用户使用 RADIUS 方案 rd 进行授权，并且使用 **local** 作为备选授权方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization ipoe radius-scheme rd local
```

【相关命令】

- **authorization default**
- **local-user**
- **radius scheme**

1.1.19 authorization lan-access

authorization lan-access 命令用来为 lan-access 用户配置授权方法。

undo authorization lan-access 命令用来恢复缺省情况。

【命令】

```
authorization lan-access { local [ radius-scheme radius-scheme-name ]
[ none ] | none | radius-scheme radius-scheme-name [ local ] [ none ] }
undo authorization lan-access
```

【缺省情况】

lan-access 用户采用当前 ISP 域的缺省授权方法。

【视图】

ISP 域视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

local：本地授权。

none：不授权。接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权，认证通过的 lan-access 用户可直接访问网络。

radius-scheme radius-scheme-name: 指定 RADIUS 方案。其中, *radius-scheme-name* 表示 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

在一个 ISP 域中, 只有配置的认证和授权方法中引用了相同的 RADIUS 方案时, RADIUS 授权过程才能生效。

可以指定多个备选的授权方法, 在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成授权。例如, **radius-scheme radius-scheme-name local none** 表示, 先进行 RADIUS 授权, 若 RADIUS 授权无效则进行本地授权, 若本地授权也无效则不进行授权。

当采用本地授权方案为主授权方法, 且配置了备选授权方法时, 仅当 AAA 本地授权处理过程异常或者没有本地用户配置的情况下, 用户本地授权失败后才会尝试使用备选方法进行授权, 其它情况下不会转换授权方法, 直接认为授权失败。

【举例】

在 ISP 域 test 下, 为 lan-access 用户配置授权方法为 **local**。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization lan-access local
```

在 ISP 域 test 下, 配置 lan-access 用户使用 RADIUS 方案 rd 进行授权, 并且使用 **local** 作为备选授权方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization lan-access radius-scheme rd local
```

【相关命令】

- **authorization default**
- **local-user**
- **radius scheme**

1.1.20 authorization login

authorization login 命令用来为 login 用户配置授权方法。

undo authorization login 命令用来恢复缺省情况。

【命令】

```
authorization login { hwtacacs-scheme hwtacacs-scheme-name  
[ radius-scheme radius-scheme-name ] [ local ] [ none ] | local  
[ radius-scheme radius-scheme-name | hwtacacs-scheme  
hwtacacs-scheme-name ] * [ none ] | none | radius-scheme radius-scheme-name  
[ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] [ none ] }  
undo authorization login
```

【缺省情况】

login 用户采用当前 ISP 域的缺省授权方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地授权。

none: 不授权。接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 Login 用户（通过 Console 口或者 Telnet、FTP/SFTP/SCP 访问设备的用户）只有系统给予的缺省用户角色 **level-0**，其中 FTP/SFTP/SCP 用户的工作目录是设备的根目录，但并无访问权限。关于用户角色 **level-0** 的详细介绍请参见“基础配置指导”中的“RBAC”。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

在一个 ISP 域中，只有配置的认证和授权方法中引用了相同的 RADIUS 方案时，RADIUS 授权过程才能生效。

可以指定多个备选的授权方法，在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成授权。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 授权，若 RADIUS 授权无效则进行本地授权，若本地授权也无效则不进行授权。

当采用本地授权方案为主授权方法，且配置了备选授权方法时，仅当 AAA 本地授权处理过程异常或者没有本地用户配置的情况下，用户本地授权失败后才会尝试使用备选方法进行授权，其它情况下不会转换授权方法，直接认为授权失败。

【举例】

在 ISP 域 test 下，为 login 用户配置授权方法为 **local**。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login local
```

在 ISP 域 test 下，配置 login 用户使用 RADIUS 方案 rd 进行授权，并且使用 **local** 作为备选授权方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login radius-scheme rd local
```

【相关命令】

- **authorization default**
- **hwtacacs scheme**
- **local-user**
- **radius scheme**

1.1.21 authorization-attribute (ISP domain view)

authorization-attribute 命令用来设置当前 ISP 域下的用户授权属性。

undo authorization-attribute 命令用来删除指定的授权属性，恢复用户具有的缺省访问权限。

【命令】

authorization-attribute user-group *user-group-name*

undo authorization-attribute user-group

【缺省情况】

当前 ISP 域下的用户闲置切换功能处于关闭状态，IPv4 用户可以同时点播的最大节目数为 4，IPv6 用户可以同时点播的最大节目数为 4，无其它授权属性。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-group *user-group-name*: 表示用户所属用户组。其中，*user-group-name* 表示用户组名，为 1~32 个字符的字符串，不区分大小写。用户认证成功后，将继承该用户组中的所有属性。

【使用指导】

用户上线后，设备会周期性检测用户的流量，若域内某用户在指定的闲置检测时间内产生的流量小于本命令中指定的数据流量，则会被强制下线。需要注意的是，服务器上也可以配置最大空闲时间实现对用户的闲置切断功能，具体为当用户在指定的闲置检测时间内产生的流量小于 10240 个字节（服务器上该阈值为固定值，不可配置）时，会被强制下线。但是，只有在设备上的闲置切断功能处于关闭状态时，服务器才会根据自身的配置来控制用户的闲置切断。

如果当前 ISP 域的用户认证成功，但认证服务器（包括本地认证下的接入设备）未对该 ISP 域下发授权属性，则系统使用当前 ISP 下指定的授权属性为用户授权。

需要注意的是，可通过多次执行本命令配置多个授权属性，但对于相同授权属性，最后一次执行的命令生效。

【举例】

设置 ISP 域 test 的用户授权组为 abc。

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] authorization-attribute user-group abc
```

【相关命令】

- **display domain**

1.1.22 display domain

display domain 命令用来显示所有或指定 ISP 域的配置信息。

【命令】

display domain [*isp-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

isp-name: ISP 域名，为 1~255 个字符的字符串，不区分大小写。如果不指定该参数，则表示所有 ISP 域。

【举例】

显示系统中所有 ISP 域的配置信息。

```
<Sysname> display domain
```

```
Total 2 domains
```

```
Domain: system
```

```
State: Active
```

```
Default authentication scheme: Local
```

```
Default authorization scheme: Local
```

```
Default accounting scheme: Local
```

```
Accounting start failure action: Online
```

```
Accounting update failure action: Online
```

```
Accounting quota out action: Offline
```

```
Service type: HSI
```

```
Session time: Exclude idle time
```

```
NAS-ID: N/A
```

```
Authorization attributes:
```

```
Idle cut: Disabled
```

```
Session timeout: Disabled
```

```
MLD access number: 4
```

```
Domain: dm
```

```
State: Active
```

```
Login authentication scheme: RADIUS=rad
```

```
Login authorization scheme: HWTACACS=hw
```

```
Super authentication scheme: RADIUS=rad
```

```
Command authorization scheme: HWTACACS=hw
```

```
LAN access authentication scheme: RADIUS=r4
```

Default authentication scheme: RADIUS=rad, Local, None
 Default authorization scheme: Local
 Default accounting scheme: None
 Accounting start failure action: Online
 Accounting update failure action: Online
 Accounting quota out action: Offline
 Service type: HSI
 Session time: Include idle time
 User address type: ipv4
 NAS-ID: test
 User basic service IP type: IPv4
 Authorization attributes:
 Idle cut : Enabled
 Idle timeout: 2 minutes
 Flow: 10240 bytes
 Session timeout: 34 minutes
 IP pool: appy
 Session group profile: abc
 Inbound CAR: CIR 64000 bps PIR 640000 bps
 Outbound CAR: CIR 64000 bps PIR 640000 bps
 ACL number: 3000
 User group: ugg
 IPv6 prefix: 1::1/34
 IPv6 pool: ipv6pool
 Primary DNS server: 6.6.6.6
 Secondary DNS server: 3.6.2.3
 URL: http://test
 VPN instance: vpn1
 MLD access number: 4

Default domain name: system

表1-1 display domain 命令显示信息描述表

字段	描述
Total 2 domains	总计2个ISP域
Domain	ISP域名
State	ISP域的状态
Default authentication scheme	缺省的认证方案
Default authorization scheme	缺省的授权方案
Default accounting scheme	缺省的计费方案
ADVPN authentication scheme	ADVPN用户认证方案
ADVPN authorization scheme	ADVPN用户授权方案
ADVPN accounting scheme	ADVPN用户计费方案
Login authentication scheme	Login用户认证方案

字段	描述
Login authorization scheme	Login用户授权方案
Login accounting scheme	Login用户计费方案
Super authentication scheme	用户角色切换认证方案
PPP authentication scheme	PPP用户的认证方案
PPP authorization scheme	PPP用户的授权方案
PPP accounting scheme	PPP用户的计费方案
Command authorization scheme	命令行授权方案
Command accounting scheme	命令行计费方案
LAN access authentication scheme	lan-access用户认证方案
LAN access authorization scheme	lan-access用户授权方案
LAN access accounting scheme	lan-access用户计费方案
IKE authentication scheme	IKE扩展认证方案
IKE authorization scheme	IKE扩展认证的授权方案
IPoE authentication scheme	IPoE用户认证方案
IPoE authorization scheme	IPoE用户授权方案
IPoE accounting scheme	IPoE用户计费方案
SSL VPN authentication scheme	SSL VPN用户认证方案
SSL VPN authorization scheme	SSL VPN用户授权方案
SSL VPN accounting scheme	SSL VPN用户计费方案
RADIUS	RADIUS方案
HWTACACS	HWTACACS方案
LDAP	LDAP方案
Local	本地方案
None	不认证、不授权和不计费
Accounting start failure action	用户计费开始失败的动作，包括以下取值： • Online: 如果用户计费开始失败，则保持用户在线 • Offline: 如果用户计费开始失败，则强制用户下线
Accounting update failure max-times	允许用户连续计费更新失败的次数
Accounting update failure action	用户计费更新失败的动作，包括以下取值： • Online: 如果用户计费更新失败，则保持用户在线 • Offline: 如果用户计费更新失败，则强制用户下线

字段	描述
Accounting quota out action	用户计费配额耗尽策略，包括以下取值： - Online: 如果用户计费配额耗尽，则保持用户在线 - Offline: 如果用户计费配额耗尽，则强制用户下线
Service type	ISP域的业务类型，取值为HSI, STB和VoIP
Session time	当用户异常下线时，设备上传到服务器的用户在线时间情况： - Include idle time: 保留用户闲置切断时间 - Exclude idle time: 扣除用户闲置切断时间
User address type	用户地址类型
NAS-ID	设备的NAS-ID 若未配置，则显示为N/A
User basic service IP type	PPPoE/L2TP用户主业务依赖的IP地址类型，包括以下取值： - IPv4: IPv4 地址类型 - IPv6: IPv6 地址类型 - IPv6-PD: IPv6 PD (Prefix Delegation, 前缀授权) 类型
DHCPv6-follow-IPv6CP timeout	PPPoE/L2TP用户等待分配IPv6/PD地址的最大时长，单位为秒
Authorization attributes	ISP的用户授权属性
Idle cut	用户闲置切断功能，包括以下取值： - Enabled: 处于开启状态，表示当ISP域中的用户在指定的最大闲置切断时间内产生的流量小于指定的最小数据流量时，会被强制下线 - Disabled: 处于关闭状态，表示不对用户进行闲置切断控制，它为缺省状态
Idle timeout	用户闲置切断时间（单位为分钟）
Flow	用户数据流量阈值（单位为字节）
Session timeout	用户的会话超时时间（单位为分钟）
IP pool	授权IPv4地址池的名称
User profile	授权User Profile的名称
Session group profile	授权Session Group Profile的名称
Inbound CAR	授权的入方向CAR（CIR: 承诺信息速率，单位为bps; PIR: 峰值信息速率，单位为bps）
Outbound CAR	授权的出方向CAR（CIR: 承诺信息速率，单位为bps; PIR: 峰值信息速率，单位为bps）
ACL number	授权ACL编号
User group	授权User group的名称

字段	描述
IPv6 prefix	授权IPv6前缀
IPv6 pool	授权IPv6地址池的名称
Primary DNS server	授权主DNS服务器IPv4地址
Secondary DNS server	授权从DNS服务器IPv4地址
Primary DNSV6 server	授权主DNS服务器IPv6地址
Secondary DNSV6 server	授权从DNS服务器IPv6地址
URL	授权重定向URL
VPN instance	授权VPN实例名称
IGMP access limit	授权IPv4用户可以同时点播的最大节目数
MLD access limit	授权IPv6用户可以同时点播的最大节目数
Default domain name	缺省ISP域名

1.1.23 domain

domain 命令用来创建 ISP 域，并进入 ISP 域视图。如果指定的 ISP 域已经存在，则直接进入 ISP 域视图。

undo domain 命令用来删除指定的 ISP 域。

【命令】

domain *isp-name*

undo domain *isp-name*

【缺省情况】

存在一个 ISP 域，名称为 **system**。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

isp-name: ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“”、“.”、“*”、“?”、“<”、“>” 以及 “@” 字符，且不能为字符串 “d”、“de”、“def”、“defa”、“defau”、“default”、“i”、“if”、“if-”、“if-u”、“if-un”、“if-unk”、“if-unkn”、“if-unkno”、“if-unknow” 和 “if-unknown”。

【使用指导】

所有的 ISP 域在创建后即处于 **active** 状态。

不能删除系统中预定义的 ISP 域 **system**，只能修改该域的配置。

不能删除作为系统缺省 ISP 域的 ISP 域。如需删除一个系统缺省 ISP 域，请先使用 **undo domain default enable** 命令将其恢复为非缺省的 ISP 域。

建议设备上配置的 ISP 域名尽量短，避免用户输入的包含域名的用户名长度超过客户端可支持的最大用户名长度。

【举例】

创建一个名称为 test 的 ISP 域，并进入其视图。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test]
```

【相关命令】

- **display domain**
- **domain default enable**
- **domain if-unknown**
- **state** (ISP domain view)

1.1.24 domain default enable

domain default enable 命令用来配置系统缺省的 ISP 域，所有在登录时没有提供 ISP 域名的用户都属于这个域。

undo domain default enable 命令用来恢复缺省情况。

【命令】

```
domain default enable isp-name
undo domain default enable
```

【缺省情况】

存在一个系统缺省的 ISP 域，名称为 system。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

isp-name: ISP 域名，为 1~255 个字符的字符串，不区分大小写，且必须已经存在。

【使用指导】

系统中只能存在一个缺省的 ISP 域。

配置为缺省的 ISP 域不能被删除。如需删除一个系统缺省 ISP 域，请先使用 **undo domain default enable** 命令将其恢复为非缺省的 ISP 域。

【举例】

创建一个新的 ISP 域 test，并设置为系统缺省的 ISP 域。

```
<Sysname> system-view
```

```
[Sysname] domain test
[Sysname-isp-test] quit
[Sysname] domain default enable test
```

【相关命令】

- **display domain**
- **domain**

1.1.25 domain if-unknown

domain if-unknown 命令用来为未知域名的用户指定 ISP 域。

undo domain if-unknown 命令用来恢复缺省情况。

【命令】

```
domain if-unknown isp-name
undo domain if-unknown
```

【缺省情况】

没有为未知域名的用户指定 ISP 域。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

isp-name: ISP 域名。为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“””、“.”、“*”、“?”、“<”、“>” 以及 “@” 字符，且不能为字符串 “d”、“de”、“def”、“defa”、“defau”、“defaul”、“default”、“i”、“if”、“if-”、“if-u”、“if-un”、“if-unk”、“if-unkn”、“if-unkno”、“if-unknow” 和 “if-unknown”。

【使用指导】

设备将按照如下先后顺序选择认证域：接入模块指定的认证域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。其中，仅部分接入模块支持指定认证域。

如果根据以上原则决定的认证域在设备上不存在，但设备上为未知域名的用户指定了 ISP 域，则最终使用该指定的 ISP 域认证，否则，用户将无法认证。

【举例】

```
# 为未知域名的用户指定 ISP 域为 test。
<Sysname> system-view
[Sysname] domain if-unknown test
```

【相关命令】

- **display domain**

1.1.26 nas-id

nas-id 命令用来在 ISP 域视图下配置 NAS-ID。

undo nas-id 命令用来恢复缺省情况。

【命令】

nas-id nas-identifier

undo nas-id

【缺省情况】

未配置 ISP 域下的 NAS-ID。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

nas-identifier: NAS-ID 名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

用户进行 RADIUS 认证时，系统会获取设备的 NAS-ID 来设置 RADIUS 报文中的 NAS-Identifier 属性，该属性用于向 RADIUS 服务器标识用户的接入位置。

设备支持多种途径配置 NAS-ID，按照获取优先级从高到低的顺序依次包括：NAS-ID Profile 中与用户接入 VLAN 绑定的 NAS-ID、ISP 域视图下的 NAS-ID。若以上配置都不存在，则使用设备的名称作为 NAS-ID。

【举例】

在 ISP 域 test 下配置 NAS-ID 为 test。

```
<Sysname> system-view
```

```
[Sysname] domain test
```

```
[Sysname-isp-test] nas-id test
```

【相关命令】

- **aaa nas-id profile**

1.1.27 nas-id bind vlan

nas-id bind vlan 命令用来设置 NAS-ID 与 VLAN 的绑定关系。

undo nas-id bind vlan 命令用来删除指定的 NAS-ID 和 VLAN 的绑定关系。

【命令】

nas-id nas-identifier bind vlan vlan-id

undo nas-id nas-identifier bind vlan vlan-id

【缺省情况】

不存在 NAS-ID 与 VLAN 的绑定关系。

【视图】

NAS-ID Profile 视图

【缺省用户角色】

network-admin
context-admin

【参数】

nas-identifier: NAS-ID 名称，为 1~31 个字符的字符串，区分大小写。

vlan-id: 与 NAS-ID 绑定的 VLAN ID，取值范围为 1~4094。

【使用指导】

一个 NAS-ID Profile 视图下，可以指定多个 NAS-ID 与 VLAN 的绑定关系。

一个 NAS-ID 可以与多个 VLAN 绑定，但是一个 VLAN 只能与一个 NAS-ID 绑定。若多次将一个 VLAN 与不同的 NAS-ID 进行绑定，则最后的绑定关系生效。

【举例】

在名称为 aaa 的 NAS-ID Profile 视图下，配置 NAS-ID 222 与 VLAN 2 的绑定关系。

```
<Sysname> system-view  
[Sysname] aaa nas-id profile aaa  
[Sysname-nas-id-prof-aaa] nas-id 222 bind vlan 2
```

【相关命令】

- **aaa nas-id profile**

1.1.28 session-time include-idle-time

session-time include-idle-time 命令用来配置设备上传到服务器的用户在线时间中保留闲置切断时间。

undo session-time include-idle-time 命令用来恢复缺省情况。

【命令】

```
session-time include-idle-time  
undo session-time include-idle-time
```

【缺省情况】

设备上传到服务器的用户在线时间中扣除闲置切断时间。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

请根据实际的计费策略决定是否在用户在线时间中保留闲置切断时间。该闲置切断时间在用户认证成功后由 AAA 授权。

当用户正常下线时，设备上传到服务器上的用户在线时间为实际在线时间；当用户异常下线时，上传到服务器的用户在线时间具体如下：

- 若配置为保留闲置切断时间，则上传到服务器上的用户在线时间中包含了一定的闲置切断时间。此时，服务器上记录的用户时长将大于用户实际在线时长。
- 若配置为扣除闲置切断时间，则上传到服务器上的用户在线时间为，闲置切断检测机制计算出的用户已在线时长扣除掉一个闲置切断时间。此时，服务器上记录的用户时长将小于用户实际在线时长。

【举例】

在 ISP 域 test 下，配置设备上传到服务器的用户在线时间中保留闲置切断时间。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] session-time include-idle-time
```

【相关命令】

- **display domain**

1.1.29 state (ISP domain view)

state 命令用来设置当前 ISP 域的状态。

undo state 命令用来恢复缺省情况。

【命令】

```
state { active | block }
undo state
```

【缺省情况】

当前 ISP 域处于活动状态。

【视图】

ISP 域视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

active: 指定当前 ISP 域处于活动状态，即系统允许该域下的用户请求网络服务。

block: 指定当前 ISP 域处于阻塞状态，即系统不允许该域下的用户请求网络服务。

【使用指导】

当某个 ISP 域处于阻塞状态时，将不允许该域下的用户请求网络服务，但不影响已经在线的用户。

【举例】

设置当前 ISP 域 test 处于阻塞状态。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] state block
```

【相关命令】

- **display domain**

1.1.30 user-address-type

user-address-type 命令用来设置当前 ISP 域的用户地址类型。

undo user-address-type 命令用来恢复缺省情况。

【命令】

```
user-address-type { private-ipv4 | public-ds | public-ipv4 }  
undo user-address-type
```

【缺省情况】

未指定当前 ISP 域的用户地址类型。

【视图】

ISP 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

private-ipv4: 表示当前用户的地址类型为私网 IPv4 地址。

public-ds: 表示当前用户的地址类型为公网双栈地址。

public-ipv4: 表示当前用户的地址类型为公网 IPv4 地址。

【使用指导】

当更改当前 ISP 域的用户地址类型时，不影响已经在线的用户。

【举例】

```
# 设置当前 ISP 域用户地址类型为私网 IPv4 地址。  
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] user-address-type private-ipv4
```

【相关命令】

- **display domain**

1.2 本地用户配置命令

1.2.1 access-limit

access-limit 命令用来设置使用当前本地用户名接入设备的最大用户数。

undo access-limit 命令用来恢复缺省情况。

【命令】

```
access-limit max-user-number
```


undo access-limit

【缺省情况】

不限制使用当前本地用户名接入的用户数。

【视图】

本地用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

max-user-number: 表示使用当前本地用户名接入设备的最大用户数，取值范围为 1~1024。

【使用指导】

本地用户视图下的 **access-limit** 命令只在该用户采用了本地计费方法的情况下生效。

由于 FTP/SFTP/SCP 用户不支持计费，因此 FTP/SFTP/SCP 用户不受此属性限制。

【举例】

允许同时以本地用户名 abc 在线的用户数为 5。

```
<Sysname> system-view
```

```
[Sysname] local-user abc
```

```
[Sysname-luser-manage-abc] access-limit 5
```

【相关命令】

- **display local-user**

1.2.2 access-user email authentication

access-user email authentication 命令用来配置登录为网络接入类本地用户发送 Email 使用的 SMTP 服务器所需要的用户名和密码。

undo access-user email authentication 命令用来恢复缺省情况。

【命令】

```
access-user email authentication username user-name password { cipher | simple } string
```

```
undo access-user email authentication
```

【缺省情况】

未配置登录 SMTP 服务器的用户名和密码。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

username *user-name*: 登录用户名。其中, *user-name* 为 1~63 个字符的字符串, 区分大小写。

password: 登录密码。

cipher: 以密文方式设置密码。

simple: 以明文方式设置密码, 该密码将以密文形式存储。

string: 密码字符串, 区分大小写。其中, 明文密码为 1~63 个字符的字符串, 密文密码为 1~117 个字符的字符串。

【使用指导】

如果登录 SMTP 邮箱服务器时需要提供登录用户名和密码, 则必须通过本配置设置相应的登录用户名和密码。

多次执行本命令, 最后一次执行的命令生效。

【举例】

配置登录为网络接入类本地用户发送 Email 使用的 SMTP 服务器所需要的用户名为 abc、密码为明文 123。

```
<Sysname> system-view
```

```
[Sysname] access-user email authentication username abc password simple 123
```

【相关命令】

- **access-user email format**
- **access-user email sender**
- **access-user email smtp-server**

1.2.3 access-user email format

access-user email format 命令用来配置网络接入类本地用户通知邮件的主题和内容。

undo access-user email format 命令用来恢复缺省情况。

【命令】

```
access-user email format { body body-string | subject sub-string }
```

```
undo access-user email format { body | subject }
```

【缺省情况】

缺省邮件主题: Password reset notification。

缺省邮件内容:

A random password has been generated for your account.

Username: xxx

Password: yyy

Validity: YYYY/MM/DD hh:mm:ss to YYYY/MM/DD hh:mm:ss

其中, xxx 为用户名, yyy 为用户密码, YYYY/MM/DD hh:mm:ss to YYYY/MM/DD hh:mm:ss 为用户账户有效期。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

body *body-string*: 邮件的内容。其中, *body-string* 为 1~255 个字符的字符串, 区分大小写。

subject *sub-string*: 邮件的主题。其中, *sub-string* 为 1~127 个字符的字符串, 区分大小写。

【使用指导】

管理员通过 Web 页面创建网络接入类本地用户、重置网络接入类用户密码时, 如果由设备为用户生成随机密码, 设备将在生成随机密码后向用户发送通知邮件告知为其生成的随机密码, 该通知邮件的主题和内容通过本命令设置。

实际发送的邮件内容将包括设置的 *body-string* 与如下三项固定内容:

Username: xxx

Password: yyy

Validity: YYYY/MM/DD hh:mm:ss to YYYY/MM/DD hh:mm:ss

其中, xxx 为用户名, yyy 为用户密码, YYYY/MM/DD hh:mm:ss to YYYY/MM/DD hh:mm:ss 为用户账户有效期。

多次执行本命令, 最后一次执行的命令生效。

【举例】

配置网络接入类本地用户通知邮件的主题和内容。

```
<Sysname> system-view
```

```
[Sysname] access-user email format subject new password setting
```

```
[Sysname] access-user email format body The username, password, and validity period of the account are given below.
```

【相关命令】

- **access-user email authentication**
- **access-user email sender**
- **access-user email smtp-server**

1.2.4 access-user email sender

access-user email sender 命令用来配置网络接入类本地用户通知邮件的发件人地址。

undo access-user email sender 命令用来恢复缺省情况。

【命令】

access-user email sender *email-address*

undo access-user email sender

【缺省情况】

未配置网络接入类本地用户通知邮件的发件人地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

email-address: 邮件发件人地址，为 1~255 个字符的字符串，区分大小写，必须且最多只能携带一个“@”符号，不能仅为“@”。

【使用指导】

未配置发件人地址的情况下，设备无法向任何收件人发送关于网络接入类本地用户的通知邮件。
只能存在一个网络接入类本地用户的发件人地址。多次执行本命令，最后一次执行的命令生效。

【举例】

配置网络接入类本地用户通知邮件的发件人地址为 abc@yyy.com。

```
<Sysname> system-view
```

```
[Sysname] access-user email sender abc@yyy.com
```

【相关命令】

- **access-user email authentication**
- **access-user email format**
- **access-user email smtp-server**

1.2.5 access-user email smtp-server

access-user email smtp-server 命令用来配置为网络接入类本地用户发送 Email 使用的 SMTP 服务器。

undo access-user email smtp-server 命令用来恢复缺省情况。

【命令】

```
access-user email smtp-server url-string
```

```
undo access-user email smtp-server
```

【缺省情况】

未配置为网络接入类本地用户发送 Email 使用的 SMTP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

url-string: SMTP 服务器的 URL, 为 1~255 个字符的字符串, 区分大小写, 符合标准 SMTP 协议规范, 以 **smtp://** 开头。

【使用指导】

只能存在一个发送 Email 使用的 SMTP 服务器。多次执行本命令, 最后一次执行的命令生效。

【举例】

```
# 配置为网络接入类本地用户发送 Email 使用的 SMTP 服务器 URL 为 smtp://www.test.com/smtp。  
<Sysname> system-view  
[Sysname] access-user email smtp-server smtp://www.test.com/smtp
```

【相关命令】

- **access-user email authentication**
- **access-user email format**
- **access-user email sender**

1.2.6 authorization-attribute (Local user view/user group view)

authorization-attribute 命令用来设置本地用户或用户组的授权属性, 该属性在本地用户认证通过之后, 由设备下发给用户。

undo authorization-attribute 命令用来删除指定的授权属性, 恢复用户具有的缺省访问权限。

【命令】

```
authorization-attribute { user-role role-name | work-directory directory-name } *  
undo authorization-attribute { user-role role-name | work-directory } *
```

【缺省情况】

授权 FTP/SFTP/SCP 用户可以访问的目录为设备的根目录, 但无访问权限。

在缺省 Context 中由用户角色为 **network-admin** 或者 **level-15** 的用户创建的本地用户被授权用户角色 **network-operator**; 在非缺省 Context 中由用户角色为 **context-admin** 或者 **level-15** 的用户创建的本地用户被授权用户角色 **context-operator**。

【视图】

本地用户视图

用户组视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-role *role-name*: 指定本地用户的授权用户角色。其中, *role-name* 表示用户角色名称, 为 1~63 个字符的字符串, 区分大小写。可以为每个用户最多指定 64 个用户角色。本地用

户角色的相关命令请参见“基础配置命令参考”中的“RBAC”。该授权属性只能在本地用户视图下配置，不能在本地用户组视图下配置。

work-directory *directory-name*: 授权 FTP/SFTP/SCP 用户可以访问的目录。其中，*directory-name* 表示 FTP/SFTP/SCP 用户可以访问的目录，为 1~255 个字符的字符串，不区分大小写，且该目录必须已经存在。

【使用指导】

可配置的授权属性都有其明确的使用环境和用途，请针对用户的服务类型配置对应的授权属性：

- 对于 IPoE 用户，仅授权属性 **idle-cut**、**ip-pool**、**ipv6-pool**、**ipv6-prefix**、**primary-dns**、**secondary-dns**、**session-timeout**、**user-profile**、**vpn-instance** 有效。
- 对于 lan-access 用户，仅授权属性 **acl**、**idle-cut**、**session-timeout**、**vlan** 有效。其中，属性 **idle-cut** 目前仅适用于无线用户。
- 对于 Telnet、Terminal、SSH 用户，仅授权属性 **idle-cut**、**user-role** 有效。
- 对于 http、https 用户，仅授权属性 **user-role** 有效。
- 对于 FTP 用户，仅授权属性 **user-role**、**work-directory** 有效。
- 对于其它类型的本地用户，所有授权属性均无效。

用户组的授权属性对于组内的所有本地用户生效，因此具有相同属性的用户可通过加入相同的用户组来统一配置和管理。

本地用户视图下未配置的授权属性继承所属用户组的授权属性配置，但是如果本地用户视图与所属的用户组视图下都配置了某授权属性，则本地用户视图下的授权属性生效。

在多台设备组成 IRF 的环境下，为了避免 IRF 系统进行主从倒换后 FTP/SFTP/SCP 用户无法正常登录，建议用户在指定工作目录时不要携带 slot 信息。

为确保本地用户仅使用本命令指定的授权用户角色，请先使用 **undo authorization-attribute user-role** 命令删除该用户已有的缺省用户角色。

被授权安全日志管理员的本地用户登录设备后，仅可执行安全日志文件管理相关的命令以及安全日志文件操作相关的命令，具体命令可通过 **display role name security-audit** 命令查看。安全日志文件管理相关命令的介绍，请参见“网络管理与监控”中的“信息中心”。文件系统管理相关命令的介绍，请参见“基础配置命令参考”中的“文件系统管理”。

为本地用户授权安全日志管理员角色时，需要注意的是：

- 安全日志管理员角色和其它用户角色互斥：
 - 为一个用户授权安全日志管理员角色时，系统会通过提示信息请求确认是否删除当前用户的所有其它用户角色；
 - 如果已经授权当前用户安全日志管理员角色，再授权其它的用户角色时，系统会通过提示信息请求确认是否删除当前用户的安全日志管理员角色。
- 系统中的最后一个安全日志管理员角色的本地用户不可被删除。

为本地用户授权 **system-admin**、**security-admin**、**audit-admin** 角色时，需要注意的是：

- 被授权此类角色的本地用户登录设备后，仅有执行指定 Web 页面的操作权限，以及执行 **ping** 和 **tracert** 命令的命令行权限，具体权限介绍请参见“基础配置指导”中的“RBAC”。
- 这些角色和其它用户角色互斥，且彼此之间也互斥。为一个用户授权用户角色时，系统会通过提示信息请求确认是否删除与当前用户角色互斥的其它用户角色。

【举例】

```
# 配置用户组 abc 的授权 VLAN 为 VLAN 3。
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc] authorization-attribute vlan 3
# 配置设备管理类本地用户 xyz 的授权用户角色为 security-audit（安全日志管理员）。
<Sysname> system-view
[Sysname] local-user xyz class manage
[Sysname-luser-manage-xyz] authorization-attribute user-role security-audit
This operation will delete all other roles of the user. Are you sure? [Y/N]:y
```

【相关命令】

- **display local-user**
- **display user-group**

1.2.7 display local-user

display local-user 命令用来显示本地用户的配置信息和在线用户数的统计信息。

【命令】

```
display local-user [ class { manage | network } | idle-cut { disable | enable }  
| service-type { ftp | http | https | ike | ipoe | lan-access | ppp | ssh |  
telnet | terminal } | state { active | block } | user-name user-name class  
{ manage | network } | vlan vlan-id ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin  
network-operator  
context-admin  
context-operator
```

【参数】

class: 显示指定用户类别的本地用户信息。

manage: 设备管理类用户。

idle-cut { disable | enable }: 显示开启或关闭闲置切断功能的本地用户信息。其中，**disable** 表示未启用闲置切断功能的本地用户；**enable** 表示启用了闲置切断功能并配置了闲置切断时间的本地用户。

service-type: 显示指定用户类型的本地用户信息。

- **ftp**: FTP 用户。
- **http**: HTTP 用户。
- **https**: HTTPS 用户。
- **ipoe**: IPoE 用户（主要指 IP 接入用户，比如二/三层专线用户，数字机顶盒接入用户）。

- **lan-access**: lan-access 类型用户。
- **ssh**: SSH 用户。
- **telnet**: Telnet 用户。
- **terminal**: 从 Console 口登录的终端用户。

state { active | block }: 显示处于指定状态的本地用户信息。其中，**active** 表示用户处于活动状态，即系统允许该用户请求网络服务；**block** 表示用户处于阻塞状态，即系统不允许用户请求网络服务。

user-name user-name: 显示指定用户名的本地用户信息。其中，**user-name** 表示本地用户名，为 1~55 个字符的字符串，区分大小写，不能携带域名，不能包括符号 “\”、“|”、“/”、“:”、“*”、“?”、“<”、“>” 和 “@”，且不能为 “a”、“al” 或 “all”。

vlan vlan-id: 显示指定 VLAN 内的所有本地用户信息。其中，**vlan-id** 为 VLAN 编号，取值范围为 1~4094。

【使用指导】

如果不指定任何参数，则显示所有本地用户信息。

【举例】

```
# 显示所有本地用户的相关信息。
<Sysname> display local-user
Device management user root:
  State:                               Active
  Service type:                         SSH/Telnet/Terminal
  Access limit:                         Enabled           Max access number: 3
  Current access number:                1
  User group:                           system
  Bind attributes:
  Authorization attributes:
    Work directory:                     flash:
    User role list:                     network-admin
  Password control configurations:
    Password aging:                     3 days
Total 1 local users matched.
```

表1-2 display local-user 命令显示信息描述表

字段	描述
State	本地用户状态 • Active: 活动状态 • Block: 阻塞状态
Service type	本地用户使用的服务类型
Access limit	是否对使用该用户名的接入用户数进行限制
Max access number	最大接入用户数
Current access number	使用该用户名的当前接入用户数

字段	描述
User group	本地用户所属的用户组
Bind attributes	本地用户的绑定属性
IP address	本地用户的IP地址
Location bound	本地用户绑定的端口
MAC address	本地用户的MAC地址
VLAN ID	本地用户绑定的VLAN
Authorization attributes	本地用户的授权属性
Idle timeout	本地用户闲置切断时间（单位为分钟）
Session-timeout	本地用户的会话超时时间（单位为分钟）
Work directory	FTP/SFTP/SCP用户可以访问的目录
ACL number	本地用户授权ACL
VLAN ID	本地用户授权VLAN
User role list	本地用户的授权用户角色列表
IP pool	本地用户的授权IPv4地址池
IP address	本地用户的授权IPv4地址
IPv6 address	本地用户的授权IPv6地址
IPv6 prefix	本地用户的授权IPv6前缀
IPv6 pool	本地用户的授权IPv6地址池
Primary DNS server	本地用户的授权主DNS服务器IPv4地址
Secondary DNS server	本地用户的授权从DNS服务器IPv4地址
Primary DNSV6 server	本地用户的授权主DNS服务器IPv6地址
Secondary DNSV6 server	本地用户的授权从DNS服务器IPv6地址
URL	本地用户的授权PADM URL
VPN instance	本地用户的授权VPN实例
Password control configurations	本地用户的密码控制属性
Password aging	密码老化时间
Password length	密码最小长度
Password composition	密码组合策略（密码元素的组合类型、至少要包含每种元素的个数）
Password complexity	密码复杂度检查策略（是否包含用户名或者颠倒的用户名；是否包含三个或以上相同字符）
Maximum login attempts	用户最大登录尝试次数
Action for exceeding login attempts	登录尝试次数达到设定次数后的用户帐户锁定行为

字段	描述
Password history was last reset	上一次清除密码历史记录的时间
Total x local users matched.	总计有x个本地用户匹配

1.2.8 display user-group

display user-group 命令用来显示用户组的配置信息。

【命令】

```
display user-group { all | name group-name } [ identity-member { all | group | user } ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

all: 显示所有用户组的配置信息。

name *group-name*: 显示指定用户组的配置。*group-name* 表示用户组名称，为 1~32 个字符的字符串，不区分大小写。

identity-member { **all** | **group** | **user** }: 显示用户组的身份识别成员信息。其中，**all** 表示所有身份识别成员，包括所有用户组类型和用户类型的成员；**group** 表示用户组类型的身份识别成员；**user** 表示仅显示用户类型的身份识别成员信息。若不指定该参数，则不显示用户组的身份识别成员信息。

【举例】

显示所有用户组的相关配置。

```
<Sysname> display user-group all
Total 2 user groups matched.
```

```
User group: system
  Authorization attributes:
    Work directory:      flash:
User group: jj
  Authorization attributes:
    Idle timeout:        2 minutes
    Work directory:      flash:/
    ACL number:          2000
    VLAN ID:             2
  Password control configurations:
```

Password aging: 2 days

表1-3 display user-group 命令显示信息描述表

字段	描述
Total x user groups matched.	总计有x个用户组匹配
User group	用户组名称
Authorization attributes	授权属性信息
Idle timeout	闲置切断时间（单位：分钟）
Session-timeout	会话超时时间（单位：分钟）
Work directory	FTP/SFTP/SCP用户可以访问的目录
ACL number	授权ACL号
VLAN ID	授权VLAN ID
IP pool	授权IPv4地址池
IPv6 prefix	授权IPv6前缀
IPv6 pool	授权IPv6地址池
Primary DNS server	授权主DNS服务器IPv4地址
Secondary DNS server	授权从DNS服务器IPv6地址
Primary DNSV6 server	授权主DNS服务器IPv6地址
Secondary DNSV6 server	授权从DNS服务器IPv6地址
URL	授权PADM URL
VPN instance	授权VPN实例
Password control configurations	用户组的密码控制属性
Password aging	密码老化时间
Password length	密码最小长度
Password composition	密码组合策略（密码元素的组合类型、至少要包含每种元素的个数）
Password complexity	密码复杂度检查策略（是否包含用户名或者颠倒的用户名；是否包含三个或以上相同字符）
Maximum login attempts	用户最大登录尝试次数
Action for exceeding login attempts	登录尝试次数达到设定次数后的用户帐户锁定行为

1.2.9 group

group 命令用来设置本地用户所属的用户组。

undo group 命令用来恢复缺省配置。

【命令】

```
group group-name  
undo group
```

【缺省情况】

本地用户属于用户组 **system**。

【视图】

本地用户视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

group-name：用户组名称，为 1~32 个字符的字符串，不区分大小写。

【举例】

设置设备管理类本地用户 **111** 所属的用户组为 **abc**。

```
<Sysname> system-view  
[Sysname] local-user 111 class manage  
[Sysname-luser-manage-111] group abc
```

【相关命令】

- **display local-user**

1.2.10 local-user

local-user 命令用来添加本地用户，并进入本地用户视图。如果指定的本地用户已经存在，则直接进入本地用户视图。

undo local-user 命令用来删除指定的本地用户。

【命令】

```
local-user user-name [ class manage ]  
undo local-user { user-name class { manage | network } | all [ service-type  
{ ftp | http | https | ipoe | lan-access | ssh | telnet | terminal } | class  
manage ] }
```

【缺省情况】

不存在本地用户。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

user-name: 表示本地用户名，为 1~55 个字符的字符串，区分大小写。用户名不能携带域名，不能包括符号“\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和“@”，且不能为“a”、“al”或“all”。

class: 指定本地用户的类别。若不指定本参数，则表示设备管理类用户。

manage: 设备管理类用户，用于登录设备，对设备进行配置和监控。此类用户可以提供 **ftp**、**http**、**https**、**telnet**、**ssh**、**terminal** 服务。

all: 所有的用户。

service-type: 指定用户的类型。

- **ftp**: 表示 FTP 类型用户。
- **http**: 表示 HTTP 类型用户。
- **https**: 表示 HTTPS 类型用户。
- **ipoe**: 表示 IPoE 类型用户（主要指以 IP 接入用户，比如二三层专线，数字机顶盒接入的用户）。
- **lan-access**: 表示 lan-access 类型用户。
- **ssh**: 表示 SSH 用户。
- **telnet**: 表示 Telnet 用户。
- **terminal**: 表示从 Console 口、AUX 口、Asyn 口登录的终端用户。

【举例】

添加名称为 **user1** 的设备管理类本地用户。

```
<Sysname> system-view
```

```
[Sysname] local-user user1 class manage
```

```
[Sysname-luser-manage-user1]
```

【相关命令】

- **display local-user**
- **service-type**

1.2.11 password

password 命令用来设置本地用户的密码。

undo password 命令用来恢复缺省情况。

【命令】

```
password [ { hash | simple } string ]
```

```
undo password
```

【缺省情况】

不存在本地用户密码，且本地用户认证时不能成功。

【视图】

本地用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

hash: 表示以哈希方式设置密码。

simple: 表示以明文方式设置密码，该密码将以哈希方式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串；哈希密码为 1~110 个字符的字符串。

【使用指导】

如果不指定任何参数，则表示以交互式设置明文形式的密码。

可以不为本地用户设置密码。若不为本地用户设置密码，则该用户认证时无需输入密码，只要用户名有效且其它属性验证通过即可认证成功。为提高用户帐户的安全性，建议设置本地用户密码。

在全局 Password Control 功能处于开启的情况下，需要注意的是：

- 所有历史密码都以哈希方式存储。
- 当前登录用户以明文方式修改自己的密码时，需要首先提供现有的明文密码，然后保证输入的新密码与所有历史密码不同，且至少要与现有密码存在 4 个不同字符的差异。
- 当前登录用户以明文方式修改其它用户的密码时，需要保证新密码与所有历史密码不同。
- 当前登录用户删除自己的密码时，需要提供现有的明文密码。
- 其它情况下，均不需要提供现有明文密码，也不与历史密码进行比较。

【举例】

设置设备管理类本地用户 user1 的密码为明文 123456TESTplat&!

```
<Sysname> system-view
```

```
[Sysname] local-user user1 class manage
```

```
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
```

以交互式方式设置设备管理类本地用户 test 的密码。

```
<Sysname> system-view
```

```
[Sysname] local-user test class manage
```

```
[Sysname-luser-manage-test] password
```

```
Password:
```

```
confirm :
```

【相关命令】

- **display local-user**

1.2.12 service-type (Local user view)

service-type 命令用来设置用户可以使用服务类型。

undo service-type 命令用来删除用户可以使用服务类型。

【命令】

```
service-type {ftp | ipoe | lan-access | { http | https | ssh | telnet | terminal } *}
```

```
undo service-type { ftp | ipoe | lan-access | { http | https | ssh | telnet | terminal } *}
```

【缺省情况】

系统不对用户授权任何服务，即用户不能使用任何服务。

【视图】

本地用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

ftp：指定用户可以使用 FTP 服务。若授权 FTP 服务，授权目录可以通过 **authorization-attribute work-directory** 命令来设置。

http：指定用户可以使用 HTTP 服务。

https：指定用户可以使用 HTTPS 服务。

ipoe：指定用户可以使用 IPoE 服务。

lan-access：指定用户可以使用 lan-access 服务。

ssh：指定用户可以使用 SSH 服务。

telnet：指定用户可以使用 Telnet 服务。

terminal：指定用户可以使用 terminal 服务（即从 Console 口登录）。

【使用指导】

可以通过多次执行本命令，设置用户可以使用多种服务类型。

【举例】

指定设备管理类用户可以使用 Telnet 服务和 FTP 服务。

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] service-type telnet
[Sysname-luser-manage-user1] service-type ftp
```

【相关命令】

- **display local-user**

1.2.13 state (Local user view)

state 命令用来设置当前本地用户的状态。

undo state 命令用来恢复缺省情况。

【命令】

```
state { active | block }
undo state
```

【缺省情况】

本地用户处于活动状态。

【视图】

本地用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

active: 指定当前本地用户处于活动状态，即系统允许当前本地用户请求网络服务。

block: 指定当前本地用户处于“阻塞”状态，即系统不允许当前本地用户请求网络服务。

【举例】

设置设备管理类本地用户 **user1** 处于“阻塞”状态。

```
<Sysname> system-view
```

```
[Sysname] local-user user1 class manage
```

```
[Sysname-luser-manage-user1] state block
```

【相关命令】

- **display local-user**

1.2.14 user-group

user-group 命令用来创建用户组，并进入用户组视图。如果指定的用户组已经存在，则直接进入用户组视图。

undo user-group 命令用来删除指定的用户组。

【命令】

user-group *group-name*

undo user-group *group-name*

【缺省情况】

存在一个用户组，名称为 **system**。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name: 用户组名称，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

用户组是一个本地用户的集合，某些需要集中管理的属性可在用户组中统一配置和管理。

不允许使用 **undo user-group** 命令删除一个包含本地用户的用户组。

不能删除系统中存在的默认用户组 **system**，但可以修改该用户组的配置。

【举例】

```
# 创建名称为 abc 的用户组并进入其视图。  
<Sysname> system-view  
[Sysname] user-group abc  
[Sysname-ugroup-abc]
```

【相关命令】

- **display user-group**

1.3 RADIUS配置命令

1.3.1 aaa device-id

aaa device-id 命令用来配置设备 ID。
undo aaa debice-id 命令用来恢复缺省情况。

【命令】

```
aaa device-id device-id  
undo aaa device-id
```

【缺省情况】

设备 ID 为 0。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

device-id: 设备 ID，取值范围为 1~255。

【使用指导】

RADIUS 计费过程使用 Acct-Session-Id 属性作为用户的计费 ID。设备会为每个在线用户生成一个唯一的 Acct-Session-Id 值。设备 ID 是 Acct-Session-Id 属性值中的一个组成字段。
修改后的设备 ID 仅对新上线用户生效。

【举例】

```
# 配置设备 ID 为 1。  
<Sysname> system-view  
[Sysname] aaa device-id 1
```

1.3.2 accounting-on enable

accounting-on enable 命令用来开启 accounting-on 功能。
undo accounting-on enable 命令用来关闭 accounting-on 功能。

【命令】

```
accounting-on enable [ interval interval | send send-times ] *  
undo accounting-on enable
```

【缺省情况】

accounting-on 功能处于关闭状态。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval *interval*: 指定 accounting-on 报文重发时间间隔，取值范围为 1~15，单位为秒，缺省值为 3。

send *send-times*: 指定 accounting-on 报文的最大发送次数，取值范围为 1~255，缺省值为 50。

【使用指导】

accounting-on 功能使得整个设备在重启之后通过发送 accounting-on 报文通知该方案所使用的 RADIUS 计费服务器，要求 RADIUS 服务器停止计费且强制该设备的用户下线。

开启 accounting-on 功能后，请执行 **save** 命令保证 accounting-on 功能在整个设备下次重启后生效。关于命令的详细介绍请参见“基础配置命令参考”中的“配置文件管理”。

本命令设置的 accounting-on 参数会立即生效。

【举例】

在 RADIUS 方案 radius1 中，开启 accounting-on 功能并配置 accounting-on 报文重发时间间隔为 5 秒、accounting-on 报文的最大发送次数为 15 次。

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] accounting-on enable interval 5 send 15
```

【相关命令】

- **display radius scheme**

1.3.3 attribute 15 check-mode

attribute 15 check-mode 命令用来配置对 RADIUS Attribute 15 的检查方式。

undo attribute 15 check-mode 命令用来恢复缺省情况。

【命令】

```
attribute 15 check-mode { loose | strict }  
undo attribute 15 check-mode
```

【缺省情况】

对 RADIUS Attribute 15 的检查方式为 **strict** 方式。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

loose: 松散检查方式，设备使用 RADIUS Attribute 15 的标准属性值对用户业务类型进行检查。对于 SSH、FTP、Terminal 用户，在 RADIUS 服务器下发的 Login-Service 属性值为 0（表示用户业务类型为 Telnet）时才，这类用户才能够通过认证。

strict: 严格检查方式，设备使用 RADIUS Attribute 15 的标准属性值以及扩展属性值对用户业务类型进行检查。对于 SSH、FTP、Terminal 用户，当 RADIUS 服务器下发的 Login-Service 属性值为对应的扩展取值时，这类用户才能够通过认证。

【使用指导】

由于某些 RADIUS 服务器不支持自定义的属性，无法下发扩展的 Login-Service 属性，若要使用这类 RADIUS 服务器对 SSH、FTP、Terminal 用户进行认证，建议设备上对 RADIUS 15 号属性值采用松散检查方式。

【举例】

```
# 在 RADIUS 方案 radius1 中，配置对 RADIUS Attribute 15 采用松散检查方式。
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 15 check-mode loose
```

【相关命令】

- **display radius scheme**

1.3.4 attribute 25 car

attribute 25 car 命令用来开启 RADIUS Attribute 25 的 CAR 参数解析功能。

undo attribute 25 car 命令用来关闭 RADIUS Attribute 25 的 CAR 参数解析功能。

【命令】

```
attribute 25 car
undo attribute 25 car
```

【缺省情况】

RADIUS Attribute 25 的 CAR 参数解析功能处于关闭状态。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

RADIUS 的 25 号属性为 class 属性，该属性由 RADIUS 服务器下发给设备。目前，某些 RADIUS 服务器利用 class 属性来对用户下发 CAR 参数，可以通过本特性来控制设备是否将 RADIUS 25 号属性解析为 CAR 参数，解析出的 CAR 参数可被用来进行基于用户的流量监管控制。

【举例】

在 RADIUS 方案 radius1 中，开启 RADIUS Attribute 25 的 CAR 参数解析功能。

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] attribute 25 car
```

【相关命令】

- **display radius scheme**

1.3.5 attribute 31 mac-format

attribute 31 mac-format 命令用来配置 RADIUS Attribute 31 中的 MAC 地址格式。

undo attribute 31 mac-format 命令用来恢复缺省情况。

【命令】

```
attribute 31 mac-format section { six | three } separator  
separator-character { lowercase | uppercase }  
undo attribute 31 mac-format
```

【缺省情况】

RADIUS Attribute 31 中的 MAC 地址为大写字母格式，且被分隔符“-”分成 6 段，即为 HH-HH-HH-HH-HH-HH 的格式。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

section: 指定 MAC 地址分段数。

six: 表示 MAC 地址被分为 6 段，格式为 HH-HH-HH-HH-HH-HH。

three: 表示 MAC 地址被分为 3 段，格式为 HHHH-HHHH-HHHH。

separator separator-character: MAC 地址的分隔符，为单个字符，区分大小写。

lowercase: 表示 MAC 地址为小写字母格式。

uppercase: 表示 MAC 地址为大写字母格式。

【使用指导】

不同的 RADIUS 服务器对填充在 RADIUS Attribute 31 中的 MAC 地址有不同的格式要求, 为了保证 RADIUS 报文的正常交互, 设备发送给服务器的 RADIUS Attribute 31 号属性中 MAC 地址的格式必须与服务器的要求保持一致。

【举例】

在 RADIUS 方案 radius1 中, 配置 RADIUS Attribute 31 的 MAC 地址格式为 hh:hh:hh:hh:hh:hh。

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] attribute 31 mac-format section six separator : lowercase
```

【相关命令】

- **display radius scheme**

1.3.6 attribute convert (RADIUS DAE server view)

attribute convert 命令用来配置 RADIUS 属性转换规则。

undo attribute convert 命令用来删除 RADIUS 属性转换规则。

【命令】

```
attribute convert src-attr-name to dest-attr-name { { coa-ack | coa-request }  
* | { received | sent } * }
```

```
undo attribute convert [ src-attr-name ]
```

【缺省情况】

不存在 RADIUS 属性转换规则, 系统按照标准 RADIUS 协议对 RADIUS 属性进行处理。

【视图】

RADIUS DAE 服务器视图

【缺省用户角色】

network-admin

context-admin

【参数】

src-attr-name: 源属性名称, 为 1~63 个字符的字符串, 不区分大小写。该属性必须为系统支持的属性。

dest-attr-name: 目的属性名称, 为 1~63 个字符的字符串, 不区分大小写。该属性必须为系统支持的属性。

coa-ack: COA 应答报文。

coa-request: COA 请求报文。

received: 接收到的 DAE 报文。

sent: 发送的 DAE 报文。

【使用指导】

RADIUS 属性转换规则中的源属性内容将被按照目的属性的含义来处理。

只有在 RADIUS 属性解释功能开启之后, RADIUS 属性转换规则才能生效。

配置 RADIUS 属性转换规则时，需要遵循以下原则：

- 源属性内容和目的属性内容的数据类型必须相同。
- 源属性和目的属性的名称不能相同。
- 一个属性只能按照一种方式（按报文类型或报文处理方向）进行转换。
- 一个源属性不能同时转换为多个目的属性。

执行 **undo attribute convert** 命令时，如果不指定源属性名称，则表示删除所有 RADIUS 属性转换规则。

【举例】

在 RADIUS DAE 服务器视图下，配置一条 RADIUS 属性转换规则，指定将接收到的 DAE 报文中的 Hw-Server-String 属性转换为 Connect-Info 属性。

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] attribute convert Hw-Server-String to Connect-Info received
```

【相关命令】

- **attribute translate**

1.3.7 attribute convert (RADIUS scheme view)

attribute convert 命令用来配置 RADIUS 属性转换规则。

undo attribute convert 命令用来删除 RADIUS 属性转换规则。

【命令】

```
attribute convert src-attr-name to dest-attr-name { { access-accept | access-request | accounting } * | { received | sent } * }
undo attribute convert [ src-attr-name ]
```

【缺省情况】

不存在 RADIUS 属性转换规则，系统按照标准 RADIUS 协议对 RADIUS 属性进行处理。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

src-attr-name：源属性名称，为 1~63 个字符的字符串，不区分大小写。该属性必须为系统支持的属性。

dest-attr-name：目的属性名称，为 1~63 个字符的字符串，不区分大小写。该属性必须为系统支持的属性。

access-accept：RADIUS 认证成功报文。

access-request：RADIUS 认证请求报文。

accounting：RADIUS 计费报文。

received: 接收到的 RADIUS 报文。

sent: 发送的 RADIUS 报文。

【使用指导】

RADIUS 属性转换规则中的源属性内容将被按照目的属性的含义来处理。

只有在 RADIUS 属性解释功能开启之后，RADIUS 属性转换规则才能生效。

配置 RADIUS 属性转换规则时，需要遵循以下原则：

- 源属性内容和目的属性内容的数据类型必须相同。
- 源属性和目的属性的名称不能相同。
- 一个属性只能按照一种方式（按报文类型或报文处理方向）进行转换。
- 一个源属性不能同时转换为多个目的属性。

执行 **undo attribute convert** 命令时，如果不指定源属性名称，则表示删除所有 RADIUS 属性转换规则。

【举例】

在 RADIUS 方案 radius1 中，配置一条 RADIUS 属性转换规则，指定将接收到的 RADIUS 报文中的 Hw-Server-String 属性转换为 Connect-Info 属性。

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] attribute convert Hw-Server-String to Connect-Info received
```

【相关命令】

- **attribute translate**

1.3.8 attribute reject (RADIUS DAE server view)

attribute reject 命令用来配置 RADIUS 属性禁用。

undo attribute reject 命令用来取消配置的 RADIUS 属性禁用。

【命令】

```
attribute reject attr-name { { coa-ack | coa-request } * | { received | sent } * }
```

```
undo attribute reject [ attr-name ]
```

【缺省情况】

不存在 RADIUS 属性禁用规则。

【视图】

RADIUS DAE 服务器视图

【缺省用户角色】

network-admin

context-admin

【参数】

attr-name: RADIUS 属性名称，为 1~63 个字符的字符串，不区分大小写。该属性必须为系统支持的属性。

coa-ack: COA 应答报文。

coa-request: COA 请求报文。

received: 接收到的 DAE 报文。

sent: 发送的 DAE 报文。

【使用指导】

当设备发送的 RADIUS 报文中携带了 RADIUS 服务器无法识别的属性时,可以定义基于发送方向的属性禁用规则,使得设备发送 RADIUS 报文时,将该属性从报文中删除。

当 RADIUS 服务器发送给设备的某些属性是设备不希望收到的属性时,可以定义基于接收方向的属性禁用规则,使得设备接收 RADIUS 报文时,不处理报文中的该属性。

当某些类型的属性是设备不希望处理的属性时,可以定义基于类型的属性禁用规则。

只有在 RADIUS 属性解释功能开启之后, RADIUS 属性禁用规则才能生效。

一个属性只能按照一种方式(按报文类型或报文处理方向)进行禁用。

执行 **undo attribute reject** 命令时,如果不指定属性名称,则表示删除所有 RADIUS 属性禁用规则。

【举例】

在 RADIUS DAE 服务器视图下,配置一条 RADIUS 属性禁用规则,指定禁用发送的 DAE 报文中的 Connect-Info 属性。

```
<Sysname> system-view
```

```
[Sysname] radius dynamic-author server
```

```
[Sysname-radius-da-server] attribute reject Connect-Info sent
```

【相关命令】

- **attribute translate**

1.3.9 attribute reject (RADIUS scheme view)

attribute reject 命令用来配置 RADIUS 属性禁用规则。

undo attribute reject 命令用来删除 RADIUS 属性禁用规则。

【命令】

```
attribute reject attr-name { { access-accept | access-request | accounting }  
* | { received | sent } * }
```

```
undo attribute reject [ attr-name ]
```

【缺省情况】

不存在 RADIUS 属性禁用规则。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

attr-name: RADIUS 属性名称，为 1~63 个字符的字符串，不区分大小写。该属性必须为系统支持的属性。

access-accept: RADIUS 认证成功报文。

access-request: RADIUS 认证请求报文。

accounting: RADIUS 计费报文。

received: 接收到的 RADIUS 报文。

sent: 发送的 RADIUS 报文。

【使用指导】

当设备发送的 RADIUS 报文中携带了 RADIUS 服务器无法识别的属性时，可以定义基于发送方向的属性禁用规则，使得设备发送 RADIUS 报文时，将该属性从报文中删除。

当 RADIUS 服务器发送给设备的某些属性是不希望收到的属性时，可以定义基于接收方向的属性禁用规则，使得设备接收 RADIUS 报文时，不处理报文中的该属性。

当某些类型的属性是设备不希望处理的属性时，可以定义基于类型的属性禁用规则。

只有在 RADIUS 属性解释功能开启之后，RADIUS 属性禁用规则才能生效。

一个属性只能按照一种方式（按报文类型或报文处理方向）进行禁用。

执行 **undo attribute reject** 命令时，如果不指定属性名称，则表示删除所有 RADIUS 属性禁用规则。

【举例】

在 RADIUS 方案 radius1 中，配置一条 RADIUS 属性禁用规则，指定禁用发送的 RADIUS 报文中的 Connect-Info 属性。

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] attribute reject Connect-Info sent
```

【相关命令】

- **attribute translate**

1.3.10 attribute remanent-volume

attribute remanent-volume 命令用来配置 RADIUS Remanent-Volume 属性的流量单位。

undo attribute remanent-volume 命令用来恢复缺省情况。

【命令】

attribute remanent-volume unit { byte | giga-byte | kilo-byte | mega-byte }

undo attribute remanent-volume unit

【缺省情况】

Remanent-Volume 属性的流量单位是千字节。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

byte: 表示流量单位为字节。
giga-byte: 表示流量单位为千兆字节。
kilo-byte: 表示流量单位为千字节。
mega-byte: 表示流量单位为兆字节。

【使用指导】

Remanent-Volume 属性为 UNIS 自定义 RADIUS 属性，携带在 RADIUS 服务器发送给接入设备的认证响应或实时计费响应报文中，用于向接入设备通知在线用户的剩余流量值。设备管理员通过本命令设置的流量单位应与 RADIUS 服务器上统计用户流量的单位保持一致，否则设备无法正确使用 Remanent-Volume 属性值对用户进行计费。

【举例】

在 RADIUS 方案 radius1 中，设置 RADIUS 服务器下发的 Remanent-Volume 属性的流量单位为千字节。

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] attribute remanent-volume unit kilo-byte
```

【相关命令】

- **display radius scheme**

1.3.11 attribute translate

attribute translate 命令用来开启 RADIUS 属性解释功能。
undo attribute translate 命令用来关闭 RADIUS 属性解释功能。

【命令】

attribute translate
undo attribute translate

【缺省情况】

RADIUS 属性解释功能处于关闭状态。

【视图】

RADIUS 方案视图/RADIUS DAE 服务器视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

不同厂商的 RADIUS 服务器所支持的 RADIUS 属性集有所不同,而且相同属性的用途也可能不同。为了兼容不同厂商的服务器的 RADIUS 属性,需要开启 RADIUS 属性解释功能,并定义相应的 RADIUS 属性转换规则和 RADIUS 属性禁用规则。

【举例】

在 RADIUS 方案 radius1 中,开启 RADIUS 属性解释功能。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute translate
```

【相关命令】

- **attribute convert**
- **attribute reject**

1.3.12 attribute vendor-id 2011 version

attribute vendor-id 2011 version 命令用来配置 Vendor ID 为 2011 的 RADIUS 服务器版本号。

undo attribute vendor-id 2011 version 命令用来恢复缺省情况。

【命令】

```
attribute vendor-id 2011 version { 1.0 | 1.1 }
undo attribute vendor-id 2011 version
```

【缺省情况】

设备采用版本 1.0 与 Vendor ID 为 2011 的 RADIUS 服务器交互。

【视图】

RADIUS 方案视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

- 1.0:** 版本 1.0。
- 1.1:** 版本 1.1。

【使用指导】

当设备与 Vendor ID 为 2011 的 RADIUS 服务器交互时,需要保证本命令设置的服务器版本号与对端服务器的实际版本号一致,否则会导致部分 RADIUS 属性解析错误。该厂商相关 RADIUS 属性在设备上的解析情况如下:

- 当 RADIUS 服务器下发属性 HW_ARRT_26_1 时,如果设备采用 1.0 版本,则将该属性解析为用户的上行峰值速率;如果设备采用 1.1 版本,则将其解析为上行突发尺寸。
- 当 RADIUS 服务器下发属性 HW_ARRT_26_2 时,无论设备采用 1.0 版本或 1.1 版本,均将该属性解析为用户的上行平均速率。

- 当 RADIUS 服务器下发属性 HW_ARRT_26_3 时，如果设备采用 1.0 版本，则不处理该属性；如果设备采用 1.1 版本，则将其解析为上行峰值速率。
- 当 RADIUS 服务器下发属性 HW_ARRT_26_4 时，如果设备采用 1.0 版本，则将该属性解析为用户的下行峰值速率；如果设备采用 1.1 版本，则将其解析为下行突发尺寸。
- 当 RADIUS 服务器下发属性 HW_ARRT_26_5 时，无论设备采用 1.0 版本或 1.1 版本，均将该属性解析为用户的下行平均速率。
- 当 RADIUS 服务器下发属性 HW_ARRT_26_6 时，如果设备采用 1.0 版本，则不处理该属性；如果设备采用 1.1 版本，则将其解析为下行峰值速率。

【举例】

在 RADIUS 方案 radius1 中，配置 Vendor ID 为 2011 的 RADIUS 服务器版本号为 1.1。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute vendor-id 2011 version 1.1
```

【相关命令】

- **display radius scheme**

1.3.13 client

client 命令用来指定 RADIUS DAE 客户端。

undo client 命令用来删除指定的 RADIUS DAE 客户端。

【命令】

```
client { ip ipv4-address | ipv6 ipv6-address } [ key { cipher | simple }
string | vendor-id 2011 version { 1.0 | 1.1 } | vpn-instance
vpn-instance-name ] *
undo client { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance
vpn-instance-name ]
```

【缺省情况】

未指定 RADIUS DAE 客户端。

【视图】

RADIUS DAE 服务器视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip *ipv4-address*: RADIUS DAE 客户端 IPv4 地址。

ipv6 *ipv6-address*: RADIUS DAE 客户端 IPv6 地址。

key: 与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥。此共享密钥的设置必须与 RADIUS DAE 客户端的共享密钥设置保持一致。如果此处未指定本参数，则对应的 RADIUS DAE 客户端上也必须未指定。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

vendor-id 2011: 表示 RADIUS DAE 客户端的 Vendor-ID 为 2011。

version: 版本号。

1.0: 版本 1.0。

1.1: 版本 1.1。

string: 密钥字符串，区分大小写。明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。

vpn-instance vpn-instance-name: RADIUS DAE 客户端所属的 VPN 实例。

vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 RADIUS DAE 客户端位于公网中。

【使用指导】

开启 RADIUS DAE 服务之后，设备会监听并处理指定的 RADIUS DAE 客户端发起的 DAE 请求消息（用于动态授权修改或断开连接），并向其发送应答消息。对于非指定的 RADIUS DAE 客户端的 DAE 报文进行丢弃处理。

可通过多次执行本命令指定多个 RADIUS DAE 客户端。

缺省情况下，设备支持与版本 1.0 的 Vendor-ID 为 2011 的 RADIUS DAE 客户端通信，若对端为 1.1 版本，则需要通过指定 **vendor-id 2011 version 1.1** 参数来保证版本的一致性，否则无法正确解析部分 DAE 请求。

【举例】

设置 RADIUS DAE 客户端的 IP 地址为 10.110.1.2，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 123456。

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] client ip 10.110.1.2 key simple 123456
```

【相关命令】

- **radius dynamic-author server**
- **port**

1.3.14 data-flow-format (RADIUS scheme view)

data-flow-format 命令用来配置发送到 RADIUS 服务器的数据流及数据包的单位。

undo data-flow-format 命令用来恢复缺省情况。

【命令】

```
data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet  
{ giga-packet | kilo-packet | mega-packet | one-packet } } *  
undo data-flow-format { data | packet }
```

【缺省情况】

数据流的单位为字节，数据包的单位为包。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

data: 设置数据流的单位。

- **byte:** 数据流的单位为字节。
- **giga-byte:** 数据流的单位千兆字节。
- **kilo-byte:** 数据流的单位为千字节。
- **mega-byte:** 数据流的单位为兆字节。

packet: 设置数据包的单位。

- **giga-packet:** 数据包的单位为千兆包。
- **kilo-packet:** 数据包的单位为千包。
- **mega-packet:** 数据包的单位为兆包。
- **one-packet:** 数据包的单位为包。

【使用指导】

设备上配置的发送给 RADIUS 服务器的数据流单位及数据包单位应与 RADIUS 服务器上的流量统计单位保持一致，否则无法正确计费。

【举例】

在 RADIUS 方案 radius1 中，设置发往 RADIUS 服务器的数据流单位为千字节、数据包单位为千包。

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

【相关命令】

- **display radius scheme**

1.3.15 display radius scheme

display radius scheme 命令用来显示 RADIUS 方案的配置信息。

【命令】

display radius scheme [*radius-scheme-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

context-admin
context-operator

【参数】

radius-scheme-name: RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。如果不指定该参数, 则表示所有 RADIUS 方案。

【举例】

显示所有 RADIUS 方案的配置信息。

<Sysname> display radius scheme

Total 1 RADIUS schemes

RADIUS scheme name: radius1

Index : 0

Primary authentication server:

IP : 2.2.2.2 Port: 1812

VPN : vpn1

State: Active

Test profile: 132

Probe username: test

Probe interval: 60 minutes

Primary accounting server:

IP : 1.1.1.1 Port: 1813

VPN : Not configured

State: Active

Second authentication server:

IP : 3.3.3.3 Port: 1812

VPN : Not configured

State: Block

Test profile: Not configured

Second accounting server:

IP : 3.3.3.3 Port: 1813

VPN : Not configured

State: Block (Mandatory)

Accounting-On function : Enabled

extended function : Disabled

retransmission times : 5

retransmission interval(seconds) : 2

Timeout Interval(seconds) : 3

Retransmission Times : 3

Retransmission Times for Accounting Update : 5

Server Quiet Period(minutes) : 5

Realtime Accounting Interval(seconds) : 22

NAS IP Address : 1.1.1.1

VPN : Not configured

User Name Format : with-domain

Data flow unit : Megabyte

```

Packet unit                : One
Attribute 15 check-mode    : Strict
Attribute 25               : CAR
Attribute Remanent-Volume unit : Mega
RADIUS server version (vendor ID 2011) : 1.0
Attribute 31 MAC format    : hh:hh:hh:hh:hh:hh
Attribute 17 carry old password : Disabled

```

表1-4 display radius scheme 命令显示信息描述表

字段	描述
Total 1 RADIUS schemes.	共计1个RADIUS方案
RADIUS scheme name	RADIUS方案的名称
Index	RADIUS方案的索引号
Primary authentication server	主RADIUS认证服务器
Primary accounting server	主RADIUS计费服务器
Second authentication server	从RADIUS认证服务器
Second accounting server	从RADIUS计费服务器
IP	RADIUS认证/计费服务器IP地址 未配置时，显示为Not configured
Port	RADIUS认证/计费服务器接入端口号 未配置时，显示缺省值
State	RADIUS认证/计费服务器目前状态 - Active: 激活状态 - Block: 自动转换的静默状态 - Block(Mandatory): 手工配置的静默状态
VPN	RADIUS认证/计费服务器或RADIUS方案所在的VPN 未配置时，显示为Not configured
Test profile	探测服务器状态使用的模板名称
Probe username	探测服务器状态使用的用户名
Probe interval	探测服务器状态的周期（单位为分钟）
Accounting-On function	accounting-on功能的开启情况
extended function	accounting-on扩展功能的开启情况
retransmission times	accounting-on报文的发送尝试次数
retransmission interval(seconds)	accounting-on报文的重发间隔（单位为秒）
Timeout Interval(seconds)	RADIUS服务器超时时间（单位为秒）
Retransmission Times	发送RADIUS报文的最大尝试次数
Retransmission Times for Accounting Update	实时计费更新报文的最大尝试次数

字段	描述
Server Quiet Period(minutes)	RADIUS服务器恢复激活状态的时间（单位为分钟）
Realtime Accounting Interval(seconds)	实时计费更新报文的发送间隔（单位为秒）
NAS IP Address	发送RADIUS报文的源IP地址或源接口 未配置时，显示为Not configured
User Name Format	发送给RADIUS服务器的用户名格式 • with-domain: 携带域名 • without-domain: 不携带域名 • keep-original: 与用户输入保持一致
Data flow unit	数据流的单位
Packet unit	数据包的单位
Attribute 15 check-mode	对RADIUS Attribute 15的检查方式，包括以下两种取值： • Strict: 表示使用 RADIUS 标准属性值和私有扩展的属性值进行检查 • Loose: 表示使用 RADIUS 标准属性值进行检查
Attribute 25	对RADIUS Attribute 25的处理，包括以下两种取值： • Standard: 表示不对 RADIUS Attribute 25 进行解析 • CAR: 表示将 RADIUS 25 号属性解析为 CAR 参数
Attribute Remanent-Volume unit	RADIUS Remanent-Volume属性的流量单位
RADIUS server version (vendor ID 2011)	Vendor ID为2011的RADIUS服务器版本号，包括1.0和1.1两种取值
Attribute 31 MAC format	RADIUS Attribute 31中携带的MAC地址格式

1.3.16 display radius statistics

display radius statistics 命令用来显示 RADIUS 报文的统计信息。

【命令】

display radius statistics

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 RADIUS 报文的统计信息。

<Sysname> display radius statistics

	Auth.	Acct.	SessCtrl.
Request Packet:	0	0	0
Retry Packet:	0	0	-
Timeout Packet:	0	0	-
Access Challenge:	0	-	-
Account Start:	-	0	-
Account Update:	-	0	-
Account Stop:	-	0	-
Terminate Request:	-	-	0
Set Policy:	-	-	0
Packet With Response:	0	0	0
Packet Without Response:	0	0	-
Access Rejects:	0	-	-
Dropped Packet:	0	0	0
Check Failures:	0	0	0

表1-5 display radius statistics 命令显示信息描述表

字段	描述
Auth.	认证报文
Acct.	计费报文
SessCtrl.	Session-control报文
Request Packet	发送的请求报文总数
Retry Packet	重传的请求报文总数
Timeout Packet	超时的请求报文总数
Access Challenge	Access challenge报文数
Account Start	计费开始报文的数目
Account Update	计费更新报文的数目
Account Stop	计费结束报文的数目
Terminate Request	服务器强制下线报文的数目
Set Policy	更新用户授权信息报文的数目
Packet With Response	有回应信息的报文数
Packet Without Response	无回应信息的报文数
Access Rejects	认证拒绝报文的数目
Dropped Packet	丢弃的报文数
Check Failures	报文校验错误的报文数目

【相关命令】

- **reset radius statistics**

1.3.17 key (RADIUS scheme view)

key 命令用来配置 RADIUS 报文的共享密钥。

undo key 命令用来删除 RADIUS 报文的共享密钥。

【命令】

```
key { accounting | authentication } { cipher | simple } string
undo key { accounting | authentication }
```

【缺省情况】

未配置 RADIUS 报文的共享密钥。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

accounting: 指定 RADIUS 计费报文的共享密钥。

authentication: 指定 RADIUS 认证报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。

【使用指导】

设备优先采用配置 RADIUS 认证/计费服务器时指定的报文共享密钥，本配置中指定的报文共享密钥仅在配置 RADIUS 认证/计费服务器时未指定相应密钥的情况下使用。

必须保证设备上设置的共享密钥与 RADIUS 服务器上的完全一致。

【举例】

在 RADIUS 方案 radius1 中，配置计费报文的共享密钥为明文 ok。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting simple ok
```

【相关命令】

- **display radius scheme**

1.3.18 nas-ip (RADIUS scheme view)

nas-ip 命令用来设置设备发送 RADIUS 报文使用的源 IP 地址。

undo nas-ip 命令用来删除指定类型的发送 RADIUS 报文使用的源 IP 地址。

【命令】

```
nas-ip { ipv4-address | ipv6 ipv6-address }  
undo nas-ip [ ipv6 ]
```

【缺省情况】

未指定设备发送 RADIUS 报文使用的源 IP 地址，使用系统视图下由命令 **radius nas-ip** 指定的源 IP 地址。

【视图】

RADIUS 方案视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

ipv4-address: 指定的源 IPv4 地址，应该为本机的地址，禁止配置全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

ipv6 ipv6-address: 指定的源 IPv6 地址，应该为本机的地址，必须是单播地址，不能为环回地址与本地链路地址。

【使用指导】

RADIUS 服务器上通过 IP 地址来标识接入设备，并根据收到的 RADIUS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证或计费请求。因此，为保证 RADIUS 报文可被服务器正常接收并处理，接入设备上发送 RADIUS 报文使用的源地址必须与 RADIUS 服务器上指定的接入设备的 IP 地址保持一致。

为避免物理接口故障时从服务器返回的报文不可达，推荐使用 Loopback 接口地址为发送 RADIUS 报文使用的源 IP 地址。

RADIUS 方案视图和系统视图下均可以配置发送 RADIUS 报文使用的源 IP 地址，具体生效情况如下：

- RADIUS 方案视图下配置的源 IP 地址（通过 **nas-ip** 命令）只对本方案有效。
- 系统视图下的配置的源 IP 地址（通过 **radius nas-ip** 命令）对所有 RADIUS 方案有效。
- RADIUS 方案视图下的设置具有更高的优先级。

一个 RADIUS 方案视图下，最多允许指定一个 IPv4 源地址和一个 IPv6 源地址。

如果 **undo nas-ip** 命令中不指定任何参数，则表示删除配置的发送 RADIUS 报文使用的源 IPv4 地址。

【举例】

在 RADIUS 方案 radius1 中，设置设备发送 RADIUS 报文使用的源 IP 地址为 10.1.1.1。

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] nas-ip 10.1.1.1
```

【相关命令】

- **display radius scheme**
- **radius nas-ip**

1.3.19 port

port 命令用来指定 RADIUS DAE 服务端口。

undo port 命令用来恢复缺省情况。

【命令】

port *port-number*
undo port

【缺省情况】

RADIUS DAE 服务端口为 3799。

【视图】

RADIUS DAE 服务器视图

【缺省用户角色】

network-admin
context-admin

【参数】

port-number: DAE 服务器接收 DAE 请求消息的 UDP 端口，取值范围为 1~65535。

【使用指导】

必须保证设备上的 RADIUS DAE 服务端口与 RADIUS DAE 客户端发送 DAE 报文的目的 UDP 端口一致。

【举例】

开启 RADIUS DAE 服务后，指定 DAE 服务端口为 3790。

```
<Sysname> system-view  
[Sysname] radius dynamic-author server  
[Sysname-radius-da-server] port 3790
```

【相关命令】

- **client**
- **radius dynamic-author server**

1.3.20 primary accounting (RADIUS scheme view)

primary accounting 命令用来配置主 RADIUS 计费服务器。

undo primary accounting 命令用来恢复缺省情况。

【命令】

primary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *

undo primary accounting

【缺省情况】

未配置主 RADIUS 计费服务器。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-address: 主 RADIUS 计费服务器的 IPv4 地址。

ipv6 ipv6-address: 主 RADIUS 计费服务器的 IPv6 地址。

port-number: 主 RADIUS 计费服务器的 UDP 端口号, 取值范围为 1~65535, 缺省值为 1813。

key: 与主 RADIUS 计费服务器交互的计费报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥, 该密钥将以密文形式存储。

string: 密钥字符串, 区分大小写。明文密钥为 1~64 个字符的字符串; 密文密钥为 1~117 个字符的字符串。

vpn-instance vpn-instance-name: 主 RADIUS 计费服务器所属的 VPN 实例。

vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示主 RADIUS 计费服务器位于公网中。

【使用指导】

配置的主计费服务器的 UDP 端口号以及计费报文的共享密钥必须与服务器的配置保持一致。

在同一个方案中指定的主计费服务器和从计费服务器的 VPN、IP 地址、端口号不能完全相同。

设备与主计费服务器通信时优先使用本命令设置的共享密钥, 如果此处未设置, 则使用 **key accounting** 命令设置的共享密钥。

如果在计费开始请求报文发送过程中修改或删除了正在使用的主计费服务器配置, 则设备在与当前服务器通信超时后, 将会重新按照优先级顺序开始依次查找状态为 **active** 的服务器进行通信; 如果在线用户正在使用的计费服务器被删除, 则设备将无法发送用户的实时计费请求和停止计费请求, 且停止计费报文不会被缓存到本地, 这将造成对用户计费的不准确。

【举例】

在 RADIUS 方案 radius1 中, 配置主计费服务器的 IP 地址为 10.110.1.2, 使用 UDP 端口 1813 提供 RADIUS 计费服务, 计费报文的共享密钥为明文 123456TESTacct&!

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813 key simple 123456TESTacct&!
```

【相关命令】

- **display radius scheme**
- **key** (RADIUS scheme view)

- **secondary accounting** (RADIUS scheme view)

1.3.21 primary authentication (RADIUS scheme view)

primary authentication 命令用来配置主 RADIUS 认证服务器。

undo primary authentication 命令用来恢复缺省情况。

【命令】

```
primary authentication { ipv4-address | ipv6 ipv6-address } [ port-number |
key { cipher | simple } string | test-profile profile-name | vpn-instance
vpn-instance-name ] *
undo primary authentication
```

【缺省情况】

未配置 RADIUS 主认证服务器。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-address: 主 RADIUS 认证服务器的 IPv4 地址。

ipv6 ipv6-address: 主 RADIUS 认证服务器的 IPv6 地址。

port-number: 主 RADIUS 认证服务器的 UDP 端口号,取值范围为 1~65535,缺省值为 1812。
此端口号必须与服务器提供认证服务的端口号保持一致。

key: 与主 RADIUS 认证服务器交互的认证报文的共享密钥。此共享密钥必须与服务器上配置的共享密钥保持一致。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥,该密钥将以密文形式存储。

string: 密钥字符串,区分大小写。明文密钥为 1~64 个字符的字符串;密文密钥为 1~117 个字符的字符串。

test-profile profile-name: RADIUS 服务器探测模板名称,为 1~31 个字符的字符串,区分大小写。

vpn-instance vpn-instance-name: 主 RADIUS 认证服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称,为 1~31 个字符的字符串,区分大小写。如果未指定本参数,则表示主 RADIUS 认证服务器位于公网中。

【使用指导】

配置的主认证服务器的 UDP 端口号以及认证报文的共享密钥必须与服务器的配置保持一致。

在同一个方案中指定的主认证服务器和从认证服务器的 VPN、IP 地址、端口号不能完全相同。

设备与主认证服务器通信时优先使用本命令设置的共享密钥,如果本命令中未设置,则使用 **key authentication** 命令设置的共享密钥。

RADIUS 认证服务器引用了存在的服务器探测模板后，将会触发对该服务器的探测功能。

如果在认证过程中修改或删除了正在使用的主认证服务器配置，则设备在与当前服务器通信超时后，将会重新按照优先级顺序开始依次查找状态为 **active** 的服务器进行通信。

【举例】

在 RADIUS 方案 radius1 中，配置主认证服务器的 IP 地址为 10.110.1.1，使用 UDP 端口 1812 提供 RADIUS 认证/授权服务，认证报文的共享密钥为明文 123456TESTauth&!

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812 key simple
123456TESTauth&!
```

【相关命令】

- **display radius scheme**
- **key** (RADIUS scheme view)
- **radius-server test-profile**
- **secondary authentication** (RADIUS scheme view)
- **vpn-instance** (RADIUS scheme view)

1.3.22 radius attribute extended

radius attribute extended 命令用来定义 RADIUS 扩展属性。

undo radius attribute extended 命令用来删除定义的 RADIUS 扩展属性。

【命令】

```
radius attribute extended attribute-name [ vendor vendor-id ] code
attribute-code type { binary | date | integer | interface-id | ip | ipv6 |
ipv6-prefix | octets | string }
undo radius attribute extended [ attribute-name ]
```

【缺省情况】

不存在自定义 RADIUS 扩展属性。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

attribute-name: RADIUS 属性名称，为 1~63 个字符的字符串，不区分大小写。该名称不能与系统已支持的（包括标准的以及自定义的）RADIUS 属性名称相同。

vendor vendor-id: RADIUS 属性所属的设备厂商标识。**vendor-id** 为厂商标识号码，取值范围为 1~65535。如果不指定该参数，则表示 RADIUS 属性为标准属性。

code attribute-code: RADIUS 属性在 RADIUS 属性集里的序号，取值范围为 1~255。

type: 属性内容的数据类型，包括以下取值：

- **binary:** 二进制类型。
- **date:** 时间类型。
- **integer:** 整数类型。
- **interface-id:** 接口 ID 类型。
- **ip:** IPv4 地址类型。
- **ipv6:** IPv6 地址类型。
- **ipv6-prefix:** IPv6 地址前缀类型。
- **octets:** 八进制类型。
- **string:** 字符串类型。

【使用指导】

当系统需要支持其他厂商的私有 RADIUS 属性时，可以通过 **radius attribute extended** 命令为其定义为一个扩展属性，并通过 **attribute convert** 命令将其映射到系统可以识别的一个已知属性。这样，当 RADIUS 服务器发送给设备的 RADIUS 报文中携带了此类不可识别的私有属性时，设备将根据已定义的属性转换规则将其转换为可处理的属性。同理，设备在发送 RADIUS 报文时也可以将自己可识别的属性转换为服务器能识别的属性。

每一个 RADIUS 属性有唯一的属性名称，且该属性的名称、设备厂商标识以及序号的组合必须在设备上唯一。

执行 **undo radius attribute extended** 命令时，如果不指定属性名称，则表示删除所有已定义 RADIUS 扩展属性。

【举例】

配置一个 RADIUS 扩展属性，名称为 Owner-Password，Vendor ID 为 122，属性序号为 80，类型为字符串。

```
<Sysname> system-view
```

```
[Sysname] radius attribute extended Owner-Password vendor 122 code 80 type string
```

【相关命令】

- **attribute convert**
- **attribute reject**

1.3.23 radius dscp

radius dscp 命令用来配置 RADIUS 协议报文的 DSCP 优先级。

undo radius dscp 命令用来恢复缺省情况。

【命令】

```
radius [ ipv6 ] dscp dscp-value
```

```
undo radius [ ipv6 ] dscp
```

【缺省情况】

RADIUS 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6: 表示设置 IPv6 RADIUS 报文。若不指定该参数，则表示设置 IPv4 RADIUS 报文。

dscp-value: RADIUS 报文的 DSCP 优先级，取值范围为 0～63。取值越大，优先级越高。

【使用指导】

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

通过本命令可以指定设备发送的 RADIUS 报文携带的 DSCP 优先级的取值。

【举例】

配置 IPv4 RADIUS 报文的 DSCP 优先级为 10。

```
<Sysname> system-view  
[Sysname] radius dscp 10
```

1.3.24 radius dynamic-author server

radius dynamic-author server 命令用来开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

undo radius dynamic-author server 命令用来关闭 RADIUS DAE 服务。

【命令】

radius dynamic-author server

undo radius dynamic-author server

【缺省情况】

RADIUS DAE 服务处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启 RADIUS DAE 服务后，设备将会监听指定的 RADIUS DAE 客户端发送的 DAE 请求消息，然后根据请求消息修改用户授权信息、断开用户连接请求。

【举例】

开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

```
<Sysname> system-view  
[Sysname] radius dynamic-author server
```

[Sysname-radius-da-server]

【相关命令】

- **client**
- **port**

1.3.25 radius nas-ip

radius nas-ip 命令用来设置设备发送 RADIUS 报文使用的源 IP 地址。

undo radius nas-ip 命令用来删除指定的发送 RADIUS 报文使用的源 IP 地址。

【命令】

radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

undo radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

【缺省情况】

未指定发送 RADIUS 报文使用的源 IP 地址，设备将使用到达 RADIUS 服务器的路由出接口的主 IPv4 地址或 IPv6 地址作为发送 RADIUS 报文的源 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4-address: 指定的源 IPv4 地址，应该为本机的地址，不能为全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

ipv6 ipv6-address: 指定的源 IPv6 地址，应该为本机的地址，必须是单播地址，不能为环回地址与本地链路地址。

vpn-instance vpn-instance-name: 指定私网源 IP 地址所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若不指定该参数，则表示配置的是公网源地址。

【使用指导】

RADIUS 服务器上通过 IP 地址来标识接入设备，并根据收到的 RADIUS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证或计费请求。为保证 RADIUS 报文可被服务器正常接收并处理，接入设备上发送 RADIUS 报文使用的源地址必须与 RADIUS 服务器上指定的接入设备的 IP 地址保持一致。

为避免物理接口故障时从服务器返回的报文不可达，推荐使用 Loopback 接口地址为发送 RADIUS 报文使用的源 IP 地址。

RADIUS 方案视图和系统视图下均可以配置发送 RADIUS 报文使用的源 IP 地址，具体情况如下：

- RADIUS 方案视图下配置的源 IP 地址（通过 **nas-ip** 命令）只对本 RADIUS 方案有效。

- 系统视图下的配置的源 IP 地址（通过 **radius nas-ip** 命令）对所有 RADIUS 方案有效。
- RADIUS 方案视图下的设置具有更高的优先级。

【举例】

设置设备发送 RADIUS 报文使用的源 IP 地址为 129.10.10.1。

```
<Sysname> system-view
[Sysname] radius nas-ip 129.10.10.1
```

【相关命令】

- **nas-ip** (RADIUS scheme view)

1.3.26 radius scheme

radius scheme 命令用来创建 RADIUS 方案，并进入 RADIUS 方案视图。如果指定的 RADIUS 方案已经存在，则直接进入 RADIUS 方案视图。

undo radius scheme 命令用来删除指定的 RADIUS 方案。

【命令】

```
radius scheme radius-scheme-name
undo radius scheme radius-scheme-name
```

【缺省情况】

不存在 RADIUS 方案。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

radius-scheme-name: RADIUS 方案的名称，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

一个 RADIUS 方案可以同时被多个 ISP 域引用。

系统最多支持配置 16 个 RADIUS 方案。

【举例】

创建名为 radius1 的 RADIUS 方案并进入其视图。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

【相关命令】

- **display radius scheme**

1.3.27 radius session-control client

radius session-control client 命令用来指定 session control 客户端。

undo radius session-control client 命令用来删除指定的 session control 客户端。

【命令】

```
radius session-control client { ip ipv4-address | ipv6 ipv6-address } [ key  
{ cipher | simple } string | vpn-instance vpn-instance-name ] *  
undo radius session-control client { all | { ip ipv4-address | ipv6  
ipv6-address } [ vpn-instance vpn-instance-name ] }
```

【缺省情况】

未指定 session control 客户端。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip ipv4-address: session control 客户端的 IPv4 地址。

ipv6 ipv6-address: session control 客户端的 IPv6 地址。

key: 与 session control 客户端交互的计费报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。

vpn-instance vpn-instance-name: session control 客户端所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果不指定本参数，则表示 session control 客户端属于公网。

all: 表示所有 session control 客户端。

【使用指导】

设备和 UNIS 的 iMC RADIUS 服务器配合使用时，将作为 session control 服务器端与其交互，因此需要指定 session control 客户端来验证收到的 session control 报文的合法性。当设备收到服务器发送的 session control 报文时，直接根据报文的源 IP 地址、VPN 属性与已有的 session control 客户端配置进行匹配，并使用匹配到的客户端共享密钥对报文进行验证。如果报文匹配失败或设备上未配置 session control 客户端，则使用已有的 RADIUS 方案配置进行匹配，并使用匹配到的认证服务器的共享密钥对报文进行验证。

指定的 session control 客户端仅在 RADIUS session control 功能处于开启状态时生效。

配置的 session control 客户端参数必须与服务器的配置保持一致。

系统支持指定多个 session control 客户端。

【举例】

```
# 指定一个 session control 客户端 IP 地址为 10.110.1.2，共享密钥为明文 12345。
<Sysname> system-view
[Sysname] radius session-control client ip 10.110.1.2 key simple 12345
```

【相关命令】

- **radius session-control enable**

1.3.28 radius session-control enable

radius session-control enable 命令用来开启 RADIUS session control 功能。

undo radius session-control enable 命令用来关闭 RADIUS session control 功能。

【命令】

```
radius session-control enable
undo radius session-control enable
```

【缺省情况】

RADIUS session control 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

UNIS iMC RADIUS 服务器使用 session control 报文向设备发送授权信息的动态修改请求以及断开连接请求。开启 RADIUS session control 功能后，设备会打开知名 UDP 端口 1812 来监听并接收 RADIUS 服务器发送的 session control 报文。

该功能仅能和 UNIS iMC 的 RADIUS 服务器配合使用。

【举例】

```
# 开启 RADIUS session control 功能。
<Sysname> system-view
[Sysname] radius session-control enable
```

1.3.29 radius-server test-profile

radius-server test-profile 命令用来配置 RADIUS 服务器探测模板。

undo radius-server test-profile 命令用来删除指定的 RADIUS 服务器探测模板。

【命令】

```
radius-server test-profile profile-name username name [ interval interval ]
undo radius-server test-profile profile-name
```

【缺省情况】

不存在 RADIUS 服务器探测模板。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

profile-name: 探测模板名称，为 1~31 个字符的字符串，区分大小写。

username name: 探测报文中的用户名，为 1~253 个字符的字符串，区分大小写。

interval interval: 发送探测报文的周期，取值范围为 1~3600，单位为分钟，缺省值为 60。

【使用指导】

RADIUS 方案视图下的 RADIUS 服务器配置成功引用了某探测模板后，若被引用的探测模板存在，则设备将会启动对该 RADIUS 服务器的可达性探测。若被引用的探测模板暂不存在，则当该探测模板被成功配置时，针对该服务器的探测过程才会开始。

设备采用探测模板中配置的探测用户名、密码构造一个认证请求报文，并在探测周期内选择随机时间点向引用了探测模板的 RADIUS 服务器发送该报文。如果在本次探测周期内收到服务器的认证响应报文，则认为当前探测周期内该服务器可达。

删除一个 RADIUS 服务器探测模板时，引用该探测模板的所有 RADIUS 方案中的 RADIUS 服务器的探测功能也会被关闭。

系统支持配置多个 RADIUS 服务器探测模板。

【举例】

配置 RADIUS 服务器探测模板 abc，探测报文中携带的用户名为 admin，探测报文的发送间隔为 10 分钟。

```
<Sysname> system-view
```

```
[Sysname] radius-server test-profile abc username admin interval 10
```

【相关命令】

- **primary authentication** (RADIUS scheme view)
- **secondary authentication** (RADIUS scheme view)

1.3.30 reset radius statistics

reset radius statistics 命令用来清除 RADIUS 协议的统计信息。

【命令】

reset radius statistics

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【举例】

清除 RADIUS 协议的统计信息。
<Sysname> reset radius statistics

【相关命令】

- **display radius statistics**

1.3.31 retry

retry 命令用来设置发送 RADIUS 报文的最大尝试次数。

undo retry 命令用来恢复缺省情况。

【命令】

retry *retries*
undo **retry**

【缺省情况】

发送 RADIUS 报文的最大尝试次数为 3 次。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

retries: 发送 RADIUS 报文的最大尝试次数，取值范围为 1~20。

【使用指导】

由于 RADIUS 协议采用 UDP 报文来承载数据，因此其通信过程是不可靠的。如果设备在应答超时定时器规定的时长内（由 **timer response-timeout** 命令配置）没有收到 RADIUS 服务器的响应，则设备有必要向 RADIUS 服务器重传 RADIUS 请求报文。如果累计的传送次数已达到最大传送次数而 RADIUS 服务器仍旧没有响应，则设备将认为本次请求失败。

需要注意的是：

- 发送 RADIUS 报文的最大尝试次数、RADIUS 服务器响应超时时间以及配置的 RADIUS 服务器总数，三者的乘积不能超过接入模块定义的用户认证超时时间，否则在 RADIUS 认证过程完成之前用户就有可能被强制下线。
- 设备在按照配置顺序尝试与下一个 RADIUS 服务器通信之前，会首先判断当前累计尝试持续时间是否达到或超过 300 秒，如果超过或达到 300 秒，将不再向下一个 RADIUS 服务器发送 RADIUS 请求报文，即认为该 RADIUS 请求发送失败。因此，为了避免某些已部署的 RADIUS 服务器由于此超时机制而无法被使用到，建议基于配置的 RADIUS 服务器总数，合理设置发送 RADIUS 报文的最大尝试次数以及 RADIUS 服务器响应超时时间。

【举例】

在 RADIUS 方案 radius1 中，设置发送 RADIUS 报文的最大尝试次数为 5 次。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry 5
```

【相关命令】

- **radius scheme**
- **timer response-timeout** (RADIUS scheme view)

1.3.32 retry realtime-accounting

retry realtime-accounting 命令用来设置允许发起实时计费请求的最大尝试次数。

undo retry realtime-accounting 命令用来恢复缺省情况。

【命令】

```
retry realtime-accounting retries
undo retry realtime-accounting
```

【缺省情况】

设备允许发起实时计费请求的最大尝试次数为 5。

【视图】

RADIUS 方案视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

retries: 允许发起实时计费请求的最大尝试次数，取值范围为 1~255。

【使用指导】

RADIUS 服务器通常通过连接超时定时器来判断用户是否在线。如果 RADIUS 服务器在连接超时时间之内一直收不到设备传来的实时计费报文，它会认为线路或设备故障并停止对用户记帐。为了配合 RADIUS 服务器的这种特性，有必要在不可预见的故障条件下，尽量保持设备端与 RADIUS 服务器同步切断用户连接。设备提供对实时计费请求连续无响应次数限制的设置，保证设备尽可能得在 RADIUS 服务器的连接超时时长内向 RADIUS 服务器尝试发出实时计费请求。如果设备没有收到响应的次数超过了设定的限度，才会切断用户连接。

假设 RADIUS 服务器的应答超时时长（**timer response-timeout** 命令设置）为 3 秒，发送 RADIUS 报文的最大尝试次数（**retry** 命令设置）为 3，设备的实时计费间隔（**timer realtime-accounting** 命令设置）为 12 分钟，设备允许实时计费无响应的最大次数为 5 次（**retry realtime-accounting** 命令设置），则其含义为：设备每隔 12 分钟发起一次计费请求，如果 3 秒钟得不到回应就重新发起一次请求，如果 3 次发送都没有得到回应就认为该次实时计费失败，然后每隔 12 分钟再发送一次，5 次均失败以后，设备将切断用户连接。

【举例】

在 RADIUS 方案 radius1 中，设置允许发起实时计费请求的最大尝试次数为 10。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry realtime-accounting 10
```

【相关命令】

- **retry**
- **timer realtime-accounting** (RADIUS scheme view)
- **timer response-timeout** (RADIUS scheme view)

1.3.33 secondary accounting (RADIUS scheme view)

secondary accounting 命令用来配置从 RADIUS 计费服务器。

undo secondary accounting 命令用来删除指定的从 RADIUS 计费服务器。

【命令】

```
secondary accounting { ipv4-address | ipv6 ipv6-address } [ port-number |  
key { cipher | simple } string ] *  
undo secondary accounting [ { ipv4-address | ipv6 ipv6-address } ]
```

【缺省情况】

未配置从 RADIUS 计费服务器。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4-address: 从 RADIUS 计费服务器的 IPv4 地址。

ipv6 ipv6-address: 从 RADIUS 计费服务器的 IPv6 地址。

port-number: 从 RADIUS 计费服务器的 UDP 端口号，取值范围为 1~65535，缺省值为 1813。

key: 与从 RADIUS 计费服务器交互的计费报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。

vpn-instance vpn-instance-name: 从 RADIUS 计费服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示从 RADIUS 计费服务器位于公网中。

【使用指导】

配置的从计费服务器的 UDP 端口号以及计费报文的共享密钥必须与服务器的配置保持一致。

每个 RADIUS 方案中最多支持配置 16 个从 RADIUS 计费服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。

在同一个方案中指定的主计费服务器和从计费服务器的 VPN、IP 地址、端口号不能完全相同，并且各从计费服务器的 VPN、IP 地址、端口号也不能完全相同。

设备与从计费服务器通信时优先使用本命令设置的共享密钥，如果此处未设置，则使用命令 **key accounting** 命令设置的共享密钥。

如果在计费开始请求报文发送过程中删除了正在使用的从服务器配置，则设备在与当前服务器通信超时后，将会重新按照优先级顺序开始依次查找状态为 **active** 的服务器进行通信。

如果在线用户正在使用的计费服务器被删除，则设备将无法发送用户的实时计费请求和停止计费请求，且停止计费报文不会被缓存到本地。

【举例】

在 RADIUS 方案 radius1 中，配置从计费服务器的 IP 地址为 10.110.1.1，使用 UDP 端口 1813 提供 RADIUS 计费服务。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813
```

在 RADIUS 方案 radius2 中，配置两个从计费服务器，IP 地址分别为 10.110.1.1、10.110.1.2，且均使用 UDP 端口 1813 提供 RADIUS 计费服务。

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary accounting 10.110.1.1 1813
[Sysname-radius-radius2] secondary accounting 10.110.1.2 1813
```

【相关命令】

- **display radius scheme**
- **key** (RADIUS scheme view)
- **primary accounting**

1.3.34 secondary authentication (RADIUS scheme view)

secondary authentication 命令用来配置从 RADIUS 认证服务器。

undo secondary authentication 命令用来删除指定的从 RADIUS 认证服务器。

【命令】

```
secondary authentication { ipv4-address | ipv6 ipv6-address } [ port-number  
| key { cipher | simple } string | test-profile profile-name | vpn-instance  
vpn-instance-name ] *
```

```
undo secondary authentication [ { ipv4-address | ipv6 ipv6-address }  
[ port-number | vpn-instance vpn-instance-name ] * ]
```

【缺省情况】

未配置从 RADIUS 认证服务器。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4-address: 从 RADIUS 认证服务器的 IPv4 地址。

ipv6 ipv6-address: 从 RADIUS 认证服务器的 IPv6 地址。

port-number: 从 RADIUS 认证服务器的 UDP 端口号, 取值范围为 1~65535, 缺省值为 1812。

key: 与从 RADIUS 认证服务器交互的认证报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥, 该密钥将以密文形式存储。

string: 密钥字符串, 区分大小写。明文密钥为 1~64 个字符的字符串; 密文密钥为 1~117 个字符的字符串。

test-profile profile-name: RADIUS 服务器探测模板名称, 为 1~31 个字符的字符串, 区分大小写。

vpn-instance vpn-instance-name: 从 RADIUS 认证服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示从 RADIUS 认证服务器位于公网中。

【使用指导】

配置的从认证服务器的 UDP 端口号以及认证报文的共享密钥必须与服务器的配置保持一致。

每个 RADIUS 方案中最多支持配置 16 个从 RADIUS 认证服务器。当主服务器不可达时, 设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。

RADIUS 认证服务器引用了存在的服务器探测模板后, 将会触发对该服务器的探测功能。

在同一个方案中指定的主认证服务器和从认证服务器的 VPN、IP 地址、端口号不能完全相同, 并且各从认证服务器的 VPN、IP 地址、端口号也不能完全相同。

设备与从认证服务器通信时优先使用本命令设置的共享密钥, 如果此处未设置, 则使用命令 **key authentication** 命令设置的共享密钥。

如果在认证过程中删除了正在使用的从服务器配置, 则设备在与当前服务器通信超时后, 将会重新按照优先级顺序开始依次查找状态为 **active** 的服务器进行通信。

【举例】

在 RADIUS 方案 radius1 中, 配置从认证服务器的 IP 地址为 10.110.1.2, 使用 UDP 端口 1812 提供 RADIUS 认证/授权服务。

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```

在 RADIUS 方案 radius2 中, 配置两个从认证服务器, IP 地址分别为 10.110.1.1、10.110.1.2, 且均使用 UDP 端口 1812 提供 RADIUS 认证/授权服务。

```
<Sysname> system-view  
[Sysname] radius scheme radius2  
[Sysname-radius-radius2] secondary authentication 10.110.1.1 1812  
[Sysname-radius-radius2] secondary authentication 10.110.1.2 1812
```

【相关命令】

- **display radius scheme**
- **key** (RADIUS scheme view)
- **primary authentication** (RADIUS scheme view)
- **radius-server test-profile**
- **vpn-instance** (RADIUS scheme view)

1.3.35 snmp-agent trap enable radius

snmp-agent trap enable radius 命令用来开启 RADIUS 告警功能。

undo snmp-agent trap enable radius 命令用来关闭指定的 RADIUS 告警功能。

【命令】

```
snmp-agent trap enable radius [ accounting-server-down |  
accounting-server-up | authentication-error-threshold |  
authentication-server-down | authentication-server-up ] *  
undo snmp-agent trap enable radius [ accounting-server-down |  
accounting-server-up | authentication-error-threshold |  
authentication-server-down | authentication-server-up ] *
```

【缺省情况】

所有类型的 RADIUS 告警功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

accounting-server-down: 表示 RADIUS 计费服务器可达状态变为 down 时发送告警信息。

accounting-server-up: 表示 RADIUS 计费服务器可达状态变为 up 时发送告警信息。

authentication-error-threshold: 表示认证失败次数超过阈值时发送告警信息。该阈值为认证失败次数占认证请求总数的百分比数值,目前仅能通过 MIB 方式配置,取值范围为 1~100,缺省为 30。

authentication-server-down: 表示 RADIUS 认证服务器可达状态变为 down 时发送告警信息。

authentication-server-up: 表示 RADIUS 认证服务器可达状态变为 up 时发送告警信息。

【使用指导】

不指定任何参数时,表示开启或关闭所有类型的 RADIUS 告警功能。

开启 RADIUS 服务器告警功能后,系统将会生成以下几种告警信息:

- **RADIUS 服务器不可达的告警：**当 NAS 向 RADIUS 服务器发送计费或认证请求没有收到响应时，会重传请求，当重传次数达到最大传送次数时仍然没有收到响应时，则发送该告警信息。
- **RADIUS 服务器可达的告警：**当 **timer quiet** 定时器设定的时间到达后，NAS 将服务器的状态置为激活状态并发送该告警信息。
- **认证失败次数超过阈值的告警：**当 NAS 发现认证失败次数与认证请求总数的百分比超过阈值时，会发送该告警信息。

【举例】

开启 RADIUS 计费服务器可达状态变为 down 时的告警功能。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent trap enable radius accounting-server-down
```

1.3.36 state primary

state primary 命令用来设置主 RADIUS 服务器的状态。

【命令】

```
state primary { accounting | authentication } { active | block }
```

【缺省情况】

主 RADIUS 服务器状态为 **active**。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

accounting：主 RADIUS 计费服务器。

authentication：主 RADIUS 认证服务器。

active：正常工作状态。

block：通信中断状态。

【使用指导】

每次用户发起认证或计费，如果主服务器状态为 **active**，则设备都会首先尝试与主服务器进行通信，如果主服务器不可达，则将主服务器的状态置为 **block**，同时启动主服务器的 **timer quiet** 定时器，然后设备会严格按照从服务器的配置先后顺序依次查找状态为 **active** 的从服务器。在 **timer quiet** 定时器设定的时间到达之后，主服务器状态将由 **block** 恢复为 **active**。若该定时器超时之前，通过本命令将主服务器的状态手工设置为 **block**，则定时器超时之后主服务器状态不会自动恢复为 **active**，除非通过本命令手工将其设置为 **active**。

当主/从服务器状态都是 **block** 时，若主服务器状态是自动设置为 **block** 且已配置主服务器，则采用主服务器进行认证或计费；若主服务器状态是被手工设置为 **block** 或未配置主服务器，则在自动设置为 **block** 状态的所有从服务器中按顺序选择从服务器进行认证或计费。

认证服务器的状态会影响设备对该服务器可达性探测功能的开启。当指定的服务器状态为 **active**，且该服务器通过 **radius-server test-profile** 命令成功引用了一个已存在的服务器探测模板时，则设备会开启对该服务器的可达性探测功能。当手工将该服务器状态置为 **block** 时，会关闭对该服务器的可达性探测功能。

【举例】

在 RADIUS 方案 radius1 中，设置主认证服务器的状态为 **block**。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state primary authentication block
```

【相关命令】

- **display radius scheme**
- **radius-server test-profile**
- **state secondary**

1.3.37 state secondary

state secondary 命令用来设置从 RADIUS 服务器的状态。

【命令】

```
state secondary { accounting | authentication } [ { ipv4-address | ipv6  
ipv6-address } [ port-number | vpn-instance vpn-instance-name ] * ] { active  
| block }
```

【缺省情况】

从 RADIUS 服务器状态为 **active**。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

accounting: 从 RADIUS 计费服务器。

authentication: 从 RADIUS 认证服务器。

ipv4-address: 从 RADIUS 服务器的 IPv4 地址。

ipv6 ipv6-address: 从 RADIUS 服务器的 IPv6 地址。

port-number: 从 RADIUS 服务器的 UDP 端口号，取值范围为 1~65535，从 RADIUS 计费服务器的缺省 UDP 端口号为 1813，从 RADIUS 认证服务器的缺省 UDP 端口号为 1812。

vpn-instance vpn-instance-name: 从 RADIUS 服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

active: 正常工作状态。

block: 通信中断状态。

【使用指导】

如果不指定从服务器 IP 地址, 那么本命令将会修改所有已配置的从认证服务器或从计费服务器的状态。

如果设备查找到的状态为 **active** 的从服务器不可达, 则设备会将该从服务器的状态置为 **block**, 同时启动该服务器的 **timer quiet** 定时器, 并继续查找下一个状态为 **active** 的从服务器。在 **timer quiet** 定时器设定的时间到达之后, 从服务器状态将由 **block** 恢复为 **active**。若该定时器超时之前, 通过本命令将从服务器的状态手工设置为 **block**, 则定时器超时之后从服务器状态不会自动恢复为 **active**, 除非通过本命令手工将其设置为 **active**。如果所有已配置的从服务器都不可达, 则本次认证或计费失败。

认证服务器的状态会影响设备对该服务器可达性探测功能的开启。当指定的服务器状态为 **active**, 且该服务器通过 **radius-server test-profile** 命令成功引用了一个已存在的服务器探测模板时, 则设备会开启对该服务器的可达性探测功能。当手工将该服务器状态置为 **block** 时, 会关闭对该服务器的可达性探测功能。

【举例】

在 RADIUS 方案 radius1 中, 设置从认证服务器的状态设置为 **block**。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication block
```

【相关命令】

- **display radius scheme**
- **radius-server test-profile**
- **state primary**

1.3.38 timer quiet (RADIUS scheme view)

timer quiet 命令用来设置服务器恢复激活状态的时间。

undo timer quiet 命令用来恢复缺省情况。

【命令】

```
timer quiet minutes
undo timer quiet
```

【缺省情况】

服务器恢复激活状态的时间为 5 分钟。

【视图】

RADIUS 方案视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

minutes: 恢复激活状态的时间, 取值范围为 1~255, 单位为分钟。

【使用指导】

建议合理设置服务器恢复激活状态的时间：

- 如果服务器恢复激活状态时间设置的过短，就会出现设备反复尝试与状态 **active** 但实际不可达的服务器通信而导致的认证或计费频繁失败的问题。
- 如果服务器恢复激活状态时间设置的过长，当服务器恢复可达后，设备不能及时与其进行通信，会降低对用户进行认证或计费的效率。

【举例】

在 RADIUS 方案 radius1 中，配置服务器恢复激活状态的时间为 10 分钟。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer quiet 10
```

【相关命令】

- **display radius scheme**

1.3.39 timer realtime-accounting (RADIUS scheme view)

timer realtime-accounting 命令用来设置实时计费的时间间隔。

undo timer realtime-accounting 命令用来恢复缺省情况。

【命令】

```
timer realtime-accounting interval [ second ]
undo timer realtime-accounting
```

【缺省情况】

实时计费的时间间隔为 12 分钟。

【视图】

RADIUS 方案视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interval：实时计费的时间间隔，取值范围为 0～71582。

second：表示实时计费的时间间隔以秒为单位，缺省以分钟为单位。

【使用指导】

为了对用户实施实时计费，有必要设置实时计费的时间间隔。不同的取值的处理有所不同：

- 若实时计费间隔不为 0，则每隔设定的时间，设备会向 RADIUS 服务器发送一次在线用户的计费信息。
- 若实时计费间隔设置为 0，且服务器上配置了实时计费间隔，则设备按照服务器上配置的实时计费间隔向 RADIUS 服务器发送在线用户的计费信息；如果服务器上没有配置该值，则设备不向 RADIUS 服务器发送在线用户的计费信息。

实时计费间隔的取值小，计费准确性高，但对设备和 RADIUS 服务器的性能要求就高。

表1-6 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1~99	3
100~499	6
500~999	12
大于等于1000	大于等于15

不同情况下修改的实时计费间隔，对于已在线用户的生效情况有所不同：

- 将实时计费间隔从非 0 有效值改为 0，或者从 0 修改为非 0 有效值后，已在线用户会依然采用原有取值，修改后的取值对其不生效。
- 将实时计费间隔从某非 0 有效值修改为其它非 0 有效值后，已在线用户将会采用修改后的取值。

需要注意的是，无论实时计费间隔取值为多少，对于双栈用户，设备缺省会在用户申请到 IPv4 地址时为其发送一个计费开始报文，并在随后用户申请到 IPv6 地址/PD 时再发送一个计费更新报文。

对于未进行 RADIUS 认证和授权，仅进行 RADIUS 计费的用户，只能使用计费方案下设置的实时计费间隔，不会使用 RADIUS 服务器设置的实时计费间隔。

【举例】

在 RADIUS 方案 radius1 中，设置实时计费的时间间隔为 51 分钟。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

【相关命令】

- **retry realtime-accounting**

1.3.40 timer response-timeout (RADIUS scheme view)

timer response-timeout 命令用来设置 RADIUS 服务器响应超时时间。

undo timer response-timeout 命令用来恢复缺省情况。

【命令】

```
timer response-timeout seconds
undo timer response-timeout
```

【缺省情况】

RADIUS 服务器响应超时时间为 3 秒。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

seconds: RADIUS 服务器响应超时时间，取值范围为 1~10，单位为秒。

【使用指导】

如果在 RADIUS 请求报文传送出去一段时间后，设备还没有得到 RADIUS 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户尽可能地获得 RADIUS 服务，这段时间被称为 RADIUS 服务器响应超时时间，本命令用于调整这个时间。

需要注意的是：

- 发送 RADIUS 报文的最大尝试次数、RADIUS 服务器响应超时时间以及配置的 RADIUS 服务器总数，三者的乘积不能超过接入模块定义的用户认证超时时间，否则在 RADIUS 认证过程完成之前用户就有可能被强制下线。
- 设备在按照配置顺序尝试与下一个 RADIUS 服务器通信之前，会首先判断当前累计尝试持续时间是否达到或超过 300 秒，如果超过或达到 300 秒，将不再向下一个 RADIUS 服务器发送 RADIUS 请求报文，即认为该 RADIUS 请求发送失败。因此，为了避免某些已部署的 RADIUS 服务器由于此超时机制而无法被使用到，建议基于配置的 RADIUS 服务器总数，合理设置发送 RADIUS 报文的最大尝试次数以及 RADIUS 服务器响应超时时间。

【举例】

在 RADIUS 方案 radius1 中，设置服务器响应超时时间设置为 5 秒。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

【相关命令】

- **display radius scheme**
- **retry**

1.3.41 user-name-format (RADIUS scheme view)

user-name-format 命令用来设置发送给 RADIUS 服务器的用户名格式。

undo user-name-format 命令用来恢复缺省情况。

【命令】

```
user-name-format { keep-original | with-domain | without-domain }
undo user-name-format
```

【缺省情况】

发送给 RADIUS 服务器的用户名携带 ISP 域名。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

keep-original: 发送给 RADIUS 服务器的用户名与用户的输入保持一致。

with-domain: 发送给 RADIUS 服务器的用户名携带 ISP 域名。

without-domain: 发送给 RADIUS 服务器的用户名不携带 ISP 域名。

【使用指导】

接入用户通常以“*userid@isp-name*”的格式命名，“@”后面的部分为 ISP 域名，设备就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 RADIUS 服务器。因此，设备提供此命令以指定发送给 RADIUS 服务器的用户名是否携带有 ISP 域名。

如果指定某个 RADIUS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个或两个以上的 ISP 域中同时设置使用该 RADIUS 方案。否则，会出现虽然实际用户不同（在不同的 ISP 域中），但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

【举例】

在 RADIUS 方案 radius1 中，设置发送给 RADIUS 服务器的用户名不得携带域名。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain
```

【相关命令】

- **display radius scheme**

1.3.42 vpn-instance (RADIUS scheme view)

vpn-instance 命令用来配置 RADIUS 方案所属的 VPN。

undo vpn-instance 命令用来恢复缺省情况。

【命令】

vpn-instance *vpn-instance-name*

undo vpn-instance

【缺省情况】

RADIUS 方案属于公网。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

vpn-instance-name: MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

本命令配置的 VPN 对于该方案下的所有 RADIUS 认证/计费服务器生效，但设备优先使用配置 RADIUS 认证/计费服务器时为各服务器单独指定的 VPN。

【举例】

```
# 配置 RADIUS 方案 radius1 所属的 VPN 为 test。
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] vpn-instance test
```

【相关命令】

- **display radius scheme**

1.4 HWTACACS配置命令

1.4.1 data-flow-format (HWTACACS scheme view)

data-flow-format 命令用来配置发送到 HWTACACS 服务器的数据流及数据包的单位。

undo data-flow-format 命令用来恢复缺省情况。

【命令】

```
data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet  
{ giga-packet | kilo-packet | mega-packet | one-packet } } *  
undo data-flow-format { data | packet }
```

【缺省情况】

数据流的单位为 **byte**，数据包的单位为 **one-packet**。

【视图】

HWTACACS 方案视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

data: 设置数据流的单位。

- **byte:** 数据流的单位为字节。
- **giga-byte:** 数据流的单位千兆字节。
- **kilo-byte:** 数据流的单位为千字节。
- **mega-byte:** 数据流的单位为兆字节。

packet: 设置数据包的单位。

- **giga-packet:** 数据包的单位为千兆包。
- **kilo-packet:** 数据包的单位为千包。
- **mega-packet:** 数据包的单位为兆包。
- **one-packet:** 数据包的单位为包。

【使用指导】

设备上配置的发送给 HWTACACS 服务器的数据流单位及数据包单位应与 HWTACACS 服务器上的流量统计单位保持一致，否则无法正确计费。

【举例】

在 HWTACACS 方案 hwt1 中，设置发往 HWTACACS 服务器的数据流的数据单位为千字节、数据包的单位为千包。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo-packet
```

【相关命令】

- **display hwtacacs scheme**

1.4.2 display hwtacacs scheme

display hwtacacs scheme 命令用来显示 HWTACACS 方案的配置信息或 HWTACACS 服务相关的统计信息。

【命令】

```
display hwtacacs scheme [ hwtacacs-scheme-name [ statistics ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

hwtacacs-scheme-name: HWTACACS 方案的名称，为 1~32 个字符的字符串，不区分大小写。如果不指定该参数，则显示所有 HWTACACS 方案的配置信息。

statistics: 显示 HWTACACS 服务相关的统计信息。不指定该参数，则显示 HWTACACS 方案的配置信息。

【举例】

显示所有 HWTACACS 方案的配置情况。

```
<Sysname> display hwtacacs scheme
Total 1 HWTACACS schemes

-----
HWTACACS Scheme Name : hwtac
Index : 0
Primary Auth Server:
  IP   : 2.2.2.2          Port: 49      State: Active
  VPN Instance: 2
```

```

Single-connection: Enabled
Primary Author Server:
  IP   : 2.2.2.2          Port: 49      State: Active
  VPN Instance: 2
  Single-connection: Disabled
Primary Acct Server:
  IP   : Not Configured  Port: 49      State: Block
  VPN Instance: Not configured
  Single-connection: Disabled

VPN Instance           : 2
NAS IP Address         : 2.2.2.3
Server Quiet Period(minutes) : 5
Realtime Accounting Interval(minutes) : 12
Response Timeout Interval(seconds) : 5
Username Format         : with-domain
Data flow unit         : Byte
Packet unit            : one
All-server-block action : Attempt the top-priority server

```

表1-7 display hwtacacs scheme 命令显示信息描述表

字段	描述
Total 1 HWTACACS schemes	共计1个HWTACACS方案
HWTACACS Scheme Name	HWTACACS方案的名称
Index	HWTACACS方案的索引号
Primary Auth Server	主HWTACACS认证服务器
Primary Author Server	主HWTACACS授权服务器
Primary Acct Server	主HWTACACS计费服务器
Secondary Auth Server	从HWTACACS认证服务器
Secondary Author Server	从HWTACACS授权服务器
Secondary Acct Server	从HWTACACS计费服务器
IP	HWTACACS服务器的IP地址 未配置时，显示为Not configured
Port	HWTACACS服务器的端口号 未配置时，显示缺省值
State	HWTACACS服务器目前状态 - Active: 激活状态 - Block: 静默状态
VPN Instance	HWTACACS服务器或HWTACACS方案所在的VPN 未配置时，显示为Not configured

字段	描述
Single-connection	单连接状态 - Enabled: 使用一条 TCP 连接与服务器通信 - Disabled: 每次新建 TCP 连接与服务器通信
NAS IP Address	配置的发送HWTACACS报文的源IP地址或源接口 未配置时，显示为Not configured
Server Quiet Period(minutes)	主HWTACACS服务器恢复激活状态的时间（分钟）
Realtime Accounting Interval(minutes)	实时HWTACACS计费更新报文的发送间隔（分钟）
Response Timeout Interval(seconds)	HWTACACS服务器超时时间（秒）
Username Format	用户名格式 - with-domain: 携带域名 - without-domain: 不携带域名 - keep-original: 与用户输入保持一致
Data flow unit	数据流的单位
Packet unit	数据包的单位
All-server-block action	当前方案中的服务器都处于block状态后 - Attempt the top-priority server: 尝试与当前方案中高优先级的服务器建立一次连接 - Skip all servers in the scheme: 跳过当前方案中的所有服务器

<Sysname> display hwtacacs scheme tac statistics

HWTACACS scheme name: tac

Primary authentication server: 3.3.3.3

Round trip time:	0 seconds
Request packets:	1
Login request packets:	1
Change-password request packets:	0
Request packets including plaintext password:	0
Request packets including ciphertext password:	0
Response packets:	2
Pass response packets:	1
Failure response packets:	0
Get-data response packets:	0
Get-username response packets:	0
Get-password response packets:	1
Restart response packets:	0
Error response packets:	0
Follow response packets:	0
Malformed response packets:	0
Continue packets:	1
Continue-abort packets:	0


```

Pending request packets:          0
Timeout packets:                  0
Unknown type response packets:    0
Dropped response packets:         0

```

Primary authorization server: 3.3.3.3

```

Round trip time:                  1 seconds
Request packets:                  1
Response packets:                 1
PassAdd response packets:        1
PassReply response packets:      0
Failure response packets:        0
Error response packets:          0
Follow response packets:         0
Malformed response packets:      0
Pending request packets:         0
Timeout packets:                 0
Unknown type response packets:    0
Dropped response packets:         0

```

Primary accounting server: 3.3.3.3

```

Round trip time:                  0 seconds
Request packets:                  2
Accounting start request packets: 1
Accounting stop request packets: 1
Accounting update request packets: 0
Pending request packets:         0
Response packets:                 2
Success response packets:        2
Error response packets:          0
Follow response packets:         0
Malformed response packets:      0
Timeout response packets:        0
Unknown type response packets:    0
Dropped response packets:         0

```

表1-8 display hwtacacs scheme statistics 命令显示信息描述表

字段	描述
HWTACACS scheme name	HWTACACS方案名称
Primary authentication server	主HWTACACS认证服务器
Primary authorization server	主HWTACACS授权服务器
Primary accounting server	主HWTACACS计费服务器
Secondary authentication server	从HWTACACS认证服务器
Secondary authorization server	从HWTACACS授权服务器
Secondary accounting server	从HWTACACS计费服务器

字段	描述
Round trip time	设备处理最近一组响应报文和请求报文的时间间隔（单位为秒）
Request packets	发送的请求报文个数
Response packets	接收到的响应报文个数
Failure response packets	认证或授权失败的响应报文个数
Error response packets	错误类型的响应报文个数
Follow response packets	Follow 类型的响应报文的个数
Malformed response packets	不合法的响应报文个数
Pending request packets	等待响应的请求报文个数
Timeout packets	超时的请求报文个数
Unknown type response packets	未知报文类型的响应报文个数
Dropped response packets	被丢弃响应报文个数
Login request packets	登录认证的请求报文个数
Change-password request packets	更改密码的请求报文个数
Request packets including plaintext passwords	发送明文密码的请求报文个数
Request packets including ciphertext passwords	发送密文密码的请求报文个数
Pass response packets	表示认证通过的响应报文个数
Get-data response packets	表示获取数据的响应报文个数
Get-username response packets	表示获取用户名的响应报文个数
Get-password response packets	表示获取密码的响应报文个数
Restart response packets	要求重认证的响应报文个数
Continue packets	发送的 Continue 报文个数
Continue-abort packets	发送的 Continue-abort 报文个数
PassAdd response packets	接收到的 PassAdd 类型的响应报文个数。此报文表示同意授权所有请求的属性，并添加其他授权属性
PassReply response packets	接收到的 PassReply 类型的响应报文个数。此报文表示采用响应报文中指定的授权属性替换请求的授权属性
Accounting start request packets	发送的计费开始请求报文个数
Accounting stop request packets	发送的计费结束请求报文个数
Accounting update request packets	发送的计费更新报文个数
Accounting start-and-update request packets	发送的赋值的计费开始报文的个数
Success response packets	接收到的计费成功的响应报文个数

【相关命令】

- **reset hwtacacs statistics**

1.4.3 hwtacacs nas-ip

hwtacacs nas-ip 命令用来设置设备发送 HWTACACS 报文使用的源 IP 地址。

undo hwtacacs nas-ip 命令用来删除指定的发送 HWTACACS 报文使用的源 IP 地址。

【命令】

```
hwtacacs nas-ip { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

```
undo hwtacacs nas-ip { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未指定发送 HWTACACS 报文使用的源 IP 地址，设备将使用到达 HWTACACS 服务器的路由出接口的主 IPv4 地址或 IPv6 地址作为发送 HWTACACS 报文的源 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-address: 指定的源 IPv4 地址，应该为本机的地址，不能为全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

ipv6 ipv6-address: 指定的源 IPv6 地址，应该为本机的地址，必须是单播地址，不能为环回地址与本地链路地址。

vpn-instance vpn-instance-name: 指定私网源 IP 地址所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若不指定该参数，则表示配置的是公网源地址。

【使用指导】

HWTACACS 服务器上通过 IP 地址来标识接入设备，并根据收到的 HWTACACS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证或计费请求。因此，为保证 HWTACACS 报文可被服务器正常接收并处理，接入设备上发送 HWTACACS 报文使用的源地址必须与 HWTACACS 服务器上指定的接入设备的 IP 地址保持一致。

为避免物理接口故障时从服务器返回的报文不可达，推荐使用 Loopback 接口地址为发送 HWTACACS 报文使用的源 IP 地址。

HWTACACS 方案视图和系统视图下均可以配置发送 HWTACACS 报文使用的源 IP 地址，具体生效情况如下：

- HWTACACS 方案视图下配置的源 IP 地址（通过 **nas-ip** 命令）只对本方案有效。

- 系统视图下的配置的源 IP 地址（通过 **hwtacacs nas-ip** 命令）对所有 HWTACACS 方案有效。
- HWTACACS 方案视图下的设置具有更高的优先级。

系统视图下，最多允许指定一个源接口，请确保指定的源接口与 RADIUS 服务器路由可达。

【举例】

设置设备发送 HWTACACS 报文使用的源 IP 地址为 129.10.10.1。

```
<Sysname> system-view
```

```
[Sysname] hwtacacs nas-ip 129.10.10.1
```

【相关命令】

- **nas-ip** (HWTACACS scheme view)

1.4.4 hwtacacs scheme

hwtacacs scheme 命令用来创建 HWTACACS 方案，并进入 HWTACACS 方案视图。如果指定的 HWTACACS 方案已经存在，则直接进入 HWTACACS 方案视图。

undo hwtacacs scheme 命令用来删除指定的 HWTACACS 方案。

【命令】

```
hwtacacs scheme hwtacacs-scheme-name
```

```
undo hwtacacs scheme hwtacacs-scheme-name
```

【缺省情况】

不存在 HWTACACS 方案。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

hwtacacs-scheme-name: HWTACACS 方案名称，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

一个 HWTACACS 方案可以同时被多个 ISP 域引用。

最多可以配置 16 个 HWTACACS 方案。

【举例】

创建名称为 hwt1 的 HWTACACS 方案并进入相应的 HWTACACS 视图。

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1]
```

【相关命令】

- **display hwtacacs scheme**

1.4.5 key (HWTACACS scheme view)

key 命令用来配置 HWTACACS 认证、授权、计费报文的共享密钥。

undo key 命令用来删除指定的 HWTACACS 报文的共享密钥。

【命令】

key { accounting | authentication | authorization } { cipher | simple } string

undo key { accounting | authentication | authorization }

【缺省情况】

未配置 HWTACACS 报文的共享密钥。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

accounting: 指定 HWTACACS 计费报文的共享密钥。

authentication: 指定 HWTACACS 认证报文的共享密钥。

authorization: 指定 HWTACACS 授权报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。

【使用指导】

必须保证设备上设置的共享密钥与 HWTACACS 服务器上的完全一致。

【举例】

在 HWTACACS 方案 hwt1 中,配置 HWTACACS 认证报文共享密钥为明文 123456TESTauth&!

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] key authentication simple 123456TESTauth&!
```

配置 HWTACACS 授权报文共享密钥为明文 123456TESTautr&!

```
[Sysname-hwtacacs-hwt1] key authorization simple 123456TESTautr&!
```

配置 HWTACACS 计费报文共享密钥为明文 123456TESTacct&!

```
[Sysname-hwtacacs-hwt1] key accounting simple 123456TESTacct&!
```

【相关命令】

- **display hwtacacs scheme**

1.4.6 nas-ip (HWTACACS scheme view)

nas-ip 命令用来设置设备发送 HWTACACS 报文使用的源 IP 地址。

undo nas-ip 命令用来删除指定类型的发送 HWTACACS 报文使用的源 IP 地址。

【命令】

```
nas-ip { ipv4-address | ipv6 ipv6-address }  
undo nas-ip [ ipv6 ]
```

【缺省情况】

未指定设备发送 HWTACACS 报文使用的源 IP 地址,使用系统视图下由命令 **hwtacacs nas-ip** 指定的源 IP 地址。

【视图】

HWTACACS 方案视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

ipv4-address: 指定的源 IPv4 地址,应该为本机的地址,不能为全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

ipv6 ipv6-address: 指定的源 IPv6 地址,应该为本机的地址,必须是单播地址,不能为环回地址与本地链路地址。

【使用指导】

HWTACACS 服务器上通过 IP 地址来标识接入设备,并根据收到的 HWTACACS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配,来决定是否处理来自该接入设备的认证、授权、计费请求。因此,为保证 HWTACACS 报文可被服务器正常接收并处理,接入设备上发送 HWTACACS 报文使用的源地址必须与 HWTACACS 服务器上指定的接入设备的 IP 地址保持一致。为避免物理接口故障时从服务器返回的报文不可达,推荐使用 Loopback 接口地址为发送 HWTACACS 报文使用的源 IP 地址。

HWTACACS 方案视图和系统视图下均可以配置发送 HWTACACS 报文使用的源 IP 地址,具体生效情况如下:

- HWTACACS 方案视图下配置的源 IP 地址(通过 **nas-ip** 命令)只对本方案有效。
- 系统视图下的配置的源 IP 地址(通过 **hwtacacs nas-ip** 命令)对所有 HWTACACS 方案有效。
- HWTACACS 方案视图下的设置具有更高的优先级。

一个 HWTACACS 方案视图下,最多允许指定一个 IPv4 源地址和一个 IPv6 源地址。

如果 **undo nas-ip** 命令中不指定任何关键字,则表示删除发送 HWTACACS 报文使用的源 IPv4 地址。

【举例】

在 HWTACACS 方案 hwt1 中,设置设备发送 HWTACACS 报文使用的源 IP 地址为 10.1.1.1。

```
<Sysname> system-view  
[Sysname] hwtacacs scheme hwt1  
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

【相关命令】

- **display hwtacacs scheme**

- **hwtaacs nas-ip**

1.4.7 primary accounting (HWTACACS scheme view)

primary accounting 命令用来配置主 HWTACACS 计费服务器。

undo primary accounting 命令用来恢复缺省情况。

【命令】

```
primary accounting { ipv4-address | ipv6 ipv6-address } [ port-number | key
{ cipher | simple } string | single-connection | vpn-instance
vpn-instance-name ] *
undo primary accounting
```

【缺省情况】

未配置 HWTACACS 主计费服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-address: 主 HWTACACS 计费服务器的 IPv4 地址。

ipv6 *ipv6-address*: 主 HWTACACS 计费服务器的 IPv6 地址。

port-number: 主 HWTACACS 计费服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。

key: 与主 HWTACACS 计费服务器交互的计费报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。

single-connection: 所有与主 HWTACACS 计费服务器交互的计费报文使用同一个 TCP 连接。如果未指定本参数，则表示每次计费都会使用一个新的 TCP 连接。

vpn-instance *vpn-instance-name*: 主 HWTACACS 计费服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示主 HWTACACS 计费服务器位于公网中。

【使用指导】

配置的主计费服务器的 TCP 端口号以及计费报文的共享密钥必须与服务器的配置保持一致。

在同一个方案中指定的主计费服务器和从计费服务器的 VPN、IP 地址、端口号不能完全相同。

只有在设备与计费服务器没有报文交互时，才允许删除该服务器。计费服务器删除后，只对之后的计费过程有影响。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 HWTACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

【举例】

在 HWTACACS 方案 hwt1 中，配置主 HWTACACS 计费服务器的 IP 地址为 10.163.155.12，使用 TCP 端口 49 与 HWTACACS 计费服务器通信，计费报文的共享密钥为明文 123456TESTacct&！。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hw1
[Sysname-hwtacacs-hw1] primary accounting 10.163.155.12 49 key simple 123456TESTacct&！
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)
- **secondary accounting**
- **vpn-instance** (HWTACACS scheme view)

1.4.8 primary authentication (HWTACACS scheme view)

primary authentication 命令用来配置主 HWTACACS 认证服务器。

undo primary authentication 命令用来恢复缺省情况。

【命令】

```
primary authentication { ipv4-address | ipv6 ipv6-address } [ port-number |  
key { cipher | simple } string | single-connection | vpn-instance  
vpn-instance-name ] *  
undo primary authentication
```

【缺省情况】

未配置主 HWTACACS 认证服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4-address: 主 HWTACACS 认证服务器的 IPv4 地址。

ipv6 *ipv6-address*: 主 HWTACACS 认证服务器的 IPv6 地址。

port-number: 主 HWTACACS 认证服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。

key: 与主 HWTACACS 认证服务器交互的认证报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。

single-connection: 所有与主 HWTACACS 认证服务器交互的计费报文使用同一个 TCP 连接。如果未指定本参数，则表示向主 HWTACACS 计费服务器发送计费报文都会使用一个新的 TCP 连接。

vpn-instance vpn-instance-name: 主 HWTACACS 认证服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示主 HWTACACS 认证服务器位于公网中。

【使用指导】

配置的主认证服务器的 TCP 端口号以及认证报文的共享密钥必须与服务器的配置保持一致。

在同一个方案中指定的主认证服务器和从认证服务器的 VPN、IP 地址、端口号不能完全相同。

只有在设备与认证服务器没有报文交互时，才允许删除该服务器。认证服务器删除后，只对之后的认证过程有影响。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 HWTACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

【举例】

在 HWTACACS 方案 hwt1 中，配置主 HWTACACS 认证服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 与 HWTACACS 认证服务器通信，认证报文的共享密钥为明文 123456TESTauth&!。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49 key simple
123456TESTauth&!
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)
- **secondary authentication**
- **vpn-instance** (HWTACACS scheme view)

1.4.9 primary authorization

primary authorization 命令用来配置主 HWTACACS 授权服务器。

undo primary authorization 命令用来恢复缺省情况。

【命令】

```
primary authorization { ipv4-address | ipv6 ipv6-address } [ port-number |  
key { cipher | simple } string | single-connection | vpn-instance  
vpn-instance-name ] *  
undo primary authorization
```

【缺省情况】

未配置主 HWTACACS 授权服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-address: 主 HWTACACS 授权服务器的 IPv4 地址。

ipv6 ipv6-address: 主 HWTACACS 授权服务器的 IPv6 地址。

port-number: 主 HWTACACS 授权服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。

key: 与主 HWTACACS 授权服务器交互的授权报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。

single-connection: 所有与主 HWTACACS 授权服务器交互的授权报文使用同一个 TCP 连接。如果未指定本参数，则表示每次授权都会使用一个新的 TCP 连接。

vpn-instance vpn-instance-name: 主 HWTACACS 授权服务器所属的 VPN 实例。

vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示主 HWTACACS 授权服务器位于公网中。

【使用指导】

配置的主授权服务器的 TCP 端口号以及授权报文的共享密钥必须与服务器的配置保持一致。

在同一个方案中指定的主授权服务器和从授权服务器的 VPN、IP 地址、端口号不能完全相同。

只有在设备与授权服务器没有报文交互时，才允许删除该服务器。授权服务器删除后，只对之后的授权过程有影响。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 HWTACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

【举例】

在 HWTACACS 方案 hwt1 中，配置主 HWTACACS 授权服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 与 HWTACACS 授权服务器通信，授权报文的共享密钥为明文 123456TESTautr&！。

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49 key simple 123456TESTautr&！
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)

- **secondary authorization**
- **vpn-instance** (HWTACACS scheme view)

1.4.10 reset hwtacacs statistics

reset hwtacacs statistics 命令用来清除 HWTACACS 协议的统计信息。

【命令】

```
reset hwtacacs statistics { accounting | all | authentication |
authorization }
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

accounting: 清除 HWTACACS 协议关于计费的统计信息。

all: 清除 HWTACACS 的所有统计信息。

authentication: 清除 HWTACACS 协议关于认证的统计信息。

authorization: 清除 HWTACACS 协议关于授权的统计信息。

【举例】

```
# 清除 HWTACACS 协议的所有统计信息。
<Sysname> reset hwtacacs statistics all
```

【相关命令】

- **display hwtacacs scheme**

1.4.11 secondary accounting (HWTACACS scheme view)

secondary accounting 命令用来配置从 HWTACACS 计费服务器。

undo secondary accounting 命令用来删除指定的从 HWTACACS 计费服务器。

【命令】

```
secondary accounting { ipv4-address | ipv6 ipv6-address } [ port-number |
key { cipher | simple } string | single-connection | vpn-instance
vpn-instance-name ] *
undo secondary accounting [ { ipv4-address | ipv6 ipv6-address }
[ port-number | vpn-instance vpn-instance-name ] * ]
```

【缺省情况】

未配置从 HWTACACS 计费服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4-address: 从 HWTACACS 计费服务器的 IPv4 地址。

ipv6 ipv6-address: 从 HWTACACS 计费服务器的 IPv6 地址。

port-number: 从 HWTACACS 计费服务器的端口号，取值范围为 1~65535，缺省值为 49。

key: 与从 HWTACACS 计费服务器交互的计费报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。

single-connection: 所有与从 HWTACACS 计费服务器交互的计费报文使用同一个 TCP 连接。如果未指定本参数，则表示每次计费都会使用一个新的 TCP 连接。

vpn-instance vpn-instance-name: 从 HWTACACS 计费服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示从 HWTACACS 计费服务器位于公网中。

【使用指导】

配置的从计费服务器的 TCP 端口号以及计费报文的共享密钥必须与服务器的配置保持一致。

每个 HWTACACS 方案中最多支持配置 16 个从 HWTACACS 计费服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。

如果不指定任何参数，则 **undo** 命令将删除所有从计费服务器。

在同一个方案中指定的主计费服务器和从计费服务器的 VPN、IP 地址、端口号不能完全相同，并且各从计费服务器的 VPN、IP 地址、端口号也不能完全相同。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 TACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

只有在设备与计费服务器没有报文交互时，才允许删除该服务器。计费服务器删除后，只对之后的计费过程有影响。

【举例】

在 HWTACACS 方案 hwt1 中，配置从 HWTACACS 计费服务器的 IP 地址为 10.163.155.12，使用 TCP 端口 49 与 HWTACACS 计费服务器通信，计费报文的共享密钥为明文 123456TESTacct&!。

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49 key simple 123456TESTacct&!
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)

- **primary accounting** (HWTACACS scheme view)
- **vpn-instance** (HWTACACS scheme view)

1.4.12 secondary authentication (HWTACACS scheme view)

secondary authentication 命令用来配置从 HWTACACS 认证服务器。

undo secondary authentication 命令用来删除指定的从 HWTACACS 认证服务器。

【命令】

```
secondary authentication { ipv4-address | ipv6 ipv6-address } [ port-number
| key { cipher | simple } string | single-connection | vpn-instance
vpn-instance-name ] *
undo secondary authentication [ { ipv4-address | ipv6 ipv6-address }
[ port-number | vpn-instance vpn-instance-name ] * ]
```

【缺省情况】

未配置从 HWTACACS 认证服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4-address: 从 HWTACACS 认证服务器的 IPv4 地址。

ipv6 ipv6-address: 从 HWTACACS 认证服务器的 IPv6 地址。

port-number: 从 HWTACACS 认证服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。

key: 与从 HWTACACS 认证服务器交互的认证报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。

single-connection: 所有与从 HWTACACS 认证服务器交互的认证报文使用同一个 TCP 连接。如果未指定本参数，则表示每次认证都会使用一个新的 TCP 连接。

vpn-instance vpn-instance-name: 从 HWTACACS 认证服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示从 HWTACACS 服务器位于公网中。

【使用指导】

配置的从认证服务器的 TCP 端口号以及认证报文的共享密钥必须与服务器的配置保持一致。

每个 HWTACACS 方案中最多支持配置 16 个从 HWTACACS 认证服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。

如果不指定任何参数，则 **undo** 命令将删除所有从认证服务器。

在同一个方案中指定的主认证服务器和从认证服务器的 VPN、IP 地址、端口号不能完全相同，并且各从认证服务器的 VPN、IP 地址、端口号也不能完全相同。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 TACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

只有在设备与认证服务器没有报文交互时，才允许删除该服务器。认证服务器删除后，只对之后的认证过程有影响。

【举例】

在 HWTACACS 方案 hwt1 中，配置从 HWTACACS 认证服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 与 HWTACACS 认证服务器通信，认证报文的共享密钥为明文 123456TESTauth&！。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49 key simple
123456TESTauth&！
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)
- **primary authentication** (HWTACACS scheme view)
- **vpn-instance** (HWTACACS scheme view)

1.4.13 secondary authorization

secondary authorization 命令用来配置从 HWTACACS 授权服务器。

undo secondary authorization 命令用来删除指定的从 HWTACACS 授权服务器。

【命令】

```
secondary authorization { ipv4-address | ipv6 ipv6-address } [ port-number  
| key { cipher | simple } string | single-connection | vpn-instance  
vpn-instance-name ] *  
undo secondary authorization [ { ipv4-address | ipv6 ipv6-address }  
[ port-number | vpn-instance vpn-instance-name ] * ]
```

【缺省情况】

未配置从 HWTACACS 授权服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4-address: 从 HWTACACS 授权服务器的 IPv4 地址。

ipv6 ipv6-address: 从 HWTACACS 授权服务器的 IPv6 地址。

port-number: 从 HWTACACS 授权服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。

key: 与从 HWTACACS 授权服务器交互的授权报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。

single-connection: 所有与从 HWTACACS 授权服务器交互的授权报文使用同一个 TCP 连接。如果未指定本参数，则表示每次授权都会使用一个新的 TCP 连接。

vpn-instance vpn-instance-name: 从 HWTACACS 授权服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示从 HWTACACS 授权服务器位于公网中。

【使用指导】

配置的从授权服务器的 TCP 端口号以及授权报文的共享密钥必须与服务器的配置保持一致。

每个 HWTACACS 方案中最多支持配置 16 个从 HWTACACS 授权服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。

如果不指定任何参数，则 **undo** 命令将删除所有从授权服务器。

在同一个方案中指定的主授权服务器和从授权服务器的 VPN、IP 地址、端口号不能完全相同，并且各从授权服务器的 VPN、IP 地址、端口号也不能完全相同。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 TACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

只有在设备与授权服务器没有报文交互时，才允许删除该服务器。授权服务器删除后，只对之后的授权过程有影响。

【举例】

在 HWTACACS 方案 hwt1 中，配置从 HWTACACS 授权服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 与 HWTACACS 授权服务器通信，授权报文的共享密钥为明文 123456TESTautr&!

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49 key simple
123456TESTautr&!
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)
- **primary authorization** (HWTACACS scheme view)
- **vpn-instance** (HWTACACS scheme view)

1.4.14 server-block-action (HWTACACS scheme view)

server-block-action 命令用来设置服务器都处于 block 状态后的请求动作。

undo server-block-action 命令用来恢复缺省情况。

【命令】

```
server-block-action { attempt | skip }  
undo server-block-action
```

【缺省情况】

所有服务器都处于 block 状态后的请求动作为 **attempt**。

【视图】

HWTACACS 方案视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

attempt: Attempt 方式，表示该方案下的所有服务器都处于 block 状态后，设备收到用户的认证/授权/计费请求时，仍然会尝试与一个认证/授权/计费服务器（优先选择主服务器，若未配置则选择配置的第一个从服务器）建立一次连接，如果与该服务器建立连接失败，才会切换到为该用户配置的下一个认证/授权/计费方法去处理这个请求。

skip: Skip 方式，表示该方案下的所有服务器都处于 block 状态后，设备收到用户的认证/授权/计费请求时，会跳过当前方案中的所有服务器，直接使用为该用户配置的下一个认证/授权/计费方法去处理这个请求。

【使用指导】

Attempt 方式下，由于该方案下的所有服务器都处于 block 状态后，设备仍会首先尝试与一个服务器建立连接，与该服务器建立连接失败后，才会切换到配置的下一个认证/授权/计费方法，此方法保证了设备尽量优先使用第一个认证/授权/计费方法处理用户请求，但同时会增加请求的响应时间。因此，对于对 AAA 响应时间要求比较高的场合，建议选择 Skip 方式。

设备处理一个认证/授权/计费请求的过程中，如果已经跳过了当前方案中的所有服务器，则后续就算该方案中有服务器状态切换回 active，设备也不会再使用该方案来处理它。

【举例】

在 HWTACACS 方案 hwt1 中，设置服务器都处于 block 状态后的动作为跳过当前方案中的所有服务器。

```
<Sysname> system-view  
[Sysname] hwtacacs scheme hwt1  
[Sysname-hwtacacs-hwt1] server-block-action skip
```

【相关命令】

- **display hwtacacs scheme**

1.4.15 timer quiet (HWTACACS scheme view)

timer quiet 命令用来设置服务器恢复激活状态的时间。

undo timer quiet 命令用来恢复缺省情况。

【命令】

timer quiet *minutes*

undo timer quiet

【缺省情况】

服务器恢复激活状态的时间为 5 分钟。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

minutes: 恢复激活状态的时间，取值范围为 1~255，单位为分钟。

【举例】

设置服务器恢复激活状态的时间为 10 分钟。

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] timer quiet 10
```

【相关命令】

- **display hwtacacs scheme**

1.4.16 timer realtime-accounting (HWTACACS scheme view)

timer realtime-accounting 命令用来设置实时计费的时间间隔。

undo timer realtime-accounting 命令用来恢复缺省情况。

【命令】

timer realtime-accounting *minutes*

undo timer realtime-accounting

【缺省情况】

实时计费的时间间隔为 12 分钟。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

minutes: 实时计费的时间间隔，取值范围为 0~60，单位为分钟。0 表示设备不向 HWTACACS 服务器发送在线用户的计费信息。

【使用指导】

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，设备会向 HWTACACS 服务器发送一次在线用户的计费信息。

实时计费间隔的取值小，计费准确性高，但对设备和 HWTACACS 服务器的性能要求就高。

表1-9 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1~99	3
100~499	6
500~999	12
大于等于1000	大于等于15

【举例】

在 HWTACACS 方案 hwt1 中，设置实时计费的时间间隔为 51 分钟。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

【相关命令】

- **display hwtacacs scheme**

1.4.17 timer response-timeout (HWTACACS scheme view)

timer response-timeout 命令用来设置 HWTACACS 服务器响应超时时间。

undo timer response-timeout 命令用来恢复缺省情况。

【命令】

```
timer response-timeout seconds
undo timer response-timeout
```

【缺省情况】

HWTACACS 服务器响应超时时间为 5 秒。

【视图】

HWTACACS 方案视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

seconds: HWTACACS 服务器响应超时时间，取值范围为 1~300，单位为秒。

【使用指导】

由于 HWTACACS 是基于 TCP 实现的，因此，服务器响应超时或 TCP 超时都可能导致与 HWTACACS 服务器的连接断开。

HWTACACS 服务器响应超时时间与配置的 HWTACACS 服务器总数的乘积不能超过接入模块定义的用户认证超时时间，否则在 HWTACACS 认证过程完成之前用户就有可能被强制下线。

【举例】

在 HWTACACS 方案 hwt1 中，设置 HWTACACS 服务器响应超时时间为 30 秒。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

【相关命令】

- **display hwtacacs scheme**

1.4.18 user-name-format (HWTACACS scheme view)

user-name-format 命令用来设置发送给 HWTACACS 服务器的用户名格式。

undo user-name-format 命令用来恢复缺省情况。

【命令】

```
user-name-format { keep-original | with-domain | without-domain }
undo user-name-format
```

【缺省情况】

发送给 HWTACACS 服务器的用户名携带 ISP 域名。

【视图】

HWTACACS 方案视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

keep-original: 发送给 HWTACACS 服务器的用户名与用户输入的保持一致。

with-domain: 发送给 HWTACACS 服务器的用户名携带 ISP 域名。

without-domain: 发送给 HWTACACS 服务器的用户名不携带 ISP 域名。

【使用指导】

接入用户通常以“*userid@isp-name*”的格式命名，“@”后面的部分为 ISP 域名，设备就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些 HWTACACS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 HWTACACS 服务器。因此，设备提供此命令以指定发送给 HWTACACS 服务器的用户名是否携带有 ISP 域名。

如果指定某个 HWTACACS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 HWTACACS 方案。否则，会出现虽然实际用户不同（在不同的 ISP 域中），但 HWTACACS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

【举例】

在 HWTACACS 方案 hwt1 中，设置发送给 HWTACACS 服务器的用户名不携带 ISP 域名。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

【相关命令】

- **display hwtacacs scheme**

1.4.19 vpn-instance (HWTACACS scheme view)

vpn-instance 命令用来配置 HWTACACS 方案所属的 VPN。

undo vpn-instance 命令用来恢复缺省情况。

【命令】

```
vpn-instance vpn-instance-name
undo vpn-instance
```

【缺省情况】

HWTACACS 方案属于公网。

【视图】

HWTACACS 方案视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

vpn-instance-name: MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

本命令配置的 VPN 对于该方案下的所有 HWTACACS 认证/授权/计费服务器生效，但设备优先使用配置认证/授权/计费服务器时指定的各服务器所属的 VPN。

【举例】

配置 HWTACACS 方案 hw1 所属的 VPN 为 test。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] vpn-instance test
```

【相关命令】

- **display hwtacacs scheme**

1.5 LDAP配置命令

1.5.1 attribute-map

attribute-map 命令用来在 LDAP 方案中引用 LDAP 属性映射表。

undo attribute-map 命令用来恢复缺省情况。

【命令】

attribute-map *map-name*

undo attribute-map

【缺省情况】

未引用任何 LDAP 属性映射表。

【视图】

LDAP 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

map-name: LDAP 属性映射表的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

在使用 LDAP 授权方案的情况下，可以通过在 LDAP 方案中引用 LDAP 属性映射表，将 LDAP 授权服务器下发给用户的 LDAP 属性映射为 AAA 模块可以解析的某类属性。

一个 LDAP 方案视图中只能引用一个 LDAP 属性映射表，后配置的生效。

如果在 LDAP 授权过程中修改了引用的 LDAP 属性映射表，或者修改了引用的 LDAP 属性映射表的内容，则该修改对当前的授权过程不会生效，只对修改后新的 LDAP 授权过程生效。

【举例】

在 LDAP 方案 ldap1 中，引用名称为 map1 的 LDAP 属性映射表。

```
<Sysname> system-view
```

```
[Sysname] ldap scheme test
```

```
[Sysname-ldap-test] attribute-map map1
```

【相关命令】

- **display ldap-scheme**
- **ldap attribute-map**

1.5.2 authentication-server

authentication-server 命令用来指定 LDAP 认证服务器。

undo authentication-server 命令用来恢复缺省情况。

【命令】

authentication-server *server-name*

undo authentication-server

【缺省情况】

未指定 LDAP 认证服务器。

【视图】

LDAP 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

server-name: LDAP 服务器的名称，为 1~64 个字符的字符串，不区分大小写。

【使用指导】

一个 LDAP 方案视图下仅能指定一个 LDAP 认证服务器，多次执行本命令，最后一次执行的命令生效。

【举例】

在 LDAP 方案 ldap1 中，指定 LDAP 认证服务器为 ccc。

```
<Sysname> system-view
```

```
[Sysname] ldap scheme ldap1
```

```
[Sysname-ldap-ldap1] authentication-server ccc
```

【相关命令】

- **display ldap scheme**
- **ldap server**

1.5.3 authorization-server

authorization-server 命令用来指定 LDAP 授权服务器。

undo authorization-server 命令用来恢复缺省情况。

【命令】

authorization-server *server-name*

undo authorization-server

【缺省情况】

未指定 LDAP 授权服务器。

【视图】

LDAP 方案视图

【缺省用户角色】

network-admin

context-admin

【参数】

server-name: LDAP 服务器的名称，为 1~64 个字符的字符串，不区分大小写。

【使用指导】

一个 LDAP 方案视图下仅能指定一个 LDAP 授权服务器，多次执行本命令，最后一次执行的命令生效。

【举例】

在 LDAP 方案 ldap1 中，指定 LDAP 授权服务器为 ccc。

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1] authorization-server ccc
```

【相关命令】

- **display ldap scheme**
- **ldap server**

1.5.4 display ldap scheme

display ldap scheme 命令用来查看 LDAP 方案的配置信息。

【命令】

display ldap scheme [*ldap-scheme-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ldap-scheme-name: LDAP 方案的名称，为 1~32 个字符的字符串，不区分大小写。如果不指定该参数，则显示所有 LDAP 方案的配置信息。

【举例】

查看所有 LDAP 方案的配置信息。

```
<Sysname> display ldap scheme
Total 1 LDAP schemes

-----
LDAP scheme name      : aaa
Authentication server : aaa
IP                    : 1.1.1.1
Port                  : 111
VPN instance          : Not configured
```

```

LDAP protocol version      : LDAPv3
Server timeout interval   : 10 seconds
Login account DN          : Not configured
Base DN                   : Not configured
Search scope              : all-level
User searching parameters:
  User object class       : Not configured
  Username attribute      : cn
  Username format         : with-domain
  Group filter            : (objectclass=group)
Authorization server      : aaa
  IP                      : 1.1.1.1
  Port                    : 111
  VPN instance            : Not configured
  LDAP protocol version   : LDAPv3
  Server timeout interval : 10 seconds
  Login account DN        : Not configured
  Base DN                 : Not configured
  Search scope            : all-level
  User searching parameters:
    User object class     : Not configured
    Username attribute     : cn
    Username format       : with-domain
    Group filter          : (objectclass=group)
Attribute map             : map1

```

表1-10 display ldap scheme 命令显示信息描述表

字段	描述
Total 1 LDAP schemes	总共有1个LDAP方案
LDAP Scheme Name	LDAP方案名称
Authentication Server	LDAP认证服务器名称 未配置时，显示为Not configured
Authorization server	LDAP授权服务器名称 未配置时，显示为Not configured
IP	LDAP认证服务器的IP地址 未配置认证服务器IP时，IP地址显示为Not configured
Port	LDAP认证服务器的端口号 未配置认证服务器IP时，端口号显示为缺省值
VPN Instance	VPN实例名称 未配置时，显示为Not configured
LDAP Protocol Version	LDAP协议的版本号（LDAPv2、LDAPv3）
Server Timeout Interval	LDAP服务器连接超时时间（单位为秒）

字段	描述
Login Account DN	管理员用户的DN
Base DN	用户DN查询的起始DN
Search Scope	用户DN查询的范围（all-level: 所有子目录查询，single-level: 下级目录查询）
User Searching Parameters	用户查询参数
User Object Class	查询用户DN时使用的用户对象类型 未配置时，显示为Not configured
Username Attribute	用户登录账号的属性类型
Username Format	发送给服务器的用户名格式
Group filter	LDAP用户组过滤条件
Attribute map	引用的LDAP属性映射表名称 未配置时，显示为Not configured

1.5.5 group-filter

group-filter 命令用来配置用户组过滤条件。

undo group-filter 命令用来恢复缺省情况。

【命令】

group-filter *group-filter*

undo group-filter

【缺省情况】

用户组的过滤条件是"(objectclass=group)"。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-filter: 组过滤条件，为 1~127 个字符的字符串，不区分大小写。组过滤条件字符串的写作规则由 LDAP 服务器定义。

【使用指导】

设备从 LDAP 服务器上导入用户组信息时，LDAP 服务器会根据设置的用户组过滤条件筛选出符合条件的用户组信息发送给设备。

【举例】

在 LDAP 服务器视图 ccc 下，配置用户组过滤条件为(&(objectclass=group)(name=group1))。

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] group-filter (&(objectclass=group)(name=group1))
```

【相关命令】

- **display ldap scheme**

1.5.6 ip

ip 命令用来配置 LDAP 服务器的 IP 地址。

undo ip 命令用来恢复缺省情况。

【命令】

```
ip ip-address [ port port-number ] [ vpn-instance vpn-instance-name ]
undo ip
```

【缺省情况】

未配置 LDAP 服务器的 IP 地址。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: LDAP 服务器的 IP 地址。

port port-number: LDAP 服务器所使用的 TCP 端口号，取值范围为 1~65535，缺省值为 389。

vpn-instance vpn-instance-name: LDAP 服务器所属的 VPN 实例。**vpn-instance-name** 表示 MPLS L3VPN 实例的名称，为 1~31 个字符的字符串，区分大小写。不指定该参数时，表示 LDAP 服务器属于公网。

【使用指导】

需保证设备上的 LDAP 服务端口与 LDAP 服务器上使用的端口设置一致。

更改后的服务器 IP 地址和端口号，只对更改之后进行的 LDAP 认证生效。

【举例】

配置 LDAP 服务器 ccc 的 IP 地址为 192.168.0.10、端口号为 4300。

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] ip 192.168.0.10 port 4300
```

【相关命令】

- **ldap server**

1.5.7 ipv6

ipv6 命令用来配置 LDAP 服务器的 IPv6 地址。

undo ipv6 命令用来恢复缺省情况。

【命令】

ipv6 *ipv6-address* [**port** *port-number*] [**vpn-instance** *vpn-instance-name*]

undo ipv6

【缺省情况】

未配置 LDAP 服务器的 IP 地址。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address: LDAP 服务器的 IPv6 地址。

port port-number: LDAP 服务器所使用的 TCP 端口号，取值范围为 1~65535，缺省值为 389。

vpn-instance vpn-instance-name: LDAP 服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 实例的名称，为 1~31 个字符的字符串，区分大小写。不指定该参数时，表示 LDAP 服务器属于公网。

【使用指导】

需保证设备上的 LDAP 服务端口与 LDAP 服务器上使用的端口设置一致。

更改后的服务器 IP 地址和端口号，只对更改之后的 LDAP 认证生效。

【举例】

配置 LDAP 服务器 ccc 的 IPv6 地址为 1:2::3:4、端口号为 4300。

```
<Sysname> system-view
```

```
[Sysname] ldap server ccc
```

```
[Sysname-ldap-server-ccc] ipv6 1:2::3:4 port 4300
```

【相关命令】

- **ldap server**

1.5.8 ldap attribute-map

ldap attribute-map 命令用来创建 LDAP 属性映射表，并进入 LDAP 属性映射表视图。如果指定的 LDAP 属性映射表已经存在，则直接进入 LDAP 属性映射表视图。

undo ldap attribute-map 命令用来删除指定的 LDAP 属性映射表。

【命令】

ldap attribute-map *map-name*

undo ldap attribute-map *map-name*

【缺省情况】

不存在 LDAP 属性映射表。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

map-name: LDAP 属性映射表的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

一个 LDAP 的属性映射表中可以添加多个 LDAP 属性映射表项，每个表项表示一个 LDAP 属性和一个 AAA 属性的映射关系。

可以通过多次执行本命令配置多个 LDAP 的属性映射表。

【举例】

创建名称为 map1 的 LDAP 属性映射表，并进入该属性映射表视图。

```
<Sysname> system-view
[Sysname] ldap attribute-map map1
[Sysname-ldap-map-map1]
```

【相关命令】

- **attribute-map**
- **ldap scheme**
- **map**

1.5.9 ldap scheme

ldap scheme 命令用来创建 LDAP 方案，并进入 LDAP 方案视图。如果指定的 LDAP 方案已经存在，则直接进入 LDAP 方案视图。

undo ldap scheme 命令用来删除指定的 LDAP 方案。

【命令】

```
ldap scheme ldap-scheme-name
undo ldap scheme ldap-scheme-name
```

【缺省情况】

不存在 LDAP 方案。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ldap-scheme-name: LDAP 方案的名称, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

一个 LDAP 方案可以同时被多个 ISP 域引用。

系统最多支持配置 16 个 LDAP 方案。

【举例】

创建名称为 ldap1 的 LDAP 方案并进入其视图。

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1]
```

【相关命令】

- **display ldap scheme**

1.5.10 ldap server

ldap server 用来创建 LDAP 服务器, 并进入 LDAP 服务器视图。如果指定的 LDAP 服务器已经存在, 则直接进入 LDAP 服务器视图。

undo ldap server 命令用来删除指定的 LDAP 服务器。

【命令】

```
ldap server server-name
undo ldap server server-name
```

【缺省情况】

不存在 LDAP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

server-name: LDAP 服务器的名称, 为 1~64 个字符的字符串, 不区分大小写。

【举例】

创建 LDAP 服务器 ccc 并进入其视图。

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc]
```

【相关命令】

- **display ldap scheme**

1.5.11 login-dn

login-dn 命令用来配置具有管理员权限的用户 DN。

undo login-dn 命令用来恢复缺省情况。

【命令】

login-dn *dn-string*

undo login-dn

【缺省情况】

未配置具有管理员权限的用户 DN。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

context-admin

【参数】

dn-string: 具有管理员权限的用户 DN，是绑定服务器时使用的用户标识名，为 1~255 个字符的字符串，不区分大小写。

【使用指导】

设备上的管理员 DN 必须与服务器上管理员的 DN 一致。

更改后的管理员 DN，只对更改之后的 LDAP 认证生效。

【举例】

在 LDAP 服务器视图 ccc 下，配置管理员权限的用户 DN 为 uid=test, ou=people, o=example, c=city。

```
<Sysname> system-view
```

```
[Sysname] ldap server ccc
```

```
[Sysname-ldap-server-ccc] login-dn uid=test,ou=people,o=example,c=city
```

【相关命令】

- **display ldap scheme**

1.5.12 login-password

login-password 命令用来配置 LDAP 认证中，绑定服务器时所使用的具有管理员权限的用户密码。

undo login-password 命令用来恢复缺省情况。

【命令】

login-password { *cipher* | *simple* } *string*

undo login-password

【缺省情况】

未配置具有管理权限的用户密码。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin
context-admin

【参数】

cipher: 表示以密文方式设置密码。

simple: 表示以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~128 个字符的字符串，密文密码为 1~201 个字符的字符串。

【使用指导】

该命令只有在配置了 **login-dn** 的情况下生效。当未配置 **login-dn** 时，该命令不生效。

【举例】

在 LDAP 服务器视图 ccc 下，配置具有管理员权限的用户密码为明文 abcdefg。

```
<Sysname> system-view
```

```
[Sysname] ldap server ccc
```

```
[Sysname-ldap-server-ccc] login-password simple abcdefg
```

【相关命令】

- **display ldap scheme**
- **login-dn**

1.5.13 map

map 命令用来配置 LDAP 属性映射表项。

undo map 命令用来删除指定的 LDAP 属性映射表项。

【命令】

```
map ldap-attribute ldap-attribute-name [ prefix prefix-value delimiter  
delimiter-value ] aaa-attribute user-group
```

```
undo map [ ldap-attribute ldap-attribute-name ]
```

【缺省情况】

未指定 LDAP 属性映射关系。

【视图】

LDAP 属性映射表视图

【缺省用户角色】

network-admin
context-admin

【参数】

ldap-attribute *ldap-attribute-name*: 表示要映射的 LDAP 属性。其中, *ldap-attribute-name* 表示 LDAP 属性名称, 为 1~63 个字符的字符串, 不区分大小写。

prefix *prefix-value* **delimiter** *delimiter-value*: 表示按照一定的格式提取 LDAP 属性字符串中的内容映射为 AAA 属性。其中, *prefix-value* 表示 LDAP 属性字符串中的某内容前缀 (例如 cn=), 为 1~7 个字符的字符串, 不区分大小写; *delimiter-value* 表示 LDAP 属性字符串中的内容分隔符 (例如逗号)。若不指定该可选参数, 则表示要将一个完整的 LDAP 属性字符串映射为指定的 AAA 属性。

aaa-attribute: 表示要映射为的 AAA 属性。

user-group: 表示 User group 类型的 AAA 属性。

【使用指导】

如果某 LDAP 服务器下发给用户的属性不能被 AAA 模块解析, 则该属性将被忽略。因此, 需要通过本命令指定要获取哪些 LDAP 属性, 以及 LDAP 服务器下发的这些属性将被 AAA 模块解析为什么类型的 AAA 属性, 具体映射为哪种类型的 AAA 属性由实际应用需求决定。

一个 LDAP 服务器属性只能映射为一个 AAA 属性, 但不同的 LDAP 服务器属性可映射为同一个 AAA 属性。

如果 **undo map** 命令中不指定 **ldap-attribute** 参数, 则表示删除所有的 LDAP 属性映射表项。

【举例】

在 LDAP 属性映射表视图 **map1** 下, 配置将 LDAP 服务器属性 **memberof** 按照前缀为 **cn=**、分隔符为逗号 (,) 的格式提取出的内容映射成 AAA 属性 **User group**。

```
<Sysname> system-view
[Sysname] ldap attribute-map map1
[Sysname-ldap-map-map1] map ldap-attribute memberof prefix cn= delimiter , aaa-attribute
user-group
```

【相关命令】

- **ldap attribute-map**
- **user-group**

1.5.14 protocol-version

protocol-version 命令用来配置 LDAP 认证中所支持的 LDAP 协议的版本号。

undo protocol-version 命令用来恢复缺省情况。

【命令】

```
protocol-version { v2 | v3 }
undo protocol-version
```

【缺省情况】

LDAP 版本号为 LDAPv3。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin
context-admin

【参数】

v2: 表示 LDAP 协议版本号为 LDAPv2。

v3: 表示 LDAP 协议版本号为 LDAPv3。

【使用指导】

为保证 LDAP 认证成功，请保证设备上的 LDAP 版本号与 LDAP 服务器上使用的版本号一致。
更改后的服务器版本号，只对更改之后的 LDAP 认证生效。

Microsoft 的 LDAP 服务器只支持 LDAPv3，配置 LDAP 版本为 v2 时无效。

【举例】

在 LDAP 服务器视图 ccc 下，配置 LDAP 协议版本号为 LDAPv2。

```
<Sysname> system-view  
[Sysname] ldap server ccc  
[Sysname-ldap-server-ccc] protocol-version v2
```

【相关命令】

- **display ldap scheme**

1.5.15 search-base-dn

search-base-dn 命令用来配置用户查询的起始 DN。

undo search-base-dn 命令用来恢复缺省情况。

【命令】

```
search-base-dn base-dn  
undo search-base-dn
```

【缺省情况】

未指定用户查询的起始 DN。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin
context-admin

【参数】

base-dn: 查询待认证用户的起始 DN 值，为 1~255 个字符的字符串，不区分大小写。

【举例】

在 LDAP 服务器视图 ccc 下，配置用户查询的起始 DN 为 dc=ldap,dc=com。

```
<Sysname> system-view  
[Sysname] ldap server ccc
```

```
[Sysname-ldap-server-ccc] search-base-dn dc=ldap,dc=com
```

【相关命令】

- **display ldap scheme**
- **ldap server**

1.5.16 search-scope

search-scope 命令用来配置用户查询的范围。

undo search-scope 命令用来恢复缺省情况。

【命令】

```
search-scope { all-level | single-level }  
undo search-scope
```

【缺省情况】

用户查询的范围为 **all-level**。

【视图】

LDAP 服务器视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

all-level: 表示在起始 DN 的所有子目录下进行查询。

single-level: 表示只在起始 DN 的下一级子目录下进行查询。

【举例】

在 LDAP 服务器视图 ccc 下，配置在起始 DN 的所有子目录下查询 LDAP 认证用户。

```
<Sysname> system-view  
[Sysname] ldap server ccc  
[Sysname-ldap-server-ccc] search-scope all-level
```

【相关命令】

- **display ldap scheme**
- **ldap server**

1.5.17 server-timeout

server-timeout 命令用来配置 LDAP 服务器连接超时时间，即认证、授权时等待 LDAP 服务器回应的最大时间。

undo server-timeout 命令用来恢复缺省情况。

【命令】

```
server-timeout time-interval  
undo server-timeout
```

【缺省情况】

LDAP 服务器连接超时时间为 10 秒。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin
context-admin

【参数】

time-interval: LDAP 服务器连接超时时间，取值范围为 5~20，单位为秒。

【使用指导】

更改后的连接超时时间，只对更改之后的 LDAP 认证生效。

【举例】

```
# 在 LDAP 服务器视图 ccc 下，配置 LDAP 服务器连接超时时间为 15 秒。
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] server-timeout 15
```

【相关命令】

- **display ldap scheme**

1.5.18 user-parameters

user-parameters 命令用来配置 LDAP 用户查询的属性参数，包括用户名属性、用户名格式和自定义用户对象类型。

undo user-parameters 命令用来将指定的 LDAP 用户查询的属性参数恢复为缺省值。

【命令】

```
user-parameters { user-name-attribute { name-attribute | cn | uid } |  
user-name-format { with-domain | without-domain } | user-object-class  
object-class-name }  
undo user-parameters { user-name-attribute | user-name-format |  
user-object-class }
```

【缺省情况】

user-name-attribute 为 **cn**；**user-name-format** 为 **without-domain**；未指定自定义 **user-object-class**，根据使用的 LDAP 服务器的类型使用各服务器缺省的用户对象类型。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin
context-admin

【参数】

user-name-attribute { *name-attribute* | **cn** | **uid** }: 表示用户名的属性类型。其中, *name-attribute* 表示属性类型值, 为 1~64 个字符的字符串, 不区分大小写; **cn** 表示用户登录账号的属性为 cn (Common Name); **uid** 表示用户登录账号的属性为 uid (User ID)。

user-name-format { **with-domain** | **without-domain** }: 表示发送给服务器的用户名格式。其中, **with-domain** 表示发送给服务器的用户名带 ISP 域名; **without-domain** 表示发送给服务器的用户名不带 ISP 域名。

user-object-class *object-class-name*: 表示查询用户 DN 时使用的用户对象类型。其中, *object-class-name* 表示对象类型值, 为 1~64 个字符的字符串, 不区分大小写。

【使用指导】

如果 LDAP 服务器上的用户名不包含域名, 必须配置 **user-name-format** 为 **without-domain**, 将用户名的域名去除后再传送给 LDAP 服务器; 如果包含域名则需配置 **user-name-format** 为 **with-domain**。

【举例】

在 LDAP 服务器视图 ccc 下, 配置用户对象类型为 person。

```
<Sysname> system-view
```

```
[Sysname] ldap server ccc
```

```
[Sysname-ldap-server-ccc] user-parameters user-object-class person
```

【相关命令】

- **display ldap scheme**
- **login-dn**

目 录

1 Password Control	1-1
1.1 Password Control 配置命令	1-1
1.1.1 display password-control	1-1
1.1.2 display password-control blacklist	1-2
1.1.3 password-control { aging composition history length } enable	1-3
1.1.4 password-control aging	1-5
1.1.5 password-control alert-before-expire	1-6
1.1.6 password-control change-password first-login enable	1-6
1.1.7 password-control complexity	1-7
1.1.8 password-control composition	1-8
1.1.9 password-control enable	1-9
1.1.10 password-control expired-user-login	1-10
1.1.11 password-control history	1-11
1.1.12 password-control length	1-12
1.1.13 password-control login idle-time	1-13
1.1.14 password-control login-attempt	1-14
1.1.15 password-control super aging	1-15
1.1.16 password-control super composition	1-16
1.1.17 password-control super length	1-17
1.1.18 password-control update-interval	1-17
1.1.19 reset password-control blacklist	1-18
1.1.20 reset password-control history-record	1-19

1 Password Control

1.1 Password Control 配置命令

1.1.1 display password-control

display password-control 命令用来显示密码管理的配置信息。

【命令】

display password-control [super]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

super: 显示 super 密码管理的配置信息。如果不指定该参数，将显示全局密码管理的配置信息。

【举例】

显示全局密码管理的配置信息。

```
<Sysname> display password-control
Global password control configurations:
Password control:                Enabled
Password aging:                  Enabled (90 days)
Password length:                 Enabled (10 characters)
Password composition:            Enabled (1 types, 1 characters per type)
Password history:                Enabled (max history records:4)
Early notice on password expiration: 7 days
Maximum login attempts:          3
Action for exceeding login attempts: Lock user for 1 minutes
Minimum interval between two updates: 24 hours
User account idle time:          90 days
Logins with aged password:       3 times in 30 days
Password complexity:             Disabled (username checking)
                                 Disabled (repeated characters checking)
Password change:                 Enabled (first login)
```

显示 super 密码管理的配置信息。

```
<Sysname> display password-control super
Super password control configurations:
Password aging:                  Enabled (90 days)
```

Password length: Enabled (10 characters)
 Password composition: Enabled (1 types, 1 characters per type)

表1-1 display password-control 命令显示信息描述表

字段	描述
Global password control configurations	全局密码管理配置
Super password control configurations	Super密码管理配置
Password control	全局密码管理功能的开启状态
Password aging	密码老化功能的开启状态（密码的老化时间）
Password length	密码最小长度功能的开启状态（密码的最小长度）
Password composition	密码组合策略的开启状态（密码元素的组合类型、至少要包含每种元素的个数）
Password history	密码历史记录功能的开启状态（密码历史记录的最大条数）
Early notice on password expiration	密码过期前的提醒时间
Maximum login attempts	用户最大登录尝试次数
Action for exceeding login attempts	登录尝试次数达到设定次数后的用户帐户锁定行为
Minimum interval between two updates	密码更新的最小时间间隔
User account idle time	用户帐号闲置时间
Logins with aged password	密码过期后允许用户登录的次数和时间
Password complexity	密码复杂度检查功能的开启状态（检查是否包含用户名或者颠倒的用户名；检查是否包含三个或以上相同字符）
Password change	修改密码功能的状态： - Enabled (first login): 开启首次登录修改密码功能 - Disabled (first login): 关闭首次登录修改密码功能

1.1.2 display password-control blacklist

display password-control blacklist 命令用来显示用户认证失败后，被加入密码管理黑名单中的用户信息。

【命令】

display password-control blacklist [*user-name user-name* | *ip ipv4-address* | *ipv6 ipv6-address*]

【视图】

任意视图

【缺省用户角色】

network-admin
 network-operator

context-admin
context-operator

【参数】

user-name *user-name*: 显示密码管理黑名单中指定用户名的用户信息。其中，*user-name* 表示用户名，为 1~55 个字符的字符串，区分大小写。

ip *ipv4-address*: 显示密码管理黑名单中指定 IPv4 地址的用户信息。

ipv6 *ipv6-address*: 显示密码管理黑名单中指定 IPv6 地址的用户信息。

【使用指导】

如果不指定任何参数，则显示密码管理黑名单中的所有用户信息。

用户在认证失败后，其 IP 地址和用户名会被加入密码管理的黑名单。通过本命令可以查看被加入密码管理黑名单中的 FTP 用户和通过 Web 或 VTY 方式访问设备的用户。

通过 Console 口连接到设备的用户，由于系统无法获得其 IP 地址，且这类访问设备的用户已经具备了一定的权限和安全性，所以认证失败后不会被加入密码管理的黑名单。

【举例】

显示用户认证失败后，被加入密码管理黑名单中的用户信息。

```
<Sysname> display password-control blacklist
Blacklist items matched: 2.
Username                IP address             Login failures  Lock flag
-----
abcd                    169::168:34:1          4              lock
admin                   192.168.34.1           1              unlock
```

表1-2 display password-control blacklist 命令显示信息描述表

字段	描述
Blacklist items matched	匹配的黑名单表项数目
Username	用户名
IP address	用户的IP地址
Login failures	用户登录失败的次数
Lock flag	该用户是否被锁定 - unlock: 表示未锁定，允许用户再次尝试登录 - lock: 表示锁定，暂时或永久禁止用户通过登录失败 IP 地址尝试登录（具体由 password-control login-attempt 命令的配置情况决定）

1.1.1.3 password-control { aging | composition | history | length } enable

password-control { aging | composition | history | length } enable 命令用来使能指定的密码管理功能。

undo password-control { aging | composition | history | length } enable 命令用来关闭指定的密码管理功能。

【命令】

```
password-control { aging | composition | history | length } enable
undo password-control { aging | composition | history | length } enable
```

【缺省情况】

各密码管理功能均处于使能状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

aging: 使能密码老化管理功能。

composition: 使能密码的组合检测管理功能。

history: 使能密码历史记录管理功能。

length: 使能密码最小长度管理功能。

【使用指导】

要使指定的密码管理功能生效，首先必须保证全局密码管理功能处于使能状态，其次要保证对应的密码管理功能处于使能状态。例如，若全局密码管理功能或密码最小长度管理功能处于未使能状态，则 **password-control length** 命令配置的具体长度限制就不会生效。

密码历史记录管理功能关闭后，系统将不再记录历史密码，但之前已经存在的密码历史记录依然保存。

使能了全局密码管理功能，未使能密码最小长度管理功能时，密码的最小长度为 4 个字符，且至少要有四个字符不同。

【举例】

```
# 使能全局密码管理功能。
<Sysname> system-view
[Sysname] password-control enable
# 使能密码组合检测管理功能。
[Sysname] password-control composition enable
# 使能密码老化功能。
[Sysname] password-control aging enable
# 使能密码最小长度功能。
[Sysname] password-control length enable
# 使能密码历史记录功能。
[Sysname] password-control history enable
```

【相关命令】

- **display password-control**
- **password-control enable**

1.1.4 password-control aging

password-control aging 命令用来配置密码的老化时间。

undo password-control aging 命令用来恢复缺省情况。

【命令】

password-control aging aging-time

undo password-control aging

【缺省情况】

全局的密码老化时间为 90 天；用户组的密码老化时间为全局配置的密码老化时间；本地用户的密码老化时间为所属用户组的密码老化时间。

【视图】

系统视图

用户组视图

本地用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

aging-time: 密码的老化时间，取值范围为 1~365，单位为天。

【使用指导】

系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。

该配置的生效优先级顺序由高到低依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

【举例】

配置全局的密码老化时间为 80 天。

```
<Sysname> system-view
```

```
[Sysname] password-control aging 80
```

配置用户组 test 的密码老化时间为 90 天。

```
[Sysname] user-group test
```

```
[Sysname-ugroup-test] password-control aging 90
```

```
[Sysname-ugroup-test] quit
```

配置设备管理类本地用户 abc 的密码老化时间为 100 天。

```
[Sysname] local-user abc class manage
```

```
[Sysname-luser-manage-abc] password-control aging 100
```

【相关命令】

- **display local-user**（安全命令参考/AAA）
- **display password-control**

- **display user-group** (安全命令参考/AAA)
- **password-control aging enable**

1.1.5 password-control alert-before-expire

password-control alert-before-expire 命令用来配置密码过期前的提醒时间。

undo password-control alert-before-expire 命令用来恢复缺省情况。

【命令】

```
password-control alert-before-expire alert-time
undo password-control alert-before-expire
```

【缺省情况】

密码过期前的提醒时间为 7 天，表示在密码过期之前 7 天内，系统会在用户登录时提醒其密码即将过期。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

alert-time: 密码过期前的提醒时间，取值范围为 1~30，单位为天。

【使用指导】

不允许 FTP 用户更改密码，只能由管理员修改 FTP 用户的密码，因此本命令配置的过期提醒时间仅对非 FTP 类型的 Login 用户有效。

【举例】

```
# 设定密码过期前的提醒时间为 10 天。
<Sysname> system-view
[Sysname] password-control alert-before-expire 10
```

【相关命令】

- **display password-control**

1.1.6 password-control change-password first-login enable

password-control change-password first-login enable 命令用来开启首次登录修改密码功能。

undo password-control change-password first-login enable 命令用来用来关闭首次登录修改密码功能。

【命令】

```
password-control change-password first-login enable
undo password-control change-password first-login enable
```

【缺省情况】

用户首次登录设备时修改密码功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

若要首次登录修改密码功能生效，必须保证全局密码管理功能和首次登录修改密码功能均处于开启状态。

【举例】

开启首次登录修改密码功能。

```
<Sysname> system-view
```

```
[Sysname] password-control change-password first-login enable
```

【相关命令】

- **display password-control**
- **password-control enable**

1.1.7 password-control complexity

password-control complexity 命令用来配置用户密码的复杂度检查策略。

undo password-control complexity 命令用来取消指定的密码复杂度检查策略。

【命令】

```
password-control complexity { same-character | user-name } check
```

```
undo password-control complexity { same-character | user-name } check
```

【缺省情况】

全局的密码复杂度检查策略为：不对用户密码进行复杂度检查，允许密码中包含用户名或者字符顺序颠倒的用户名，也允许包含连续三个或以上的相同字符；用户组的密码复杂度检查策略为全局的密码复杂度检查策略；本地用户的密码复杂度检查策略为所属用户组的密码复杂度检查策略。

【视图】

系统视图

用户组视图

本地用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

same-character: 指定检查密码中是否包含连续三个或以上相同的字符。例如，密码 **aaabc** 就不符合该项复杂度检查。

user-name: 指定检查密码中是否包含用户名或者字符顺序颠倒的用户名。例如，用户名为 **123**，则密码 **abc123**、**321df** 就不符合该项复杂度检查。

【使用指导】

系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。

该配置的生效优先级顺序由高到低依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

可以通过多次执行本命令同时打开用户名检查以及连续字符检查功能。

【举例】

配置密码复杂度检测策略为，检查配置的密码中是否包含用户名或者字符顺序颠倒的用户名。

```
<Sysname> system-view
[Sysname] password-control complexity user-name check
```

【相关命令】

- **display local-user**（安全命令参考/AAA）
- **display password-control**
- **display user-group**（安全命令参考/AAA）

1.1.8 password-control composition

password-control composition 命令用来配置用户密码的组合策略。

undo password-control composition 命令用来恢复缺省情况。

【命令】

```
password-control composition type-number type-number [ type-length  
type-length ]  
undo password-control composition
```

【缺省情况】

全局的密码元素的最少组合类型为 **1** 种，至少要包含每种元素的个数为 **1** 个；用户组的密码组合策略为全局配置的密码组合策略；本地用户的密码组合策略为所属用户组的密码组合策略。

【视图】

系统视图

用户组视图

本地用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

type-number *type-number*: 密码元素的最少组合类型。其中, *type-number* 表示组合类型的个数, 取值范围为 1~4。

type-length *type-length*: 密码中至少要包含每种元素的个数。其中, *type-length* 表示元素个数, 取值范围为 1~63。

【使用指导】

系统视图下配置具有全局性, 对所有用户组有效, 用户组视图下的配置对用户组内所有本地用户有效, 本地用户视图下的配置只对当前本地用户有效。

该配置的生效优先级顺序由高到低依次为本地用户视图、用户组视图、全局视图。即, 系统优先采用本地用户视图下的配置, 若本地用户视图下未配置, 则采用用户组视图下的配置, 若用户组视图下也未配置, 则采用全局视图下的配置。

密码元素的最少组合类型数以及每种元素的最小个数的乘积应该小于允许的最大密码长度。

【举例】

```
# 配置全局的密码元素的最少组合类型为 4 种, 至少要包含每种元素的个数为 5 个。
<Sysname> system-view
[Sysname] password-control composition type-number 4 type-length 5
# 配置用户组 test 的密码元素的最少组合类型为 4 种, 至少要包含每种元素的个数为 5 个。
[Sysname] user-group test
[Sysname-ugroup-test] password-control composition type-number 4 type-length 5
[Sysname-ugroup-test] quit
# 配置设备管理类本地用户 abc 的密码元素的最少组合类型为 4 种, 至少要包含每种元素的个数为 5 个。
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control composition type-number 4 type-length 5
```

【相关命令】

- **display local-user** (安全命令参考/AAA)
- **display password-control**
- **display user-group** (安全命令参考/AAA)
- **password-control composition enable**

1.1.9 password-control enable

password-control enable 命令用来使能全局密码管理功能。

undo password-control enable 命令用来关闭全局密码管理功能。

【命令】

```
password-control enable
undo password-control enable
```

【缺省情况】

全局密码管理功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

只有在使能了全局密码管理功能的情况下，其它指定的密码管理功能才能生效。

使能全局密码管理功能后，设备管理类本地用户密码以及 **super** 密码的配置将不被显示，即无法通过相应的 **display** 命令查看到设备管理类本地用户密码以及 **super** 密码的配置。网络接入类本地用户密码不受密码管理功能控制，其配置显示也不受影响。

使能全局密码管理功能后，首次设置的设备管理类本地用户密码必须至少由四个不同的字符组成。

【举例】

使能全局密码管理功能。

```
<Sysname> system-view
```

```
[Sysname] password-control enable
```

【相关命令】

- **display password-control**
- **password-control { aging | composition | history | length } enable**

1.1.10 password-control expired-user-login

password-control expired-user-login 命令用来配置密码过期后允许用户登录的时间和次数。

undo password-control expired-user-login 命令用来恢复缺省情况。

【命令】

```
password-control expired-user-login delay delay times times
```

```
undo password-control expired-user-login
```

【缺省情况】

密码过期后允许登录的时间为 30 天，允许登录的次数为 3 次，即密码过期后系统还允许用户在 30 天内使用老密码登录 3 次，超过 30 天或登录次数超过 3 次后，系统提示用户设置新密码。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

delay delay: 密码过期后允许用户登录的时长，取值范围为 1~90，单位为天。

times times: 密码过期后允许用户登录的最大次数，取值范围为 0~10。0 表示密码过期后系统直接提示用户设置新密码。

【使用指导】

该配置仅对非 FTP 类型的 Login 用户生效。对于 FTP 用户，密码过期后，系统不允许其继续登录。

【举例】

```
# 设定允许用户在密码过期之后的 60 天内登录 5 次。  
<Sysname> system-view  
[Sysname] password-control expired-user-login delay 60 times 5
```

【相关命令】

- **display password-control**

1.1.11 password-control history

password-control history 命令用来配置每个用户密码历史记录的最大条数。

undo password-control history 命令用来恢复缺省情况。

【命令】

```
password-control history max-record-number  
undo password-control history
```

【缺省情况】

每个用户密码历史记录的最大条数为 4 条。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

max-record-number: 每个用户密码历史记录的最大条数，取值范围为 2~15。

【使用指导】

当记录的某用户的历史密码条数达到最大值后，该用户的后续新密码历史记录将覆盖最老的一条密码历史记录。

密码历史记录管理功能关闭后，系统将不再记录历史密码，但之前已经存在的密码历史记录依然保存。只有当关闭全局密码管理功能（**undo password-control enable**）或手动清除历史密码记录时（**reset password-control history-record**），历史密码记录才会被清除掉。

【举例】

```
# 配置每个用户密码历史记录的最大条数为 10 条。  
<Sysname> system-view  
[Sysname] password-control history 10
```


【相关命令】

- **display password-control**
- **password-control history enable**
- **reset password-control blacklist**

1.1.12 password-control length

password-control length 命令用来配置密码的最小长度。

undo password-control length 命令用来恢复缺省情况。

【命令】

password-control length *length*

undo password-control length

【缺省情况】

全局的密码最小长度为 10 个字符；用户组的密码最小长度为全局配置的密码最小长度；本地用户的密码最小长度为所属用户组的密码最小长度。

【视图】

系统视图

用户组视图

本地用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

length: 密码的最小长度，取值范围为 4~32。

【使用指导】

系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。

该配置的生效优先级顺序由高到低依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

【举例】

配置全局的密码最小长度为 16 个字符。

```
<Sysname> system-view
```

```
[Sysname] password-control length 16
```

配置用户组 test 的密码最小长度为 16 个字符。

```
[Sysname] user-group test
```

```
[Sysname-ugroup-test] password-control length 16
```

```
[Sysname-ugroup-test] quit
```

配置设备管理类本地用户 abc 的密码最小长度为 16 个字符。

```
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control length 16
```

【相关命令】

- **display local-user**（安全命令参考/AAA）
- **display password-control**
- **display user-group**（安全命令参考/AAA）
- **password-control length enable**

1.1.13 password-control login idle-time

password-control login idle-time 命令用来配置用户帐号的闲置时间。

undo password-control login idle-time 命令用来恢复缺省情况。

【命令】

```
password-control login idle-time idle-time
undo password-control login idle-time
```

【缺省情况】

用户帐号的闲置时间为 90 天。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

idle-time: 用户帐号的闲置时间，取值范围为 0~365，单位为天。0 表示对用户帐号闲置时间无限制。

【使用指导】

如果用户自最后一次成功登录后，在指定的闲置时间内再未成功登录过设备，那么该用户帐号将会失效。

用户最后一次登录设备成功后，若系统时间变化，也可能导致用户账号失效。

账号失效后，用户将无法正常使用设备。若不需要账号闲置时间检查功能，可将 **idle-time** 配置为 0，表示 Password Control 功能对用户账号闲置时间无限制。

【举例】

设定用户帐号的闲置时间为 30 天，表示自最后一次成功登录后，若用户在 30 天内再未成功登录过设备，那么该用户帐号将会失效。

```
<Sysname> system-view
[Sysname] password-control login idle-time 30
```

【相关命令】

- **display password-control**

1.1.14 password-control login-attempt

password-control login-attempt 命令用来配置允许用户登录的最大尝试次数以及登录尝试失败后的处理措施。

undo password-control login-attempt 命令用来恢复缺省情况。

【命令】

```
password-control login-attempt login-times [ exceed { lock | lock-time time  
| unlock } ]  
undo password-control login-attempt
```

【缺省情况】

全局的用户登录尝试次数限制策略为：用户登录尝试的最大次数为3次。如果某用户登录尝试失败，则1分钟后再允许该用户重新登录；用户组的用户登录尝试次数限制策略为全局配置的用户登录尝试次数限制策略；本地用户的登录尝试次数限制策略为所属用户组的用户登录尝试次数限制策略。

【视图】

系统视图
用户组视图
本地用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

login-times：用户登录尝试的最大次数，取值范围为2~10。

exceed：对登录尝试失败次数超过最大值的用户所采取的处理措施。

lock：表示永久禁止该用户通过登录失败IP地址登录。

lock-time time：表示禁止该用户通过登录失败IP地址登录，经过一段时间后，再允许该用户重新登录。其中，*time*为禁止该用户的时间，取值范围为1~360，单位为分钟。

unlock：表示不禁止该用户，允许其继续通过现有IP地址登录。

【使用指导】

系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。

该配置的生效优先级顺序由高到低依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

FTP用户和通过Web或VTY方式访问设备的用户登录认证失败后，系统会将其用户名和IP地址加入密码管理的黑名单。当登录失败次数超过指定值后，系统将会根据此处配置的处理措施对其之后的登录行为进行相应的限制，并且该用户只能在满足相应的条件后才可重新登录：

- 对于被永久禁止登录的用户，只有管理员使用 **reset password-control blacklist** 命令把该用户从密码管理的黑名单中删除后，该用户才能重新登录。

- 对于被禁止一段时间内登录的用户，当配置的禁止时间超时或者管理员使用 **reset password-control blacklist** 命令将其从密码管理的黑名单中删除，该用户才可以重新登录。
 - 对于不禁止登录的用户，只要用户登录成功后，该用户就会从该黑名单中删除。
- 本命令生效后，会立即影响密码管理黑名单中当前用户的锁定状态以及这些用户后续的登录。

【举例】

管理员设定用户登录尝试次数为 4 次，并且永久禁止该用户通过现有 IP 地址登录。

```
<Sysname> system-view
```

```
[Sysname] password-control login-attempt 4 exceed lock
```

之后，若有用户连续尝试认证的失败累加次数达到 4 次，管理员可通过命令查看到被加入密码管理黑名单中的用户锁定状态由之前的 **unlock** 切换为 **lock**，且该用户无法再次通过现有 IP 地址成功登录。

```
[Sysname] display password-control blacklist
```

Username	IP address	Login failures	Lock flag
test	192.168.44.1	4	lock

管理员设定用户登录尝试次数为 2 次，并且限制该用户在 3 分钟后才能重新登录。

```
<Sysname> system-view
```

```
[Sysname] password-control login-attempt 2 exceed lock-time 3
```

之后，若有用户连续尝试认证的失败累加次数达到 2 次，管理员可通过命令查看到被加入密码管理黑名单中的用户锁定状态由之前的 **unlock** 切换为 **lock**。

```
[Sysname] display password-control blacklist
```

Username	IP address	Login failures	Lock flag
test	192.168.44.1	2	lock

若用户被禁止通过现有的 IP 地址登录，经过 3 分钟后，将被从密码管理黑名单中删除，且可以重新登录。

【相关命令】

- **display local-user**（安全命令参考/AAA）
- **display password-control**
- **display password-control blacklist**
- **display user-group**（安全命令参考/AAA）
- **reset password-control blacklist**

1.1.15 password-control super aging

password-control super aging 命令用来配置 super 密码的老化时间。

undo password-control super aging 命令用来恢复缺省情况。

【命令】

```
password-control super aging aging-time
```

```
undo password-control super aging
```

【缺省情况】

密码的老化时间为 90 天。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

aging-time: super 密码的老化时间，取值范围为 1~365，单位为天。

【举例】

设定 super 密码的老化时间为 10 天。

```
<Sysname> system-view
```

```
[Sysname] password-control super aging 10
```

【相关命令】

- **display password-control**
- **password-control aging**

1.1.16 password-control super composition

password-control super composition 命令用来配置 super 密码的组合策略。

undo password-control super composition 命令用来恢复缺省情况。

【命令】

```
password-control super composition type-number type-number [ type-length  
type-length ]
```

```
undo password-control super composition
```

【缺省情况】

super 密码的最少组合类型为 1 种，每种类型至少包含 1 个字符。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

type-number *type-number*: super 密码的最少组合类型。其中，*type-number* 表示组合类型，取值范围为 1~4。

type-length *type-length*: super 密码中每种类型的最少字符个数。其中，*type-length* 表示字符个数，取值范围为 1~63。

【使用指导】

密码元素的最少组合类型数以及每种元素的最小个数的乘积应该小于密码允许的最大长度。

【举例】

配置 super 密码的最少组合类型为 4 种，每种类型的最少字符个数为 5 个。

```
<Sysname> system-view
```

```
[Sysname] password-control super composition type-number 4 type-length 5
```

【相关命令】

- **display password-control**
- **password-control composition**

1.1.17 password-control super length

password-control super length 命令用来配置 super 密码的最小长度。

undo password-control super length 命令用来恢复缺省情况。

【命令】

```
password-control super length length
```

```
undo password-control super length
```

【缺省情况】

super 密码的最小长度为 10 个字符。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

length: super 密码的最小字符长度，取值范围为 4~63。

【举例】

设定 super 密码的最小长度为 16 个字符。

```
<Sysname> system-view
```

```
[Sysname] password-control super length 16
```

【相关命令】

- **display password-control**
- **password-control length**

1.1.18 password-control update-interval

password-control update-interval 命令用来配置密码更新的最小时间间隔。

undo password-control update-interval 命令用来恢复缺省情况。

【命令】

```
password-control update-interval interval
```

```
undo password-control update-interval
```

【缺省情况】

密码更新的最小时间间隔为 24 小时。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval: 密码更新的最小时间间隔，取值范围为 0~168，单位为小时。0 表示对密码更新的时间间隔无限制。

【使用指导】

有两种情况下的密码更新并不受该功能的约束：用户首次登录设备时系统要求用户修改密码；密码老化后系统要求用户修改密码。

【举例】

```
# 设定密码更新的最小时间间隔为 36 小时。  
<Sysname> system-view  
[Sysname] password-control update-interval 36
```

【相关命令】

- **display password-control**

1.1.19 reset password-control blacklist

reset password-control blacklist 命令用来清除密码管理黑名单中的用户。

【命令】

```
reset password-control blacklist [ user-name user-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-name user-name: 清除密码管理黑名单中指定的用户。其中，*user-name* 表示用户名，为 1~55 个字符的字符串，区分大小写。

【使用指导】

对于因为登录认证时密码尝试的失败次数超过最大值而被禁止通过现有 IP 地址登录的用户，管理员可以使用本命令将其从黑名单中删除，使其可以重新登录。

【举例】

```
# 清除密码管理黑名单中的用户 test。
<Sysname> reset password-control blacklist user-name test
Are you sure to delete the specified user in blacklist? [Y/N]:
```

【相关命令】

- **display password-control blacklist**

1.1.20 reset password-control history-record

reset password-control history-record 命令用来清除用户的密码历史记录。

【命令】

```
reset password-control history-record [ super [ role role-name ] | user-name user-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

super: 删除 super 密码的历史记录。

role *role-name*: 删除指定用户角色的用户密码历史记录。其中，*role-name* 表示用户角色，为 1~63 个字符的字符串，区分大小写。如果不指定参数此参数，将删除所有 super 密码的历史记录。

user-name *user-name*: 删除指定用户名的密码历史记录。其中，*user-name* 表示用户名，为 1~55 个字符的字符串，区分大小写。

【使用指导】

如果不指定任何参数，将删除所有本地用户的密码历史记录。

【举例】

```
# 清除所有本地用户的密码历史记录。当用户输入 Y，系统将删除所有本地用户的密码历史记录。
<Sysname> reset password-control history-record
Are you sure to delete all local user's history records? [Y/N]:y
```

【相关命令】

- **password-control history**

目 录

1 公钥管理.....	1-1
1.1 公钥管理配置命令.....	1-1
1.1.1 display public-key local public.....	1-1
1.1.2 display public-key peer	1-5
1.1.3 peer-public-key end.....	1-6
1.1.4 public-key local create	1-7
1.1.5 public-key local destroy.....	1-10
1.1.6 public-key local export dsa.....	1-11
1.1.7 public-key local export ecdsa	1-14
1.1.8 public-key local export rsa	1-15
1.1.9 public-key local import	1-17
1.1.10 public-key peer	1-18
1.1.11 public-key peer import sshkey.....	1-19

1 公钥管理

1.1 公钥管理配置命令

1.1.1 display public-key local public

display public-key local public 命令用来显示本地非对称密钥对中的公钥信息。

【命令】

display public-key local { dsa | ecdsa | rsa } public [name key-name]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

dsa: 显示本地 DSA 密钥对中的公钥信息。

ecdsa: 显示本地 ECDSA 密钥对中的公钥信息。

rsa: 显示本地 RSA 密钥对中的公钥信息。

name key-name: 显示指定的本地非对称密钥对的公钥信息。**key-name** 为本地非对称密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示指定类型的所有本地非对称密钥对的公钥信息。

【使用指导】

如果通过手工配置方式将本地的主机公钥保存到远端设备上，则需要事先在本地设备上执行本命令显示主机公钥信息，并记录该信息。

对于默认名称的密钥对，不能通过指定 **name key-name** 参数显示；显示指定类型的所有本地非对称密钥对时会显示默认名称的密钥对。

【举例】

显示所有本地 RSA 密钥对中的公钥信息。

<Sysname> display public-key local rsa public

```
=====
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
```

```

667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
2DA4C04EF5AE0835090203010001
=====
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
307C300D06092A864886F70D0101010500036B003068026100CAB4CACC16442AD5F453442
762F03897E0D494FEDE69224F5C051A441D290976733A278C9F0C0F5A198E66143EAB54A64
DB608269CAE844B1E7CC64AD7E808972E7CF887F3B657F056E7930FC84FBF1AD83A01CC47E
9D85C13413996ECD093B0203010001
=====
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
92D8C6D940890BF4290203010001
# 显示所有本地 DSA 密钥对中的公钥信息。
<Sysname> display public-key local dsa public

=====
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 15:41:37 2011/05/12
Key code:
308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
585DA7F42519718CC9B09EEF0381840002818041912CE34D12BCD2157E7AB1C2F03B3EF395
100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
=====
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:

```

```
308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

显示所有本地 ECDSA 密钥对中的公钥信息。

```
<Sysname> display public-key local ecdsa public
```

```
=====
Key name: ecdsakey (default)
Key type: ECDSA
Time when key pair created: 15:42:04 2011/05/12
Key code:
3049301306072A8648CE3D020106082A8648CE3D03010103320004C10CF7CE42193F7FC2AF
68F5DC877835A43009DB6135558A7FB8316C361B0690B4FD84A14C0779C76DD6145BF9362B
1D
```

```
=====
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
4D
```

显示名称为 rsa1 的本地 RSA 密钥对中的公钥信息。

```
<Sysname> display public-key local rsa public name rsa1
```

```
=====
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
92D8C6D940890BF4290203010001
```

显示名称为 dsa1 的本地 DSA 密钥对中的公钥信息。

```
<Sysname> display public-key local dsa public name dsa1
```

```
=====
```

```
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

显示名称为 **ecdsa1** 的本地 **ECDSA** 密钥对中的公钥信息。

```
<Sysname> display public-key local ecdsa public name ecdsa1
```

```
=====
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
4D
```

表1-1 display public-key local public 命令显示信息描述表

字段	描述
Key name	本地非对称密钥对的名称 default表示该名称为密钥对的默认名称，即执行 public-key local create 命令没有指定密钥名称时，生成的密钥对的名称 - hostkey: RSA 主机密钥对的默认名称 - serverkey: RSA 服务器密钥对的默认名称。只有密钥类型为 RSA 时，才会存在服务器密钥对 - dsakey: DSA 主机密钥对的默认名称 - ecdsakey: ECDSA 主机密钥对的默认名称
Key type	密钥类型，取值包括： - RSA: 密钥类型为 RSA - DSA: 密钥类型为 DSA - ECDSA: 密钥类型为 ECDSA
Storage device serial number	生成该密钥对的加密设备序列号，如果密钥对由软件算法生成，则不显示本字段
Time when key pair created	本地非对称密钥对产生的时间

字段	描述
Key code	本地非对称密钥对的公钥数据

【相关命令】

- **public-key local create**

1.1.2 display public-key peer

display public-key peer 命令用来显示保存在本地的远端主机的公钥信息。

【命令】

display public-key peer [**brief** | **name** *publickey-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

brief: 显示保存在本地的所有远端主机公钥的简要信息。

name *publickey-name*: 显示保存在本地的指定远端主机公钥的详细信息, *publickey-name* 为远端主机公钥的名称, 为 1~64 个字符的字符串, 区分大小写。

【使用指导】

如果没有指定任何参数, 则显示所有保存在本地的远端主机公钥的详细信息。

可以通过 **public-key peer** 命令或 **public-key peer import sshkey** 命令将远端主机的公钥配置到本地。

【举例】

显示保存在本地的公钥名称为 **idrsa** 的远端主机公钥的详细信息。

```
<Sysname> display public-key peer name idrsa
```

```
=====
Key name: idrsa
Key type: RSA
Key modulus: 1024
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
918F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
6D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
42C142D41BB4884FEB0203010001
```

表1-2 display public-key peer name 命令显示信息描述表

字段	描述
Key name	远端主机公钥的名称
Key type	密钥类型，取值包括RSA、DSA和ECDSA
Key modulus	密钥模数的长度，单位为比特
Key code	公钥数据

显示保存在本地的所有远端主机公钥的简要信息。

```
<Sysname> display public-key peer brief
```

```
Type Modulus Name
```

```
-----
```

```
RSA 1024 idrsa
```

```
DSA 1024 10.1.1.1
```

表1-3 display public-key peer brief 命令显示信息描述表

字段	描述
Type	密钥类型，取值包括RSA、DSA和ECDSA
Modulus	密钥模数的长度，单位为比特
Name	远端主机公钥的名称

【相关命令】

- **public-key peer**
- **public-key peer import sshkey**

1.1.3 peer-public-key end

peer-public-key end 命令用来从公钥视图退回到系统视图，并保存用户输入的公钥。

【命令】

```
peer-public-key end
```

【视图】

公钥视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

本命令用于通过手工配置方式将远端主机的公钥保存到本地设备上。手工配置方式是指：

- (1) 执行 **public-key peer** 命令进入公钥视图。
- (2) 在公钥视图手工输入远端主机的公钥。

(3) 执行 **peer-public-key end** 命令退出公钥视图，并保存输入的公钥。

输入的公钥数据必须满足一定的格式要求。在保存公钥之前，设备会进行公钥合法性的检测：

- 如果用户配置的公钥字符串不满足格式要求，那么将会显示相关提示信息，用户配置的公钥将被丢弃，本次配置失败；
- 如果用户配置的公钥字符串合法，例如输入的公钥数据为通过 **display public-key local public** 命令显示的公钥，则保存该公钥。

【举例】

退出公钥视图，并保存用户输入的公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key peer key1
```

```
Enter public key view. Return to system view with "peer-public-key end" command.
```

```
[Sysname-pkey-public-key-key1]30819F300D06092A864886F70D010101050003818D0030818902818100  
C0EC8014F82515F6335A0A
```

```
[Sysname-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719  
D1643135877E13B1C531B4
```

```
[Sysname-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952  
ADF6B80EB5F52698FCF3D6
```

```
[Sysname-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4  
A9B1DDE675AC30CB020301
```

```
[Sysname-pkey-public-key-key1]0001
```

```
[Sysname-pkey-public-key-key1] peer-public-key end
```

```
[Sysname]
```

【相关命令】

- **display public-key local public**
- **display public-key peer**
- **public-key peer**

1.1.4 public-key local create

public-key local create 命令用来生成本地非对称密钥对。

【命令】

```
public-key local create { dsa | ecdsa [ secp192r1 | secp256r1 | secp384r1 |  
secp521r1 ] | rsa } [ name key-name ]
```

【缺省情况】

不存在本地非对称密钥对。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

dsa: 本地密钥对类型为 DSA。

ecdsa: 本地密钥对类型为 ECDSA。

- **secp192r1:** 采用名称为 secp192r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 192 比特。
- **secp256r1:** 采用名称为 secp256r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 256 比特。
- **secp384r1:** 采用名称为 secp384r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 384 比特。
- **secp521r1:** 采用名称为 secp521r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 521 比特。

如果不指定以上任一种密钥对算法参数，则采用名称为 secp192r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 192 比特。

rsa: 本地密钥对类型为 RSA。

name key-name: 生成指定名称的本地非对称密钥对。**key-name** 为本地非对称密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中只能包含字母、数字及“-”。如果不指定本参数，则生成的 RSA 主机密钥对的默认名称为 hostkey，RSA 服务器密钥对的默认名称为 serverkey，DSA 密钥对的默认名称为 dsakey，ECDSA 密钥对的默认名称为 ecdsakey。

【使用指导】

创建RSA和DSA密钥对时，设备会提示用户输入密钥模数的长度。密钥模数越长，安全性越好，但是生成密钥的时间越长。创建ECDSA密钥对时，可使用不同密钥长度的椭圆曲线，密钥越长，安全性越好，但是生成密钥的时间越长。关于密钥模数长度的配置限制和注意事项请参见 表 1-4。

生成密钥对时，如果不指定密钥对名称，系统会以缺省名称命名密钥对，并把该密钥对标记为默认（default）。

用户可以使用缺省的密钥对名称创建其他密钥对，但系统不会把该密钥对标记为默认（default）。

非默认名称密钥对的密钥类型和名称不能完全相同，否则需要用户确认是否覆盖原有的密钥对。不同类型的密钥对，名称可以相同。

执行此命令后，生成的密钥对将保存在设备中，设备重启后密钥不会丢失。

表1-4 不同类型密钥对对比

密钥对类型	生成的密钥对	密钥模数长度
RSA	• 不指定密钥对名称时，将同时生成两个密钥对服务器密钥对和主机密钥对 • 指定密钥对名称时，只生成一个主机密钥对  说明 目前，只有 SSH1.5 中应用了 RSA 服务器密钥对	长度取值范围为512~2048比特，缺省值为1024比特，建议密钥模数的长度大于或等于768比特
DSA	只生成一个主机密钥对	长度取值范围为512~2048比特，缺省值为1024比特，建议密钥模数的长度大于或等于768比特

[illegible]

【相关命令】

- `display public-key local public`
- `public-key local destroy`

1.1.5 public-key local destroy

public-key local destroy 命令用来销毁本地非对称密钥对。

【命令】

```
public-key local destroy { dsa | ecdsa | rsa } [ name key-name ]
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

dsa: 本地密钥对类型为 DSA。
ecdsa: 本地密钥对类型为 ECDSA。
rsa: 本地密钥对类型为 RSA。

name key-name: 销毁指定名称的本地非对称密钥对。**key-name** 为本地非对称密钥对名称，为 1~64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则销毁指定类型默认名称的本地非对称密钥对。

【使用指导】

在如下几种情况下，建议用户销毁旧的非对称密钥对，并生成新的密钥对：

- 本地设备的私钥泄露。这种情况下，非法用户可能会冒充本地设备访问网络。
- 保存密钥对的存储设备出现故障，导致设备上没有公钥对应的私钥，无法再利用旧的非对称密钥对进行加解密和数字签名。
- 密钥对使用了较长时间，可能存在密钥泄露或破译的风险。
- 本地证书到达有效期，需要删除对应的本地密钥对。本地证书的详细介绍，请参见“安全配置指导”中的“PKI”。

【举例】

```
# 销毁默认名称的本地 RSA 非对称密钥对。
<Sysname> system-view
[Sysname] public-key local destroy rsa
Confirm to destroy the key pair? [Y/N]:y
# 销毁默认名称的本地 DSA 非对称密钥对。
<Sysname> system-view
[Sysname] public-key local destroy dsa
Confirm to destroy the key pair? [Y/N] :y
# 销毁默认名称的本地 ECDSA 非对称密钥对。
<Sysname> system-view
[Sysname] public-key local destroy ecdsa
Confirm to destroy the key pair? [Y/N]:y
# 销毁名称为 rsa1 的本地 RSA 非对称密钥对。
<Sysname> system-view
[Sysname] public-key local destroy rsa name rsa1
Confirm to destroy the key pair? [Y/N]:y
# 销毁名称为 dsa1 的本地 DSA 非对称密钥对。
<Sysname> system-view
[Sysname] public-key local destroy dsa name dsa1
Confirm to destroy the key pair? [Y/N] :y
# 销毁名称为 ecdsa1 的本地 ECDSA 非对称密钥对。
<Sysname> system-view
[Sysname] public-key local destroy ecdsa name ecdsa1
Confirm to destroy the key pair? [Y/N]:y
```

【相关命令】

- **public-key local create**

1.1.6 public-key local export dsa

public-key local export dsa 命令用来根据指定格式显示本地 DSA 主机公钥或将其导出到指定文件。

【命令】

public-key local export dsa [*name key-name*] { **openssh** | **ssh2** } [*filename*]

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

name key-name: 显示或导出指定本地 DSA 密钥对的主机公钥。*key-name* 为本地密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示或导出默认名称的本地 DSA 密钥对的主机公钥。

openssh: 主机公钥格式为 OpenSSH。

ssh2: 主机公钥格式为 SSH2.0。

filename: 指定存储导出公钥的文件的名称，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsakey”、“ecdsakey”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符串“./”和“../”。设备支持的文件名长度为 1~128。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。如果不指定本参数，则按照指定格式显示本地 DSA 主机公钥。

【使用指导】

通过以下操作，采用从公钥文件中导入的方式将本地的主机公钥保存到远端设备上：

(1) 通过以下任一方法将导出的公钥保存到文件中：

- 在本地设备上执行 **public-key local export** 命令按照指定格式显示本地主机公钥（执行命令时不指定 *filename* 参数），再通过粘贴复制方式将显示的主机公钥保存到文件中。
- 在本地设备上执行 **public-key local export** 命令按照指定格式将本地主机公钥导出到指定文件（执行命令时指定 *filename* 参数）。需要注意的是，不能将主机公钥导出到工作路径 **pkey** 目录以及 **pkey** 的子目录中。

(2) 将所获得的证书文件通过 FTP 的二进制模式或 TFTP 上传到远端主机。有关 FTP 和 TFTP 的详细使用请参见“基础配置指导”中的“FTP 和 TFTP”。

(3) 在远端主机上，执行 **public-key peer import sshkey** 命令将主机公钥保存到本地。

SSH2.0 和 OpenSSH 是两种不同类型的公钥格式，用户需要根据服务器端支持的对端公钥格式，来选择导出的主机公钥格式。

【举例】

以 OpenSSH 格式导出默认名称的本地 DSA 密钥对的主机公钥，存储导出公钥的文件名为 **key.pub**。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa openssh key.pub
```

以 SSH2.0 格式显示默认名称的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa ssh2
```

```
---- BEGIN SSH2 PUBLIC KEY ----
```

Comment: "dsa-key-2011/05/12"

```
AAAAB3NzaC1kc3MAAACBANDXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzT09yzhSg06UiL+CM70Zb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNL/BnjXcittQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPS02s6RXwAAAIeAgiaQCeF0xHS68pMuad0x8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPfKYDNNdAkkroVnsZJliW8T6UilLiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni
/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBINxx2eF3LLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3s
TwmIfLQeweUwLVAPa0esKaCERjxg+e4maYwLAvySGT4c9NJlXLo=
```

----- END SSH2 PUBLIC KEY -----

以 OpenSSH 格式显示默认名称的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa openssh
```

```
ssh-dss
```

```
AAAAB3NzaC1kc3MAAACBANDXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzT09yzhSg06UiL+CM70Zb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNL/BnjXcittQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPS02s6RXwAAAIeAgiaQCeF0xHS68pMuad0x8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPfKYDNNdAkkroVnsZJliW8T6UilLiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni
/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBINxx2eF3LLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3s
TwmIfLQeweUwLVAPa0esKaCERjxg+e4maYwLAvySGT4c9NJlXLo= dsa-key
```

以 OpenSSH 格式导出名称为 dsa1 的本地 DSA 密钥对的主机公钥，文件名为 dsa1.pub。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa name dsa1 openssh dsa1.pub
```

以 SSH2.0 格式显示名称为 dsa1 的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa name dsa1 ssh2
```

----- BEGIN SSH2 PUBLIC KEY -----

Comment: "dsa-key-2011/05/12"

```
AAAAB3NzaC1kc3MAAACBANDXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzT09yzhSg06UiL+CM70Zb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNL/BnjXcittQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPS02s6RXwAAAIeAgiaQCeF0xHS68pMuad0x8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPfKYDNNdAkkroVnsZJliW8T6UilLiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtabonKk0YEAK
Rdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7
CrcV+ft7UUVBF0FV3W4H0x/L0idJ5sX+qBAD4WcpSX00rZEF4+dq
```

----- END SSH2 PUBLIC KEY -----

以 OpenSSH 格式显示名称为 dsa1 的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa name dsa1 openssh
```

```
ssh-dss
```

```
AAAAB3NzaC1kc3MAAACBANDXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzT09yzhSg06UiL+CM70Zb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNL/BnjXcittQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPS02s6RXwAAAIeAgiaQCeF0xHS68pMuad0x8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPfKYDNNdAkkroVnsZJliW8T6UilLiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtabonKk0YEAK
Rdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7
CrcV+ft7UUVBF0FV3W4H0x/L0idJ5sX+qBAD4WcpSX00rZEF4+dq dsa-key
```

【相关命令】

- **public-key local create**
- **public-key peer import sshkey**

1.1.7 public-key local export ecdsa

public-key local export ecdsa 命令用来根据指定格式显示本地 ECDSA 主机公钥或将其导出到指定文件。

【命令】

```
public-key local export ecdsa [ name key-keyname ] { openssh | ssh2 }  
[ filename ]
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

name *key-name*: 显示或导出指定本地 ECDSA 密钥对的主机公钥。*key-name* 为本地密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示或导出默认名称的本地 ECDSA 密钥对的主机公钥。

openssh: 主机公钥格式为 OpenSSH。

ssh2: 主机公钥格式为 SSH2.0。

filename: 指定存储导出公钥的文件的名称，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsakey”、“ecdsakey”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符串“./”和“../”。设备支持的文件名长度为 1~128。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。如果不指定本参数，则按照指定格式显示本地 ECDSA 主机公钥。

【使用指导】

通过以下操作，采用从公钥文件中导入的方式将本地的主机公钥保存到远端设备上：

(1) 通过以下任一方法将导出的公钥保存到文件中：

- 在本地设备上执行 **public-key local export** 命令按照指定格式显示本地主机公钥（执行命令时不指定 *filename* 参数），再通过粘贴复制方式将显示的主机公钥保存到文件中。
- 在本地设备上执行 **public-key local export** 命令按照指定格式将本地主机公钥导出到指定文件（执行命令时指定 *filename* 参数）。需要注意的是，不能将主机公钥导出到工作路径 **pkey** 目录以及 **pkey** 的子目录中。

(2) 将所获得的证书文件通过 FTP 的二进制模式或 TFTP 上传到远端主机。有关 FTP 和 TFTP 的详细使用请参见“基础配置指导”中的“FTP 和 TFTP”。

(3) 在远端主机上，执行 **public-key peer import sshkey** 命令将主机公钥保存到本地。

SSH2.0 和 OpenSSH 是两种不同类型的公钥格式，用户需要根据服务器端支持的对端公钥格式，来选择导出的主机公钥格式。

目前，只支持导出椭圆曲线为 **secp256r1** 的 ECDSA 主机公钥。

【举例】

以 OpenSSH 格式导出本地 ECDSA 主机公钥，存储导出公钥的文件名为 **key.pub**。


```

<Sysname> system-view
[Sysname] public-key local export ecdsa openssh key.pub
# 以 SSH2.0 格式显示本地 ECDSA 主机公钥。

<Sysname> system-view
[Sysname] public-key local export ecdsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "ecdsa-sha2-nistp256-2014/07/06"
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBREw5tkARpbV+sYArt/xcW+UJEAevx70ckT
tTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTIcxBjuBap+pHc919C58=
---- END SSH2 PUBLIC KEY ----
# 以 OpenSSH 格式显示本地 ECDSA 主机公钥。

<Sysname> system-view
[Sysname] public-key local export ecdsa openssh
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBREw5tkARpbV+sYArt/xcW+UJEAevx70ckT
tTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTIcxBjuBap+pHc919C58=
ecdsa-key

```

【相关命令】

```

public-key local create
public-key peer import sshkey

```

1.1.8 public-key local export rsa

public-key local export rsa 命令用来根据指定格式显示本地 RSA 主机公钥或将其导出到指定文件。

【命令】

```

public-key local export rsa [ name key-name ] { openssh | ssh1 | ssh2 }
[ filename ]

```

【视图】

系统视图

【缺省用户角色】

```

network-admin
context-admin

```

【参数】

name key-name: 显示或导出指定本地 RSA 密钥对的主机公钥。*key-name* 为本地密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示或导出默认名称的本地 RSA 密钥对的主机公钥。

openssh: 主机公钥格式为 OpenSSH。

ssh1: 主机公钥格式为 SSH1.5。

ssh2: 主机公钥格式为 SSH2.0。

filename: 指定存储导出公钥的文件的名称，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsa-key”、“ecdsa-key”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符串“./”和

“./”。设备支持的文件名长度为 1~128。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。如果不指定本参数，则按照指定格式显示本地 RSA 主机公钥。

【使用指导】

通过以下操作，采用从公钥文件中导入的方式将本地的主机公钥保存到远端设备上：

(1) 通过以下任一方法将导出的公钥保存到文件中：

- 在本地设备上执行 **public-key local export** 命令按照指定格式显示本地主机公钥（执行命令时不指定 *filename* 参数），再通过粘贴复制方式将显示的主机公钥保存到文件中。
- 在本地设备上执行 **public-key local export** 命令按照指定格式将本地主机公钥导出到指定文件（执行命令时指定 *filename* 参数）。需要注意的是，不能将主机公钥导出到工作路径 **pkey** 目录以及 **pkey** 的子目录中。

(2) 将所获得的证书文件通过 FTP 的二进制模式或 TFTP 上传到远端主机。有关 FTP 和 TFTP 的详细使用请参见“基础配置指导”中的“FTP 和 TFTP”。

(3) 在远端主机上，执行 **public-key peer import sshkey** 命令将主机公钥保存到本地。

SSH1.5、SSH2.0 和 OpenSSH 是三种不同类型的公钥格式，用户需要根据服务器端支持的对端公钥格式，来选择导出的主机公钥格式。

【举例】

以 OpenSSH 格式导出默认名称的本地 RSA 密钥对的主机公钥，存储导出公钥的文件名为 **key.pub**。

```
<Sysname> system-view
```

```
[Sysname] public-key local export rsa openssh key.pub
```

以 SSH2.0 格式显示默认名称的本地 RSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export rsa ssh2
```

```
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "rsa-key-2011/05/12"
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQDAPKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/bYcb  
gM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+X0vyvPJilneKJqhPT0xdv4t las  
+mLNloY0dImbwS2kwE71rgg1CQ==
```

```
---- END SSH2 PUBLIC KEY ----
```

以 OpenSSH 格式显示默认名称的本地 RSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export rsa openssh
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQDAPKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/bYcb  
gM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+X0vyvPJilneKJqhPT0xdv4t las  
+mLNloY0dImbwS2kwE71rgg1CQ== rsa-key
```

以 OpenSSH 格式导出名称为 **rsa1** 的本地 RSA 密钥对的主机公钥，文件名为 **rsa1.pub**。

```
<Sysname> system-view
```

```
[Sysname] public-key local export rsa name rsa1 openssh rsa1.pub
```

以 SSH2.0 格式显示名称为 **rsa1** 的本地 RSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export rsa name rsa1 ssh2
```

```
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "rsa-key-2011/05/12"
```

```

AAAAAB3NzaC1yc2EAAAADAQABAAQDevEbyF93xHUUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+q2o
lqoagn5YDyUC8ZJvUhlyMOHe0RpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8ba8UkrU
mM04fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH2 PUBLIC KEY ----
# 以 OpenSSH 格式显示名称为 rsa1 的本地 RSA 密钥对的主机公钥。
<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh
ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAQDevEbyF93xHUUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J00fBQ8XY+q2o
lqoagn5YDyUC8ZJvUhlyMOHe0RpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8ba8UkrU
mM04fUvW6zavA5LYxtlAiQv0KQ== rsa-key

```

【相关命令】

- **public-key local create**
- **public-key peer import sshkey**

1.1.9 public-key local import

public-key local import 命令用来导入本地非对称密钥对。

【命令】

```
public-key local import { ecdsa | rsa } [ key-name ] filename filename
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ecdsa: 本地密钥对类型为 ECDSA。

rsa: 本地密钥对类型为 RSA。

key-name: 指定本地非对称密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中只能包含字母、数字及“-”。如果不指定本参数，则导入的 RSA 密钥对的默认名称为 **hostkey**，ECDSA 密钥对的默认名称为 **ecdsa-key**。

filename filename: 指定待导入的密钥对所在的文件名称，为 1~128 个字符的字符串，区分大小写。必须为设备已存在的密钥对文件，且密钥对文件格式必须为 **.pem** 格式。

【使用指导】

如果证书和密钥对是分开的两个文件，设备无法通过导入证书的方式来导入密钥对，此时需要将密钥对文件通过 **FTP** 等方式上传到本地设备中，再执行本命令导入密钥对。

执行本命令后，导入的密钥对将保存在设备中，设备重启后密钥不会丢失。

当导入的密钥对类型为 **RSA** 时，设备只支持导入 **RSA** 主机密钥对，不支持导入 **RSA** 服务器密钥对。

设置密钥对名称时请注意：

- 导入密钥对时，如果不指定密钥对名称，系统会以缺省名称命名密钥对，并把该密钥对标记为默认（default）。
- 导入密钥对时，用户可以输入缺省的密钥对名称，但系统不会把该密钥对标记为默认（default）。
- 非默认名称密钥对的密钥类型和名称不能完全相同，否则需要确认是否覆盖原有的密钥对。不同类型的密钥对，名称可以相同。

如果导入的密钥对是加密后的密钥对，需要提供解密密码才能成功导入。

设备支持导入的密钥长度范围请参见 [表 1-5](#)。

表1-5 设备支持导入的密钥对长度

密钥对类型	密钥模数长度/密钥长度
RSA	长度取值范围为512～2048比特
ECDSA	长度取值为192、256、384或521比特

【举例】

```
# 导入加密后的本地 RSA 密钥对 rsa1，文件名称为 private_key.pem.
<Sysname> system-view
[Sysname] public-key local import rsa rsa1 filename private_key.pem
Please input the password:
Importing Keys...
Key pair imported successfully.
```

【相关命令】

- **display public-key local**

1.1.10 public-key peer

public-key peer 命令用来指定远端主机公钥的名称，并进入公钥视图。如果指定的远端主机公钥名称已经存在，则直接接进入该公钥视图。

undo public-key peer 命令用来删除指定的远端主机公钥。

【命令】

```
public-key peer keyname
undo public-key peer keyname
```

【缺省情况】

不存在远端主机公钥。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

keyname: 远端主机公钥的名称，为 1~64 个字符的字符串，区分大小写。

【使用指导】

进入公钥视图后，可以开始输入公钥数据。在输入公钥数据时，字符之间可以有空格，也可以按回车键继续输入数据。保存公钥数据时，将删除空格和回车符。

通过手工配置方式创建远端主机公钥时，用户需要事先获取并记录远端主机十六进制形式的公钥，并在本地设备上执行以下操作：

- (1) 执行本命令进入公钥视图。
- (2) 在公钥视图，手工输入远端主机的公钥。
- (3) 执行 **peer-public-key end** 命令，保存输入的远端主机公钥，并从公钥视图退回到系统视图。

输入的公钥数据必须满足一定的格式要求。通过 **display public-key local public** 命令显示的公钥可以作为输入的公钥数据。

【举例】

指定远端主机公钥名称为 key1，并进入公钥视图。

```
<Sysname> system-view
[Sysname] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]
```

【相关命令】

- **display public-key local public**
- **display public-key peer**
- **peer-public-key end**

1.1.11 public-key peer import sshkey

public-key peer import sshkey 命令用来配置从公钥文件中导入远端主机的公钥。

undo public-key peer 命令用来删除指定的远端主机公钥。

【命令】

```
public-key peer keyname import sshkey filename
undo public-key peer keyname
```

【缺省情况】

不存在远端主机公钥。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

keyname: 远端主机公钥的名称，为 1~64 个字符的字符串，区分大小写。

filename: 指定导入公钥数据的文件名，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsakey”、“ecdsakey”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符串“./”和“../”。设备支持的文件名长度为 1~128。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

【使用指导】

执行本命令后，系统会对指定公钥文件中的公钥进行格式转换，将其转换为 PKCS 标准编码格式，并将该远端主机的公钥保存到本地设备。

从公钥文件中导入远端主机的公钥前，需要远端主机将其公钥保存到公钥文件中，并将该公钥文件上传到本地设备。例如，在远端主机上执行 **public-key local export** 命令将其公钥导出到公钥文件中，并通过 FTP 或 TFTP，以二进制方式将该公钥文件保存到本地设备。

目前，设备支持的公钥格式为 SSH1.5、SSH2.0 和 OpenSSH。

【举例】

配置从公钥文件 key.pub 中导入远端主机的公钥，公钥名称为 key2。

```
<Sysname> system-view
```

```
[Sysname] public-key peer key2 import sshkey key.pub
```

【相关命令】

- **display public-key peer**
- **public-key local export dsa**
- **public-key local export ecdsa**
- **public-key local export rsa**

目 录

1 PKI	1-1
1.1 PKI配置命令	1-1
1.1.1 attribute	1-1
1.1.2 ca identifier	1-2
1.1.3 certificate request entity	1-3
1.1.4 certificate request from	1-4
1.1.5 certificate request mode	1-5
1.1.6 certificate request polling	1-6
1.1.7 certificate request url	1-7
1.1.8 common-name	1-8
1.1.9 country	1-8
1.1.10 crl check enable	1-9
1.1.11 crl url	1-10
1.1.12 display pki certificate access-control-policy	1-11
1.1.13 display pki certificate attribute-group	1-12
1.1.14 display pki certificate domain	1-13
1.1.15 display pki certificate renew-status	1-18
1.1.16 display pki certificate request-status	1-20
1.1.17 display pki crl domain	1-21
1.1.18 fqdn	1-23
1.1.19 ip	1-24
1.1.20 ldap-server	1-24
1.1.21 locality	1-25
1.1.22 organization	1-26
1.1.23 organization-unit	1-27
1.1.24 pkcs7-encryption-algorithm	1-27
1.1.25 pki abort-certificate-request	1-28
1.1.26 pki certificate access-control-policy	1-29
1.1.27 pki certificate attribute-group	1-29
1.1.28 pki delete-certificate	1-30
1.1.29 pki domain	1-31
1.1.30 pki entity	1-32
1.1.31 pki export	1-33

1.1.32 pki import	1-40
1.1.33 pki request-certificate	1-44
1.1.34 pki retrieve-certificate	1-45
1.1.35 pki retrieve-crl	1-46
1.1.36 pki storage	1-47
1.1.37 pki validate-certificate	1-48
1.1.38 public-key dsa	1-50
1.1.39 public-key ecdsa	1-51
1.1.40 public-key rsa	1-52
1.1.41 revocation-check method	1-54
1.1.42 root-certificate fingerprint	1-54
1.1.43 rule	1-56
1.1.44 source	1-57
1.1.45 state	1-58
1.1.46 subject-dn	1-58
1.1.47 usage	1-59
1.1.48 vpn-instance	1-60

1 PKI

1.1 PKI配置命令

1.1.1 attribute

attribute 命令用来配置属性规则，用于根据证书的颁发者名、主题名以及备用主题名来过滤证书。

undo attribute 命令用来删除证书属性规则。

【命令】

```
attribute id { alt-subject-name { fqdn | ip } | { issuer-name | subject-name }  
             { dn | fqdn | ip } } { ctn | equ | nctn | nequ } attribute-value  
undo attribute id
```

【缺省情况】

不存在属性规则，即对证书的颁发者名、主题名以及备用主题名没有限制。

【视图】

证书属性组视图

【缺省用户角色】

network-admin
context-admin

【参数】

id: 证书属性规则序号，取值范围为 1~16。

alt-subject-name: 表示证书备用主题名（Subject Alternative Name）。

fqdn: 指定实体的 FQDN。

ip: 指定实体的 IP 地址。

dn: 指定实体的 DN。

issuer-name: 表示证书颁发者名（Issuer Name）。

subject-name: 表示证书主题名（Subject Name）。

ctn: 表示包含操作。

equ: 表示相等操作。

nctn: 表示不包含操作。

nequ: 表示不等操作。

attribute-value: 指定证书属性值，为 1~255 个字符的字符串，不区分大小写。

【使用指导】

各证书属性中可包含的属性域个数有所不同：

- 主题名和颁发者名中均只能包含一个 DN，但是均可以同时包含多个 FQDN 和 IP；

- 备用主题名中不能包含 DN，但是可以同时包含多个 FQDN 和 IP。

不同类型的证书属性域与操作关键字的组合代表了不同的匹配条件，具体如下表所示：

表1-1 对证书属性域的操作涵义

操作	DN	FQDN/IP
ctn	DN中包含指定的属性值	任意一个FQDN/IP中包含了指定的属性值
nctn	DN中不包含指定的属性值	所有FQDN/IP中均不包含指定的属性值
equ	DN等于指定的属性值	任意一个FQDN/IP等于指定的属性值
nequ	DN不等于指定的属性值	所有FQDN/IP均不等于指定的属性值

如果证书的相应属性中包含了属性规则里指定的属性域，且满足属性规则中定义的匹配条件，则认为该属性与属性规则相匹配。例如：属性规则 2 中定义，证书的主题名 DN 中包含字符串 **abc**。如果某证书的主题名的 DN 中确实包含了字符串 **abc**，则认为该证书的主题名与属性规则 2 匹配。

只有证书中的相应属性与某属性组中的所有属性规则都匹配上，才认为该证书与此属性组匹配。如果证书中的某属性中没有包含属性规则中指定的属性域，或者不满足属性规则中的匹配条件，则认为该证书与此属性组不匹配。

【举例】

创建一个名为 **mygroup** 的证书属性组，并进入证书属性组视图。

```
<Sysname> system-view
```

```
[Sysname] pki certificate attribute-group mygroup
```

创建证书属性规则 1，定义证书主题名中的 DN 包含字符串 **abc**。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

创建证书属性规则 2，定义证书颁发者名中的 FQDN 不等于字符串 **abc**。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

创建证书属性规则 3，定义证书主题备用名中的 IP 地址不等于 **10.0.0.1**。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

【相关命令】

- **display pki certificate attribute-group**
- **rule**

1.1.2 ca identifier

ca identifier 命令用来指定设备信任的 CA 名称。

undo ca identifier 命令用来恢复缺省情况。

【命令】

```
ca identifier name
```

```
undo ca identifier
```

【缺省情况】

未指定设备信任的 CA。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

name: 设备信任的 CA 名称，为 1~63 个字符的字符串，区分大小写。

【使用指导】

获取 CA 证书时，必须指定信任的 CA 名称，这个名称会被作为 SCEP 消息的一部分发送给 CA 服务器。但是一般情况下，CA 服务器会忽略收到的 SCEP 消息中的 CA 名称的具体内容。但是如果同一台服务器上配置了两个 CA，且它们的 URL 是相同的，则服务器将根据 SCEP 消息中的 CA 名称选择对应的 CA。因此，使用此命令指定的 CA 名称必须与希望获取的 CA 证书对应的 CA 名称一致。

【举例】

```
# 指定设备信任的 CA 名称为 new-ca。
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ca identifier new-ca
```

1.1.3 certificate request entity

certificate request entity 命令用来指定用于申请证书的 PKI 实体名称。

undo certificate request entity 命令用来恢复缺省情况。

【命令】

```
certificate request entity entity-name
undo certificate request entity
```

【缺省情况】

未指定设备申请证书所使用的 PKI 实体名称。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

entity-name: 用于申请证书的 PKI 实体名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

本命令用于在 PKI 域中指定申请证书的 PKI 实体。PKI 实体描述了申请证书的实体的各种属性（通用名、组织部门、组织、地理区域、省、国家、FQDN、IP），这些属性用于描述 PKI 实体的身份信息。

一个 PKI 域中只能指定一个 PKI 实体名称，多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 指定申请证书的 PKI 实体名称为 en1。  
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] certificate request entity en1
```

【相关命令】

- **pki entity**

1.1.4 certificate request from

certificate request from 命令用来配置证书申请的注册受理机构。

undo certificate request from 命令用来恢复缺省情况。

【命令】

```
certificate request from { ca | ra }  
undo certificate request from
```

【缺省情况】

未指定证书申请的注册受理机构。

【视图】

PKI 域视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

ca: 表示实体从 CA 申请证书。

ra: 表示实体从 RA 申请证书。

【使用指导】

选择从 CA 还是 RA 申请证书，由 CA 服务器决定，需要了解 CA 服务器上由什么机构来受理证书申请。

推荐使用独立运行的 RA 作为注册受理机构。

【举例】

```
# 指定实体从 RA 申请证书。  
<Sysname> system-view  
[Sysname] pki domain aaa
```

[Sysname-pki-domain-aaa] certificate request from ra

1.1.5 certificate request mode

certificate request mode 命令用来配置证书申请方式。

undo certificate request mode 命令用来恢复缺省情况。

【命令】

```
certificate request mode { auto [ password { cipher | simple } string |
renew-before-expire days [ reuse-public-key ] [ automatic-append
common-name ] ] * | manual }
undo certificate request mode
```

【缺省情况】

证书申请方式为手工方式。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

auto: 表示用自动方式申请证书。

password: 指定吊销证书时使用的密码。

cipher: 以密文方式设置密码。

simple: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~31 个字符的字符串，密文密码为 1~73 个字符的字符串。

renew-before-expire days: 表示证书自动续签功能。**days** 是证书自动续签提前的时间，取值范围为 0~365，单位为天。如果取值为 0 则表示证书到期时再自动续签，会出现暂时的业务中断。

reuse-public-key: 表示证书自动续签时使用原有密钥对。若不指定该参数，则表示证书自动续签的过程中会自动生成新的密钥对，且证书续签成功后原有密钥对被立即覆盖。

automatic-append common-name: 表示证书自动续签时在 PKI 实体的通用名后添加随机值。若不指定该参数，则证书自动续签时在 PKI 实体的通用名后不添加随机值。

manual: 表示用手工方式申请证书。

【使用指导】

两种申请方式都属于在线申请，具体情况如下：

- 如果是自动方式，则设备会在与 PKI 域关联的应用（例如 IKE）需要做身份认证时，自动向证书注册机构发起获取 CA 证书和申请本地证书的操作。自动方式下，可以指定吊销证书时使用的密码，是否需要指定密码是由 CA 服务器的策略决定的。
- 如果为手工方式，则需要手工完成获取 CA 证书、申请本地证书的操作。

为避免由于证书过期造成业务中断，请在选择自动方式申请证书时配置证书自动续签功能。证书自动续签是指，系统在证书有效期到达之前自动申请新的证书，申请成功后新证书立即替换原有证书。由于某些 CA 服务器不支持 PKI 实体使用相同的通用名多次申请证书，为了保证自动续签证书成功，请配置 **automatic-append common-name** 参数使设备每次都使用新的通用名为 PKI 实体申请新的证书。

【举例】

指定证书申请方式为自动方式。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto
```

指定证书申请方式为自动方式，并设置吊销证书时使用的密码为明文 123456。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto password simple 123456
```

指定证书申请方式为自动方式，并设置吊销证书时使用的口令为明文 123456，设置证书到期前 60 天自动申请新证书替换原有证书，申请新证书时生成新密钥对。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request mode auto password simple 123456
renew-before-expire 60
```

【相关命令】

- **pki request-certificate**

1.1.6 certificate request polling

certificate request polling 命令用来配置证书申请状态的查询周期和最大次数。

undo certificate request polling 命令用来恢复缺省情况。

【命令】

```
certificate request polling { count count | interval interval }
undo certificate request polling { count | interval }
```

【缺省情况】

证书申请状态的查询周期为 20 分钟，最多查询 50 次。

【视图】

PKI 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

count count: 表示证书申请状态的查询次数，取值范围为 1~100。

interval interval: 表示证书申请状态的查询周期，取值范围为 5~168，单位为分钟。

【使用指导】

设备发送证书申请后,如果 CA 服务器采用手工方式来签发证书申请,则不会立刻响应设备的申请。这种情况下,设备通过定期向 CA 服务器发送状态查询消息,能够及时获取到被 CA 签发的证书。CA 签发证书后,设备将通过发送状态查询得到证书,之后停止发送状态查询消息。如果达到最大查询次数时,CA 服务器仍未签发证书,则设备停止发送状态查询消息,本次证书申请失败。如果 CA 服务器采用自动签发证书的方式,则设备可以立刻得到证书,这种情况下设备不会向 CA 服务器发送状态查询消息。

【举例】

```
# 指定证书申请状态的查询周期为 15 分钟,最多查询 40 次。
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request polling interval 15
[Sysname-pki-domain-aaa] certificate request polling count 40
```

【相关命令】

- **display pki certificate request-status**

1.1.7 certificate request url

certificate request url 命令用来配置实体通过 SCEP 进行证书申请的注册受理机构服务器的 URL。

undo certificate request url 命令用来恢复缺省情况。

【命令】

```
certificate request url url-string
undo certificate request url
```

【缺省情况】

未指定注册受理机构服务器的 URL。

【视图】

PKI 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

url-string: 表示证书申请的注册受理机构服务器的 URL,为 1~511 个字符的字符串,区分大小写。实际可输入的 URL 长度受命令行允许输入的最大字符数限制。

【使用指导】

本命令配置的 URL 内容包括注册受理机构服务器的位置及 CGI 命令接口脚本位置,格式为 `http://server_location/cgi_script_location`。

【举例】

```
# 指定实体进行证书申请的注册受理机构服务器的 URL 为
http://169.254.0.1/certsrv/mscep/mscep.dll。
<Sysname> system-view
[Sysname] pki domain a
[Sysname-pki-domain-a] certificate request url http://169.254.0.1/certsrv/mscep/mscep.dll
```

1.1.8 common-name

common-name 命令用来配置 PKI 实体的通用名，比如用户名称。

undo common-name 命令用来恢复缺省情况。

【命令】

```
common-name common-name-string
undo common-name
```

【缺省情况】

未配置 PKI 实体的通用名。

【视图】

PKI 实体视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

common-name-string: PKI 实体的通用名，为 1~63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

```
# 配置 PKI 实体 en 的通用名为 test。
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] common-name test
```

1.1.9 country

country 命令用来配置 PKI 实体所属的国家代码。

undo country 命令用来恢复缺省情况。

【命令】

```
country country-code-string
undo country
```

【缺省情况】

未配置 PKI 实体所属的国家代码。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

country-code-string: PKI 实体所属的国家代码，为标准的两字符代码，区分大小写，例如中国为 CN。

【举例】

配置 PKI 实体 en 所属的国家代码为 CN。

```
<Sysname> system-view
```

```
[Sysname] pki entity en
```

```
[Sysname-pki-entity-en] country CN
```

1.1.10 crl check enable

crl check enable 命令用来开启 CRL 检查。

undo crl check enable 命令用来关闭 CRL 检查。

【命令】

crl check enable

undo crl check enable

【缺省情况】

CRL 检查处于开启状态。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

CRL（Certificate Revocation List，证书废除列表）是一个由 CA 签发的文件，该文件中包含被该 CA 吊销的所有证书的列表。一个证书有可能在有效期达到之前被 CA 吊销。使能 CRL 检查的目的是查看设备上的实体证书或者即将要导入、获取到设备上的实体证书是否已经被 CA 吊销，若检查结果表明实体证书已被吊销，那么该证书就不被设备信任。

【举例】

关闭 CRL 检查。

```
<Sysname> system-view
```

```
[Sysname] pki domain aaa
```

```
[Sysname-pki-domain-aaa] undo crl check enable
```


【相关命令】

- **pki import**
- **pki retrieve-certificate**
- **pki validate-certificate**

1.1.11 **crl url**

crl url 命令用来设置 CRL 发布点的 URL。

undo crl url 命令用来恢复缺省情况。

【命令】

crl url *url-string*
undo crl url

【缺省情况】

未设置 CRL 发布点的 URL。

【视图】

PKI 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

url-string: 表示 CRL 发布点的 URL，为 1~511 个字符的字符串，区分大小写。格式为 *ldap://server_location* 或 *http://server_location*，其中 *server_location* 可以为 IP 地址和 DNS 域名。实际可输入的 URL 长度受命令行允许输入的最大字符数限制。

【使用指导】

如果 CRL 检查处于使能状态，则进行 CRL 检查之前，需要首先从 PKI 域指定的 CRL 发布点获取 CRL。若 PKI 域中未配置 CRL 发布点的 URL 时，从该待验证的证书中获取发布点信息：优先获取待验证的证书中记录的发布点，如果待验证的证书中没有记录发布点，则获取 CA 证书中记录的发布点（若待验证的证书为 CA 证书，则获取上一级 CA 证书中记录的发布点）。如果无法通过任何途径得到发布点，则通过 SCEP 协议获取 CRL。

若配置了 LDAP 格式的 CRL 发布点 URL，则表示要通过 LDAP 协议获取 CRL。若该 URL 中未携带主机名，则需要根据 PKI 域中配置的 LDAP 服务器地址信息来得到完整的 LDAP 发布点 URL。

【举例】

```
# 指定 CRL 发布点的 URL 为 http://169.254.0.30。  
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] crl url http://169.254.0.30
```

【相关命令】

- **ldap-server**

- **pki retrieve-crl**

1.1.12 **display pki certificate access-control-policy**

display pki certificate access-control-policy 命令用来显示证书访问控制策略的配置信息。

【命令】

display pki certificate access-control-policy [*policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

policy-name: 指定证书访问控制策略名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

若不指定证书访问控制策略的名称，则显示所有证书访问控制策略的配置信息。

【举例】

```
# 显示证书访问控制策略 mypolicy 的配置信息。
<Sysname> display pki certificate access-control-policy mypolicy
Access control policy name: mypolicy
    Rule 1 deny    mygroup1
    Rule 2 permit  mygroup2
# 显示所有证书属性访问控制策略的配置信息。
<Sysname> display pki certificate access-control-policy
Total PKI certificate access control policies: 2
Access control policy name: mypolicy1
    Rule 1 deny    mygroup1
    Rule 2 permit  mygroup2
Access control policy name: mypolicy2
    Rule 1 deny    mygroup3
    Rule 2 permit  mygroup4
```

表1-2 display pki certificate access-control-policy 命令显示信息描述表

字段	描述
Total PKI certificate access control policies	PKI证书访问控制策略的总数
Access control policy name	证书访问控制策略名
Rule <i>number</i>	访问控制规则编号

字段	描述
permit	当证书的属性与属性组里定义的属性匹配时，认为该证书有效，通过了访问控制策略的检测
deny	当证书的属性与属性组里定义的属性匹配时，认为该证书无效，未通过访问控制策略的检测

【相关命令】

- **pki certificate access-control-policy**
- **rule**

1.1.13 display pki certificate attribute-group

display pki certificate attribute-group 命令用来显示证书属性组的配置信息。

【命令】

display pki certificate attribute-group [*group-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

group-name: 指定证书属性组名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

若不指定证书属性组的名称，则显示所有证书属性组的配置信息。

【举例】

显示证书属性组 mygroup 的信息。

```
<Sysname> display pki certificate attribute-group mygroup
Attribute group name: mygroup
Attribute 1 subject-name      dn      ctn      abc
Attribute 2 issuer-name      fqdn    nctn     app
```

显示所有证书属性组的信息。

```
<Sysname> display pki certificate attribute-group
Total PKI certificate attribute groups: 2.
Attribute group name: mygroup1
Attribute 1 subject-name      dn      ctn      abc
Attribute 2 issuer-name      fqdn    nctn     app
Attribute group name: mygroup2
Attribute 1 subject-name      dn      ctn      def
```

Attribute 2 issuer-name fqdn nctn fqd

表1-3 display pki certificate attribute-group 命令显示信息描述表

字段	描述
Total PKI certificate attribute groups	PKI证书属性组的总数
Attribute group name	证书属性组名称
Attribute number	属性规则编号
subject-name	证书主题名
alt-subject-name	证书备用主题名
issuer-name	证书颁发者名
dn	实体的DN
fqdn	实体的FQDN
ip	实体的IP地址
ctn	表示包含操作
nctn	表示不包含操作
equ	表示等于操作
nequ	表示不等操作
Attribute 1 subject-name dn ctn abc	属性规则内容，包括以下参数： - alt-subject-name: 表示证书备用主题名 - issuer-name: 表示证书颁发者名 - subject-name: 表示证书主题名 - fqdn: 表示实体的 FQDN - ip: 表示实体的 IP 地址 - dn: 表示实体的 DN - ctn: 表示包含操作 - equ: 表示相等操作 - nctn: 表示不包含操作 - nequ: 表示不等操作

【相关命令】

- attribute
- pki certificate attribute-group

1.1.14 display pki certificate domain

display pki certificate domain 命令用来显示证书的内容。

【命令】

```
display pki certificate domain domain-name { ca | local | peer [ serial  
serial-num ] }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

domain-name: 显示指定证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

ca: 显示 CA 证书。

local: 显示本地证书。

peer: 显示对端证书。

serial serial-num: 指定要显示的对端证书的序列号。

【使用指导】

显示 CA 证书时，会显示此 PKI 域中所有 CA 证书的详细信息，若 PKI 域中存在 RA 证书，则同时显示 RA 证书的详细信息。

显示本地证书时，会显示此 PKI 域中所有本地证书的详细信息。

显示对端证书时，如果不指定序列号，将显示所有对端证书的简要信息；如果指定序列号，将显示该序号对应的指定对端证书的详细信息。

【举例】

显示 PKI 域 aaa 中的 CA 证书。

```
<Sysname> display pki certificate domain aaa ca
```

Certificate:

Data:

Version: 1 (0x0)

Serial Number:

5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=cn, O=docm, OU=rnd, CN=rootca

Validity

Not Before: Jan 6 02:51:41 2011 GMT

Not After : Dec 7 03:12:05 2013 GMT

Subject: C=cn, O=ccc, OU=ppp, CN=rootca

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

```
00:c4:fd:97:2c:51:36:df:4c:ea:e8:c8:70:66:f0:
28:98:ec:5a:ee:d7:35:af:86:c4:49:76:6e:dd:40:
4a:9e:8d:c0:cb:d9:10:9b:61:eb:0c:e0:22:ce:f6:
57:7c:bb:bb:1b:1d:b6:81:ad:90:77:3d:25:21:e6:
7e:11:0a:d8:1d:3c:8e:a4:17:1e:8c:38:da:97:f6:
6d:be:09:e3:5f:21:c5:a0:6f:27:4b:e3:fb:9f:cd:
c1:91:18:ff:16:ee:d8:cf:8c:e3:4c:a3:1b:08:5d:
84:7e:11:32:5f:1a:f8:35:25:c0:7e:10:bd:aa:0f:
52:db:7b:cd:5d:2b:66:5a:fb
```

Exponent: 65537 (0x10001)

Signature Algorithm: sha1WithRSAEncryption

```
6d:b1:4e:d7:ef:bb:1d:67:53:67:d0:8f:7c:96:1d:2a:03:98:
3b:48:41:08:a4:8f:a9:c1:98:e3:ac:7d:05:54:7c:34:d5:ee:
09:5a:11:e3:c8:7a:ab:3b:27:d7:62:a7:bb:bc:7e:12:5e:9e:
4c:1c:4a:9f:d7:89:ca:20:46:de:c5:b3:ce:36:ca:5e:6e:dc:
e7:c6:fe:3f:c5:38:dd:d5:a3:36:ad:f4:3d:e6:32:7f:48:df:
07:f0:a2:32:89:86:72:22:cd:ed:e5:0f:95:df:9c:75:71:e7:
fe:34:c5:a0:64:1c:f0:5c:e4:8f:d3:00:bd:fa:90:b6:64:d8:
88:a6
```

显示 PKI 域 aaa 中的本地证书。

<Sysname> display pki certificate domain aaa local

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

bc:05:70:1f:0e:da:0d:10:16:1e

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=CN, O=sec, OU=software, CN=abdfdc

Validity

Not Before: Jan 7 20:05:44 2011 GMT

Not After : Jan 7 20:05:44 2012 GMT

Subject: O=OpenCA Labs, OU=Users, CN=fips fips-sec

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

```
00:b2:38:ad:8c:7d:78:38:37:88:ce:cc:97:17:39:
52:e1:99:b3:de:73:8b:ad:a8:04:f9:a1:f9:0d:67:
d8:95:e2:26:a4:0b:c2:8c:63:32:5d:38:3e:fd:b7:
4a:83:69:0e:3e:24:e4:ab:91:6c:56:51:88:93:9e:
12:a4:30:ad:ae:72:57:a7:ba:fb:bc:ac:20:8a:21:
46:ea:e8:93:55:f3:41:49:e9:9d:cc:ec:76:13:fd:
a5:8d:cb:5b:45:08:b7:d1:c5:b5:58:89:47:ce:12:
bd:5c:ce:b6:17:2f:e0:fc:c0:3e:b7:c4:99:31:5b:
8a:f0:ea:02:fd:2d:44:7a:67
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

```

CA:FALSE
Netscape Cert Type:
  SSL Client, S/MIME
X509v3 Key Usage:
  Digital Signature, Non Repudiation, Key Encipherment
X509v3 Extended Key Usage:
  TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
Netscape Comment:
  User Certificate of OpenCA Labs
X509v3 Subject Key Identifier:
  91:95:51:DD:BF:4F:55:FA:E4:C4:D0:10:C2:A1:C2:99:AF:A5:CB:30
X509v3 Authority Key Identifier:
  keyid:DF:D2:C9:1A:06:1F:BC:61:54:39:FE:12:C4:22:64:EB:57:3B:11:9F

X509v3 Subject Alternative Name:
  email:fips@ccc.com
X509v3 Issuer Alternative Name:
  email:pki@openca.org
Authority Information Access:
  CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
  OCSP - URI:http://titan:2560/
  1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

X509v3 CRL Distribution Points:

  Full Name:
    URI:http://titan/pki/pub/crl/cacrl.crl

```

```

Signature Algorithm: sha256WithRSAEncryption
94:ef:56:70:48:66:be:8f:9d:bb:77:0f:c9:f4:65:77:e3:bd:
ea:9a:b8:24:ae:a1:38:2d:f4:ab:e8:0e:93:c2:30:33:c8:ef:
f5:e9:eb:9d:37:04:6f:99:bd:b2:c0:e9:eb:b1:19:7e:e3:cb:
95:cd:6c:b8:47:e2:cf:18:8d:99:f4:11:74:b1:1b:86:92:98:
af:a2:34:f7:1b:15:ee:ea:91:ed:51:17:d0:76:ec:22:4c:56:
da:d6:d1:3c:f2:43:31:4f:1d:20:c8:c2:c3:4d:e5:92:29:ee:
43:c6:d7:72:92:e8:13:87:38:9a:9c:cd:54:38:b2:ad:ba:aa:
f9:a4:68:b5:2a:df:9a:31:2f:42:80:0c:0c:d9:6d:b3:ab:0f:
dd:a0:2c:c0:aa:16:81:aa:d9:33:ca:01:75:94:92:44:05:1a:
65:41:fa:1e:41:b5:8a:cc:2b:09:6e:67:70:c4:ed:b4:bc:28:
04:50:a6:33:65:6d:49:3c:fc:a8:93:88:53:94:4c:af:23:64:
cb:af:e3:02:d1:b6:59:5f:95:52:6d:00:00:a0:cb:75:cf:b4:
50:c5:50:00:65:f4:7d:69:cc:2d:68:a4:13:5c:ef:75:aa:8f:
3f:ca:fa:eb:4d:d5:5d:27:db:46:c7:f4:7d:3a:b2:fb:a7:c9:
de:18:9d:c1

```

显示 PKI 域 aaa 中的所有对端证书的简要信息。

```

<Sysname> display pki certificate domain aaa peer
Total peer certificates: 1

```

Serial Number: 9a0337eb2156ba1f5476e4d754a5a9f7

Subject Name: CN=sldsslserver

显示 PKI 域 aaa 中的一个特定序号的对端证书的详细信息。

<Sysname> display pki certificate domain aaa peer serial 9a0337eb2156ba1f5476e4d754a5a9f7

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

9a:03:37:eb:21:56:ba:1f:54:76:e4:d7:54:a5:a9:f7

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=cn, O=ccc, OU=sec, CN=ssl

Validity

Not Before: Oct 15 01:23:06 2010 GMT

Not After : Jul 26 06:30:54 2012 GMT

Subject: CN=sldsslserver

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

00:c2:cf:37:76:93:29:5e:cd:0e:77:48:3a:4d:0f:

a6:28:a4:60:f8:31:56:28:7f:81:e3:17:47:78:98:

68:03:5b:72:f4:57:d3:bf:c5:30:32:0d:58:72:67:

04:06:61:08:3b:e9:ac:53:b9:e7:69:68:1a:23:f2:

97:4c:26:14:c2:b5:d9:34:8b:ee:c1:ef:af:1a:f4:

39:da:c5:ae:ab:56:95:b5:be:0e:c3:46:35:c1:52:

29:9c:b7:46:f2:27:80:2d:a4:65:9a:81:78:53:d4:

ca:d3:f5:f3:92:54:85:b3:ab:55:a5:03:96:2b:19:

8b:a3:4d:b2:17:08:8d:dd:81

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Authority Key Identifier:

keyid:9A:83:29:13:29:D9:62:83:CB:41:D4:75:2E:52:A1:66:38:3C:90:11

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key

Agreement

Netscape Cert Type:

SSL Server

X509v3 Subject Alternative Name:

DNS:docm.com

X509v3 Subject Key Identifier:

3C:76:95:9B:DD:C2:7F:5F:98:83:B7:C7:A0:F8:99:1E:4B:D7:2F:26

X509v3 CRL Distribution Points:

Full Name:

URI:http://s03130.ccc.sec.com:447/ssl.crl

Signature Algorithm: sha1WithRSAEncryption

61:2d:79:c7:49:16:e3:be:25:bb:8b:70:37:31:32:e5:d3:e3:
31:2c:2d:c1:f9:bf:50:ad:35:4b:c1:90:8c:65:79:b6:5f:59:
36:24:c7:14:63:44:17:1e:e4:cf:10:69:fc:93:e9:70:53:3c:
85:aa:40:7e:b5:47:75:0f:f0:b2:da:b4:a5:50:dd:06:4a:d5:
17:a5:ca:20:19:2c:e9:78:02:bd:19:77:da:07:1a:42:df:72:
ad:07:7d:e5:16:d6:75:eb:6e:06:58:ee:76:31:63:db:96:a2:
ad:83:b6:bb:ba:4b:79:59:9d:59:6c:77:59:5b:d9:07:33:a8:
f0:a5

表1-4 display pki certificate 命令显示信息描述表

字段	描述
Version	证书版本号
Serial Number	证书序列号
Signature Algorithm	签名算法
Issuer	证书颁发者
Validity	证书有效期
Subject	证书所属的实体信息
Subject Public Key Info	证书所属的实体的公钥信息
X509v3 extensions	X.509版本3格式的证书扩展属性

【相关命令】

- **pki domain**
- **pki retrieve-certificate**

1.1.15 display pki certificate renew-status

display pki certificate renew-status 命令用来显示 PKI 域的证书续签状态。

【命令】

display pki certificate renew-status [domain domain-name]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

domain domain-name: 指定 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。若未指定 PKI 域的名称，则显示所有 PKI 域的证书续签状态。

【举例】

显示所有 PKI 域的证书续签状态，其中 PKI 域 domain1 的证书申请方式配置中未指定 **reuse-public-key**，续签时生成了新的密钥对。

```
<Sysname> display pki certificate renew-status
Domain Name: domain1
Renew Time : 03:12:05 2016-06-13
Renew public key:
  Key type: RSA
  Time when key pair created: 15:40:48 2016/06/13
  Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
    667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
    C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
    FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
    2DA4C04EF5AE0835090203010001
```

显示指定 PKI 域的证书续签状态。

```
<Sysname> display pki certificate renew-status domain domain1
Domain Name: domain1
Renew Time : 03:12:05 2016-06-13
Renew public key:
  Key type: RSA
  Time when key pair created: 15:40:48 2016/06/13
  Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
    667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
    C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
    FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
    2DA4C04EF5AE0835090203010001
```

表1-5 display pki certificate renew-status 命令显示信息描述表

字段	描述
Domain Name	PKI域名
Renew Time	预计证书续签发生的时刻
Renew public key	证书续签时使用的新密钥对的信息，只有在证书续签过程比较慢或续签失败的情况下才会显示出此密钥对信息
Key type	密钥对的类型，取值包括：RSA、DSA、ECDSA
Time when key pair created	密钥对的创建时间和日期
Key code	密钥对的密钥信息

【相关命令】

- **certificate request mode**
- **pki domain**

1.1.16 display pki certificate request-status

display pki certificate request-status 命令用来显示证书的申请状态。

【命令】

display pki certificate request-status [domain *domain-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

domain *domain-name*: 指定证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

【使用指导】

若不指定 PKI 域的名称，则显示所有 PKI 域的证书申请状态。

【举例】

显示 PKI 域 aaa 的证书申请状态。

```
<Sysname> display pki certificate request-status domain aaa
Certificate Request Transaction 1
  Domain name: aaa
  Status: Pending
  Key usage: General
  Remain polling attempts: 10
  Next polling attempt after : 1191 seconds
```

显示所有 PKI 域的证书申请状态。

```
<Sysname> display pki certificate request-status
Certificate Request Transaction 1
  Domain name: domain1
  Status: Pending
  Key usage: General
  Remain polling attempts: 10
  Next polling attempt after : 1191 seconds
Certificate Request Transaction 2
  Domain name: domain2
  Status: Pending
```

Key usage: Signature
Remain polling attempts: 10
Next polling attempt after : 188 seconds

表1-6 display pki certificate request 命令显示信息描述表

字段	描述
Certificate Request Transaction <i>number</i>	证书申请任务的编号，从1开始顺序编号
Domain name	PKI域名
Status	证书申请状态。目前，仅有一种取值Pending，表示等待
Key usage	证书用途，包括以下取值： • General: 表示通用，既可以用于加密也可以用于签名 • Signature: 表示用于签名 • Encryption: 表示用于加密
Remain polling attempts	剩余的证书申请状态的查询次数
Next polling attempt after	当前到下次查询证书申请状态的时间间隔，单位为秒

【相关命令】

- **certificate request polling**
- **pki domain**
- **pki retrieve-certificate**

1.1.17 display pki crl domain

display pki crl domain 命令用来显示存储在本地的 CRL。

【命令】

display pki crl domain *domain-name*

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

domain *domain-name*: 指定 CRL 所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

【使用指导】

用户可以通过该命令查看证书吊销列表，看所需的证书是否已经被吊销。

【举例】

```
# 显示 PKI 域 aaa 存储在本地的 CRL。
<Sysname> display pki crl domain aaa
Certificate Revocation List (CRL):
    Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: /C=cn/O=docm/OU=sec/CN=therootca
    Last Update: Apr 28 01:42:13 2011 GMT
    Next Update: NONE
    CRL extensions:
        X509v3 CRL Number:
            6
        X509v3 Authority Key Identifier:
            keyid:49:25:DB:07:3A:C4:8A:C2:B5:A0:64:A5:F1:54:93:69:14:51:11:EF

Revoked Certificates:
    Serial Number: CDE626BF7A44A727B25F9CD81475C004
    Revocation Date: Apr 28 01:37:52 2011 GMT
    CRL entry extensions:
        Invalidity Date:
            Apr 28 01:37:49 2011 GMT
    Serial Number: FCADFA81E1F56F43D3F2D3EF7EB56DE5
    Revocation Date: Apr 28 01:33:28 2011 GMT
    CRL entry extensions:
        Invalidity Date:
            Apr 28 01:33:09 2011 GMT
    Signature Algorithm: sha1WithRSAEncryption
    57:ac:00:3e:1e:e2:5f:59:62:04:05:9b:c7:61:58:2a:df:a4:
    5c:e5:c0:14:af:c8:e7:de:cf:2a:0a:31:7d:32:da:be:cd:6a:
    36:b5:83:e8:95:06:bd:b4:c0:36:fe:91:7c:77:d9:00:0f:9e:
    99:03:65:9e:0c:9c:16:22:ef:4a:40:ec:59:40:60:53:4a:fc:
    8e:47:57:23:e0:75:0a:a4:1c:0e:2f:3d:e0:b2:87:4d:61:8a:
    4a:cb:cb:37:af:51:bd:53:78:76:a1:16:3d:0b:89:01:91:61:
    52:d0:6f:5c:09:59:15:be:b8:68:65:0c:5d:1b:a1:f8:42:04:
    ba:aa
```

表1-7 display pki crl domain 显示信息描述表

字段	描述
Version	CRL版本号
Signature Algorithm	CA签名该CRL采用的签名算法
Issuer	颁发该CRL的CA证书名称
Last Update	上次更新CRL的时间
Next Update	下次更新CRL的时间
CRL extensions	CRL扩展属性

字段	描述
X509v3 CRL Number	X509版本3格式的CRL序号
X509v3 Authority Key Identifier	X509版本3格式的签发该CRL的CA的标识符
keyid	公钥标识符 一个CA可能有多个密钥对，该字段用于标识CA用哪个密钥对对该CRL进行签名
Revoked Certificates	撤销的证书信息
Serial Number	被吊销证书的序列号
Revocation Date	证书被吊销的日期
CRL entry extensions:	CRL项目扩展属性
Signature Algorithm:	签名算法以及签名数据

【相关命令】

- **pki retrieve-crl**

1.1.18 fqdn

fqdn 命令用来配置 PKI 实体的 FQDN。

undo fqdn 命令用来恢复缺省情况。

【命令】

fqdn *fqdn-name-string*

undo fqdn

【缺省情况】

未配置 PKI 实体的 FQDN。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

fqdn-name-string: PKI 实体的 FQDN，为 1~255 个字符的字符串，区分大小写。形式为 *hostname@domainname*

【使用指导】

FQDN 是实体在网络中的唯一标识，由一个主机名和一个域名组成。

【举例】

配置 PKI 实体 en 的 FQDN 为 abc@pki.domain.com。

<Sysname> system-view

```
[Sysname] pki entity en
[Sysname-pki-entity-en] fqdn abc@pki.domain.com
```

1.1.19 ip

ip 命令用来配置 PKI 实体的 IP 地址。

undo ip 命令用来恢复缺省情况。

【命令】

```
ip { ip-address | interface interface-type interface-number }
undo ip
```

【缺省情况】

未配置 PKI 实体的 IP 地址。

【视图】

PKI 实体视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ip-address: 指定 PKI 实体的 IP 地址。

interface interface-type interface-number: 指定接口的主 IP 地址作为 PKI 实体的 IP 地址。*interface-type interface-number* 表示接口类型及接口编号。

【使用指导】

通过本命令，可以直接指定 PKI 实体的 IP 地址，也可以指定设备上某接口的主 IP 地址作为 PKI 实体的 IP 地址。如果指定使用某接口的 IP 地址，则不要求本配置执行时该接口上已经配置了 IP 地址，只要设备申请证书时，该接口上配置了 IP 地址，就可以直接使用该地址作为 PKI 实体身份的一部分。

【举例】

```
# 配置 PKI 实体 en 的 IP 地址为 192.168.0.2。
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] ip 192.168.0.2
```

1.1.20 ldap-server

ldap-server 命令用来指定 LDAP 服务器。

undo ldap-server 命令用来恢复缺省情况。

【命令】

```
ldap-server host hostname [ port port-number ] [ vpn-instance vpn-instance-name ]
undo ldap-server
```

【缺省情况】

未指定 LDAP 服务器。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

host *hostname*: LDAP 服务器的主机名，为 1~255 个字符的字符串，区分大小写，支持 IPv4 与 IPv6 地址的表示方法以及 DNS 域名的表示方法。

port *port-number*: LDAP 服务器的端口号，取值范围为 1~65535，缺省值为 389。

vpn-instance *vpn-instance-name*: 指定 LDAP 服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该 LDAP 服务器属于公网。

【使用指导】

以下两种情况下，需要配置 LDAP 服务器：

- 通过 LDAP 协议获取本地证书或对端证书时，需要指定 LDAP 服务器。
- 通过 LDAP 协议获取 CRL 时，若 PKI 域中配置的 LDAP 格式的 CRL 发布点 URL 中未携带主机名或 IP 地址，则需要根据此处配置的 LDAP 服务器地址来得到完整的 LDAP 发布点 URL。

在一个 PKI 域中，只能指定一个 LDAP 服务器，多次执行本命令，最后一次执行的命令生效。

【举例】

指定 LDAP 服务器的 IP 地址为 10.0.0.1。

```
<Sysname> system-view
```

```
[Sysname] pki domain aaa
```

```
[Sysname-pki-domain-aaa] ldap-server host 10.0.0.1
```

指定 LDAP 服务器，IP 地址为 10.0.0.11，端口号为 333，所在的 MPLS L3VPN 的实例名称为 vpn1。

```
<Sysname> system-view
```

```
[Sysname] pki domain aaa
```

```
[Sysname-pki-domain-aaa] ldap-server host 10.0.0.11 port 333 vpn-instance vpn1
```

【相关命令】

- **pki retrieve-certificate**
- **pki retrieve-crl**

1.1.21 locality

locality 命令用来配置 PKI 实体所在的地理区域名称，比如城市名称。

undo locality 命令用来恢复缺省情况。

【命令】

locality *locality-name*

undo locality

【缺省情况】

未配置 PKI 实体所在的地理区域名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

locality-name: PKI 实体所在的地理区域的名称，为 1~63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

配置 PKI 实体 en 所在地理区域的名称为 pukras。

```
<Sysname> system-view
```

```
[Sysname] pki entity en
```

```
[Sysname-pki-entity-en] locality pukras
```

1.1.22 organization

organization 命令用来配置 PKI 实体所属组织的名称。

undo organization 命令用来恢复缺省情况。

【命令】

organization *org-name*

undo organization

【缺省情况】

未配置 PKI 实体所属组织名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

org-name: PKI 实体所属的组织名称，为 1~63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

配置 PKI 实体 en 所属的组织名称为 abc。

```
<Sysname> system-view
```

```
[Sysname] pki entity en
```

```
[Sysname-pki-entity-en] organization abc
```

1.1.23 organization-unit

organization-unit 命令用来指定实体所属的组织部门的名称。

undo organization-unit 命令用来恢复缺省情况。

【命令】

organization-unit *org-unit-name*

undo organization-unit

【缺省情况】

未配置 PKI 实体所属组织部门的名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

org-unit-name: PKI 实体所属组织部门的名称，为 1~63 个字符的字符串，区分大小写，不能包含逗号。使用该参数可在同一个组织内区分不同部门的 PKI 实体。

【举例】

配置 PKI 实体 en 所属组织部门的名称为 rdtest。

```
<Sysname> system-view
```

```
[Sysname] pki entity en
```

```
[Sysname-pki-entity-en] organization-unit rdtest
```

1.1.24 pkcs7-encryption-algorithm

pkcs7-encryption-algorithm 命令用来指定 PKCS#7 证书使用的加密算法。

undo pkcs7-encryption-algorithm 命令用来恢复缺省情况。

【命令】

pkcs7-encryption-algorithm { 3des-cbc | aes-cbc-128 | des-cbc }

undo pkcs7-encryption-algorithm

【缺省情况】

PKCS#7 证书使用的加密算法为 **des-cbc**。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

3des-cbc: 指定证书使用的加密算法为 CBC 模式的 3DES 算法，3DES 算法采用 168 比特的密钥进行加密。

des-cbc: 指定证书使用的加密算法为 CBC 模式的 DES 算法，DES 算法采用 56 比特的密钥进行加密。

aes-cbc-128: 指定证书使用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 128 比特的密钥进行加密。

【使用指导】

在线申请证书过程中需要生成 PKCS#7 证书。本命令指定 PKCS#7 证书封装与解封过程中需要使用的加密算法类型。加密算法类型需要与 CA 服务器支持的对称加密算法类型保持一致。

【举例】

```
# 指定 PKCS#7 证书使用的加密算法为 CBC 模式的 3DES 算法。
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] pkcs7-encryption-algorithm 3des-cbc
```

1.1.25 pki abort-certificate-request

pki abort-certificate-request 命令用来停止证书申请过程。

【命令】

pki abort-certificate-request domain *domain-name*

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

domain *domain-name*: 指定证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

【使用指导】

用户在证书申请时，可能由于某种原因需要改变证书申请的一些参数，比如通用名、国家代码、FQDN 等，而此时证书申请正在运行，为了新的申请不与之前的申请发生冲突，建议先停止之前的申请程序，再进行新的申请。

【举例】

```
# 停止证书申请过程。
<Sysname> system-view
[Sysname] pki abort-certificate-request domain 1
The certificate request is in process.
Confirm to abort it? [Y/N]:y
```

【相关命令】

- **display pki certificate request-status**
- **pki request-certificate domain**

1.1.26 pki certificate access-control-policy

pki certificate access-control-policy 命令用来创建证书访问控制策略，并进入证书访问控制策略视图。如果指定的证书访问控制策略已存在，则直接进入其视图。

undo pki certificate access-control-policy 命令用来删除指定的证书访问控制策略。

【命令】

```
pki certificate access-control-policy policy-name  
undo pki certificate access-control-policy policy-name
```

【缺省情况】

不存在证书访问控制策略。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

policy-name: 表示证书访问控制策略名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

一个证书访问控制策略中可以定义多个证书属性的访问控制规则。

【举例】

```
# 配置一个名称为 mypolicy 的证书访问控制策略，并进入证书访问控制策略视图。  
<Sysname> system-view  
[Sysname] pki certificate access-control-policy mypolicy  
[Sysname-pki-cert-acp-mypolicy]
```

【相关命令】

- **display pki certificate access-control-policy**
- **rule**

1.1.27 pki certificate attribute-group

pki certificate attribute-group 命令用来创建证书属性组并进入证书属性组视图。如果指定的证书属性组已存在，则直接进入其视图。

undo pki certificate attribute-group 命令用来删除指定的证书属性组。

【命令】

```
pki certificate attribute-group group-name
```

undo pki certificate attribute-group *group-name*

【缺省情况】

不存在证书属性组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name: 证书属性组名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

一个证书属性组就是一系列证书属性规则（通过 **attribute** 命令配置）的集合，这些属性规则定义了对证书的颁发者名、主题名以及备用主题名进行过滤的匹配条件。当证书属性组下没有任何属性规则时，则认为对证书的属性没有任何限制。

【举例】

创建一个名为 **mygroup** 的证书属性组，并进入证书属性组视图。

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

【相关命令】

- **attribute**
- **display pki certificate attribute-group**
- **rule**

1.1.28 pki delete-certificate

pki delete-certificate 命令用来删除 PKI 域中的证书。

【命令】

pki delete-certificate domain *domain-name* { **ca** | **local** | **peer** [**serial** *serial-num*] }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*: 证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

ca: 表示删除 CA 证书。

local: 表示删除本地证书。

peer: 表示删除对端证书。

serial serial-num: 表示通过指定序列号删除一个指定的对端证书。*serial-num* 为对端证书的序列号，为 1~127 个字符的字符串，不区分大小写。在每个 CA 签发的证书范围内，序列号可以唯一标识一个证书。如果不指定本参数，则表示删除本 PKI 域中的所有对端证书。

【使用指导】

删除 CA 证书时将同时删除所在 PKI 域中的本地证书和所有对端证书，以及 CRL。

如果需要删除指定的对端证书，则需要首先通过 **display pki certificate** 命令查看本域中已有的对端证书的序列号，然后再通过指定序列号的方式删除该对端证书。

【举例】

删除 PKI 域 aaa 中的 CA 证书。

```
<Sysname> system-view
```

```
[Sysname] pki delete-certificate domain aaa ca
```

Local certificates, peer certificates and CRL will also be deleted while deleting the CA certificate.

```
Confirm to delete the CA certificate? [Y/N]:y
```

```
[Sysname]
```

删除 PKI 域 aaa 中的本地证书。

```
<Sysname> system-view
```

```
[Sysname] pki delete-certificate domain aaa local
```

```
[Sysname]
```

删除 PKI 域 aaa 中的所有对端证书。

```
<Sysname> system-view
```

```
[Sysname] pki delete-certificate domain aaa peer
```

```
[Sysname]
```

首先查看 PKI 域 aaa 中的对端证书，然后通过指定序列号的方式删除对端证书。

```
<Sysname> system-view
```

```
[Sysname] display pki certificate domain aaa peer
```

```
Total peer certificates: 1
```

```
Serial Number: 9a0337eb2156ba1f5476e4d754a5a9f7
```

```
Subject Name: CN=abc
```

```
[Sysname] pki delete-certificate domain aaa peer serial 9a0337eb2156ba1f5476e4d754a5a9f7
```

【相关命令】

- **display pki certificate**

1.1.29 pki domain

pki domain 命令用来创建 PKI 域，并进入 PKI 域视图。如果指定的 PKI 域已存在，则直接进入 PKI 域视图。

undo pki domain 命令用来删除指定的 PKI 域。

【命令】

```
pki domain domain-name  
undo pki domain domain-name
```

【缺省情况】

不存在 PKI 域。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

domain-name: PKI 域名，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

【使用指导】

删除 PKI 域的同时，会将该域相关的证书和 CRL 都删除掉，因此请慎重操作。

【举例】

```
# 创建 PKI 域 aaa 并进入 PKI 域视图。  
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa]
```

1.1.30 pki entity

pki entity 命令用来创建 PKI 实体，并进入 PKI 实体视图。如果指定的 PKI 实体已存在，则直接进入 PKI 实体视图。

undo pki entity 命令用来删除指定的 PKI 实体。

【命令】

```
pki entity entity-name  
undo pki entity entity-name
```

【缺省情况】

不存在 PKI 实体。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

entity-name: PKI 实体的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

在 PKI 实体视图下可配置 PKI 实体的各种属性（通用名、组织部门、组织、地理区域、省、国家、FQDN、IP），这些属性用于描述 PKI 实体的身份信息。当申请证书时，PKI 实体的信息将作为证书中主题（Subject）部分的内容。

【举例】

创建名称为 en 的 PKI 实体，并进入该实体视图。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

【相关命令】

- **pki domain**

1.1.31 pki export

pki export 命令用来将 PKI 域中的 CA 证书、本地证书导出到文件中或终端上。

【命令】

```
pki export domain domain-name der { all | ca | local } filename filename
pki export domain domain-name p12 { all | local } passphrase p12-key filename
filename
pki export domain domain-name pem { { all | local } [ { 3des-cbc | aes-128-cbc
| aes-192-cbc | aes-256-cbc | des-cbc } pem-key ] | ca } [ filename filename ]
```

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

domain *domain-name*: 证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

der: 指定证书文件格式为 DER 编码（包括 PKCS#7 格式的证书）。

p12: 指定证书文件格式为 PKCS#12 编码。

pem: 指定证书文件格式为 PEM 编码。

all: 表示导出所有证书，包括 PKI 域中所有的 CA 证书和本地证书，但不包括 RA 证书。

ca: 表示导出 CA 证书。

local: 表示导出本地证书或者本地证书和其对应私钥。

passphrase *p12-key*: 指定对 PKCS12 编码格式的本地证书对应的私钥进行加密所采用的口令。

3des-cbc: 对本地证书对应的私钥数据采用 3DES_CBC 算法进行加密。

aes-128-cbc: 对本地证书对应的私钥数据采用 128 位 AES_CBC 算法进行加密。

aes-192-cbc: 对本地证书对应的私钥数据采用 192 位 AES_CBC 算法进行加密。

aes-256-cbc: 对本地证书对应的私钥数据采用 256 位 AES_CBC 算法进行加密。

des-cbc: 对本地证书对应的私钥数据采用 DES_CBC 算法进行加密。

pem-key: 指定对 PEM 编码格式的本地证书对应的私钥进行加密所采用的口令。

filename filename: 指定保存证书的文件名，不区分大小写。如果不指定本参数，则表示要将证书直接导出到终端上显示，这种方式仅 PEM 编码格式的证书才支持。

【使用指导】

导出 CA 证书时，如果 PKI 域中只有一个 CA 证书则导出单个 CA 证书到用户指定的一个文件或终端，如果是一个 CA 证书链则导出整个 CA 证书链到用户指定的一个文件或终端。

导出本地证书时，设备上实际保存证书的证书文件名称并不一定是用户指定的名称，它与本地证书的密钥对用途相关，具体的命名规则如下（假设用户指定的文件名为 *certificate*）：

- 如果本地证书的密钥对用途为签名，则证书文件名称为 *certificate-signature*；
- 如果本地证书的密钥对用途为加密，则证书文件名称为 *certificate-encryption*；
- 如果本地证书的密钥对用途为通用（RSA/ECDSA/DSA），则证书文件名称为用户输入的 *certificate*。

导出本地证书时，如果 PKI 域中有两个本地证书，则导出结果如下：

- 若指定文件名，则将每个本地证书分别导出到一个单独的文件中；
- 若不指定文件名，则将所有本地证书一次性全部导出到终端上，并由不同的提示信息进行分割显示。

导出所有证书时，如果 PKI 域中只有本地证书或者只有 CA 证书，则导出结果与单独导出相同。如果 PKI 域中存在本地证书和 CA 证书，则具体导出结果如下：

- 若指定文件名，则将每个本地证书分别导出到一个单独的文件，该本地证书对应的完整 CA 证书链也会同时导出到该文件中。
- 若不指定文件名，则将所有的本地证书及域中的 CA 证书或者 CA 证书链一次性全部导出到终端上，并由不同的提示信息进行分割显示。

以 PKCS12 格式导出所有证书时，PKI 域中必须有本地证书，否则会导出失败。

以 PKCS12 格式导出所有证书时，如果此时本地证书没有匹配的私钥，则导出该本地证书失败。

以 PEM 格式导出本地证书或者所有证书时，若不指定私钥的加密算法和私钥加密口令，则不会导出本地证书对应的私钥信息。

以 PEM 格式导出本地证书或者所有证书时，若指定私钥加密算法和私钥加密口令，且此时本地证书有匹配的私钥，则同时导出本地证书的私钥信息；如果此时本地证书没有匹配的私钥，则导出该本地证书失败。

导出本地证书时，若当前 PKI 域中的密钥对配置已被修改，导致本地证书的公钥与该密钥对的公钥部分不匹配，则导出该本地证书失败。

导出本地证书或者所有证书时，如果 PKI 域中有两个本地证书，则导出某种密钥用途的本地证书失败并不会影响导出另外一个本地证书。

指定的文件名中可以带完整路径，当系统中不存在用户所指定路径时，则会导出失败。

【举例】

```
# 导出 PKI 域中的 CA 证书到 DER 编码的文件，文件名称为 cert-ca.der。
<Sysname> system-view
[Sysname] pki export domain domain1 der ca filename cert-ca.der
# 导出 PKI 域中的本地证书到 DER 编码的文件，文件名称为 cert-lo.der。
<Sysname> system-view
[Sysname] pki export domain domain1 der local filename cert-lo.der
# 导出 PKI 域中的所有证书到 DER 编码的文件，文件名称为 cert-all.p7b。
<Sysname> system-view
[Sysname] pki export domain domain1 der all filename cert-all.p7b
# 导出 PKI 域中的 CA 证书到 PEM 编码的文件，文件名称为 cacert。
<Sysname> system-view
[Sysname] pki export domain domain1 pem ca filename cacert
# 导出 PKI 域中的本地证书及其对应的私钥到 PEM 编码的文件，指定保护私钥信息的加密算法为
DES_CBC、加密口令为 111，文件名称为 local.pem。
<Sysname> system-view
[Sysname] pki export domain domain1 pem local des-cbc 111 filename local.pem
# 导出 PKI 域中所有证书到 PEM 编码的文件，不指定加密算法和加密口令，不导出本地证书对应
的私钥信息，文件名称为 all.pem。
<Sysname> system-view
[Sysname] pki export domain domain1 pem all filename all.pem
# 以 PEM 格式导出 PKI 域中本地证书及其对应的私钥到终端，指定保护私钥信息的加密算法为
DES_CBC、加密口令为 111。
<Sysname> system-view
[Sysname] pki export domain domain1 pem local des-cbc 111

*** The general usage local certificate: ***
Bag Attributes
    friendlyName:
        localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEqjCCA5KgAwIBAgILAOhID4rI04kBFYgWDQYJKoZIhvcNAQELBQAwRTElMAkG
A1UEBhMCQ04xFDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLEDAhzb2Z0d2Fy
ZTENMA5GA1UEAwEYVWJjZDAeFw0xMTA0MjYxMzMxMjlaFw0xMjA0MjYxMzMxMjla
ME0xCzAJBgNVBAYTAkNOMRQwEgYDVQQKDAtPcGVuQ0EgTGFIczE0MAwGA1UECwwF
VXNlcnMxGDAwBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AA0BJQAwwYkCgYEYA54rUZ0Ux2kApceE4ATpQ437CU6ovuHS5eJKZyky8fhMoTHhE
jE2KfBQIZ0ZSgo2mdgpkccjr9Ek6IUC03ed1lPn0IG/YaAl4Tjgkiv+w1NrIsvAy
cnPaSuko2Qb09sg3ycye1zqpbqj775ulGpcXyXYD90Y63/Cp5+DRQ92zGsCAWEA
Aa0CAhUwggIRMAkGA1UdEwQCMAAwUAYDVR0gBEKwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEkGMDBJAtMCSGCCsGAQUFBwIBFh9odHRwc3ovL3RpdGFuL3BraS9wdWlVY3Bz
L2Jhc2ljMBEGCWCsSAGG+EIBAQQEAWIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAWIGCCsGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCGSAGG+EIBDQQH
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMB0GA1UdDgQWBw8FY
```

```
ut7Xr2Ct/23zU/ybgU9dQjAfBgNVHSMEGDAWgBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEEzARgQ9jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIE0cGtpQG9w
ZW5jYS5vcmcwgYEGCCsGAQUFBwEBBHUwcZAYBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWIVY2FjZXJ0L2NhY2VydC5jcQWgYIKwYBBQUHMAGGEmh0dHA6
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFu0jgzMC8wPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovLzE5Mi4xNjguNDANMTI4L3BraS9wdWIVY3Js
L2NhY3JsLmNybdANBgkqhkiG9w0BAQsFAA0CAQEAGcMeSpBjiuRmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIxZhPWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHZ2oysvNQ00t6hGylMqaZ8pKUKv
UDS8c+HgIBrhmxvXztI08N1imYHq27Wy9j6NpSS60mMfM5whzCwfTSHzqlT2DNd
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
```

Bag Attributes

friendlyName:

localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D

Key Attributes: <No Attributes>

-----BEGIN ENCRYPTED PRIVATE KEY-----

```
MIICwzA9BgkqhkiG9w0BBQwMDAbBgkqhkiG9w0BBQwwDgQIAbfCE+KoYYoCAgGA
MBEGBSs0AwIHBAjB+UsJM07JRQSCAoABqtASbjGTQbdxL3n4wNHmyWLxbvL9v27C
Uu6MjYJDCipVzxHU0rExgn+6cQsK5uK99FPBmy4q9/nnrootX8BVlXAjenvgyii
WQLwnIg1IuM8j2aPkQ3wbae1+0RACjSLy1u/PCl5sp6CDxI0b9xz6cxIGxKvU0Cc
/gxdgk97XZSW/0qn0SZkhgeqBZuxq6Va8iRyho7RCStVxQaeiAZpq/WoZbcS5CKI
/WXEBQd4AX2UxN0Ld/On7Wc6KFToixR0TxWtft8SEsKGPdfrEKq3fSTW1xokB8nM
bkRtU+fUiy27V/mr1RH06+yEr+/wGGClBy5YDoD4I9xPkGUkmqx+kfYbMo4yXkSi
JdL+X3uEjHnQ/rvnPSKBEU/URwXHXMX9CdCTSqH/SajnrGuB/E4Jh0EnS/H9dIM+
DN6iz1IwPFklbcK9KMGwV1bosymXmuEbYCYmSmhZb5FnR/RIyE804Jz9ifin3g0Q
ZrykfG7LHL7Ga4nh0hpEeEIdHGEMcQU+g0Etfp0LTI8cMJf7kdNWDnI0AYCvBAAM
3CY3BELDVjJq3ioyHSJca8C+3lzcueuAF+l07Y4Zluq3dqWuJJE+/1BZJbMmaQA
X6NmXKNzmtTPcMtojf+n3+uju0le0d0QYXQz/wPsv+9IYRYasjzoXE5dhZ5sIP0d
u9x9hhp5Ns23bwyNP135qTNjx9i/CZMKvLKym3Yg+Bg8Df4bBrFrSH1U0ifmmp
ir2+0uHlc+GbH0xwNeBCa8iAq91k6FGFJ00LA2oIvChnh45tM7BjjKTHk+RZdMiA
0TKSWu0yihrwxdUEwh999GKUpkwDHLZJFd21z/kwspqThodEx8ea
```

-----END ENCRYPTED PRIVATE KEY-----

以 PEM 格式导出 PKI 域中所有证书到终端,指定保护本地证书对应私钥的加密算法为 DES_CBC、加密口令为 111。

<Sysname> system-view

[Sysname] pki export domain domain1 pem all des-cbc 111

%The signature usage local certificate:

Bag Attributes

friendlyName:

localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D

subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest

issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd

-----BEGIN CERTIFICATE-----

```
MIIEqjCCA5KgAwIBAgILA0hID4rI04kBFYgwdQYJKoZIhvcNAQELBQAwRTElMAkG
A1UEBhMCQ04xZDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLDAhzb2Z0d2Fy
```

ZTENMASGA1UEAwWEYwJjZDAeFw0xMTA0MjYxMzMzMjlaFw0xMjA0MjUxMzMzMjla
ME0xCzAJBgNVBAYTAkNOMRQwEgYDVQQKDATPcGVuQ0EgTGFIczE0MAwGA1UECwwF
VXNlcnMxGDAwBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwGykCgYEA54rUZ0Ux2kApceE4ATpQ437CU6ovuHS5eJKZyky8fhMoTHHe
jE2KfBQIzOZSgo2mdgpkccjr9Ek6IUC03ed1lPn0IG/YaAl4Tjgkiv+w1Nr1SvAy
cnPaSUKo2Qb09sg3ycye1zqpbqj775ulGpcXyXYD90Y63/Cp5+DRQ92zGsCAwEA
Aa0CAhUwggIRMAkGA1UdEwQCMAAwUAYDVR0gBEKwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEKgmDBjAtMCsGCCsGAQUFBwIBFh9odHRwczovL3RpdGFuL3BraS9wdWIVY3Bz
L2Jhc2ljMBEGCwCGSAGG+EIBAQQEAWIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAWIGCCsGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCGSAGG+EIBDQqh
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMB0GA1UdDgQWBbTPw8FY
ut7Xr2Ct/23zU/ybgu9dQjAfBgNVHSMEGDAwGBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEZARQ9jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIE0cGtpQG9w
ZW5jYS5vcmcwgYEGCCsGAQUFBwEBBHUwczAyBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWIVY2FjZXJ0L2NhY2Vydc5jcnQwHgYIKwYBBQUHMAAGGEmh0dHA6
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFu0jgzMC8wPAYD
VR0fBDUwMzAxoCgLYYraHR0cDovLzE5Mi4xNjguNDAMTI4L3BraS9wdWIVY3Js
L2NhY3JsLmNybdANBgkqhkiG9w0BAQsFAA0CAQEAGcMeSpBJiurmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIXzhPWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLckXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ00t6hGylMqaZ8pKUKv
UDS8c+HgIBrhmxvXztI08N1imYHq27Wy9j6NpSS60mMFmI5whzCwfTSHzqlT2DND
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
Bag Attributes: <No Attributes>
subject=/C=CN/0=OpenCA Labs/OU=software/CN=abcd
issuer=/C=CN/0=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEYTCCA0mgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBFMQswCQYDVQQGEwJDTjEU
MBIGA1UECgwLT3B1bkNBIExhYnMxETAPBgNVBAsMCHNvZnR3YXJlMQ0wCwYDVQQD
DARhYmNkMB4XDTEyMDQxODExNDQ0N1oXDTEyMDQxNzExNDQ0N1owRTElMAkGA1UE
BhMCQ04xZDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQLEAhzb2Z0d2FyZTEN
MASGA1UEAwWEYwJjZDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1g
vomMF8S4u6q51b0wjKFUBwxyv0y4D897Lm0SedaCyDt6Lvp+PBEHfwwBYBpsHhk7
kmnSNhX5dZ6NxunHaARZ2VlcctsYKyvAQapuaThy1tu0cphAB+jQQL9dPoqdk0xp
jvmPDLw+k832Konn9U4dIivS0n+/KMgh0g5UyzHGqUU0o7s9qFuQf5EjQon40TZg
BwUnFYRlvGe7bSQpXjwi8LTyxHPy+dDVj05CP+rXx5IiToFy1YGWewkyn/WeswDf
Yx7ZludNus5vKWtIhgx2Qalgb+sqUMwI/WUET7gh02dRxPUdUbgIYF0saTndKPYd
4oBg16M0SMsHhe9nF5UCAwEAAa0CAVowggFWMA8GA1UdEwEB/wQFMAMBAf8wCwYD
VR0PBAQDAgEGMB0GA1UdDgQWBbBQzEQ58yIC54wxodp6JzZvn/gx0CDAfBgNVHSME
GDAwGBQzEQ58yIC54wxodp6JzZvn/gx0CDAZBgNVHREEejAQgQ5wa2lAb3B1bmNh
Lm9yZzAZBgNVHRIEejAQgQ5wa2lAb3B1bmNhLm9yZzCBgQYIKwYBBQUHAQEEDTBz
MDIGCCsGAQUFBzACHiZodHRwOi8mdcGl0YW4vcGtpL3B1Yi9jYWNlcnQvY2FjZXJ0
LmNydDAeBggrBgEFBQcwAYYSaHR0cDovL3RpdGFu0jI1NjAvMB0GCCsGAQUFBzAM
hhFodHRwOi8mdcGl0YW46ODMwLzA8BgNVHR8ENTAzMDGgLG6AthitodHRwOi8vMTky
LjE2OC40MC4xMjgvcGtpL3B1Yi9jcmwvY2FjcWwvY3JsMA0GCSqGSIb3DQEBCwUA
A4IBAQC0q0SSmVnQfa5ELtRKYF62C/Y8QTLbk6lZDTZuIzN15SGKQcbNM970ffCD
Lk1zosyEVE7PLnii3bZ5khcG03byyXfluAqRy0GVJcudaw7uIQqgv0AJQ+zaQSHi

```

d4kQf5QWgYkQ55/C5pu0mcMRgCbMpR2lYkqXLDjTIAZiHRZ/sTp6c+ie2bFxi/YT
3xYb00wDMuG0KJJpsyKTKcbG9NdfbDyFgzEYAobyYqAUB3C0/bmFBduwhQWKSoyE
6vZsPGAeisCmaL3dIp49jPgVkiXoSraYF1jLsWzJGLzem8QvWYz0qKEDwq3SV0Z
cXK8gzDBcsobcUMkwIYPAmD1kAPX
-----END CERTIFICATE-----
Bag Attributes
    friendlyName:
        localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICwzA9BgkqhkiG9w0BBQwMDAbBgkqhkiG9w0BBQwwDgQICUSKSW9GVmICAggA
MBEGBSsOAuIHBai5QZM+lsYWPASCAoBKDYuLE5f2BXL9ZhI9zWAJpx2cShz/9Psw
5Qm106D+xSj1eAzkx/m4Xb4xRU8o0AuZu1DLwFSHKXoaa00oRSi0EX1eg0eo/2vv
CHCvKHfTJr4gVSSa7i4I+aQ6AItrI6q99Wlkn/e/IE5U1UE4ZhcsiFJG+IvG7S8
f9liWQ2CImy/hjgFCD9nqSLN8wUzP702SdLVlUb5z4FR6VISZdgTFE8j7ko2HtUs
HVSg0nm114EWptPMMbHefcuQ6b82y1M+dWfVxBN9K03lN4tZNFpWwLSRrPvjUzBG
dKtjF3/IFdV7/tUMy9JJSp4iFt1h7SZPc0oGp1ZW+YUR30I7YnFE+9Yp/46KWt8
bk7j0STRnZX/xMy/9E52uHkLdW1ET3TXraLLMyt/4jg4M0jUvoi3GS2Kbo+czsUn
gKqgwYnxVfRSvt8d6GBYrP2tMFS9LEyngPKXExd+m4mAryuT5PhdFTkb1B190Lp
UIBjk3IXnr7AdrhyvLkH0UuQE95emXBD/K0HlD73cMrtmogL8F4yS5B2hpIr/v5/
eW35+1QMnJ9FtHFfVSLx9wL9lX8iNfsoBhg6FQ/hNSioN7rNBe7wwIRzXPVfEh08
5ajQxwLidRn5RkzfUo6HuAcq02QTpSXI6wf2bzsvmr5sk+fRaELD/cwL6Vjtx06x
ZBLJcUyAwvScrOtTEK7Q5n0I34gQd4qcF0D1x9yQ4sqvTeU/7Jkm6XCPV05/5uiF
RLCfFAwaJMBdIQ6jDQHnpWT67uNDwdEzaPmuTVMme5Woc5zsqE5DY3hWu4oqFdDz
kPLnbX74IZ0gOLki9eIjKvswNF5HkBCKS50ejlw6TgbMNZ+Jpk2w
-----END ENCRYPTED PRIVATE KEY-----

```

以 PEM 格式导出 PKI 域中 CA 证书到终端。

```

<Sysname> system-view
[Sysname] pki export domain domain1 pem ca
-----BEGIN CERTIFICATE-----
MIIB+TCCAWICEQDMbgjRKygg3vpGFVY6pa3ZMA0GCSqGSIb3DQEBBQUAMD0xCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxETAPBgNVBAsTCGgzYy10ZXN0MQ0wCwYD
VQQDEwQ4MDQzMBA4XDTEwMDMyMjA0NDQyNFoXDTE0MDMyMzUyNFowPTELMAKG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzERMA8GA1UECzMIA0NDJLXRlc3QxDTALBgNV
BAMTBDBgNDMwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBA0vDAYQhyc++G7h5
eNDzJs220QjCn/4JqnNKIdKz1BbaJT8/+IueSn9JIsG64Ex2WBeCd/tcmnSW57ag
dCvNIUYXXV0Gca2iaS0ElqCF4CQfV9zLrBtA7giHD49T+JbxLrrJLmdIQMJ+vYdC
sCxIp3YMAiuCahVLZeXklooqWqIXAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAElm7
w2Lp9Xk4nZVIpV76CkNe8/C+Id00GCRUUVQFSMvo7PdEd76bmYX2KzJSz+DlMqy
TdVrgG9Fp6XTF080aKJGe6NapsfhJHKS+Q7mL0XpXeM0NgK+e3dX7rsDxsY7hF+j
0gwsHrjv7kVwVjvDlhZGW6xbpr4DRmdcao19Cr6o=
-----END CERTIFICATE-----

```

导出 PKI 域中 CA 证书到 PEM 编码的文件，指定文件名称为 cacert。

```

<Sysname> system-view
[Sysname] pki export domain domain1 pem ca filename cacert
# 导出 PKI 域中 CA 证书（证书链）到终端。
<Sysname> system-view
[Sysname] pki export domain domain1 pem ca

```

-----BEGIN CERTIFICATE-----

```
MIIB7jCCAVcCEQCdSVShJFEMifVG8zRRoSsWMA0GCSqGSIb3DQEBBQUAMDCxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAsTA2gzYzEMMAoGA1UEAxMD
YWNhMB4XDTEwMDExMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
Y24xMjEwMDExMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDcuJswHAXJEDmowGb5z7VDVms54TKi
xnaNJCWvB0rU64ftvpVB7xQekbkjgAS9FjDyXLLQ8IyIsYIp5ebJr8P+n9i9Pl7j
lBx5mi4XeIldyv20jfNx5oSq+gWY9/m1R8uv13RS05r3rxPg+7EvKBjmiy0Giddw
vu3Y3WrjBPP6GQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAjrQddzVQEiy4AcgtzUL
ltkmlmWoz87+jUsgFB+H+xeyiZE4sancf2UwH8kXWqZ5AuReFCCBC2fkvvQvUGnV
cso7JXAhfw8sUFok9eHz2R+GSoEk5BZFzZ8eCmNyGq9ln6mJs01hAqMpsCW6G2zh
5mus7FTHhywXpJ22/fnHg61m
```

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

```
MIIB8DCCAVKCEQD2PBux/rvslnW9uTrZB3DLMA0GCSqGSIb3DQEBBQUAMDoxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAsTA2gzYzEPMA0GA1UEAxMG
cm9mdcGNhMB4XDTEwMDExMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
BhMCY24xMjEwMDExMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBA0eklR7DpeEV72N10Lz+dydIDTx0
zVZDdPxFlgQYWSfIBwWFKJEyQ/4y8VIfDIm0EGTM4dsOX/QFwudhl/Czkio3dWLh
Q1y5XCJy68vQKR82WZ2mah5Nuekus3LSZZBoZKTA0Y5MCCMFcULM858dtSq15Sh
xF7tKSeAT7ARlJxTagMBAAEWdQYJKoZIhvcNAQEFBQADgYEADJQCo6m0RNup0ewa
ItX4XK/tYcJXAQWMA0IuwaWpr+ofqVVgYBPwVpYglhJD0uIZxKdR2pfQ0A4f35wM
Vz6kAuJLATsEA1GW9ACUWa5PHwVgJk9BDEXhKSJ2e7odmrg/iR0hJjc1NMV3pvIs
CuFiCLxRQcMGhCNHl0n4wuydssc=
```

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

```
MIIB8jCCAVsCEfxy3MSlQ835MrnBkI/dUPYwDQYJKoZIhvcNAQEFBQAwojELMAkG
A1UEBhMCY24xMjEwMDExMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEwMjEw
b290Y2EwHhcnMTewMTA2MDI1MTQxWhcnMTMxMjA3MDMxMjA1WjA6MQswCQYDVQQG
EwJjbjEMMAoGA1UEChMDaDnJMQwwCgYDVQLLEwNoM2MxMjEwMjEwMjEwMjEwMjEw
YTCBnzANBQkqhkiG9w0BAQEFAA0BjQAwYkCgYEAxP2XLFE230zq6MhwZvAom0xa
7tc1r4bESXZu3UBKno3Ay9kQm2HrDOAizvZXfLu7Gx22ga2Qdz0lIeZ+EQrYHTyO
pBcejDjal/ZtvgnjXyHfOG8nS+P7n83Bkrj/Fu7Yz4zjTKMbcF2EfHfYXxr4NSXA
fhC9qg9S23vNXStmWvsCAwEAATANBgkqhkiG9w0BAQUFAA0BQBtsU7X77sdZ1Nn
0I98lh0qA5g7SEEIpi+pwZjjrH0FVHw01e4JWhHjyHqrOyfXYqe7vH4Sxp5MHEqf
14nKIEbexbPONSpebtznxv4/xTjd1aM2rfQ95jJ/SN8H8KIyiyZyIs3t5Q+V35x1
cef+NMWgZBzwXOSP0wC9+pc2ZniIpg==
```

-----END CERTIFICATE-----

导出 PKI 域中的本地证书及其对应的私钥到 PKCS12 编码的文件，指定保护私钥信息的加密口令为 123，文件名称为 cert-lo.der。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 p12 local passphrase 123 filename cert-lo.der
```

导出 PKI 域中的所有证书到 PKCS12 编码的文件，指定文件名称为 cert-all.p7b。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 p12 all passphrase 123 filename cert-all.p7b
```

【相关命令】

- **pki domain**

1.1.32 pki import

pki import 命令用来将 CA 证书、本地证书或对端证书导入到指定的 PKI 域中保存。

【命令】

```
pki import domain domain-name { der { ca | local | peer } filename filename  
| p12 local filename filename | pem { ca | local | peer } [ filename filename ] }
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain domain-name: 保存证书的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

der: 指定证书文件格式为 DER 编码（包括 PKCS#7 格式的证书）。

p12: 指定证书文件格式为 PKCS#12 编码。

pem: 指定证书文件格式为 PEM 编码。

ca: 表示 CA 证书。

local: 表示本地证书。

peer: 表示对端证书。

filename filename: 要导入的证书所在的文件名，不区分大小写。如果不指定本参数，则表示要通过直接在终端上粘贴证书内容的方式导入证书，这种方式仅 PEM 编码格式的证书才支持。

【使用指导】

如果设备所处的环境中，没有证书的发布点，或者 CA 服务器不支持通过 SCEP 协议与设备交互，则可通过此命令将证书导入到设备。另外，当证书对应的密钥对由 CA 服务器生成时，CA 服务器会将证书和对应的密钥对打包成一个文件，使用这样的证书前也需要通过此命令将其导入到设备。只有 PKCS#12 格式或 PEM 格式的证书文件中可能包含密钥对。

证书导入之前：

- 需要通过 FTP、TFTP 等协议将证书文件传送到设备的存储介质中。如果设备所处的环境不允许使用 FTP、TFTP 等协议，则可以直接在终端上粘贴证书的内容，但是粘贴的证书必须是 PEM 格式的，因为只有 PEM 编码的证书内容为可打印字符。
- 必须存在签发本地证书（或对端证书）的 CA 证书链才能成功导入本地证书（或对端证书），这里的 CA 证书链可以是保存在设备上的 PKI 域中的，也可以是本地证书（或对端证书）中携带的。因此，若设备和本地证书（或对端证书）中都没有 CA 证书链，则需要首先执行导入 CA 证书的命令。

导入本地证书或对端证书时：

- 如果用户要导入的本地证书（或对端证书）中含有 CA 证书链，则可以通过导入本地证书（或对端证书）的命令一次性将 CA 证书和本地证书（或对端证书）均导入到设备。导入的过程中，如果发现签发此本地证书（或对端证书）的 CA 证书已经存在于设备上的任一 PKI 域中，则系统会提示用户是否将其进行覆盖。
- 如果要导入的本地证书（或对端证书）中不含有 CA 证书链，但签发此本地证书（或对端证书）的 CA 证书已经存在于设备上的任一 PKI 域中，则可以直接导入本地证书（或对端证书）。

导入 CA 证书时：

- 若要导入的 CA 证书为根 CA 或者包含了完整的证书链（即含有根证书），则可以导入到设备。
- 若要导入的 CA 证书没有包含完整的证书链（即不含有根证书），但能够与设备上已有的 CA 证书拼接成完整的证书链，则也可以导入到设备；如果不能与设备上已有的 CA 证书拼接成完成的证书链，则不能导入到设备。

一些情况下，在证书导入的过程中，需要用户确认或输入相关信息：

- 若要导入的证书文件中包含了根证书，且设备上目前还没有任何 PKI 域中有此根证书，且要导入的 PKI 域中没有配置 **root-certificate fingerprint**，则在导入过程中还需要确认该根证书的指纹信息是否与用户的预期一致。用户需要通过联系 CA 服务器管理员来获取预期的根证书指纹信息。
- 当导入含有密钥对的本地证书时，需要输入口令。用户需要联系 CA 服务器管理员取得口令的内容。

导入含有密钥对的本地证书时，系统首先会根据查找到的 PKI 域中已有的密钥对配置来保存该密钥对。若 PKI 域中已保存了对应的密钥对，则设备会提示用户选择是否覆盖已有的密钥对。若 PKI 域中没有任何密钥对的配置，则根据密钥对的算法及证书的密钥用途，生成相应的密钥对配置。密钥对的具体保存规则如下：

- 如果本地证书携带的密钥对的用途为通用，则依次查找指定 PKI 域中通用用途、签名用途、加密用途的密钥对配置，并以找到配置中的密钥对名称保存该密钥对；若以上用途的密钥对配置均不存在，则提示用户输入密钥对名称（缺省的密钥对名称为 PKI 域的名称），并生成相应的密钥对配置。此时输入的名称不能和设备上任何使用相同算法的密钥对名称相同。
- 如果本地证书携带的密钥对的用途为签名，则依次查找指定 PKI 域中通用用途、签名用途的密钥对配置，并以找到配置中的密钥对名称保存该密钥对；若以上两种用途的密钥对配置均不存在，则提示用户输入密钥对名称（缺省的密钥对名称为 PKI 域的名称），并生成相应的密钥对配置。此时输入的名称不能和设备上任何使用相同算法的密钥对名称相同。
- 如果本地证书携带的密钥对的用途为加密，则查找指定 PKI 域中加密用途的密钥对配置，并以该配置中的密钥对名称保存密钥对；若加密用途密钥对的配置不存在，则提示用户输入密钥对名称（缺省的密钥对名称为 PKI 域的名称），并生成相应的密钥对配置。此时输入的名称不能和设备上任何使用相同算法的密钥对名称相同。

由于以上过程中系统会自动更新或生成密钥对配置，因此建议用户在进行此类导入操作后，保存配置文件。

【举例】

向 PKI 域 aaa 中导入 CA 证书，证书文件格式为 PEM 编码，证书文件名称为 rootca_pem.cer，证书文件中包含根证书。

```
<Sysname> system-view
```

```
[Sysname] pki import domain aaa pem ca filename rootca_pem.cer
```


The trusted CA's finger print is:

MD5 fingerprint:FFFF 3EFF FFFF 37FF FFFF 137B FFFF 7535

SHA1 fingerprint:FFFF FF7F FF2B FFFF 7618 FF4C FFFF 0A7D FFFF FF69

Is the finger print correct?(Y/N):y

[Sysname]

向 PKI 域 bbb 中导入 CA 证书，证书文件格式为 PEM 编码，证书文件名称为 aca_pem.cer，证书文件中不包含根证书。

<Sysname> system-view

[Sysname] pki import domain bbb pem ca filename aca_pem.cer

[Sysname]

向 PKI 域 bbb 中导入本地证书，证书文件格式为 PKCS#12 编码，证书文件名称为 local-ca.p12，证书文件中包含了密钥对。

<Sysname> system-view

[Sysname] pki import domain bbb p12 local filename local-ca.p12

Please input challenge password:

[Sysname]

向 PKI 域 bbb 中通过粘贴证书内容的方式导入 PEM 编码的本地证书。证书中含有密钥对和 CA 证书链。

<Sysname> system-view

[Sysname] pki import domain bbb pem local

Enter PEM-formatted certificates.

End with a Ctrl+C on a line by itself.

Bag Attributes

localKeyID: 01 00 00 00

friendlyName: {F7619D96-3AC2-40D4-B6F3-4EAB73DEED73}

Microsoft CSP Name: Microsoft Enhanced Cryptographic Provider v1.0

Key Attributes

X509v3 Key Usage: 10

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4, ENCRYPTED

DEK-Info: DES-EDE3-CBC, 8DCE37F0A61A4B8C

k9C3KHY5S3EtnF5iQymvHYrVFy5ZdjSasU5y4XFubjdcvmpFHQteMjD0GKX6+xO
kuKbvpyCnWsPVg56sL/PDRyrRmqLmtUV3bpyQsFXgnc7p+Snj3CG2Ciow9XApYbw
Ec1TDCD75yuQckpVQdhguTvoPQXf9zHmiGu5jLkySp2k7ec/Mc97Ef+qqpfHhpQp
GDmMqnFpp59ZzB210GlbgZlPcsjoT+EGpZg6B1KrPiCyFim95L9dWVwX9sk+U1s2
+8wqac8jETwwM0UZ1NGJ50JJz1QYIzMbcw+S5WLPxACTIz1cldlBlb1kpc+7mcX
4W+MxFzsl88IJ99T72eu4iUNsy26g0BZMAcc1sJA3A4w9RNhfs9hSG43S3hAh5li
JPP720LfYBlkQHn/MgMCZASWDJ5G0eSXQt9QymHath4BiT9v7zetnQqf4q8plfd/
Xqd9zEFLBPpoJFtJqXwxHUCKgw6kJeC4CxHvi9ZCJU/upg9IpiGuFPoaDOPia+Pm
GbRqSyy55clVde5G0ccGN1DZ94DW7AypazgLPBbrkIYAdjFPRmq+zM0dyqsGMTNj
jnheI5l784pNOAKuGi0i/uXmRRcfomh6qAnK6YZGS7rOLC9CfPmy8fgY+/Sl9d9x
Q00ru01psxzh9c2YfuaiXfIX0auKl6o5+ZZYn7Rg/xy2Y0awVP+d0925GoAch040
cCl6ja/HsGAU9HkpwKHL35lmBDRLEzQeBFcaGwSm1JvRFe4tkJM7+Uz2QHJ0fP10
0VLqMgXmLpk3TvbWgzHGJDe7TdZFCDPMPHod8pi4P8gGxmQd01PbyQ==

-----END RSA PRIVATE KEY-----

Bag Attributes

localKeyID: 01 00 00 00

subject=/CN=slssslserver

issuer=/C=cn/O=ccc/OU=sec/CN=ssl

-----BEGIN CERTIFICATE-----

```
MIICjzCCAFigAwIBAgIRAJoDN+shVrofVHbk11SlqfcwDQYJKoZIhvcNAQEFBQAw
NzELMAKGA1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECXMDC2VjMQwwCgYD
VQQDEwNzc2wwHhcNMTAxMDEyMzA2WhcNMTIwNzI2MDYzMDU0WjAXMRUwEwYD
VQQDEwxbGRzc2xzZXJ2ZXIwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMLP
N3aTKV7NDndIOk0PpiikYPgxVih/geMXR3iYaANbcvRX07/FMDINWHJnBAZhCDvp
rF0552loGiPyl0wmFMK12TSL7shVrxr00drFrqtWlbw+DsNGNcFSKZy3RvIngC2k
ZZqBeFPuytP185JUhb0rVaUDlisZi6NNshcIjd2BAGMBAAGjgbowgbcwHwYDVR0j
BBgwFoAUomoPEynZYoPLQdR1LlKhZjg8kBEwDgYDVR0PAQH/BAQDAGP4MBEGCWCG
SAGG+EIBAQQEAWIGQDASBgNVHREECzAJggdoM2MuY29tMB0GA1UdDgQWB8dpWb
3cJ/X5iDt8eg+JkeS9cvJjA+BGNVHR8ENZa1MD0gMaAvhi1odHRwOi8vczAzMTMw
LmgzYy5odWF3ZWktM2NvbS5jb206NDQ3L3NzbC5jcmwwDQYJKoZIhvcNAQEFBQAD
gYEAYS15x0kw474lu4twnZey5dPjMSwtwfm/UK01S8GQjGV5t19ZniTHFGNEF7k
zxBp/JPpcFM8hapAfrVHdQ/wstq0pVDdBkrVF6XKIBks6XgCvRl32gcaQt9yrQd9
5RbwdetuBljudfJfj25airY02u7pLeVmdWwx3WvVzBZ0o8KU=
```

-----END CERTIFICATE-----

Bag Attributes: <Empty Attributes>

subject=/C=cn/O=ccc/OU=sec/CN=ssl

issuer=/C=cn/O=ccc/OU=sec/CN=ssl

-----BEGIN CERTIFICATE-----

```
MIIB7DCCAVUCEG+jJTPxxiE67pl2ff0SnOMwDQYJKoZIhvcNAQEFBQAwnZELMAKGA
1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECXMDC2VjMQwwCgYDVQQDEwNzc
2wwHhcNMDkwnZMxMDY0ODQ2WhcNMTIwNzI5MDYyODU4WjA3MQswCQYDVQQGEWJj
bjEMMAoGA1UEChMDADnjMQwwCgYDVQQLEwNzc2ZWMzDDAKBgNVBAMTA3NzbDCBnzAN
BgkqhkiG9w0BAQEFAA0BJQAwwYkCgYEAt8QSMetQ70G0NiFh7iJkvGQ8nC15zCF1
cqC/RcJhE/88LkKyQcu9j+Tz8Bk9Qj2UPaZdrk8f0rgtBsa7Lz+U03j3l30q84l+
HjWq8yxVLRQahU3gqJze6pGR2l0s76u6GRyCX/zizGrHKqYlNnxK44NyrZx2klQ2
tKQAFpXCPIkCAWEAATANBgkqhkiG9w0BAQUFAA0BgQBwsaMgRbBMTYNrrYCMjY6g
c7PBjvajVOKNUMxaDalePmXfKcxL91+PKM7+i8I/zLcoQ0+sHbva26a2/C4sNvoJ
2QZs6GtAOahP6CDqXC5VuNBu6eTKNKjL+mf6uuDeMxrlDNha0iymdrXXVIp5cuIu
fl7xgArs8Ks6aXDXM1o4DQ==
```

-----END CERTIFICATE-----

Please input the password:*****

Local certificate already exist, confirm to overwrite it? [Y/N]:y

The PKI domain already has a CA certificate. If it is overwritten, local certificates, peer certificates and CRL of this domain will also be deleted.

Overwrite it? [Y/N]:y

The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).

Please enter the key pair name [default name: bbb]:

The key pair already exists.

```
Please enter the key pair name:
import-key
```

【相关命令】

- **display pki certificate**
- **public-key dsa**
- **public-key ecdsa**
- **public-key rsa**

1.1.33 pki request-certificate

pki request-certificate 命令用来手工申请本地证书或生成 PKCS#10 证书申请。

【命令】

```
pki request-certificate domain domain-name [ password password ] [ pkcs10  
[ filename filename ] ]
```

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

domain *domain-name*: 指定证书申请所属的 PKI 域名，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

password *password*: 在证书撤销时需要提供的口令，为 1~31 个字符的字符串，区分大小写。该口令包含在提交给 CA 的证书申请中，在吊销该证书时，需要提供该口令。

pkcs10: 在终端上显示出 BASE64 格式的 PKCS#10 证书申请信息，该信息可用于带外方式（如电话、磁盘、电子邮件等）的证书请求。

filename *filename*: 将 PKCS#10 格式的证书申请信息保存到本地的文件中。其中，*filename* 表示保存证书申请信息的文件名，不区分大小写。

【使用指导】

当 SCEP 协议不能正常通信时，可以通过执行指定参数 **pkcs10** 的本命令打印出本地的证书申请信息（BASE64 格式），或者通过执行指定 **pkcs10 filename filename** 参数的本命令将证书申请信息直接保存到本地的指定文件中，然后通过带外方式将这些本地证书申请信息发送给 CA 进行证书申请。指定的文件名中可以带完整路径，当系统中不存在用户所指定路径时，则会保存失败。此命令不会被保存在配置文件中。

【举例】

在终端上显示 PKCS#10 格式的证书申请信息。

```
<Sysname> system-view  
[Sysname] pki request-certificate domain aaa pkcs10
```

```
*** Request for general certificate ***
```

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAA0BjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPB8pvH1kumampPsJmx8sGG52NftbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3oL2z7Nmdcu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmAOXVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJ0nm5K/mn1ro5TJKMTKV46PLCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQ0HS7YMvnop6hXAQlkm4C
-----END NEW CERTIFICATE REQUEST-----
```

手工申请本地证书。

```
[Sysname] pki request-certificate domain openca
Start to request certificate ...
```

.....

Certificate requested successfully.

【相关命令】

- **display pki certificate**

1.1.34 pki retrieve-certificate

pki retrieve-certificate 命令用来从证书发布服务器上在线获取证书并下载至本地。

【命令】

```
pki retrieve-certificate domain domain-name { ca | local | peer entity-name }
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*: 指定证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

ca: 表示获取 CA 证书。

local: 表示获取本地证书。

peer *entity-name*: 表示获取对端的证书。其中 *entity-name* 为对端的实体名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

获取 CA 证书是通过 SCEP 协议进行的。获取 CA 证书时，如果本地已有 CA 证书存在，则该操作将不被允许。这种情况下，若要重新获取 CA 证书，请先使用 **pki delete-certificate** 命令删除已有的 CA 证书与对应的本地证书后，再执行此命令。

获取本地证书和对端证书是通过 LDAP 协议进行的。获取本地证书或对端证书时，如果本地已有本地证书或对端证书，则该操作是被允许进行的。最终，属于一个 PKI 实体的同一种公钥算法的本地

证书只能存在一个，后者直接覆盖已有的，但对于 RSA 算法的证书而言，可以存在一个签名用途的证书和一个加密用途的证书。

所有获取到的 CA 证书、本地证书或对端证书只有通过验证之后才会被保存到本地证书库中。

此命令不会被保存在配置文件中。

【举例】

从证书发布服务器上获取 CA 证书。（需要用户确认 CA 根证书的指纹）

```
<Sysname> system-view
```

```
[Sysname] pki retrieve-certificate domain aaa ca
```

The trusted CA's finger print is:

MD5 fingerprint:5C41 E657 A0D6 ECB4 6BD6 1823 7473 AABC

SHA1 fingerprint:1616 E7A5 D89A 2A99 9419 1C12 D696 8228 87BC C266

Is the finger print correct?(Y/N):y

Retrieved the certificates successfully.

从证书发布服务器上获取本地证书。

```
<Sysname> system-view
```

```
[Sysname] pki retrieve-certificate domain aaa local
```

Retrieved the certificates successfully.

从证书发布服务器上获取对端证书。

```
<Sysname> system-view
```

```
[Sysname] pki retrieve-certificate domain aaa peer en1
```

Retrieved the certificates successfully.

【相关命令】

- **display pki certificate**
- **pki delete-certificate**

1.1.35 pki retrieve-crl

pki retrieve-crl 命令用来获取 CRL 并下载至本地。

【命令】

```
pki retrieve-crl domain domain-name
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain-name: 指定 CRL 所属的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

【使用指导】

获取 CRL 的目的是为了验证 PKI 域中的本地证书和对端证书的合法性。若要成功获取 CRL，PKI 域中必须存在 CA 证书。

设备支持通过 HTTP、LDAP 或 SCEP 协议从 CRL 发布点上获取 CRL，具体采用那种协议，由 PKI 域中 CRL 发布点的配置决定：

- 若配置的 CRL 发布点 URL 格式为 HTTP 格式，则通过 HTTP 协议获取 CRL。
- 若配置的 CRL 发布点 URL 格式为 LDAP 格式，则通过 LDAP 协议获取 CRL。若配置的 CRL 发布点 URL（通过命令 **crl url**）中缺少主机名，例如 `ldap:///CN=8088,OU=test,U=rd,C=cn`，则还需要在 PKI 域中配置 LDAP 服务器的 URL（通过命令 **ldap server**）。此时，设备会将配置的 LDAP 服务器 URL 和配置的 CRL 发布点 URL 中的不完整的 LDAP 发布点拼装成完整的 LDAP 发布点，再通过 LDAP 协议获取 CRL。
- 若 PKI 域中没有配置 CRL 发布点，则设备会依次从本地证书、CA 证书中查找 CRL 的发布点，如果从中查找到了 CRL 发布点，则通过该发布点获取 CRL；否则，通过 SCEP 协议获取 CRL。

【举例】

```
# 从 CRL 发布点上获取 CRL。
<Sysname> system-view
[Sysname] pki retrieve-crl domain aaa
Retrieve CRL of the domain aaa successfully.
```

【相关命令】

- **crl url**
- **ldap server**

1.1.36 pki storage

pki storage 命令用来配置证书和 CRL 的存储路径。

undo pki storage 命令用来恢复缺省情况。

【命令】

```
pki storage { certificates | crls } dir-path
undo pki storage { certificates | crls }
```

【缺省情况】

证书和 CRL 的存储路径为设备存储介质上的 PKI 目录。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

certificates：指定证书的存储目录。

crls：指定 CRL 的存储目录。

dir-path：存储目录的路径名称，区分大小写，不能以 ‘/’ 开头，不能包含 “..”。**dir-path** 可以是绝对路径也可以是相对路径，但必须已经存在。

【使用指导】

dir-path 只能是当前主用设备上的路径，不能是其它从设备上的路径。

设备缺省的 PKI 目录在设备首次成功申请、获取或导入证书时自动创建。

如果需要指定的目录还不存在，需要先使用 **mkdir** 命令创建这个目录，再使用此命令配存储路径。

若修改了证书或 CRL 的存储目录，则原存储路径下的证书文件（以 .cer 和 .p12 为后缀的文件）和 CRL 文件（以 .crl 为后缀的文件）将被移动到该路径下保存，且原存储路径下的其它文件不受影响。

【举例】

设置证书的存储路径为 flash:/pki-new。

```
<Sysname> system-view
```

```
[Sysname] pki storage certificates flash:/pki-new
```

设置 CRL 存储路径为 pki-new。

```
<Sysname> system-view
```

```
[Sysname] pki storage crls pki-new
```

1.1.37 pki validate-certificate

pki validate-certificate 命令用来验证证书的有效性。

【命令】

```
pki validate-certificate domain domain-name { ca | local }
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*: 指定证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

ca: 表示验证 CA 证书。

local: 表示验证本地证书。

【使用指导】

证书验证的内容包括：证书是否由用户信任的 CA 签发；证书是否仍在有效期内；如果使能了 CRL 检查功能，还会验证证书是否被吊销。如果验证证书的时候，PKI 域中没有 CRL，则会先从本地证书库中查找是否存在 CRL，如果找到 CRL，则把证书库中保存的 CRL 加载到该 PKI 域中，否则，就从 CA 服务器上获取并保存到本地。

导入证书、申请证书、获取证书以及应用程序使用 PKI 功能时，都会自动对证书进行验证，因此一般不需要使用此命令进行额外的验证。如果用户希望在没有任何前述操作的情况下单独执行证书的验证，可以使用此命令。

验证 CA 证书时，会对从当前 CA 到根 CA 的整条 CA 证书链进行 CRL 检查。

【举例】

验证 PKI 域 aaa 中的 CA 证书的有效性。

```
<Sysname> system-view
```

```
[Sysname] pki validate-certificate domain aaa ca
```

```
Verifying certificates.....
```

```
Serial Number:
```

```
f6:3c:15:31:fe:bb:ec:94:dc:3d:b9:3a:d9:07:70:e5
```

```
Issuer:
```

```
C=cn
```

```
O=ccc
```

```
OU=ppp
```

```
CN=rootca
```

```
Subject:
```

```
C=cn
```

```
O=abc
```

```
OU=test
```

```
CN=aca
```

```
Verify result: OK
```

```
Verifying certificates.....
```

```
Serial Number:
```

```
5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
```

```
Issuer:
```

```
C=cn
```

```
O=ccc
```

```
OU=ppp
```

```
CN=rootca
```

```
Subject:
```

```
C=cn
```

```
O=ccc
```

```
OU=ppp
```

```
CN=rootca
```

```
Verify result: OK
```

验证 PKI 域 aaa 中的本地证书的有效性。

```
<Sysname> system-view
```

```
[Sysname] pki validate-certificate domain aaa local
```

```
Verifying certificates.....
```

```
Serial Number:
```

```
bc:05:70:1f:0e:da:0d:10:16:1e
```

```
Issuer:
```

```
C=CN
```

```
O=sec
```

```
OU=software
```

```
CN=bca
```

```
Subject:
```

```
O=OpenCA Labs
```



```
OU=Users
CN=fips fips-sec
```

Verify result: OK

【相关命令】

- **crl check**
- **pki domain**

1.1.38 public-key dsa

public-key dsa 命令用来指定证书申请使用的 DSA 密钥对。

undo public-key 命令用来恢复缺省情况。

【命令】

```
public-key dsa name key-name [length key-length ]
undo public-key
```

【缺省情况】

未指定证书申请使用的密钥对。

【视图】

PKI 域视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

name *key-name*: 密钥对的名称，为 1~64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

length *key-length*: 密钥的长度。*key-length* 的取值范围为 512~2048，单位为比特，缺省值为 1024。密钥越长，密钥安全性越高，但相关的公钥运算越耗时。

【使用指导】

本命令中引用的密钥对并不要求已经存在，可以通过以下任意一种途径获得：

- 通过执行 **public-key local create** 命令生成。
- 通过应用程序认证过程触发生成。例如 IKE 协商过程中，如果使用数字签名认证方式，则可能会触发生成密钥对。
- 通过导入证书（使用 **pki import** 命令）的方式从外界获得。

一个 PKI 域中只能同时存在一种算法（RSA、DSA、ECDSA）的密钥对。对于 RSA 密钥对来说，一个 PKI 域中只允许单独存在一种用途的密钥对，或同时存在一个用于签名的和一个用于加密的密钥对。因此，在一个 PKI 域中，除 RSA 密钥对的签名密钥对和加密密钥对配置不会互相覆盖之外，其它类型的新的密钥对配置均会覆盖已有的密钥对配置。

本命令中指定的密钥长度仅对将要由设备生成的密钥对有效。如果执行本命令时，设备上已经存在指定名称的密钥对，则后续通过此命令指定的该密钥对的密钥长度没有意义。如果指定名称的密钥对是通过导入证书的方式获得，则通过本命令指定的密钥长度也没有意义。

【举例】

```
# 指定证书申请所使用的 DSA 密钥对为 abc，密钥的长度为 2048 比特。
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key dsa name abc length 2048
```

【相关命令】

- **pki import**
- **public-key local create**（安全命令参考/公钥管理）

1.1.39 public-key ecdsa

public-key ecdsa 命令用来指定证书申请使用的 ECDSA 密钥对。

undo public-key 命令用来恢复缺省情况。

【命令】

```
public-key ecdsa name key-name [ secp192r1 | secp256r1 | secp384r1 | secp521r1 ]
undo public-key
```

【缺省情况】

未指定证书申请使用的密钥对。

【视图】

PKI 域视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

name key-name：密钥对的名称，为 1~64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

secp192r1：密钥对使用的椭圆曲线算法的名称为 secp192r1，密钥长度为 192 比特。

secp256r1：密钥对使用的椭圆曲线算法的名称为 secp256r1，密钥长度为 256 比特。

secp384r1：密钥对使用的椭圆曲线算法的名称为 secp384r1，密钥长度为 384 比特。

secp521r1：密钥对使用的椭圆曲线算法的名称为 secp521r1，密钥长度为 521 比特。

【使用指导】

本命令中引用的密钥对并不要求已经存在，可以通过以下任意一种途径获得：

- 通过执行 **public-key local create** 命令生成。

- 通过应用程序认证过程触发生成。例如 IKE 协商过程中，如果使用数字签名认证方式，则可能会触发生成密钥对。
- 通过导入证书（使用 **pki import** 命令）的方式从外界获得。

若未指定任何参数，则缺省使用密钥对 **secp192r1**。

一个 PKI 域中只能同时存在一种算法（RSA、DSA、ECDSA）的密钥对。对于 RSA 密钥对来说，一个 PKI 域中只允许单独存在一种用途的密钥对，或同时存在一个用于签名的和一个用于加密的密钥对。因此，在一个 PKI 域中，除 RSA 密钥对的签名密钥对和加密密钥对配置不会互相覆盖之外，其它类型的新的密钥对配置均会覆盖已有的密钥对配置。

本命令中指定的密钥长度仅对将要由设备生成的密钥对有效。如果执行本命令时，设备上已经存在指定名称的密钥对，则后续通过此命令指定的该密钥对的密钥长度没有意义。如果指定名称的密钥对是通过导入证书的方式获得，则通过本命令指定的密钥长度也没有意义。

【举例】

指定证书申请所使用的 ECDSA 密钥对为 abc，椭圆曲线算法的名称为 secp384r1。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key ecdsa name abc secp384r1
```

【相关命令】

- **pki import**
- **public-key local create**（安全命令参考/公钥管理）

1.1.40 public-key rsa

public-key rsa 命令用来指定证书申请使用的 RSA 密钥对。

undo public-key 命令用来恢复缺省情况。

【命令】

```
public-key rsa { { encryption name encryption-key-name [ length key-length ]
| signature name signature-key-name [ length key-length ] } * | general name
key-name [ length key-length ] }
undo public-key
```

【缺省情况】

未指定证书申请使用的密钥对。

【视图】

PKI 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

encryption: 指定密钥对的用途为加密。

name encryption-key-name: 加密密钥对的名称，为 1~64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

signature: 指定密钥对的用途为签名。

name signature-key-name: 签名密钥对的名称，为 1~64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

general: 指定密钥对的用途为通用，既可以用于签名也可以用于加密。

name key-name: 通用密钥对的名称，为 1~64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

length key-length: 密钥的长度。**key-length** 的取值范围为 512~2048，单位为比特，缺省为 1024。密钥越长，密钥安全性越高，但相关的公钥运算越耗时。

【使用指导】

本命令中引用的密钥对并不要求已经存在，可以通过以下任意一种途径获得：

- 通过执行 **public-key local create** 命令生成。
- 通过应用程序认证过程触发生成。例如 IKE 协商过程中，如果使用数字签名认证方式，则可能会触发生成密钥对。
- 通过导入证书（使用 **pki import** 命令）的方式从外界获得。

一个 PKI 域中只能同时存在一种算法（RSA、DSA、ECDSA）的密钥对。对于 RSA 密钥对来说，一个 PKI 域中只允许单独存在一种用途的密钥对，或同时存在一个用于签名的和一个用于加密的密钥对。因此，在一个 PKI 域中，除 RSA 密钥对的签名密钥对和加密密钥对配置不会互相覆盖之外，其它类型的新的密钥对配置均会覆盖已有的密钥对配置。

分别指定 RSA 签名密钥对和 RSA 加密密钥对时，它们的密钥长度可以不相同。

本命令中指定的密钥长度仅对将要由设备生成的密钥对有效。如果执行本命令时，设备上已经存在指定名称的密钥对，则后续通过此命令指定的该密钥对的密钥长度没有意义。如果指定名称的密钥对是通过导入证书的方式获得，则通过本命令指定的密钥长度也没有意义。

【举例】

指定证书申请所使用的 RSA 密钥对为 abc，密钥用途为通用，密钥的长度为 2048 比特。

```
<Sysname> system-view
```

```
[Sysname] pki domain aaa
```

```
[Sysname-pki-domain-aaa] public-key rsa general name abc length 2048
```

指定证书申请所使用的加密 RSA 密钥对为 rsa1（密钥的长度为 2048 比特），签名 RSA 密钥对为 sig1（密钥的长度为 2048 比特）。

```
<Sysname> system-view
```

```
[Sysname] pki domain aaa
```

```
[Sysname-pki-domain-aaa] public-key rsa encryption name rsa1 length 2048
```

```
[Sysname-pki-domain-aaa] public-key rsa signature name sig1 length 2048
```

【相关命令】

- **pki import**
- **public-key local create**（安全命令参考/公钥管理）

1.1.41 revocation-check method

revocation-check method 命令用来指定证书吊销情况检查的方法。

undo revocation-check method 命令用来恢复缺省情况。

【命令】

revocation-check method *method1* [*method2*]

undo revocation-check method

【缺省情况】

使用 CRL 方法检查证书吊销情况。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

context-admin

【参数】

method1 [*method2*]：指定证书吊销情况检查的方法。*method* 取值为：

- **crl**：指定证书吊销时进行 CRL 检查。
- **none**：忽略证书吊销检查。

如果 *method1* 指定为 **none**，则 *method2* 不能再指定 **crl**。

【使用指导】

指定了 **crl** 方法，必须保证 CRL 检查功能处于开启状态（通过 **crl check enable** 命令配置）。

如果 CRL 检查功能处于关闭状态，则不进行 CRL 检查，认为所有证书可信。

指定了 **none** 方法，则忽略检查认为所有证书可信，**crl check enable** 命令不生效。

如果同时指定了 **crl** 和 **none** 方法，则先进行 CRL 检查，检查证书是否可信；如果从 CRL 发布点所在的服务器上获取不到 CRL，则使用 **none** 方式，忽略检查认为所有证书可信。

【举例】

配置使用 CRL 方式检查证书吊销情况。

```
<Sysname> system
```

```
[Sysname] pki domain abc
```

```
[Sysname-pki-domain-abc] revocation-check method crl
```

【相关命令】

- **crl check enable**

1.1.42 root-certificate fingerprint

root-certificate fingerprint 命令用来配置验证 CA 根证书时所使用的指纹。

undo root-certificate fingerprint 命令用来恢复缺省情况。

【命令】

```
root-certificate fingerprint { md5 | sha1 } string
undo root-certificate fingerprint
```

【缺省情况】

未指定验证 CA 根证书时使用的指纹。

【视图】

PKI 域视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

md5：使用 MD5 指纹。

sha1：使用 SHA1 指纹。

string：指定所使用的指纹信息。当选择 MD5 指纹时，*string* 必须为 32 个字符的字符串，并且以 16 进制的形式输入；当选择 SHA1 指纹时，*string* 必须为 40 个字符的字符串，并且以 16 进制的形式输入。

【使用指导】

当本地证书申请模式为自动方式且 PKI 域中没有 CA 证书时，必须通过本命令配置验证 CA 证书时所使用的指纹。当 IKE 协商等应用触发设备进行本地证书申请时，设备会自动从 CA 服务器上获取 CA 证书，如果获取的 CA 证书中包含了本地不存在的 CA 根证书，则设备会验证该 CA 根证书的指纹。此时，如果设备上没有配置 CA 根证书指纹或者配置了错误的 CA 根证书指纹，则本地证书申请失败。

通过 **pki import** 命令导入 CA 证书或者通过 **pki retrieve-certificate** 命令获取 CA 证书时，可以选择是否配置验证 CA 根证书使用的指纹：如果 PKI 域中配置了验证 CA 根证书使用的指纹，则当导入的 CA 证书文件或者获取的 CA 证书中包含本地不存在的 CA 根证书时，直接使用配置的 CA 根证书指纹进行验证。如果配置了错误的 CA 根证书指纹，则 CA 证书导入和 CA 证书获取均会失败；否则，需要用户来确认该 CA 证书的 CA 根证书指纹是否可信。

【举例】

配置验证 CA 根证书时使用的 MD5 指纹。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint md5 12EF53FA355CD23E12EF53FA355CD23E
```

配置验证 CA 根证书时使用的 SHA1 指纹。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDAD93
```

【相关命令】

- **certificate request mode**

- **pki import**
- **pki retrieve-certificate**

1.1.43 rule

rule 命令用来配置证书属性的访问控制规则。

undo rule 命令用来删除指定的证书属性访问控制规则。

【命令】

```
rule [ id ] { deny | permit } group-name
undo rule id
```

【缺省情况】

不存在证书属性的访问控制规则。

【视图】

证书访问控制策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

id: 证书属性访问控制规则编号，取值范围为 1~16，缺省值为当前还未被使用的且合法的最小编号，取值越小优先级越高。

deny: 当证书的属性与所关联的属性组匹配时，认为该证书无效，未通过访问控制策略的检测。

permit: 当证书的属性与所关联的属性组匹配时，认为该证书有效，通过了访问控制策略的检测。

group-name: 规则所关联的证书属性组名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

配置证书属性访问控制规则时，可以关联一个当前并不存在的证书属性组，后续可以通过命令 **pki certificate attribute-group** 完成相应的配置。

若规则所关联的证书属性组中没有定义任何属性规则（通过命令 **attribute** 配置），或关联的证书属性组不存在，则认为被检测的证书属性与该属性组匹配。

如果一个访问控制策略中有多个规则，则按照规则编号从小到大的顺序遍历所有规则，一旦证书与某一个规则匹配，则立即结束检测，不再继续匹配其它规则；若遍历完所有规则后，证书没有与任何规则匹配，则认为该证书不能通过访问控制策略的检测。

【举例】

配置一个访问控制规则，要求当证书与证书属性组 **mygroup** 匹配时，认为该证书有效，通过了访问控制策略的检测。

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

【相关命令】

- **attribute**
- **display pki certificate access-control-policy**
- **pki certificate attribute-group**

1.1.44 source

source 命令用来指定 PKI 操作产生的协议报文使用的源 IP 地址。

undo source 命令用来恢复缺省情况。

【命令】

```
source { ip | ipv6 } { ip-address | interface interface-type  
interface-number }  
undo source
```

【缺省情况】

PKI 操作产生的协议报文的源 IP 地址为系统根据路由表项查找到的出接口的地址。

【视图】

PKI 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip *ip-address*: 指定源 IPv4 地址。

ipv6 *ip-address*: 指定源 IPv6 地址。

interface *interface-type interface-number*: 指定该接口的主 IPv4 地址或接口上最小的 IPv6 地址为源 IP 地址。*interface-type interface-number* 表示接口类型和接口编号。

【使用指导】

如果希望 PKI 操作产生的协议报文的源 IP 地址是一个特定的地址，则需要配置此命令，例如 CA 服务器上的策略要求仅接受来自指定地址或网段的证书申请。如果该 IP 地址是动态获取的，则可以指定一个接口，使用该接口上的 IP 地址作为源地址。

此处指定的源 IP 地址，必须与 CA 服务器之间路由可达。

一个 PKI 域中只能存在一个源 IP 地址，后配置的生效。

【举例】

指定 PKI 操作产生的协议报文的源 IP 地址为 111.1.1.8。

```
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] source ip 111.1.1.8
```

指定 PKI 操作产生的协议报文的源 IPv6 地址为 1::8。

```
<Sysname> system-view  
[Sysname] pki domain 1
```



```

[Sysname-pki-domain-1] source ipv6 1::8
# 指定 PKI 操作产生的协议报文的源 IP 地址为接口 GigabitEthernet1/0/1 的 IP 地址。
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip interface gigabitethernet 1/0/1
# 指定 PKI 操作产生的协议报文的源 IPv6 地址为接口 GigabitEthernet1/0/1 的 IPv6 地址。
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 interface gigabitethernet 1/0/1

```

1.1.45 state

state 命令用来配置 PKI 实体所属的州或省的名称。

undo state 命令用来恢复缺省情况。

【命令】

```

state state-name
undo state

```

【缺省情况】

未配置 PKI 实体所属的州或省的名称。

【视图】

PKI 实体视图

【缺省用户角色】

```

network-admin
context-admin

```

【参数】

state-name: PKI 实体所属的州或省的名称，为 1~63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

```

# 配置 PKI 实体 en 所在省为 countryA。
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] state countryA

```

1.1.46 subject-dn

subject-dn 命令用来配置 PKI 实体的识别名，包括通用名、国家代码、地理区域名称、组织名称、组织部门名称和省份名称参数。

undo subject-dn 命令用来恢复缺省情况。

【命令】

```

subject-dn dn-string
undo subject-dn

```

【缺省情况】

未配置 PKI 实体的识别名。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

context-admin

【参数】

dn-string: PKI 实体的识别名，长度为 1~255 个字符的字符串，不区分大小写。

【使用指导】

PKI 实体识别名的参数格式为：参数=参数值，多个参数之间以逗号分隔，且可以对同一个参数多次赋值。例如 CN=aaa，CN=bbb，C=cn。PKI 实体识别名支持的参数包括：

- CN：通用名
- C：所属国家代码
- L：所在地理区域名称
- O：所属组织名称
- OU：所属组织部门名称
- ST：所属州省

本命令配置的识别名优先级高于通过 **common-name**、**country**、**locality**、**organization**、**organization-unit** 和 **state** 命令单独配置的识别名。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 PKI 实体 en 的通用名为 test，所属的国家代码为 CN，所属的组织名称为 abc，所属组织部门的名称为 rdtest，所属组织部门的名称为 rstest，所在省为 countryA，所在地理区域的名称为 pukras。

```
<Sysname> system-view
```

```
[Sysname] pki entity en
```

```
[Sysname-pki-entity-en] subject-dn
```

```
CN=test,C=CN,O=abc,OU=rdtest,OU=rstest,ST=countryA,L=pukras
```

【相关命令】

- **common-name**
- **country**
- **locality**
- **organization**
- **organization-unit**
- **state**

1.1.47 usage

usage 命令用来指定证书的扩展用途。

undo usage 命令用来删除指定证书的扩展用途。

【命令】

```
usage { ike | ssl-client | ssl-server } *  
undo usage [ ike | ssl-client | ssl-server ] *
```

【缺省情况】

未指定证书的扩展用途，表示可用于 IKE、SSL 客户端和 SSL 服务器端用途。

【视图】

PKI 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

ike: 指定证书扩展用途为 IKE，即 IKE 对等体使用的证书。

ssl-client: 指定证书扩展用途为 SSL 客户端，即 SSL 客户端使用的证书。

ssl-server: 指定证书扩展用途为 SSL 服务器端，即 SSL 服务器端使用的证书。

【使用指导】

若不指定任何参数，则 **undo usage** 命令表示删除所有指定的证书扩展用途，证书的用途由证书的使用者决定，PKI 不做任何限定。

证书中携带的扩展用途与 CA 服务器的策略相关，申请到的证书中的扩展用途可能与此处指定的不完全一致，最终请以 CA 服务器的实际情况为准。

【举例】

```
# 指定证书扩展用途为 SSL 客户端。  
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] usage ssl-client
```

1.1.48 vpn-instance

vpn-instance 指定注册受理机构服务器和 CRL 发布点所属的 VPN 实例。

undo vpn-instance 命令用来恢复缺省情况。

【命令】

```
vpn-instance vpn-instance-name  
undo vpn-instance
```

【缺省情况】

注册受理机构服务器和 CRL 发布点属于公网。

【视图】

PKI 域视图

【缺省用户角色】

network-admin
context-admin

【参数】

vpn-instance-name: 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

【举例】

指定注册受理机构服务器和 CRL 发布点所属的 VPN 实例名称为 vpn1。

```
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] vpn-instance vpn1
```

目 录

1 SSH.....	1-1
1.1 SSH服务器端配置命令	1-1
1.1.1 display ssh server	1-1
1.1.2 display ssh user-information	1-3
1.1.3 scp server enable	1-4
1.1.4 sftp server enable	1-4
1.1.5 sftp server idle-timeout	1-5
1.1.6 ssh server acl	1-5
1.1.7 ssh server acl-deny-log enable	1-6
1.1.8 ssh server authentication-retries	1-7
1.1.9 ssh server authentication-timeout	1-8
1.1.10 ssh server compatible-ssh1x enable	1-9
1.1.11 ssh server dscp	1-9
1.1.12 ssh server enable	1-10
1.1.13 ssh server ipv6 acl	1-11
1.1.14 ssh server ipv6 dscp	1-12
1.1.15 ssh server pki-domain	1-12
1.1.16 ssh server port	1-13
1.1.17 ssh server rekey-interval	1-14
1.1.18 ssh user	1-14
1.2 SSH客户端配置命令	1-17
1.2.1 bye	1-17
1.2.2 cd	1-17
1.2.3 cdup	1-18
1.2.4 delete	1-18
1.2.5 dir	1-19
1.2.6 display sftp client source	1-20
1.2.7 display ssh client source	1-20
1.2.8 exit	1-21
1.2.9 get	1-21
1.2.10 help	1-22
1.2.11 ls	1-23
1.2.12 mkdir	1-24

1.2.13 put	1-24
1.2.14 pwd	1-25
1.2.15 quit	1-25
1.2.16 remove	1-25
1.2.17 rename	1-26
1.2.18 rmdir	1-26
1.2.19 scp	1-27
1.2.20 scp ipv6	1-30
1.2.21 scp ipv6 suite-b	1-32
1.2.22 scp suite-b	1-35
1.2.23 sftp	1-36
1.2.24 sftp client ipv6 source	1-39
1.2.25 sftp client source	1-40
1.2.26 sftp ipv6	1-41
1.2.27 sftp ipv6 suite-b	1-44
1.2.28 sftp suite-b	1-46
1.2.29 ssh client ipv6 source	1-48
1.2.30 ssh client source	1-49
1.2.31 ssh2	1-49
1.2.32 ssh2 ipv6	1-52
1.2.33 ssh2 ipv6 suite-b	1-55
1.2.34 ssh2 suite-b	1-58
1.3 SSH2 协议配置命令	1-60
1.3.1 display ssh2 algorithm	1-60
1.3.2 ssh2 algorithm cipher	1-61
1.3.3 ssh2 algorithm key-exchange	1-62
1.3.4 ssh2 algorithm mac	1-63
1.3.5 ssh2 algorithm public-key	1-64

1 SSH

1.1 SSH服务器端配置命令

1.1.1 display ssh server

display ssh server 命令用来在 SSH 服务器端显示该服务器的状态信息或会话信息。

【命令】

display ssh server { session [slot slot-number] | status }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

session: 显示 SSH 服务器的会话信息。

status: 显示 SSH 服务器的状态信息。

slot slot-number: 显示指定成员设备上的 SSH 服务器的会话信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的 SSH 服务器的会话信息。

【举例】

在 SSH 服务器端显示该服务器的状态信息。

```
<Sysname> display ssh server status
Stelnet server: Disable
SSH version : 2.0
SSH authentication-timeout : 60 second(s)
SSH server key generating interval : 0 hour(s)
SSH authentication retries : 3 time(s)
SFTP server: Disable
SFTP server Idle-Timeout: 10 minute(s)
NETCONF server: Disable
SCP server: Disable
SSH Server PKI domain name: aaa
```

表1-1 display ssh server status 命令显示信息描述表

字段	描述
Stelnet server	Stelnet服务器功能的状态

字段	描述
SSH version	SSH协议版本 SSH服务器兼容SSH1时，协议版本为1.99；SSH服务器不兼容SSH1时，协议版本为2.0
SSH authentication-timeout	认证超时时间
SSH server key generating interval	RSA服务器密钥对的最小更新间隔时间
SSH authentication retries	SSH用户认证尝试的最大次数
SFTP server	SFTP服务器功能的状态
SFTP server Idle-Timeout	SFTP用户连接的空闲超时时间
NETCONF server	NETCONF over SSH服务器功能的状态
SCP server	SCP服务器功能的状态
SSH Server PKI domain name	SSH服务器PKI域配置

在 SSH 服务器端显示该服务器的会话信息。

```
<Sysname> display ssh server session
```

```
UserPid  SessID Ver  Encrypt  State          Retries  Serv  Username  Idx
184      0      2.0  aes128-cbc Established    1      Stelnet abc@123
```

表1-2 display ssh server session 显示信息描述表

字段	描述
UserPid	用户进程PID
SessID	会话ID
Ver	SSH服务器的协议版本
Encrypt	SSH服务器本端使用的加密算法
State	会话状态，包括： • Init：初始化状态 • Ver-exchange：版本协商 • Keys-exchange：密钥交换 • Auth-request：用户认证 • Serv-request：服务请求 • Established：会话已经建立 • Disconnected：断开会话
Retries	认证失败的次数
Serv	服务类型，包括SCP、SFTP、Stelnet和NETCONF
Username	客户端登录服务器时采用的用户名
Idx	客户端登录服务器时采用的用户线的绝对编号，当未进行重定向连接时，显示为空

1.1.2 display ssh user-information

display ssh user-information 命令用来在 SSH 服务器端显示 SSH 用户的信息。

【命令】

display ssh user-information [*username*]

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

username: SSH 用户名，为 1~80 个字符的字符串，区分大小写。如果没有指定本参数，则显示所有 SSH 用户的信息。

【使用指导】

本命令仅用来显示 SSH 服务器端通过 **ssh user** 命令配置的 SSH 用户信息。

【举例】

显示所有 SSH 用户的信息。

```
<Sysname> display ssh user-information
Total ssh users:2
Username           Authentication-type  User-public-key-name  Service-type
yemx                password              Stelnet|SFTP
test                publickey              pubkey                SFTP
```

表1-3 display ssh user-information 显示信息描述表

字段	描述
Total ssh users	SSH用户的总数
Username	用户名
Authentication-type	认证类型，取值包括password、publickey、password-publickey和any
User-public-key-name	用户公钥名称 如果认证类型为password，则该字段显示为空
Service-type	服务类型，取值包括SCP、SFTP、Stelnet和NETCONF 如果设备同时显示多个SSH服务类型时用 隔开

【相关命令】

- ssh user

1.1.3 scp server enable

scp server enable 命令用来开启 SCP 服务器功能。

undo scp server enable 命令用来关闭 SCP 服务器功能。

【命令】

```
scp server enable
undo scp server enable
```

【缺省情况】

SCP 服务器功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 开启 SCP 服务器功能。
<Sysname> system-view
[Sysname] scp server enable
```

【相关命令】

- **display ssh server**

1.1.4 sftp server enable

sftp server enable 命令用来开启 SFTP 服务器功能。

undo sftp server enable 命令用来关闭 SFTP 服务器功能。

【命令】

```
sftp server enable
undo sftp server enable
```

【缺省情况】

SFTP 服务器功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 开启 SFTP 服务器功能。
<Sysname> system-view
```

```
[Sysname] sftp server enable
```

【相关命令】

- **display ssh server**

1.1.5 sftp server idle-timeout

sftp server idle-timeout 命令用来在 SFTP 服务器端设置 SFTP 用户连接的空闲超时时间。

undo sftp server idle-timeout 命令用来恢复缺省情况。

【命令】

```
sftp server idle-timeout time-out-value
```

```
undo sftp server idle-timeout
```

【缺省情况】

SFTP 用户连接的空闲超时时间为 10 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

time-out-value: 超时时间，取值范围为 1~35791，单位为分钟。

【使用指导】

当 SFTP 用户连接的空闲时间超过设定的阈值后，系统会自动断开此用户的连接，从而有效避免用户长期占用连接而不进行任何操作。若同一时间内并发的 SFTP 连接数较多，可适当减小该值，及时释放系统资源给新用户接入。

【举例】

设置 SFTP 用户连接的空闲超时时间为 500 分钟。

```
<Sysname> system-view
```

```
[Sysname] sftp server idle-timeout 500
```

【相关命令】

- **display ssh server**

1.1.6 ssh server acl

ssh server acl 命令用来设置对 IPv4 SSH 客户端的访问控制。

undo ssh server acl 命令用来恢复缺省情况。

【命令】

```
ssh server acl { advanced-acl-number | basic-acl-number | mac  
mac-acl-number }
```

```
undo ssh server acl
```

【缺省情况】

允许所有 IPv4 SSH 客户端向设备发起 SSH 访问。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

advanced-acl-number: 指定 IPv4 高级 ACL，取值范围为 3000～3999。

basic-acl-number: 指定 IPv4 基本 ACL，取值范围为 2000～2999。

mac acl-number: 指定二层 ACL。**acl-number** 是二层 ACL 的编号，取值范围为 4000～4999。

【使用指导】

对 IPv4 SSH 客户端的访问控制通过引用 ACL 来实现，具体情况如下：

- 当引用的 ACL 不存在或者引用的 ACL 为空时，不允许 IPv4 SSH 客户端访问设备。
- 当引用的 ACL 非空时，则只有匹配 ACL 中 **permit** 规则的 IPv4 SSH 客户端可以访问设备，其他客户端不可以访问设备。

该配置生效后，只会过滤新建立的 SSH 连接，不会影响已建立的 SSH 连接。

对于 IPv4 SSH 客户端，本命令不能设置对 NETCONF over SSH 客户端的访问控制。如果用户需要设置对 NETCONF over SSH 客户端的访问控制，请使用 **netconf ssh acl** 命令设置访问控制。

有关 **netconf ssh acl** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“NETCONF”。

多次执行本命令，最后一次执行的命令生效。

【举例】

只允许 IPv4 地址为 1.1.1.1 的 SSH 客户端向设备发起 SSH 访问。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ssh server acl 2001
```

【相关命令】

- **display ssh server**

1.1.7 ssh server acl-deny-log enable

ssh server acl-deny-log enable 命令用来开启匹配 ACL deny 规则后打印日志信息功能。

undo ssh server acl-deny-log enable 命令用来关闭匹配 ACL deny 规则后打印日志信息功能。

【命令】

ssh server acl-deny-log enable

undo ssh server acl-deny-log enable

【缺省情况】

匹配 ACL deny 规则后打印日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

通过配置 **ssh server acl** 和 **ssh server ipv6 acl** 命令，可限制 SSH 客户端对设备的访问。此时，通过配置 **ssh server acl-deny-log enable** 命令，设备可以记录匹配 deny 规则的 IP 用户的登录日志，用户可以查看非法登录的地址信息。

执行本配置后，SSH 客户端匹配 ACL deny 规则时，将产生日志信息。生成的日志信息将被发送到设备的信息中心，通过设置信息中心的参数，决定日志信息的输出规则（即是否允许输出以及输出方向）。

【举例】

开启匹配 ACL deny 规则后打印日志信息功能。

```
<Sysname> system-view
```

```
[Sysname] ssh server acl-deny-log enable
```

【相关命令】

- **ssh server acl**
- **ssh server ipv6 acl**

1.1.8 ssh server authentication-retries

ssh server authentication-retries 命令用来设置允许 SSH 用户认证尝试的最大次数。

undo ssh server authentication-retries 命令用来恢复缺省情况。

【命令】

```
ssh server authentication-retries retries
```

```
undo ssh server authentication-retries
```

【缺省情况】

允许 SSH 用户认证尝试的最大次数为 3 次。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

retries: 指定每个 SSH 用户认证尝试的最大次数，取值范围为 1~5。

【使用指导】

通过本命令可以限制用户尝试登录的次数，防止非法用户对用户名和密码进行恶意地猜测和破解。如果用户的认证次数超过了最大认证次数，还未认证成功，则不再允许认证。不同认证方式的认证次数统计方式有所不同，具体统计方式请参考如下：

- 在 any 认证方式下，认证次数是指 SSH 客户端通过 **publickey** 和 **password** 两种方式进行认证尝试的次数总和。
- 对于 **password-publickey** 认证方式，设备首先对 SSH 用户进行 **publickey** 认证，然后进行 **password** 认证，这个过程为一次认证尝试，而不是两次认证尝试。

该配置不会影响已经登录的 SSH 用户，仅对新登录的 SSH 用户生效。

【举例】

```
# 指定允许 SSH 用户认证尝试的最大次数为 4。  
<Sysname> system-view  
[Sysname] ssh server authentication-retries 4
```

【相关命令】

- **display ssh server**

1.1.9 ssh server authentication-timeout

ssh server authentication-timeout 命令用来在 SSH 服务器端设置 SSH 用户的认证超时时间。

undo ssh server authentication-timeout 命令用来恢复缺省情况。

【命令】

```
ssh server authentication-timeout time-out-value  
undo ssh server authentication-timeout
```

【缺省情况】

SSH 用户的认证超时时间为 60 秒。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

time-out-value: 认证超时时间，取值范围为 1~120，单位为秒。

【使用指导】

如果 SSH 用户在设置的认证超时时间内没有完成认证，SSH 服务器就拒绝该用户的连接。

为了防止不法用户建立起 TCP 连接后，不进行接下来的认证，而占用系统资源，妨碍其它合法用户的正常登录，可以适当调小 SSH 用户认证超时时间。

【举例】

```
# 设置 SSH 用户认证超时时间为 10 秒。
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

【相关命令】

- **display ssh server**

1.1.10 ssh server compatible-ssh1x enable

ssh server compatible-ssh1x enable 命令用来设置 SSH 服务器兼容 SSH1 版本的客户端。
undo ssh server compatible-ssh1x [enable] 命令用来恢复缺省情况。

【命令】

```
ssh server compatible-ssh1x enable
undo ssh server compatible-ssh1x [ enable ]
```

【缺省情况】

SSH 服务器不兼容 SSH1 版本的客户端。

【视图】

系统视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【使用指导】

该配置不会影响已经登录的 SSH 用户，仅对新登录的 SSH 用户生效。
执行 **undo** 命令时，指定 **enable** 和不指定 **enable** 均表示恢复缺省情况。

【举例】

```
# 配置服务器兼容 SSH1 版本的客户端。
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

【相关命令】

- **display ssh server**

1.1.11 ssh server dscp

ssh server dscp 命令用来设置 IPv4 SSH 服务器向 SSH 客户端发送的报文的 DSCP 优先级。
undo ssh server dscp 命令用来恢复缺省情况。

【命令】

```
ssh server dscp dscp-value
undo ssh server dscp
```

【缺省情况】

IPv4 SSH 报文的 DSCP 优先级为 48。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

dscp-value: IPv4 SSH 报文的 DSCP 优先级，取值范围为 0~63。取值越大，优先级越高。

【使用指导】

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

```
# 配置 IPv4 SSH 服务器向 SSH 客户端发送的报文的 DSCP 优先级为 30。
<Sysname> system-view
[Sysname] ssh server dscp 30
```

1.1.12 ssh server enable

ssh server enable 命令用来开启 Stelnet 服务器功能。
undo ssh server enable 命令用来关闭 Stelnet 服务器功能。

【命令】

```
ssh server enable
undo ssh server enable
```

【缺省情况】

Stelnet 服务器功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 开启 Stelnet 服务器功能。
<Sysname> system-view
[Sysname] ssh server enable
```


【相关命令】

- **display ssh server**

1.1.13 ssh server ipv6 acl

ssh server ipv6 acl 命令用来设置对 IPv6 SSH 客户端的访问控制。

undo ssh server ipv6 acl 命令用来恢复缺省情况。

【命令】

ssh server ipv6 acl { ipv6 { *advanced-acl-number* | *basic-acl-number* } | mac *mac-acl-number* }

undo ssh server ipv6 acl

【缺省情况】

允许所有 IPv6 SSH 客户端向设备发起 SSH 访问。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6: 指定 IPv6 ACL。

advanced-acl-number: 指定 IPv6 高级 ACL，取值范围为 3000～3999。

basic-acl-number: 指定 IPv6 基本 ACL，取值范围为 2000～2999。

mac acl-number: 指定二层 ACL。***acl-number*** 是二层 ACL 的编号，取值范围为 4000～4999。

【使用指导】

对 IPv6 SSH 客户端的访问控制通过引用 ACL 来实现，具体情况如下：

- 当引用的 ACL 不存在、或者引用的 ACL 为空时，不允许 IPv6 SSH 客户端访问设备。
- 当引用的 ACL 非空时，则只有匹配 ACL 中 **permit** 规则的 IPv6 SSH 客户端可以访问设备，其他客户端不可以访问设备。

该配置生效后，只会过滤新建立的 SSH 连接，不会影响已建立的 SSH 连接。

对于 IPv6 SSH 客户端，本命令不能设置对 NETCONF over SSH 客户端的访问控制。

多次执行本命令，最后一次执行的命令生效。

【举例】

只允许 1::1/64 网段内的 SSH 客户端向设备发起 SSH 访问。

```
<Sysname> system-view
```

```
[Sysname] acl ipv6 basic 2001
```

```
[Sysname-acl-ipv6-basic-2001] rule permit source 1::1 64
```

```
[Sysname-acl-ipv6-basic-2001] quit
```

```
[Sysname] ssh server ipv6 acl ipv6 2001
```

【相关命令】

- **display ssh server**

1.1.14 ssh server ipv6 dscp

ssh server ipv6 dscp 命令用来设置 IPv6 SSH 服务器向 SSH 客户端发送的报文的 DSCP 优先级。

undo ssh server ipv6 dscp 命令用来恢复缺省情况。

【命令】

ssh server ipv6 dscp dscp-value

undo ssh server ipv6 dscp

【缺省情况】

IPv6 SSH 报文的 DSCP 优先级为 48。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value: IPv6 SSH 报文的 DSCP 优先级，取值范围为 0~63。取值越大，优先级越高。

【使用指导】

DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 IPv6 SSH 服务器向 SSH 客户端发送的报文的 DSCP 优先级为 30。

```
<Sysname> system-view
```

```
[Sysname] ssh server ipv6 dscp 30
```

1.1.15 ssh server pki-domain

ssh server pki-domain 命令用来配置服务器所属的 PKI 域。

undo ssh server pki-domain 命令用来恢复缺省情况。

【命令】

ssh server pki-domain domain-name

undo ssh server pki-domain

【缺省情况】

未配置服务器所属的 PKI 域。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain-name: 验证服务端的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

【举例】

配置 SSH 服务器所属的 PKI 域为 serverpkidomain。

```
<Sysname> system-view
```

```
[Sysname] ssh server pki-domain serverpkidomain
```

1.1.16 ssh server port

ssh server port 命令用来配置 SSH 服务的端口号。

undo ssh server port 命令用来恢复缺省情况。

【命令】

ssh server port *port-number*

undo ssh server port

【缺省情况】

SSH 服务的端口号为 22。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

port-number: SSH 服务的端口号，取值范围为 1~65535。

【使用指导】

如果修改端口号前 SSH 服务是开启的，则修改端口号后系统会自动重启 SSH 服务，正在访问的用户将被断开，用户需要重新建立 SSH 连接后才可以继续访问。

如果使用 1~1024 之间的知名端口号，有可能会導致其他服务启动失败。

【举例】

配置 SSH 服务的端口号为 1025。

```
<Sysname> system-view
```

```
[Sysname] ssh server port 1025
```

1.1.17 ssh server rekey-interval

ssh server rekey-interval 命令用来设置 RSA 服务器密钥对的最小更新间隔时间。

undo ssh server rekey-interval 命令用来恢复缺省情况。

【命令】

ssh server rekey-interval *interval*

undo ssh server rekey-interval

【缺省情况】

RSA 服务器密钥对的最小更新间隔时间为 0，表示系统不更新 RSA 服务器密钥对。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval：服务器密钥对的最小更新间隔时间，取值范围为 1~24，单位为小时。

【使用指导】

通过定时更新服务器密钥对，可以防止对密钥对的恶意猜测和破解，从而提高了 SSH 连接的安全性。

配置该命令后，从首个 SSH1 用户登录开始，SSH 服务器需要等待后续有新的 SSH1 用户登录，才会更新当前的 RSA 服务器密钥对，然后使用新的 RSA 服务器密钥对与新登录的这个 SSH1 用户进行密钥对的协商，其中等待的最小时长就为此处配置的最小更新间隔时间。之后，重复此过程，直到下一个新的 SSH1 用户登录才会再次触发 RSA 服务器密钥的更新。

本配置仅对 SSH 客户端版本为 SSH1 的用户有效。

【举例】

设置 RSA 服务器密钥对的最小更新间隔时间为 3 小时。

```
<Sysname> system-view
```

```
[Sysname] ssh server rekey-interval 3
```

【相关命令】

- **display ssh server**

1.1.18 ssh user

ssh user 命令用来创建 SSH 用户，并指定 SSH 用户的服务类型和认证方式。

undo ssh user 命令用来删除 SSH 用户。

【命令】

ssh user *username* **service-type** { *all* | *netconf* | *scp* | *sftp* | *stelnet* }
authentication-type { *password* | { *any* | *password-publickey* | *publickey* }
[**assign** { *pki-domain domain-name* | *publickey keyname* }] }

undo ssh user username

【缺省情况】

不存在 SSH 用户。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

username: SSH 用户名，为 1~80 个字符的字符串，区分大小写。用户名不能包括符号“\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和“@”，且不能为“a”、“al”、“all”。其中，“@”、“\”和“/”仅用于作为用户名的 ISP 域名分隔符，具体使用形式为：*pureusername@domain*、*pureusername/domain*、*domain\pureusername*。当创建 SCP 服务类型的用户时，用户名中请不要包含短横杠-，否则使用此用户名进行 SCP 登录会失败。

service-type: SSH 用户的服务类型。包括：

- **all:** 包括 **scp**、**sftp**、**stelnet** 和 **netconf** 四种服务类型。
- **scp:** 服务类型为 SCP（Secure Copy 的简称）。
- **sftp:** 服务类型为 SFTP（Secure FTP 的简称）。
- **stelnet:** 服务类型为 Stelnet（Secure Telnet 的简称）。
- **netconf:** 服务类型为 NETCONF。

authentication-type: SSH 用户的认证方式。包括：

- **password:** 强制指定该用户的认证方式为 **password**。该认证方式的加密机制简单，加密速度快，可结合 AAA（Authentication, Authorization, Accounting，认证、授权、计费）实现对用户认证、授权和计费，但容易受到攻击。
- **any:** 不指定用户的认证方式，用户既可以采用 **password** 认证，也可以采用 **publickey** 认证。
- **password-publickey:** 指定客户端版本为 SSH2 的用户认证方式为必须同时进行 **password** 和 **publickey** 两种认证，安全性更高；客户端版本为 SSH1 的用户认证方式为只要进行其中一种认证即可。
- **publickey:** 强制指定该用户的认证方式为 **publickey**。该认证方式的加密速度相对较慢，但认证强度高，不易受到暴力猜测密码等攻击方式的影响，而且具有较高的易用性。一次配置成功后，后续认证过程自动完成，不需要用户记忆和输入密码。

assign: 指定用于验证客户端的参数。

- **pki-domain domain-name:** 指定验证客户端证书的 PKI 域。*domain-name* 表示 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“'”和“'”。服务器端使用保存在该 PKI 域中的 CA 证书对客户端证书进行合法性检查，无需提前保存客户端的公钥，能够灵活满足大数量客户端的认证需求。

- **publickey keyname**: 指定 SSH 客户端的公钥。**keyname** 表示已经配置的客户端公钥名称，为 1~64 个字符的字符串，不区分大小写。服务器端使用提前保存在本地的用户公钥对用户进行合法性检查，如果客户端密钥文件改变，服务器端需要及时更新本地配置。

【使用指导】

SSH 用户的配置与服务器端采用的认证方式有关，具体如下：

- 如果服务器采用了 **publickey** 认证，则必须在设备上创建相应的 SSH 用户，以及同名的本地用户（用于下发授权属性：工作目录、用户角色）。
- 如果服务器采用了 **password** 认证，则必须在设备上创建相应的本地用户（适用于本地认证），或在远程服务器（如 RADIUS 服务器，适用于远程认证）上创建相应的 SSH 用户。这种情况下，并不需要通过本配置创建相应的 SSH 用户，如果创建了 SSH 用户，则必须保证指定了正确的服务类型以及认证方式。
- 如果服务器采用了 **password-publickey** 或 **any** 认证，则必须在设备上创建相应的 SSH 用户，以及在设备上创建同名的本地用户（适用于本地认证）或者在远程认证服务器上创建同名的 SSH 用户（如 RADIUS 服务器，适用于远程认证）。

SCP 或 SFTP 用户登录时使用的工作目录与用户使用的认证方式有关：

- 采用 **publickey** 或 **password-publickey** 认证方式的用户，使用的工作目录为对应的本地用户视图下通过 **authorization-attribute** 命令设置的工作目录。
- 只采用 **password** 认证方式的用户，使用的工作目录为通过 AAA 授权的工作目录。

SSH 用户登录时拥有的用户角色与用户使用的认证方式有关：

- 采用 **publickey** 或 **password-publickey** 认证方式的用户，用户角色为对应的本地用户视图下通过 **authorization-attribute** 命令设置的用户角色。
- 采用 **password** 认证方式的用户，用户角色为通过 AAA 授权的用户角色。

使用该命令为用户指定公钥或 PKI 域时，以最后一次指定的公钥或 PKI 域为准。若不指定 **pki-domain** 和 **publickey**，则表示该用户采用证书认证方式登录，服务器使用其所属的 PKI 域来验证客户端的证书。

对 SSH 用户配置的修改，不会影响已经登录的 SSH 用户，仅对新登录的用户生效。

【举例】

创建 SSH 用户 user1，配置 user1 的服务类型为 SFTP，认证方式为 password-publickey，并指定客户端公钥为 key1。

```
<Sysname> system-view
```

```
[Sysname] ssh user user1 service-type sftp authentication-type password-publickey assign publickey key1
```

创建设备管理类本地用户 user1，配置用户密码为明文 123456TESTplat&!，服务类型为 SSH，授权工作目录为 flash:，授权用户角色为 network-admin。

```
[Sysname] local-user user1 class manage
```

```
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
```

```
[Sysname-luser-manage-user1] service-type ssh
```

```
[Sysname-luser-manage-user1] authorization-attribute work-directory flash: user-role network-admin
```

【相关命令】

- **authorization-attribute**（安全命令参考/AAA）

- **display ssh user-information**
- **local-user**（安全命令参考/AAA）
- **pki domain**（安全命令参考/PKI）

1.2 SSH客户端配置命令

1.2.1 bye

bye 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。

【命令】

bye

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

该命令功能与 **exit**、**quit** 相同。

【举例】

```
# 终止与远程 SFTP 服务器的连接。
sftp> bye
<Sysname>
```

1.2.2 cd

cd 命令用来改变远程 SFTP 服务器上的工作路径。

【命令】

cd [*remote-path*]

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

remote-path: 目的工作路径的名称。

【使用指导】

命令“**cd ..**”用来返回到上一级目录。

命令“**cd /**”用来返回到系统的根目录。

【举例】

```
# 改变工作路径到 new1。
sftp> cd new1
Current Directory is:/new1
sftp> pwd
Remote working directory: /new1
sftp>
```

1.2.3 cdup

cdup 命令用来返回到上一级目录。

【命令】

cdup

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 从当前工作目录/test1 返回到上一级目录。
sftp> cd test1
Current Directory is:/test1
sftp> pwd
Remote working directory: /test1
sftp> cdup
Current Directory is:/
sftp> pwd
Remote working directory: /
sftp>
```

1.2.4 delete

delete 命令用来删除 SFTP 服务器上指定的文件。

【命令】

delete *remote-file*

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

remote-file: 要删除的文件的名称。

【使用指导】

该命令和 **remove** 功能相同。

【举例】

```
# 删除服务器上的文件 temp.c。
sftp> delete temp.c
Removing /temp.c
```

1.2.5 dir

dir 命令用来显示指定目录下文件及文件夹的信息。

【命令】

```
dir [ -a | -l ] [ remote-path ]
```

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

-a: 以列表的形式显示指定目录下文件及文件夹的详细信息，其中包括以 “.” 开头的文件及文件夹的详细信息。

-l: 以列表的形式显示指定目录下文件及文件夹的详细信息，但不包括以 “.” 开头的文件及文件夹的详细信息。

remote-path: 查询的目录名。如果没有指定 *remote-path*，则显示当前工作目录下文件及文件夹的信息。

【使用指导】

如果没有指定 **-a** 和 **-l** 参数，则显示指定目录下文件及文件夹的名称。

该命令功能与 **ls** 相同。

【举例】

以列表的形式显示当前工作目录下文件及文件夹的详细信息，其中包括以 “.” 开头的文件及文件夹的详细信息。

```
sftp> dir -a
drwxrwxrwx   2 1       1           512 Dec 18 14:12 .
drwxrwxrwx   2 1       1           512 Dec 18 14:12 ..
-rwxrwxrwx   1 1       1           301 Dec 18 14:11 010.pub
-rwxrwxrwx   1 1       1           301 Dec 18 14:12 011.pub
-rwxrwxrwx   1 1       1           301 Dec 18 14:12 012.pub
```

以列表的形式显示当前工作目录下文件及文件夹的详细信息，但不包括以“.”开头的文件及文件夹的详细信息。

```
sftp> dir -l
-rwxrwxrwx    1 1      1          301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1      1          301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1      1          301 Dec 18 14:12 012.pub
```

1.2.6 display sftp client source

display sftp client source 命令用来显示 SFTP 客户端的源 IP 地址配置。

【命令】

display sftp client source

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 SFTP 客户端的源 IP 地址配置。

```
<Sysname> display sftp client source
The source IP address of the SFTP client is 192.168.0.1.
The source IPv6 address of the SFTP client is 2:2::2:2.
```

【相关命令】

- **sftp client ipv6 source**
- **sftp client source**

1.2.7 display ssh client source

display ssh client source 命令用来显示 STelnet 客户端的源 IP 地址配置。

【命令】

display ssh client source

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 STelnet 客户端的源 IP 地址配置。

```
<Sysname> display ssh client source
```

The source IP address of the SSH client is 192.168.0.1.

The source IPv6 address of the SSH client is 2:2::2:2.

【相关命令】

- **ssh client ipv6 source**
- **ssh client source**

1.2.8 exit

exit 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。

【命令】

exit

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

该命令功能与 **bye**、**quit** 相同。

【举例】

终止与远程 SFTP 服务器的连接。

```
sftp> exit
```

```
<Sysname>
```

1.2.9 get

get 命令用来从远程 SFTP 服务器上下载文件并存储在本地。

【命令】

get remote-file [local-file]

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
context-admin

【参数】

remote-file: 远程 SFTP 服务器上的文件名。

local-file: 本地文件名。如果没有指定本地文件名，则认为本地保存文件的文件名与服务器上的文件名相同。

【举例】

下载远程服务器上的 **temp1.c** 文件，并以文件名 **temp.c** 在本地保存。

```
sftp> get temp1.c temp.c
Fetching /temp1.c to temp.c
/temp.c                                100% 1424      1.4KB/s   00:00
```

1.2.10 help

help 命令用来显示 SFTP 客户端命令的帮助信息。

【命令】

help

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

键入 **?** 和执行 **help** 命令的功能相同。

【举例】

查看帮助信息。

```
sftp> help
Available commands:
  bye                               Quit sftp
  cd [path]                         Change remote directory to 'path'
  cdup                             Change remote directory to the parent directory
  delete path                       Delete remote file
  dir [-a|-l][path]                Display remote directory listing
    -a                             List all filenames
    -l                             List filename including the specific
                                information of the file
  exit                             Quit sftp
  get remote-path [local-path]     Download file
  help                             Display this help text
  ls [-a|-l][path]                 Display remote directory
    -a                             List all filenames
    -l                             List filename including the specific
                                information of the file
  mkdir path                        Create remote directory
```

put local-path [remote-path]	Upload file
pwd	Display remote working directory
quit	Quit sftp
rename oldpath newpath	Rename remote file
remove path	Delete remote file
rmdir path	Delete remote empty directory
?	Synonym for help

1.2.11 ls

ls 命令用来显示指定目录下文件及文件夹的信息。

【命令】

ls [-a | -l] [remote-path]

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

-a: 以列表的形式显示指定目录下文件及文件夹的详细信息，其中包括以“.”开头的文件及文件夹的详细信息。

-l: 以列表的形式显示指定目录下文件及文件夹的详细信息，但不包括以“.”开头的文件及文件夹的详细信息。

remote-path: 查询的目录名。如果没有指定 **remote-path**，则显示当前工作目录下文件及文件夹的信息。

【使用指导】

如果没有指定 **-a** 和 **-l** 参数，则显示指定目录下文件及文件夹的名称。

该命令功能与 **dir** 相同。

【举例】

以列表的形式显示当前工作目录下文件及文件夹的详细信息，其中包括以“.”开头的文件及文件夹的详细信息。

```
sftp> ls -a
drwxrwxrwx  2 1      1      512 Dec 18 14:12 .
drwxrwxrwx  2 1      1      512 Dec 18 14:12 ..
-rwxrwxrwx  1 1      1      301 Dec 18 14:11 010.pub
-rwxrwxrwx  1 1      1      301 Dec 18 14:12 011.pub
-rwxrwxrwx  1 1      1      301 Dec 18 14:12 012.pub
```

以列表的形式显示当前工作目录下文件及文件夹的详细信息，但不包括以“.”开头的文件及文件夹的详细信息。

```
sftp> ls -l
-rwxrwxrwx  1 1      1      301 Dec 18 14:11 010.pub
-rwxrwxrwx  1 1      1      301 Dec 18 14:12 011.pub
```

1.2.12 mkdir

mkdir 命令用来在远程 SFTP 服务器上创建新的目录。

【命令】

mkdir *remote-path*

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

remote-path: 远程 SFTP 服务器上的目录名。

【举例】

在远程 SFTP 服务器上建立目录 test。

```
sftp> mkdir test
```

1.2.13 put

put 命令用来将本地的文件上传到远程 SFTP 服务器。

【命令】

put *local-file* [*remote-file*]

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

local-file: 本地的文件名。

remote-file: 远程 SFTP 服务器上的文件名。如果没有指定远程服务器上的文件名，则认为服务器上保存文件的文件名与本地的文件名相同。

【举例】

将本地 startup.bak 文件上传到远程 SFTP 服务器，并以 startup01.bak 文件名保存。

```
sftp> put startup.bak startup01.bak
```

```
Uploading startup.bak to /startup01.bak
```

```
startup01.bak
```

```
100% 1424
```

```
1.4KB/s
```

```
00:00
```

1.2.14 pwd

pwd 命令用来显示远程 SFTP 服务器上的当前工作目录。

【命令】

pwd

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【举例】

显示远程 SFTP 服务器上的当前工作目录。

```
sftp> pwd
```

```
Remote working directory: /
```

以上显示信息表示当前的工作目录为根目录。

1.2.15 quit

quit 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。

【命令】

quit

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

该命令功能与 **bye**、**exit** 相同。

【举例】

终止与远程 SFTP 服务器的连接。

```
sftp> quit
```

```
<Sysname>
```

1.2.16 remove

remove 命令用来删除远程 SFTP 服务器上指定的文件。

【命令】

remove *remote-file*

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

remote-file: 要删除的文件的名称。

【使用指导】

该命令和 **delete** 命令相同。

【举例】

删除远程 SFTP 服务器上的文件 temp.c。

```
sftp> remove temp.c
```

```
Removing /temp.c
```

1.2.17 rename

rename 命令用来改变远程 SFTP 服务器上指定的文件或者文件夹的名字。

【命令】

rename *old-name new-name*

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

old-name: 原文件名或者文件夹名。

new-name: 新文件名或者文件夹名。

【举例】

将远程 SFTP 服务器上的文件 temp1.c 改名为 temp2.c。

```
sftp> dir
```

```
aa.pub  temp1.c
```

```
sftp> rename temp1.c temp2.c
```

```
sftp> dir
```

```
aa.pub  temp2.c
```

1.2.18 rmdir

rmdir 命令用来删除远程 SFTP 服务器上指定的目录。

【命令】

rmdir *remote-path*

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

context-admin

【参数】

remote-path: 远程 SFTP 服务器上的目录名。

【举例】

删除 SFTP 服务器上当前工作目录下的 temp1 目录。

sftp> rmdir temp1

1.2.19 scp

scp 命令用来与远程的 SCP 服务器建立连接，并进行文件传输。

【命令】

scp *server* [*port-number*] [*vpn-instance* *vpn-instance-name*] { **get** | **put** } *source-file-name* [*destination-file-name*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress** **zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [{ **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type* *interface-number* | **ip** *ip-address* }] *

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

server: 服务器的 IPv4 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

vpn-instance vpn-instance-name: 服务器所属的 VPN 实例。其中, *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。

get: 指定下载文件操作。

put: 指定上传文件操作。

source-file-name: 源文件名称, 为 1~255 个字符的字符串, 区分大小写。

destination-file-name: 目的文件名称, 为 1~255 个字符的字符串, 区分大小写。若未指定该参数, 则表示使用源文件的名称作为目的文件名称。

identity-key: 客户端 **publickey** 认证时采用的公钥算法, 缺省算法为 **dsa**。如果服务器采用 **publickey** 认证, 必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa:** 公钥算法为 DSA。
- **ecdsa-sha2-nistp256:** 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384:** 指定公钥长度为 384 的 ECDSA 算法。
- **rsa:** 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256:** x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384:** x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name:** 指定客户端证书的 PKI 域, 为 1~31 个字符的字符串, 不区分大小写, 公钥算法为 x509v3 时, 指定客户端证书所在 PKI 域名称, 才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法, 缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法, 缺省算法为 **aes128-ctr**、**des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc:** 3DES-CBC 加密算法。
- **aes128-cbc:** 128 位的 AES-CBC 加密算法。
- **aes128-ctr:** 128 位 AES-CTR 加密算法。
- **aes128-gcm:** 128 位 AES-GCM 加密算法。
- **aes192-ctr:** 192 位 AES-CTR 加密算法。
- **aes256-cbc:** 256 位的 AES-CBC 加密算法。
- **aes256-ctr:** 256 位 AES-CTR 加密算法。
- **aes256-gcm:** 256 位 AES-GCM 加密算法。
- **des-cbc:** DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法, 缺省算法为 **sha2-256**、**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5:** HMAC 算法 HMAC-MD5。
- **md5-96:** HMAC 算法 HMAC-MD5-96。
- **sha1:** HMAC 算法 HMAC-SHA1。
- **sha1-96:** HMAC 算法 HMAC-SHA1-96。
- **sha2-256:** HMAC 算法 HMAC-SHA2-256。

- **sha2-512**: HMAC 算法 HMAC-SHA2-512。

prefer-kex : 密钥交换首选算法, 缺省算法为 **ecdh-sha2-nistp256**。
dh-group-exchange-sha1、**dh-group1-sha1**、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1**: 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1**: 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1**: 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256**: 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384**: 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法, 缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的首选加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法, 缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的首选 HMAC 算法相同。

public-key keyname: 指定服务器端的主机公钥, 用于验证服务器端的身份。其中, *keyname* 表示已经配置的主机公钥名称, 为 1~64 个字符的字符串, 不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中, *domain-name* 表示验证服务端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

source: 指定与服务器通信的源 IPv4 地址或者源接口。缺省情况下, 报文源 IPv4 地址为根据路由表项查找的发送此报文的出接口的主 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断, 通常建议指定 Loopback 接口作为源接口, 或者 Loopback 接口、Dialer 接口的 IPv4 地址作为源 IPv4 地址。

interface interface-type interface-number : 指定源接口。*interface-type* 为接口类型和接口编号。系统将使用该接口的 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

【使用指导】

当客户端采用证书认证时, 需要校验服务端证书是否正确, 就需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称, 这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查, 无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域, 则缺省使用客户端证书所在的 PKI 域进行验证。

【举例】

SCP 客户端采用 **publickey** 认证方式, 登录地址为 200.1.1.1 的远程 SCP 服务器, 下载名为 abc.txt 的文件, 采用如下连接策略, 并指定服务器端的公钥名称为 svkey:

- 首选密钥交换算法为 **dh-group14-sha1**;
- 服务器到客户端的首选加密算法为 **aes128-cbc**;
- 客户端到服务器的首选 HMAC 算法为 **sha1**;
- 服务器到客户端的 HMAC 算法为 **sha1-96**;
- 服务器与客户端之间的首选压缩算法为 **zlib**。

```
<Sysname> scp 200.1.1.1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc  
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
```

1.2.20 scp ipv6

scp ipv6 命令用来与远程的 IPv6 SCP 服务器建立连接，并进行文件传输。

【命令】

```
scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i  
interface-type interface-number ] { get | put } source-file-name  
[ destination-file-name ] [ identity-key { dsa | ecdsa-sha2-nistp256 |  
ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 |  
x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress  
zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |  
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } |  
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } |  
prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 |  
ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc |  
aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr |  
aes256-gcm | des-cbc } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 |  
sha2-256 | sha2-512 } ] * [ { public-key keyname | server-pki-domain  
domain-name } | source { interface interface-type interface-number | ipv6  
ipv6-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

server: 服务器的 IPv6 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

vpn-instance vpn-instance-name: 服务器所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

-i interface-type interface-number: 当前 SCP 客户端连接所使用的出接口的接口类型和接口编号。此参数用于 SCP 服务器的地址是链路本地地址的情况，而且指定的出接口必需具有链路本地地址。

get: 指定下载文件操作。

put: 指定上传文件操作。

source-file-name: 源文件名称，为 1~255 个字符的字符串，区分大小写。

destination-file-name: 目的文件名称，为 1~255 个字符的字符串，区分大小写。不指定该参数时，表示使用源文件的名称作为目的文件名称。

identity-key: 客户端 **publickey** 认证时采用的公钥算法，缺省算法为 **dsa**。如果服务器采用 **publickey** 认证，必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa:** 公钥算法为 DSA。
- **ecdsa-sha2-nistp256:** 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384:** 指定公钥长度为 384 的 ECDSA 算法。
- **rsa:** 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256:** x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384:** x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name:** 指定客户端证书的 PKI 域，为 1~31 个字符的字符串，不区分大小写，公钥算法为 x509v3 时，指定客户端证书所在 PKI 域名称，才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法，缺省算法为 **aes128-ctr.des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc:** 3DES-CBC 加密算法。
- **aes128-cbc:** 128 位的 AES-CBC 加密算法。
- **aes128-ctr:** 128 位 AES-CTR 加密算法。
- **aes128-gcm:** 128 位 AES-GCM 加密算法。
- **aes192-ctr:** 192 位 AES-CTR 加密算法。
- **aes256-cbc:** 256 位的 AES-CBC 加密算法。
- **aes256-ctr:** 256 位 AES-CTR 加密算法。
- **aes256-gcm:** 256 位 AES-GCM 加密算法。
- **des-cbc:** DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha2-256**、**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5:** HMAC 算法 HMAC-MD5。
- **md5-96:** HMAC 算法 HMAC-MD5-96。
- **sha1:** HMAC 算法 HMAC-SHA1。
- **sha1-96:** HMAC 算法 HMAC-SHA1-96。
- **sha2-256:** HMAC 算法 HMAC-SHA2-256。
- **sha2-512:** HMAC 算法 HMAC-SHA2-512。

prefer-kex : 密钥交换首选算法，缺省算法为 **ecdh-sha2-nistp256**。
dh-group-exchange-sha1、**dh-group1-sha1**、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1:** 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1:** 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1:** 密钥交换算法 diffie-hellman-group14-sha1。

- **ecdh-sha2-nistp256**: 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384**: 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法, 缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的首选加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法, 缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的首选 HMAC 算法相同。

public-key keyname: 指定服务器端的主机公钥, 用于验证服务器端的身份。其中, *keyname* 表示已经配置的主机公钥名称, 为 1~64 个字符的字符串, 不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中, *domain-name* 表示验证服务端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下, 设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断, 通常建议指定 Loopback 接口作为源接口, 或者 Loopback 接口、Dialer 接口的 IPv6 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type* *interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IP 地址。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

当客户端采用证书认证时, 需要校验服务端证书是否正确, 就需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称, 这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查, 无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域, 则缺省使用客户端证书所在的 PKI 域进行验证。

【举例】

SCP 客户端采用 **publickey** 认证方式, 登录地址为 2000::1 的远程 SCP 服务器, 下载名为 abc.txt 的文件, 采用如下连接策略, 并指定服务器端的公钥名称为 **svkey**:

- 首选密钥交换算法为 **dh-group14-sha1**;
- 服务器到客户端的首选加密算法为 **aes128-cbc**;
- 客户端到服务器的首选 HMAC 算法为 **sha1**;
- 服务器到客户端的 HMAC 算法为 **sha1-96**;
- 服务器与客户端之间的首选压缩算法为 **zlib**。

```
<Sysname> scp ipv6 2000::1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key
svkey
```

1.2.21 scp ipv6 suite-b

scp ipv6 suite-b 命令用来与远程的 ipv6 SCP 服务器建立基于 Suite B 算法集的连接, 并进行文件传输。

【命令】

```
scp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i  
interface-type interface-number ] { get | put } source-file-name  
[ destination-file-name ] suite-b [ 128-bit | 192-bit ] pki-domain  
domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ]  
[ source { interface interface-type interface-number | ipv6 ipv6-address } ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

server: 服务器的 IPv6 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

vpn-instance vpn-instance-name: 服务器所属的 VPN。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

-i interface-type interface-number: 当前 SCP 客户端连接所使用的出接口的接口类型和接口编号。本参数用于 SCP 服务器的地址是链路本地地址的情况，而且指定的出接口必须具有链路本地地址。

get: 指定下载文件操作。

put: 指定上传文件操作。

source-file-name: 源文件名称，为 1~255 个字符的字符串，区分大小写。

destination-file-name: 目的文件名称，为 1~255 个字符的字符串，区分大小写。若未指定本参数，则表示使用源文件名称作为目的文件名称。

suite-b: 指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数，则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit: 指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit: 指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain domain-name: 配置客户端证书的 PKI 域。*domain-name* 为客户端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

server-pki-domain domain-name: 配置验证服务端证书的 PKI 域。*domain-name* 为验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省情况下，不支持压缩。

zlib: 压缩算法 ZLIB。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下，设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而

中断，通常建议指定 Loopback 接口作为源接口，或者 Loopback 接口、Dialer 接口的 IPv6 地址作为源地址。

interface interface-type interface-number：指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IPv6 地址。

ipv6 ipv6-address：指定源 IPv6 地址。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**；
- 服务器到客户端的加密算法为 **aes128-gcm**；
- 客户端到服务器的加密算法为 **aes128-gcm**；
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**；
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**；
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**；
- 服务器到客户端的加密算法为 **aes256-gcm**；
- 客户端到服务器的加密算法为 **aes256-gcm**；
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**；
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**；
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**；
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**；
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**；
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**；
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**；
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

【举例】

SCP 客户端采用安全级别为 192-bit 的 Suite B 算法集，与登录地址为 2000::1 的远程 SCP 服务器建立连接，下载名为 **abc.txt** 的文件，采用如下连接策略：指定客户端证书的 PKI 域名称为 **clientpkidomain**，指定验证服务端证书的 PKI 域名称为 **serverpkidomain**。

```
<Sysname> scp ipv6 2000::1 get abc.txt suite-b 192-bit pki-domain clientpkidomain  
server-pki-domain serverpkidomain
```

Username:

1.2.22 scp suite-b

scp suite-b 命令用来与远程的 SCP 服务器建立基于 Suite B 算法集的连接，并进行文件传输。

【命令】

```
scp server [ port-number ] [ vpn-instance vpn-instance-name ] { get | put }  
source-file-name [ destination-file-name ] suite-b [ 128-bit | 192-bit ]  
pki-domain domain-name [ server-pki-domain domain-name ] [ prefer-compress  
zlib ] [ source { interface interface-type interface-number | ip ip-address } ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

server: 服务器的 IPv4 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

vpn-instance vpn-instance-name: 服务器所属的 VPN。其中，**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

get: 指定下载文件操作。

put: 指定上传文件操作。

source-file-name: 源文件名称，为 1~255 个字符的字符串，区分大小写。

destination-file-name: 目的文件名称，为 1~255 个字符的字符串，区分大小写。若未指定本参数，则表示使用源文件名称作为目的文件名称。

suite-b: 指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数，则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit: 指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit: 指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain domain-name: 配置客户端证书的 PKI 域。**domain-name** 为客户端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

server-pki-domain domain-name: 配置验证服务端证书的 PKI 域。**domain-name** 为验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省情况下，不支持压缩。

zlib: 压缩算法 ZLIB。

source: 指定与服务器通信的源 IP 地址或者源接口。缺省情况下，设备根据路由表项自动选择一个源 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者 Loopback 接口、Dialer 接口的 IP 地址作为源地址。

interface interface-type interface-number：指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address：指定源 IPv4 地址。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**；
- 服务器到客户端的加密算法为 **aes128-gcm**；
- 客户端到服务器的加密算法为 **aes128-gcm**；
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**；
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**；
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**；
- 服务器到客户端的加密算法为 **aes256-gcm**；
- 客户端到服务器的加密算法为 **aes256-gcm**；
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**；
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**；
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**；
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**；
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**；
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**；
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**；
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

【举例】

SCP 客户端采用安全级别为 128-bit 的 Suite B 算法集，与登录地址为 200.1.1.1 的远程 SCP 服务器建立连接，下载名为 abc.txt 的文件，采用如下连接策略：指定客户端证书的 PKI 域名称为 clientpkidomain，指定验证服务端证书的 PKI 域名称为 serverpkidomain。

```
<Sysname> scp 200.1.1.1 get abc.txt suite-b 128-bit pki-domain clientpkidomain  
server-pki-domain serverpkidomain  
Username:
```

1.2.23 sftp

sftp 命令用来与远程 IPv4 SFTP 服务器建立连接，并进入 SFTP 客户端视图。

【命令】

```
sftp server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { dsa | ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } ] * [ dscp dscp-value | { public-key keyname | server-pki-domain domain-name } | source { interface interface-type interface-number | ip ip-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

server: 服务器 IPv4 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

vpn-instance vpn-instance-name: 服务器所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

identity-key: 客户端 **publickey** 认证时采用的公钥算法，缺省算法为 **dsa**。如果服务器采用 **publickey** 认证，必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa**: 公钥算法为 DSA。
- **ecdsa-sha2-nistp256**: 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384**: 指定公钥长度为 384 的 ECDSA 算法。
- **rsa**: 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256**: x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384**: x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name**: 指定客户端证书的 PKI 域，为 1~31 个字符的字符串，不区分大小写，公钥算法为 x509v3 时，指定客户端证书所在 PKI 域名称，才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法, 缺省算法为 **aes128-ctr.des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc:** 3DES-CBC 加密算法。
- **aes128-cbc:** 128 位的 AES-CBC 加密算法。
- **aes128-ctr:** 128 位 AES-CTR 加密算法。
- **aes128-gcm:** 128 位 AES-GCM 加密算法。
- **aes192-ctr:** 192 位 AES-CTR 加密算法。
- **aes256-cbc:** 256 位的 AES-CBC 加密算法。
- **aes256-ctr:** 256 位 AES-CTR 加密算法。
- **aes256-gcm:** 256 位 AES-GCM 加密算法。
- **des-cbc:** DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法, 缺省算法为 **sha2-256**、**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5:** HMAC 算法 HMAC-MD5。
- **md5-96:** HMAC 算法 HMAC-MD5-96。
- **sha1:** HMAC 算法 HMAC-SHA1。
- **sha1-96:** HMAC 算法 HMAC-SHA1-96。
- **sha2-256:** HMAC 算法 HMAC-SHA2-256。
- **sha2-512:** HMAC 算法 HMAC-SHA2-512。

prefer-kex: 密钥交换首选算法, 缺省算法为 **ecdh-sha2-nistp256**。
dh-group-exchange-sha1、**dh-group1-sha1**、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1:** 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1:** 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1:** 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256:** 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384:** 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法, 缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的首选加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法, 缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的首选 HMAC 算法相同。

dscp dscp-value: 指定客户端发送的 SFTP 报文中携带的 DSCP 优先级, 取值范围为 0~63, 缺省值为 48。DSCP 携带在 IP 报文中的 ToS 字段, 用来体现报文自身的优先等级, 决定报文传输的优先程度。

public-key keyname: 指定服务器端的主机公钥, 用于验证服务器端的身份。其中, **keyname** 表示已经配置的主机公钥名称, 为 1~64 个字符的字符串, 不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中, *domain-name* 表示验证服务端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

source: 指定与服务器通信的源 IPv4 地址或者源接口。缺省情况下, 报文源 IPv4 地址为根据路由表项查找的发送此报文的出接口的主 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断, 通常建议指定 Loopback 接口作为源接口, 或者 Loopback 接口、Dialer 接口的 IPv4 地址作为源 IPv4 地址。

interface interface-type interface-number: 指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将采用该接口的主 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

【使用指导】

当客户端采用证书认证时, 需要校验服务端证书是否正确, 就需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称, 这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查, 无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域, 则缺省使用客户端证书所在的 PKI 域进行验证。

【举例】

SFTP 客户端采用 **publickey** 认证方式, 连接 IP 地址为 10.1.1.2 的 SFTP 服务器, 采用如下连接策略, 并指定服务器端的公钥名称为 **svkey**:

- 首选密钥交换算法为 **dh-group14-sha1**;
- 服务器到客户端的首选加密算法为 **aes128-cbc**;
- 客户端到服务器的首选 HMAC 算法为 **sha1**;
- 服务器到客户端的 HMAC 算法为 **sha1-96**;
- 服务器与客户端之间的首选压缩算法为 **zlib**。

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc  
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
```

1.2.24 sftp client ipv6 source

sftp client ipv6 source 命令用来配置 SFTP 客户端发送 SFTP 报文使用的源 IPv6 地址。

undo sftp client ipv6 source 命令用来恢复缺省情况。

【命令】

```
sftp client ipv6 source { interface interface-type interface-number | ipv6  
ipv6-address }  
undo sftp client ipv6 source
```

【缺省情况】

未配置 SFTP 客户端使用的源 IPv6 地址, 设备自动选择 IPv6 SFTP 报文的源 IPv6 地址, 具体选择原则请参见 RFC 3484。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface interface-type interface-number: 指定接口下与报文目的地址最匹配的 IPv6 地址作为源地址。*interface-type interface-number* 表示源接口类型与源接口编号。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

sftp client ipv6 source 命令指定的源地址对所有的 SFTP 连接有效, **sftp ipv6** 命令指定的源地址只对当前的 SFTP 连接有效。

使用该命令指定了源地址后, 若 SFTP 用户使用 **sftp ipv6** 命令登录时又指定了源地址, 则采用 **sftp ipv6** 命令中指定的源地址。

多次执行本命令, 最后一次执行的命令生效。

【举例】

指定 SFTP 客户端发送 SFTP 报文使用的源 IPv6 地址为 2:2::2:2。

```
<Sysname> system-view
```

```
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

【相关命令】

- **display sftp client source**

1.2.25 sftp client source

sftp client source 命令用来配置 SFTP 客户端发送 SFTP 报文使用的源 IPv4 地址。

undo sftp client source 命令用来恢复缺省情况。

【命令】

```
sftp client source { interface interface-type interface-number | ip  
ip-address }
```

```
undo sftp client source
```

【缺省情况】

未配置 SFTP 客户端使用的源 IPv4 地址, SFTP 客户端发送 SFTP 报文使用的源 IPv4 地址为根据路由表项查找的发送此报文的出接口的主 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface interface-type interface-number: 指定接口的主 IP 地址作为源地址。
interface-type interface-number 表示源接口类型与源接口编号。
ip ip-address: 指定源 IP 地址。

【使用指导】

sftp client source 命令指定的源地址对所有的 SFTP 连接有效, **sftp** 命令指定的源地址只对当前的 SFTP 连接有效。

使用该命令指定了源地址后, 若 SFTP 用户使用 **sftp** 命令登录时又指定了源地址, 则采用 **sftp** 命令中指定的源地址。

多次执行本命令, 最后一次执行的命令生效。

【举例】

指定 SFTP 客户端发送 SFTP 报文使用的源 IP 地址为 192.168.0.1。

```
<Sysname> system-view
```

```
[Sysname] sftp client source ip 192.168.0.1
```

【相关命令】

- **display sftp client source**

1.2.26 sftp ipv6

sftp ipv6 命令用来建立 SFTP 客户端和与远程 IPv6 SFTP 服务器建立连接, 并进入 SFTP 客户端视图。

【命令】

```
sftp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i  
interface-type interface-number ] [ identity-key { dsa | ecdsa-sha2-nistp256  
| ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 |  
x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress  
zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |  
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } |  
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } |  
prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 |  
ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc |  
aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr |  
aes256-gcm | des-cbc } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 |  
sha2-256 | sha2-512 } ] * [ dscp dscp-value | { public-key keyname |  
server-pki-domain domain-name } | source { interface interface-type  
interface-number | ipv6 ipv6-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

server: 服务器的 IPv6 地址或主机名称, 为 1~253 个字符的字符串, 不区分大小写。

port-number: 服务器端口号, 取值范围为 1~65535, 缺省值为 22。

vpn-instance vpn-instance-name: 服务器所属的 VPN 实例。其中, *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。

-i interface-type interface-number: 客户端连接服务器时使用的出接口。其中, *interface-type interface-number* 表示接口类型和接口编号。本参数仅在客户端所连接的服务器的地址是链路本地地址时使用。指定的出接口必须具有链路本地地址。

identity-key: 客户端 **publickey** 认证时采用的公钥算法, 缺省算法为 **dsa**。如果服务器采用 **publickey** 认证, 必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa**: 公钥算法为 DSA。
- **ecdsa-sha2-nistp256**: 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384**: 指定公钥长度为 384 的 ECDSA 算法。
- **rsa**: 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256**: x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384**: x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name**: 指定客户端证书的 PKI 域, 为 1~31 个字符的字符串, 不区分大小写, 公钥算法为 x509v3 时, 指定客户端证书所在 PKI 域名称, 才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法, 缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法, 缺省算法为 **aes128-ctr**。**des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc**: 3DES-CBC 加密算法。
- **aes128-cbc**: 128 位的 AES-CBC 加密算法。
- **aes128-ctr**: 128 位 AES-CTR 加密算法。
- **aes128-gcm**: 128 位 AES-GCM 加密算法。
- **aes192-ctr**: 192 位 AES-CTR 加密算法。
- **aes256-cbc**: 256 位的 AES-CBC 加密算法。
- **aes256-ctr**: 256 位 AES-CTR 加密算法。
- **aes256-gcm**: 256 位 AES-GCM 加密算法。
- **des-cbc**: DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法, 缺省算法为 **sha2-256**。**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5**: HMAC 算法 HMAC-MD5。
- **md5-96**: HMAC 算法 HMAC-MD5-96。
- **sha1**: HMAC 算法 HMAC-SHA1。

- **sha1-96**: HMAC 算法 HMAC-SHA1-96。
- **sha2-256**: HMAC 算法 HMAC-SHA2-256。
- **sha2-512**: HMAC 算法 HMAC-SHA2-512。

prefer-kex : 密钥交换首选算法，缺省算法为 **ecdh-sha2-nistp256**。
dh-group-exchange-sha1、**dh-group1-sha1**、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1**: 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1**: 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1**: 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256**: 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384**: 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法，缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的首选加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的首选 HMAC 算法相同。

dscp dscp-value: 指定客户端发送的 IPv6 SFTP 报文中携带的 DSCP 优先级，取值范围为 0~63，缺省值为 48。DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

public-key keyname: 指定服务器端的主机公钥，用于验证服务器端的身份。其中，*keyname* 表示已经配置的主机公钥名称，为 1~64 个字符的字符串，不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中，*domain-name* 表示验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下，设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者 Loopback 接口、Dialer 接口的 IPv6 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type* *interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IP 地址。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

当客户端采用证书认证时，需要校验服务端证书是否正确，就需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称，这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查，无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

【举例】

SFTP 客户端采用 publickey 认证方式，连接 IPv6 地址为 2000::1 的 SFTP 服务器，采用如下连接策略，并指定服务器端的公钥名称为 svkey:

- 首选密钥交换算法为 **dh-group14-sha1**;

- 服务器到客户端的首选加密算法为 **aes128-cbc**;
- 客户端到服务器的首选 HMAC 算法为 **sha1**;
- 服务器到客户端的 HMAC 算法为 **sha1-96**;
- 服务器与客户端之间的首选压缩算法为 **zlib**。

```
<Sysname> sftp ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
Username:
```

1.2.27 sftp ipv6 suite-b

sftp ipv6 suite-b 命令用来与远程的 IPv6 SFTP 服务器建立基于 Suite B 算法集的连接，并进入 SFTP 客户端视图。

【命令】

```
sftp ipv6 server [ port-number ] [ vpn-instance vpn-instance-name ] [ -i
interface-type interface-number ] suite-b [ 128-bit | 192-bit ] pki-domain
domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ] [ dscp
dscp-value | source { interface interface-type interface-number | ipv6
ipv6-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

server: 服务器的 IPv6 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

vpn-instance *vpn-instance-name*: 服务器所属的 VPN。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

-i interface-type interface-number: 客户端连接服务器时使用的出接口。其中，*interface-type interface-number* 表示接口类型和接口编号。本参数仅在客户端所连接的服务器的地址是链路本地地址时使用。指定的出接口必须具有链路本地地址。

suite-b: 指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数，则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit: 指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit: 指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain *domain-name*: 配置客户端证书的 PKI 域。*domain-name* 为客户端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“”。

server-pki-domain *domain-name*: 配置验证服务端证书的 PKI 域。*domain-name* 为验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、

“:”、“.”、“<”、“>”、“”和“'”。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省情况下，不支持压缩。

zlib: 压缩算法 ZLIB。

dscp dscp-value: 指定客户端发送的 IPv6 SFTP 报文中携带的 DSCP 优先级，取值范围为 0～63，缺省值为 48。DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下，设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者 Loopback 接口、Dialer 接口的 IPv6 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type* *interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IPv6 地址。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**;
- 服务器到客户端的加密算法为 **aes128-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes256-gcm**;
- 客户端到服务器的加密算法为 **aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;

- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

【举例】

SFTP 客户端采用安全级别为 192-bit 的 Suite B 算法集，与登录地址为 2000::1 的远程 SFTP 服务器建立连接，采用如下连接策略：指定客户端证书的 PKI 域名称为 **clientpkidomain**，指定验证服务端证书的 PKI 域名称为 **serverpkidomain**。

```
<Sysname> sftp ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

1.2.28 sftp suite-b

sftp suite-b 命令用来与远程的 IPv4 SFTP 服务器建立基于 Suite B 算法集的连接，并进入 SFTP 客户端视图。

【命令】

```
sftp server [ port-number ] [ vpn-instance vpn-instance-name ] suite-b
[ 128-bit | 192-bit ] pki-domain domain-name [ server-pki-domain domain-name ]
[ prefer-compress zlib ] [ dscp dscp-value | source { interface interface-type
interface-number | ip ip-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

server：服务器的 IPv4 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number：服务器端口号，取值范围为 1~65535，缺省值为 22。

vpn-instance *vpn-instance-name*：服务器所属的 VPN。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

suite-b：指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数，则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit：指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit：指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain *domain-name*：配置客户端证书的 PKI 域。*domain-name* 为客户端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

server-pki-domain *domain-name*：配置验证服务端证书的 PKI 域。*domain-name* 为验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress：服务器与客户端之间的首选压缩算法，缺省情况下，不支持压缩。

zlib: 压缩算法 ZLIB。

dscp dscp-value: 指定客户端发送的 SFTP 报文中携带的 DSCP 优先级，取值范围为 0~63，缺省值为 48。DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

source: 指定与服务器通信的源 IP 地址或者源接口。缺省情况下，设备根据路由表项自动选择一个源 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者 Loopback 接口、Dialer 接口的 IP 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**;
- 服务器到客户端的加密算法为 **aes128-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes256-gcm**;
- 客户端到服务器的加密算法为 **aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

【举例】

SFTP 客户端采用安全级别为 128-bit 的 Suite B 算法集，与登录地址为 10.1.1.2 的远程 SFTP 服务器建立连接，采用如下连接策略：指定客户端证书的 PKI 域名称为 clientpkidomain，指定验证服务端证书的 PKI 域名称为 serverpkidomain。

```
<Sysname> sftp 10.1.1.2 suite-b 128-bit pki-domain clientpkidomain server-pki-domain  
serverpkidomain  
Username:
```

1.2.29 ssh client ipv6 source

ssh client ipv6 source 命令用来为配置 Stelnet 客户端发送 SSH 报文使用的源 IPv6 地址。

undo ssh client ipv6 source 命令用来恢复缺省情况。

【命令】

```
ssh client ipv6 source { interface interface-type interface-number | ipv6  
ipv6-address }  
undo ssh client ipv6 source
```

【缺省情况】

未配置 Stelnet 客户端使用的源 IPv6 地址，设备自动选择 IPv6 SSH 报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface interface-type interface-number: 指定接口下与报文目的地址最匹配的 IPv6 地址作为源地址。*interface-type interface-number* 表示源接口类型与源接口编号。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

ssh client ipv6 source 命令指定的源地址对所有的 IPv6 Stelnet 连接有效，**ssh2 ipv6** 命令指定的源地址只对当前的 Stelnet 连接有效。

使用该命令指定了源地址后，若 SSH 用户使用 **ssh2 ipv6** 命令登录时又指定了源地址，则采用 **ssh2 ipv6** 命令中指定的源地址。

多次执行本命令，最后一次执行的命令生效。

【举例】

指定 Stelnet 客户端发送 SSH 报文使用的源 IPv6 地址为 2:2::2:2。

```
<Sysname> system-view  
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```


【相关命令】

- **display ssh client source**

1.2.30 ssh client source

ssh client source 命令用来配置 Stelnet 客户端发送 SSH 报文使用的源 IPv4 地址。

undo ssh client source 命令用来恢复缺省情况。

【命令】

```
ssh client source { interface interface-type interface-number | ip  
ip-address }  
undo ssh client source
```

【缺省情况】

未配置 Stelnet 客户端使用的源 IPv4 地址, Stelnet 客户端发送 SSH 报文使用的源 IPv4 地址为设备路由指定的 SSH 报文出口接口的主 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface *interface-type* *interface-number*: 指定接口的主 IP 地址作为源地址。

interface-type *interface-number* 表示源接口类型与源接口编号。

ip *ip-address*: 指定源 IPv4 地址。

【使用指导】

ssh client source 命令指定的源地址对所有的 Stelnet 连接有效, **ssh2** 命令指定的源地址只对当前的 Stelnet 连接有效。

使用该命令指定了源地址后, 若 SSH 用户使用 **ssh2** 命令登录时又指定了源地址, 则采用 **ssh2** 命令中指定的源地址。

多次执行本命令, 最后一次执行的命令生效。

【举例】

指定 Stelnet 客户端发送 SSH 报文使用的源 IPv4 地址为 192.168.0.1。

```
<Sysname> system-view
```

```
[Sysname] ssh client source ip 192.168.0.1
```

【相关命令】

- **display ssh client source**

1.2.31 ssh2

ssh2 命令用来建立 Stelnet 客户端和 IPv4 Stelnet 服务器端的连接。

【命令】

```
ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] [ identity-key { dsa | ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } ] * [ dscp dscp-value | escape character | { public-key keyname | server-pki-domain domain-name } | source { interface interface-type interface-number | ip ip-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

server: 服务器 IPv4 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

vpn-instance vpn-instance-name: 服务器所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

identity-key: 客户端 *publickey* 认证时采用的公钥算法，缺省算法为 **dsa**。如果服务器采用 *publickey* 认证，必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa**: 公钥算法为 DSA。
- **ecdsa-sha2-nistp256**: 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384**: 指定公钥长度为 384 的 ECDSA 算法。
- **rsa**: 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256**: x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384**: x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name**: 指定客户端证书的 PKI 域，为 1~31 个字符的字符串，不区分大小写，公钥算法为 x509v3 时，指定客户端证书所在 PKI 域名称，才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法, 缺省算法为 **aes128-ctr**。**des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc:** 3DES-CBC 加密算法。
- **aes128-cbc:** 128 位的 AES-CBC 加密算法。
- **aes128-ctr:** 128 位 AES-CTR 加密算法。
- **aes128-gcm:** 128 位 AES-GCM 加密算法。
- **aes192-ctr:** 192 位 AES-CTR 加密算法。
- **aes256-cbc:** 256 位的 AES-CBC 加密算法。
- **aes256-ctr:** 256 位 AES-CTR 加密算法。
- **aes256-gcm:** 256 位 AES-GCM 加密算法。
- **des-cbc:** DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法, 缺省算法为 **sha2-256**。**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5:** HMAC 算法 HMAC-MD5。
- **md5-96:** HMAC 算法 HMAC-MD5-96。
- **sha1:** HMAC 算法 HMAC-SHA1。
- **sha1-96:** HMAC 算法 HMAC-SHA1-96。
- **sha2-256:** HMAC 算法 HMAC-SHA2-256。
- **sha2-512:** HMAC 算法 HMAC-SHA2-512。

prefer-kex: 密钥交换首选算法, 缺省算法为 **ecdh-sha2-nistp256**。**dh-group-exchange-sha1**、**dh-group1-sha1**、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1:** 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1:** 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1:** 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256:** 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384:** 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法, 缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的首选加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法, 缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的首选 HMAC 算法相同。

dscp dscp-value: 指定客户端发送的 SFTP 报文中携带的 DSCP 优先级, 取值范围为 0~63, 缺省值为 48。DSCP 携带在 IP 报文中的 ToS 字段, 用来体现报文自身的优先等级, 决定报文传输的优先程度。

escape character: 指定退出字符。*character* 为一个字符, 区分大小写, 缺省为~, 即输入~.可以强制断开与服务端的连接。

public-key keyname: 指定服务器端的主机公钥, 用于验证服务器端的身份。其中, *keyname* 表示已经配置的主机公钥名称, 为 1~64 个字符的字符串, 不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中, *domain-name* 表示验证服务端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

source: 指定与服务器通信的源 IPv4 地址或者源接口。缺省情况下, 报文源 IPv4 地址为根据路由表项查找的发送此报文的出接口的主 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断, 通常建议指定 Loopback 接口作为源接口, 或者 Loopback 接口、Dialer 接口的 IPv4 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type* *interface-number* 为接口类型和接口编号。系统将采用该接口的主 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

【使用指导】

当客户端采用证书认证时, 需要校验服务端证书是否正确, 就需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称, 这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查, 无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域, 则缺省使用客户端证书所在的 PKI 域进行验证。

关于退出字符的使用, 需要注意的是:

- 退出字符与字符. 配合使用可以强制断开客户端与服务器连接 (该方式通常用于服务器端重启或发生异常的情况下, 客户端快速中断当前连接)。
- 必须在一行中首先输入退出字符和., 该操作才能生效, 若该行中曾经输入过其它字符或执行了其它操作 (比如退格), 则需要重新换行输入才能生效。
- 一般情况下, 建议使用缺省退出字符, 避免退出字符和. 的组合与登录用户名相同。

【举例】

Stelnet 客户端采用 **publickey** 认证方式, 登录地址为 3.3.3.3 的远程 Stelnet 服务器, 采用如下连接策略, 并指定服务器端的公钥名称为 **svkey**:

- 首选密钥交换算法为 **dh-group14-sha1**;
- 服务器到客户端的首选加密算法为 **aes128-cbc**;
- 客户端到服务器的首选 HMAC 算法为 **sha1**;
- 服务器到客户端的 HMAC 算法为 **sha1-96**;
- 服务器与客户端之间的首选压缩算法为 **zlib**;
- 输入 \$ 时强制断开客户端和服务端的连接。

```
<Sysname> ssh2 3.3.3.3 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc  
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey escape  
$
```

1.2.32 ssh2 ipv6

ssh2 ipv6 命令用来建立 Stelnet 客户端和 IPv6 Stelnet 服务器端的连接。

【命令】

ssh2 ipv6 server [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256**

```
| ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 |
x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress
zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } |
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } |
prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 |
ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc |
aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr |
aes256-gcm | des-cbc } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 |
sha2-256 | sha2-512 } ] * [ dscp dscp-value | escape character | { public-key
keyname | server-pki-domain domain-name } | source { interface
interface-type interface-number | ipv6 ipv6-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

server: 服务器的 IPv6 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

vpn-instance vpn-instance-name: 服务器所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

-i interface-type interface-number: 客户端连接服务器时使用的出接口。其中，*interface-type interface-number* 表示接口类型和接口编号。本参数仅在客户端所连接的服务器的地址是链路本地地址时使用。指定的出接口必须具有链路本地地址。

identity-key: 客户端 **publickey** 认证时采用的公钥算法，缺省算法为 **dsa**。如果服务器采用 **publickey** 认证，必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa**: 公钥算法为 DSA。
- **ecdsa-sha2-nistp256**: 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384**: 指定公钥长度为 384 的 ECDSA 算法。
- **rsa**: 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256**: x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384**: x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name**: 指定客户端证书的 PKI 域，为 1~31 个字符的字符串，不区分大小写，公钥算法为 x509v3 时，指定客户端证书所在 PKI 域名称，才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法, 缺省算法为 **aes128-ctr.des-cbc、3des-cbc、aes128-cbc、aes128-ctr、aes128-gcm、aes192-ctr、aes256-cbc、aes256-ctr、aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc:** 3DES-CBC 加密算法。
- **aes128-cbc:** 128 位的 AES-CBC 加密算法。
- **aes128-ctr:** 128 位 AES-CTR 加密算法。
- **aes128-gcm:** 128 位 AES-GCM 加密算法。
- **aes192-ctr:** 192 位 AES-CTR 加密算法。
- **aes256-cbc:** 256 位的 AES-CBC 加密算法。
- **aes256-ctr:** 256 位 AES-CTR 加密算法。
- **aes256-gcm:** 256 位 AES-GCM 加密算法。
- **des-cbc:** DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法, 缺省算法为 **sha2-256.md5、md5-96、sha1、sha1-96、sha2-256、sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5:** HMAC 算法 HMAC-MD5。
- **md5-96:** HMAC 算法 HMAC-MD5-96。
- **sha1:** HMAC 算法 HMAC-SHA1。
- **sha1-96:** HMAC 算法 HMAC-SHA1-96。
- **sha2-256:** HMAC 算法 HMAC-SHA2-256。
- **sha2-512:** HMAC 算法 HMAC-SHA2-512。

prefer-kex: 密钥交换首选算法, 缺省算法为 **ecdh-sha2-nistp256.dh-group-exchange-sha1、dh-group1-sha1、dh-group14-sha1、ecdh-sha2-nistp256、ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1:** 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1:** 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1:** 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256:** 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384:** 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法, 缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的首选加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法, 缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的首选 HMAC 算法相同。

dscp dscp-value: 指定客户端发送的 IPv6 SSH 报文中携带的 DSCP 优先级, 取值范围为 0~63, 缺省值为 48。DSCP 携带在 IPv6 报文中的 Traffic class 字段, 用来体现报文自身的优先等级, 决定报文传输的优先程度。

escape character: 指定退出字符。*character* 为一个字符, 区分大小写, 缺省为~, 即输入~.可以强制断开与服务端的连接。

public-key keyname: 指定服务器端的主机公钥, 用于验证服务器端的身份。其中, *keyname* 表示已经配置的主机公钥名称, 为 1~64 个字符的字符串, 不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中, *domain-name* 表示验证服务端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下, 设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断, 通常建议指定 Loopback 接口作为源接口, 或者 Loopback 接口、Dialer 接口的 IPv6 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type* *interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IP 地址。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

当客户端采用证书认证时, 需要校验服务端证书是否正确, 就需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称, 这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查, 无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域, 则缺省使用客户端证书所在的 PKI 域进行验证。

关于退出字符的使用, 需要注意的是:

- 退出字符与字符.配合使用可以强制断开客户端与服务器连接 (该方式通常用于服务器端重启或发生异常的情况下, 客户端快速中断当前连接)。
- 必须在一行中首先输入退出字符和., 该操作才能生效, 若该行中曾经输入过其它字符或执行了其它操作 (比如退格), 则需要重新换行输入才能生效。
- 一般情况下, 建议使用缺省退出字符, 避免退出字符和.的组合与登录用户名相同。

【举例】

SSH 客户端采用 **publickey** 认证方式, 登录地址为 2000::1 的远程 Stelnet 服务器, 采用如下连接策略, 并指定服务器端的公钥名称为 **svkey**:

- 首选密钥交换算法为 **dh-group14-sha1**;
- 服务器到客户端的首选加密算法为 **aes128-cbc**;
- 客户端到服务器的首选 HMAC 算法为 **sha1**;
- 服务器到客户端的 HMAC 算法为 **sha1-96**;
- 服务器与客户端之间的首选压缩算法为 **zlib**;
- 输入 \$ 时强制断开客户端和服务端的连接。

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc  
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey escape  
$
```

1.2.33 ssh2 ipv6 suite-b

ssh2 ipv6 suite-b 命令用来与远程的 IPv6 Stelnet 服务器建立基于 Suite B 算法集的连接。

【命令】

ssh2 ipv6 server [*port-number*] [**vpn-instance** *vpn-instance-name*] [**-i** *interface-type interface-number*] **suite-b** [**128-bit** | **192-bit**] **pki-domain**

domain-name [**server-pki-domain** *domain-name*] [**prefer-compress** *zlib*] [**dscp** *dscp-value* | **escape** *character* | **source** { **interface** *interface-type* *interface-number* | **ipv6** *ipv6-address* }] *

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

server: 服务器的 IPv6 地址或主机名称, 为 1~253 个字符的字符串, 不区分大小写。

port-number: 服务器端口号, 取值范围为 1~65535, 缺省值为 22。

vpn-instance *vpn-instance-name*: 服务器所属的 VPN。其中, *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。

-i *interface-type interface-number*: 客户端连接服务器时使用的出接口。其中, *interface-type interface-number* 表示接口类型和接口编号。本参数仅在客户端所连接的服务器的地址是链路本地地址时使用。指定的出接口必须具有链路本地地址。

suite-b: 指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数, 则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit: 指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit: 指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain *domain-name*: 配置客户端证书的 PKI 域。*domain-name* 为客户端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

server-pki-domain *domain-name*: 配置验证服务端证书的 PKI 域。*domain-name* 为验证服务端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。如果客户端没有指定验证服务端证书所在的 PKI 域, 则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法, 缺省情况下, 不支持压缩。

zlib: 压缩算法 ZLIB。

dscp *dscp-value*: 指定客户端发送的 IPv6 SSH 报文中携带的 DSCP 优先级, 取值范围为 0~63, 缺省值为 48。DSCP 携带在 IPv6 报文中的 Traffic class 字段, 用来体现报文自身的优先等级, 决定报文传输的优先程度。

escape character: 指定退出字符, 该退出字符与字符.配合使用可以强制断开客户端与服务器连接(该方式通常用于服务器端重启或发生异常的情况下, 客户端快速中断当前连接)。*character* 为一个字符, 区分大小写, 缺省为~, 即输入~.可以强制断开与服务端的连接。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下, 设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断, 通常建议指定 Loopback 接口作为源接口, 或者 Loopback 接口、Dialer 接口的 IPv6 地址作为源地址。

interface interface-type interface-number：指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IPv6 地址。

ipv6 ipv6-address：指定源 IPv6 地址。

关于退出字符的使用，需要注意的是：

- 必须在一行中首先输入退出字符和.，该操作才能生效，若该行中曾经输入过其它字符或执行了其它操作（比如退格），则需要重新换行输入才能生效。
- 一般情况下，建议使用缺省退出字符，避免退出字符和.的组合与登录用户名相同。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**；
- 服务器到客户端的加密算法为 **aes128-gcm**；
- 客户端到服务器的加密算法为 **aes128-gcm**；
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**；
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**；
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**；
- 服务器到客户端的加密算法为 **aes256-gcm**；
- 客户端到服务器的加密算法为 **aes256-gcm**；
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**；
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**；
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**；
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**；
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**；
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**；
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**；
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

【举例】

SSH 客户端采用安全级别为 192-bit 的 Suite B 算法集，与登录地址为 2000::1 的远程 Stelnet 服务器建立连接，采用如下连接策略：指定客户端证书的 PKI 域名称为 clientpkidomain，指定验证服务端证书的 PKI 域名称为 serverpkidomain。

```
<Sysname> ssh2 ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain serverpkidomain
```

Username:

1.2.34 ssh2 suite-b

ssh2 suite-b 命令用来与远程的 IPv4 Stelnet 服务器建立基于 Suite B 算法集的连接。

【命令】

```
ssh2 server [ port-number ] [ vpn-instance vpn-instance-name ] suite-b
[ 128-bit | 192-bit ] pki-domain domain-name [ server-pki-domain domain-name ]
[ prefer-compress zlib ] [ dscp dscp-value | escape character | source
{ interface interface-type interface-number | ip ip-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

server: 服务器的 IPv4 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

vpn-instance vpn-instance-name: 服务器所属的 VPN。其中，**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

suite-b: 指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数，则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit: 指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit: 指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain domain-name: 配置客户端证书的 PKI 域。**domain-name** 为客户端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

server-pki-domain domain-name: 配置验证服务端证书的 PKI 域。**domain-name** 为验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省情况下，不支持压缩。

zlib: 压缩算法 ZLIB。

dscp dscp-value: 指定客户端发送的 SFTP 报文中携带的 DSCP 优先级，取值范围为 0~63，缺省值为 48。DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

escape character: 指定退出字符，该退出字符与字符.配合使用可以强制断开客户端与服务器连接（该方式通常用于服务器端重启或发生异常的情况下，客户端快速中断当前连接）。**character** 为一个字符，区分大小写，缺省为~，即输入~.可以强制断开与服务端的连接。

source: 指定与服务器通信的源 IP 地址或者源接口。缺省情况下,设备根据路由表项自动选择一个源 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断,通常建议指定 Loopback 接口作为源接口,或者 Loopback 接口、Dialer 接口的 IP 地址作为源地址。

interface interface-type interface-number : 指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时,客户端算法要求:

- 密钥交换算法为 **ecdh-sha2-nistp256**;
- 服务器到客户端的加密算法为 **aes128-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时,客户端算法要求:

- 密钥交换算法为 **ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes256-gcm**;
- 客户端到服务器的加密算法为 **aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时,客户端算法要求:

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

关于退出字符的使用,需要注意的是:

- 必须在一行中首先输入退出字符和.,该操作才能生效,若该行中曾经输入过其它字符或执行了其它操作(比如退格),则需要重新换行输入才能生效。
- 一般情况下,建议使用缺省退出字符,避免退出字符和.的组合与登录用户名相同。

【举例】

Stelnet 客户端采用 128-bit 的 Suite B 算法集，与登录地址为 3.3.3.3 的远程 Stelnet 服务器建立连接，采用如下连接策略：指定客户端证书的 PKI 域名称为 clientpkidomain，指定验证服务端证书的 PKI 域名称为 serverpkidomain。

```
<Sysname> ssh2 3.3.3.3 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

1.3 SSH2协议配置命令

1.3.1 display ssh2 algorithm

display ssh2 algorithm 命令用来显示设备上配置的 SSH2 协议使用的算法优先列表。

【命令】

display ssh2 algorithm

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示设备上配置的 SSH2 协议使用的算法优先列表。

```
<Sysname> display ssh2 algorithm
Key exchange algorithms: ecdh-sha2-nistp256 ecdh-sha2-nistp384 dh-group-exchange-sha1
dh-group14-sha1 dh-group1-sha1
Public key algorithms: x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 rsa dsa
Encryption algorithms: aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm aes128-cbc
3des-cbc aes256-cbc des-cbc
MAC algorithms: sha2-256 sha2-512 sha1 md5 sha1-96 md5-96
```

表1-4 display ssh2 algorithm 命令显示信息描述表

字段	描述
Key exchange algorithms	按优先级前后顺序显示当前使用的密钥交换算法列表
Public key algorithms	按优先级前后顺序显示当前使用的主机算法列表
Encryption algorithms	按优先级前后顺序显示当前使用的加密算法列表
MAC algorithms	按优先级前后顺序显示当前使用的HMAC算法列表

【相关命令】

- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

1.3.2 ssh2 algorithm cipher

ssh2 algorithm cipher 命令用来配置 SSH2 协议使用的加密算法列表。

undo ssh2 algorithm cipher 命令用来恢复缺省情况。

【命令】

```
ssh2 algorithm cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |  
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } *  
undo ssh2 algorithm cipher
```

【缺省情况】

SSH2 协议采用的缺省加密算法从高到底的优先级列表为 **aes128-ctr**、**aes192-ctr**、**aes256-ctr**、**aes128-gcm**、**aes256-gcm**、**aes128-cbc**、**3des-cbc**、**aes256-cbc** 和 **des-cbc**。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

3des-cbc: 3DES-CBC 加密算法。

aes128-cbc: 128 位 AES-CBC 加密算法。

aes128-ctr: 128 位 AES-CTR 加密算法。

aes128-gcm: 128 位 AES-GCM 加密算法。

aes192-ctr: 192 位 AES-CTR 加密算法。

aes256-cbc: 256 位 AES-CBC 加密算法。

aes256-ctr: 256 位 AES-CTR 加密算法。

aes256-gcm: 256 位 AES-GCM 加密算法。

des-cbc: DES-CBC 加密算法。

【使用指导】

当设备运行环境要求 SSH2 只能采用特定加密算法的情况下，可采用本命令将设备上的 SSH2 客户端、SSH2 服务器所能使用的加密算法限定在配置的范围。算法的配置顺序即为算法的优先级顺序。

【举例】

配置 SSH2 协议所使用的加密算法为 **aes256-cbc**。

```
<Sysname> system-view
[Sysname] ssh2 algorithm cipher aes256-cbc
```

【相关命令】

- **display ssh2 algorithm**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

1.3.3 ssh2 algorithm key-exchange

ssh2 algorithm key-exchange 命令用来配置 SSH2 协议使用的密钥交换算法列表。

undo ssh2 algorithm key-exchange 命令用来恢复缺省情况。

【命令】

```
ssh2 algorithm key-exchange { dh-group-exchange-sha1 | dh-group1-sha1 |
dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } *
undo ssh2 algorithm key-exchange
```

【缺省情况】

SSH2 协议采用的缺省密钥交换算法从高到底的优先级列表为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**、**dh-group-exchange-sha1**、**dh-group14-sha1** 和 **dh-group1-sha1**。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

dh-group-exchange-sha1: 密钥交换算法 diffie-hellman-group-exchange-sha1。

dh-group1-sha1: 密钥交换算法 diffie-hellman-group1-sha1。

dh-group14-sha1: 密钥交换算法 diffie-hellman-group14-sha1。

ecdh-sha2-nistp256: 密钥交换算法 ecdh-sha2-nistp256。

ecdh-sha2-nistp384: 密钥交换算法 ecdh-sha2-nistp384。

【使用指导】

当设备运行环境要求 SSH2 只能采用特定密钥交换算法的情况下，可采用本命令将设备上的 SSH2 客户端、SSH2 服务器所能使用的密钥交换算法限定在配置的范围。算法的配置顺序即为算法的优先级顺序。

【举例】

```
# 配置 SSH2 协议所使用的密钥交换算法为 dh-group1-sha1。
<Sysname> system-view
[Sysname] ssh2 algorithm key-exchange dh-group1-sha1
```

【相关命令】

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

1.3.4 ssh2 algorithm mac

ssh2 algorithm mac 命令用来配置 SSH2 协议使用的 HMAC 算法列表。

undo ssh2 algorithm mac 命令用来恢复缺省情况。

【命令】

```
ssh2 algorithm mac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } *  
undo ssh2 algorithm mac
```

【缺省情况】

SSH2 协议使用的缺省 HMAC 算法从高到底的优先级列表为 **sha2-256**、**sha2-512**、**sha1**、**md5**、**sha1-96** 和 **md5-96**。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

md5: HMAC 算法 HMAC-MD5。
md5-96: HMAC 算法 HMAC-MD5-96。
sha1: HMAC 算法 HMAC-SHA1。
sha1-96: HMAC 算法 HMAC-SHA1-96。
sha2-256: HMAC 算法 HMAC-SHA2-256。
sha2-512: HMAC 算法 HMAC-SHA2-512。

【使用指导】

当设备运行环境要求 SSH2 只能采用特定 HMAC 算法的情况下，可采用本命令将设备上的 SSH2 客户端、SSH2 服务器所能使用的 HMAC 算法限定在配置的范围。算法的配置顺序即为算法的优先级顺序。

【举例】

```
# 配置 SSH2 协议所使用的 HMAC 算法为 md5。  
<Sysname> system-view  
[Sysname] ssh2 algorithm mac md5
```

【相关命令】

- **display ssh2 algorithm**

- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm public-key**

1.3.5 ssh2 algorithm public-key

ssh2 algorithm public-key 命令用来配置 SSH2 协议使用的主机签名算法列表。

undo ssh2 algorithm public-key 命令用来恢复缺省情况。

【命令】

```
ssh2 algorithm public-key { dsa | ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384
| rsa | x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } *
undo ssh2 algorithm public-key
```

【缺省情况】

SSH2 协议使用的缺省主机签名算法从高到底的优先级列表为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**、**ecdsa-sha2-nistp256**、**ecdsa-sha2-nistp384**、**rsa** 和 **dsa**。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

dsa: 公钥算法为 DSA。

ecdsa-sha2-nistp256: 指定公钥长度为 256 的 ECDSA 算法。

ecdsa-sha2-nistp384: 指定公钥长度为 384 的 ECDSA 算法。

rsa: 公钥算法为 RSA。

x509v3-ecdsa-sha2-nistp256: x509v3-ecdsa-sha2-nistp256 公钥算法。

x509v3-ecdsa-sha2-nistp384: x509v3-ecdsa-sha2-nistp384 公钥算法。

【使用指导】

当设备运行环境要求 SSH2 只能采用特定主机签名算法的情况下，可采用本命令将设备上的 SSH2 客户端、SSH2 服务器所能使用的主机签名算法限定在配置的范围。算法的配置顺序即为算法的优先级顺序。

【举例】

配置 SSH2 协议所使用的主机签名算法为 **dsa**。

```
<Sysname> system-view
```

```
[Sysname] ssh2 algorithm public-key dsa
```

【相关命令】

- **display ssh2 algorithm**

- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**

目 录

1 SSL	1-1
1.1 SSL配置命令	1-1
1.1.1 certificate-chain-sending enable	1-1
1.1.2 ciphersuite	1-1
1.1.3 client-verify	1-4
1.1.4 display ssl client-policy	1-5
1.1.5 display ssl server-policy	1-6
1.1.6 pki-domain (SSL client policy view)	1-7
1.1.7 pki-domain (SSL server policy view)	1-8
1.1.8 prefer-cipher	1-9
1.1.9 server-verify enable	1-11
1.1.10 session	1-12
1.1.11 ssl client-policy	1-13
1.1.12 ssl renegotiation disable	1-14
1.1.13 ssl server-policy	1-14
1.1.14 ssl version disable	1-15
1.1.15 version	1-16
1.1.16 version disable	1-17

1 SSL

1.1 SSL配置命令

1.1.1 certificate-chain-sending enable

certificate-chain-sending enable 命令用来配置 SSL 协商时 SSL 服务器端发送完整的证书链。

undo certificate-chain-sending enable 命令用来恢复缺省情况。

【命令】

```
certificate-chain-sending enable
undo certificate-chain-sending enable
```

【缺省情况】

SSL 协商时，SSL 服务器端只发送本地证书，不发送证书链。

【视图】

SSL 服务器端策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

仅当 SSL 客户端没有完整的证书链对服务器端的数字证书进行验证时，请通过本命令要求 SSL 服务器端在握手协商时向对端发送完整的证书链，以保证 SSL 会话的正常建立。否则，建议关闭此功能，减轻协商阶段的网络开销。

【举例】

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] certificate-chain-sending enable
```

1.1.2 ciphersuite

ciphersuite 命令用来配置 SSL 服务器端策略支持的加密套件。

undo ciphersuite 命令用来恢复缺省情况。

【命令】

```
ciphersuite {  dhe_rsa_aes_128_cbc_sha  |  dhe_rsa_aes_128_cbc_sha256  |
dhe_rsa_aes_256_cbc_sha                |  dhe_rsa_aes_256_cbc_sha256  |
ecdhe_ecdsa_aes_128_cbc_sha256         |  ecdhe_ecdsa_aes_128_gcm_sha256  |
ecdhe_ecdsa_aes_256_cbc_sha384         |  ecdhe_ecdsa_aes_256_gcm_sha384  |
ecdhe_rsa_aes_128_cbc_sha256           |  ecdhe_rsa_aes_128_gcm_sha256   |
```

```

ecdhe_rsa_aes_256_cbc_sha384      |      ecdhe_rsa_aes_256_gcm_sha384      |
exp_rsa_des_cbc_sha      |      exp_rsa_rc2_md5      |      exp_rsa_rc4_md5      |
rsa_3des_edc_cbc_sha      |      rsa_aes_128_cbc_sha      |      rsa_aes_128_cbc_sha256      |
rsa_aes_256_cbc_sha      |      rsa_aes_256_cbc_sha256      |      rsa_des_cbc_sha      |
rsa_rc4_128_md5      |      rsa_rc4_128_sha      } *
undo ciphersuite

```

【缺省情况】

SSL 服务器端策略支持所有的加密套件。

【视图】

SSL 服务器端策略视图

【缺省用户角色】

```

network-admin
context-admin

```

【参数】

dhe_rsa_aes_128_cbc_sha: 密钥交换算法采用 DHE RSA、数据加密算法采用 128 位的 AES、MAC 算法采用 SHA。

dhe_rsa_aes_128_cbc_sha256: 密钥交换算法采用 DHE RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

dhe_rsa_aes_256_cbc_sha: 密钥交换算法采用 DHE RSA、数据加密算法采用 256 位的 AES、MAC 算法采用 SHA。

dhe_rsa_aes_256_cbc_sha256: 密钥交换算法采用 DHE RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_128_cbc_sha256: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_128_gcm_sha256: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 128 位的 AES_GCM、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_256_cbc_sha384: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA384。

ecdhe_ecdsa_aes_256_gcm_sha384: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 256 位的 AES_GCM、MAC 算法采用 SHA384。

ecdhe_rsa_aes_128_cbc_sha256: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_rsa_aes_128_gcm_sha256: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 128 位的 AES_GCM、MAC 算法采用 SHA256。

ecdhe_rsa_aes_256_cbc_sha384: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA384。

ecdhe_rsa_aes_256_gcm_sha384: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 256 位的 AES_GCM、MAC 算法采用 SHA384。

exp_rsa_des_cbc_sha: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

exp_rsa_rc2_md5: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 RC2、MAC 算法采用 MD5。

exp_rsa_rc4_md5: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 RC4、MAC 算法采用 MD5。

rsa_3des_ede_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 3DES_EDE_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 128 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha256: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

rsa_aes_256_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 256 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_256_cbc_sha256: 密钥交换算法采用 RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA256。

rsa_des_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

rsa_rc4_128_md5: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 MD5。

rsa_rc4_128_sha: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 SHA。

【使用指导】

为了提高安全性，SSL 协议采用了如下算法：

- 数据加密算法：用来对传输的数据进行加密，以保证数据传输的私密性。常用的数据加密算法通常为对称密钥算法，如 DES_CBC、3DES_EDE_CBC、AES_CBC、RC4 等。使用对称密钥算法时，要求 SSL 服务器端和 SSL 客户端具有相同的密钥。
- MAC（Message Authentication Code，消息验证码）算法：用来计算数据的 MAC 值，以防止发送的数据被篡改。常用的 MAC 算法有 MD5、SHA 等。使用 MAC 算法时，要求 SSL 服务器端和 SSL 客户端具有相同的密钥。
- 密钥交换算法：用来实现密钥交换，以保证对称密钥算法、MAC 算法中使用的密钥在 SSL 服务器端和 SSL 客户端之间安全地传递。常用的密钥交换算法通常为非对称密钥算法，如 RSA。

通过本命令可以配置 SSL 服务器端策略支持的各种算法组合。例如，**rsa_des_cbc_sha** 表示 SSL 服务器端策略支持的密钥交换算法为 RSA、数据加密算法为 DES_CBC、MAC 算法为 SHA。

SSL 服务器接收到 SSL 客户端发送的客户端加密套件后，将服务器支持的加密套件与 SSL 客户端支持的加密套件比较。如果 SSL 服务器支持的加密套件中存在 SSL 客户端支持的加密套件，则加密套件协商成功；否则，加密套件协商失败。

执行本命令时，一次最多可以指定 11 个加密套件。如果多次执行本命令，那么 SSL 服务器端策略支持的加密套件是指定的加密套件的合集。

【举例】

指定 SSL 服务器端策略支持如下加密套件：

- 密钥交换算法为 DHE RSA、数据加密算法为 128 位的 AES、MAC 算法为 SHA
- 密钥交换算法为 RSA、数据加密算法为 128 位的 AES、MAC 算法为 SHA

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite dhe_rsa_aes_128_cbc_sha
rsa_aes_128_cbc_sha
```

【相关命令】

- **display ssl server-policy**
- **prefer-cipher**

1.1.3 client-verify

client-verify 命令用来配置 SSL 服务器端对 SSL 客户端的身份验证方案。

undo client-verify 命令用来恢复缺省情况。

【命令】

```
client-verify { enable | optional }
undo client-verify [ enable ]
```

【缺省情况】

SSL 服务器端不对 SSL 客户端进行基于数字证书的身份验证。

【视图】

SSL 服务器端策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

enable: 表示 SSL 服务器端要求对 SSL 客户端进行基于数字证书的身份验证。

optional: 表示 SSL 服务器端不强制要求对 SSL 客户端进行基于数字证书的身份验证，即身份验证可选。

【使用指导】

SSL 通过数字证书实现对对端的身份进行验证。数字证书的详细介绍，请参见“安全配置指导”中的“PKI”。

设备作为 SSL 服务器端，支持灵活的 SSL 客户端认证方案，具体如下：

- 执行了 **client-verify enable** 命令的情况下，则 SSL 客户端必须将自己的数字证书提供给服务器，以便服务器对客户端进行基于数字证书的身份验证。只有身份验证通过后，SSL 客户端才能访问 SSL 服务器。
- 执行了 **client-verify optional** 命令的情况下，若 SSL 客户端未提供数字证书给服务器，SSL 客户端也能访问 SSL 服务器；若 SSL 客户端提供数字证书给服务器，只有身份验证通过后，SSL 客户端才能访问 SSL 服务器。

- 执行了 **undo client-verify [enable]** 命令的情况下，SSL 服务器端不要求 SSL 客户端提供数字证书，也不会对其进行基于数字证书的身份验证，SSL 客户端可以直接访问 SSL 服务器。

SSL 服务器端在基于数字证书对 SSL 客户端进行身份验证时，除了对 SSL 客户端发送的证书链进行验证，还要检查证书链中的除根 CA 证书外的每个证书是否均未被吊销。

【举例】

配置 SSL 服务器端要求对 SSL 客户端进行基于数字证书的身份验证。

```
<Sysname> system-view
```

```
[Sysname] ssl server-policy policy1
```

```
[Sysname-ssl-server-policy-policy1] client-verify enable
```

配置 SSL 服务器端对 SSL 客户端进行基于数字证书的身份验证是可选的。

```
<Sysname> system-view
```

```
[Sysname] ssl server-policy policy1
```

```
[Sysname-ssl-server-policy-policy1] client-verify optional
```

配置 SSL 服务器端不要求对 SSL 客户端进行基于数字证书的身份验证。

```
<Sysname> system-view
```

```
[Sysname] ssl server-policy policy1
```

```
[Sysname-ssl-server-policy-policy1] undo client-verify
```

【相关命令】

- **display ssl server-policy**

1.1.4 display ssl client-policy

display ssl client-policy 命令用来显示 SSL 客户端策略的信息。

【命令】

```
display ssl client-policy [ policy-name ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

policy-name: 显示指定的 SSL 客户端策略的信息，为 1~31 个字符的字符串，不区分大小写。如果不指定本参数，则显示所有 SSL 客户端策略的信息。

【举例】

显示名为 policy1 的 SSL 客户端策略的信息。

```
<Sysname> display ssl client-policy policy1
```

```
SSL client policy: policy1
```

```

SSL version: SSL 3.0
PKI domain: client-domain
Preferred ciphersuite:
    RSA_AES_128_CBC_SHA
Server-verify: enabled

```

表1-1 display ssl client-policy 命令显示信息描述表

字段	描述
SSL client policy	SSL客户端策略名
SSL version	SSL客户端策略使用的SSL协议版本： • SSL3.0。 • TLS1.0 • TLS1.1 • TLS1.2
PKI domain	SSL客户端策略使用的PKI域
Preferred ciphersuite	SSL客户端策略支持的加密套件
Server-verify	SSL客户端策略的服务器端验证模式，取值包括： • disabled：不要求对 SSL 服务器进行基于数字证书的身份验证 • enabled：要求对 SSL 服务器进行基于数字证书的身份验证

1.1.5 display ssl server-policy

display ssl server-policy 命令用来显示 SSL 服务器端策略的信息。

【命令】

display ssl server-policy [*policy-name*]

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

policy-name：显示指定的 SSL 服务器端策略的信息，为 1～31 个字符的字符串，不区分大小写。如果不指定本参数，则显示所有 SSL 服务器端策略的信息。

【举例】

```

# 显示名为 policy1 的 SSL 服务器端策略的信息。
<Sysname> display ssl server-policy policy1
SSL server policy: policy1

```

```

Version info:
    SSL3.0: Disabled
    TLS1.0: Enabled
    TLS1.1: Disabled
    TLS1.2: Enabled
PKI domain: server-domain
Ciphersuites:
    DHE_RSA_AES_128_CBC_SHA
    RSA_AES_128_CBC_SHA
Session cache size: 600
Caching timeout: 3600 seconds
Client-verify: Enabled

```

表1-2 display ssl server-policy 命令显示信息描述表

字段	描述
SSL server policy	SSL服务器端策略名
Version info	SSL服务器端实际使用的版本： • SSL3.0 • TLS1.0 • TLS1.1 • TLS1.2 SSL服务器端是否允许使用版本： • Enabled: 允许使用 • Disabled: 不允许使用
PKI domain	SSL服务器端策略使用的PKI域
Ciphersuites	SSL服务器端策略支持的加密套件
Session cache size	SSL服务器端可以缓存的最大会话数目
Caching timeout	SSL服务器端会话缓存超时时间（单位为秒）
Client-verify	SSL服务器端策略的客户端验证模式，取值包括： • Disabled: 不要求对客户端进行基于数字证书的身份验证 • Enabled: 要求对客户端进行基于数字证书的身份验证 • Optional: SSL 服务器端对 SSL 客户端进行基于数字证书的身份验证是可选的

1.1.6 pki-domain (SSL client policy view)

pki-domain 命令用来配置 SSL 客户端策略所使用的 PKI 域。

undo pki-domain 命令用来恢复缺省情况。

【命令】

pki-domain *domain-name*

undo pki-domain

【缺省情况】

未指定 SSL 客户端策略所使用的 PKI 域。

【视图】

SSL 客户端策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain-name: PKI 域的域名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

如果通过本命令指定了 SSL 客户端策略使用的 PKI 域，则引用该客户端策略的 SSL 客户端将通过该 PKI 域获取客户端的数字证书。

【举例】

```
# 配置 SSL 客户端策略所使用的 PKI 域为 client-domain。  
<Sysname> system-view  
[Sysname] ssl client-policy policy1  
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

【相关命令】

- **display ssl client-policy**
- **pki domain**（安全命令参考/PKI）

1.1.7 pki-domain (SSL server policy view)

pki-domain 命令用来配置 SSL 服务器端策略所使用的 PKI 域。

undo pki-domain 命令用来恢复缺省情况。

【命令】

pki-domain *domain-name*

undo pki-domain

【缺省情况】

未指定 SSL 服务器端策略所使用的 PKI 域。

【视图】

SSL 服务器端策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain-name: PKI 域的域名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

如果通过本命令指定了 SSL 服务器端策略使用的 PKI 域，则引用该服务器端策略的 SSL 服务器将通过该 PKI 域获取服务器端的数字证书。

【举例】

```
# 配置 SSL 服务器端策略所使用的 PKI 域为 server-domain。
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

【相关命令】

- **display ssl server-policy**
- **pki domain**（安全命令参考/PKI）

1.1.8 prefer-cipher

prefer-cipher 命令用来配置 SSL 客户端策略支持的加密套件。

undo prefer-cipher 命令用来恢复缺省情况。

【命令】

```
prefer-cipher { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_128_cbc_sha256 |  
dhe_rsa_aes_256_cbc_sha | dhe_rsa_aes_256_cbc_sha256 |  
ecdhe_ecdsa_aes_128_cbc_sha256 | ecdhe_ecdsa_aes_128_gcm_sha256 |  
ecdhe_ecdsa_aes_256_cbc_sha384 | ecdhe_ecdsa_aes_256_gcm_sha384 |  
ecdhe_rsa_aes_128_cbc_sha256 | ecdhe_rsa_aes_128_gcm_sha256 |  
ecdhe_rsa_aes_256_cbc_sha384 | ecdhe_rsa_aes_256_gcm_sha384 |  
exp_rsa_des_cbc_sha | exp_rsa_rc2_md5 | exp_rsa_rc4_md5 |  
rsa_3des_edc_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_128_cbc_sha256 |  
rsa_aes_256_cbc_sha | rsa_aes_256_cbc_sha256 | rsa_des_cbc_sha |  
rsa_rc4_128_md5 | rsa_rc4_128_sha } *  
undo prefer-cipher
```

【缺省情况】

SSL 客户端策略支持的加密套件为 **dhe_rsa_aes_128_cbc_sha** 、
dhe_rsa_aes_256_cbc_sha 、 **rsa_3des_edc_cbc_sha** 、 **rsa_aes_128_cbc_sha** 、
rsa_aes_256_cbc_sha。

【视图】

SSL 客户端策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

dhe_rsa_aes_128_cbc_sha: 密钥交换算法采用 DHE RSA、数据加密算法采用 128 位的 AES、MAC 算法采用 SHA。

dhe_rsa_aes_128_cbc_sha256: 密钥交换算法采用 DHE RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

dhe_rsa_aes_256_cbc_sha: 密钥交换算法采用 DHE RSA、数据加密算法采用 256 位的 AES、MAC 算法采用 SHA。

dhe_rsa_aes_256_cbc_sha256: 密钥交换算法采用 DHE RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_128_cbc_sha256: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_128_gcm_sha256: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 128 位的 AES_GCM、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_256_cbc_sha384: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA384。

ecdhe_ecdsa_aes_256_gcm_sha384: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 256 位的 AES_GCM、MAC 算法采用 SHA384。

ecdhe_rsa_aes_128_cbc_sha256: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_rsa_aes_128_gcm_sha256: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 128 位的 AES_GCM、MAC 算法采用 SHA256。

ecdhe_rsa_aes_256_cbc_sha384: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA384。

ecdhe_rsa_aes_256_gcm_sha384: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 256 位的 AES_GCM、MAC 算法采用 SHA384。

exp_rsa_des_cbc_sha: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

exp_rsa_rc2_md5: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 RC2、MAC 算法采用 MD5。

exp_rsa_rc4_md5: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 RC4、MAC 算法采用 MD5。

rsa_3des_ede_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 3DES_EDE_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 128 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha256: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

rsa_aes_256_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 256 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_256_cbc_sha256: 密钥交换算法采用 RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA256。

rsa_des_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

rsa_rc4_128_md5: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 MD5。

rsa_rc4_128_sha: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 SHA。

【使用指导】

为了提高安全性，SSL 协议采用了如下算法：

- **数据加密算法：**用来对传输的数据进行加密，以保证数据传输的私密性。常用的数据加密算法通常为对称密钥算法。使用对称密钥算法时，要求 SSL 服务器端和 SSL 客户端具有相同的密钥。
- **MAC（Message Authentication Code，消息验证码）算法：**用来计算数据的 MAC 值，以防止发送的数据被篡改。常用的 MAC 算法有 MD5、SHA 等。使用 MAC 算法时，要求 SSL 服务器端和 SSL 客户端具有相同的密钥。
- **密钥交换算法：**用来实现密钥交换，以保证对称密钥算法、MAC 算法中使用的密钥在 SSL 服务器端和 SSL 客户端之间安全地传递。常用的密钥交换算法通常为非对称密钥算法，如 RSA。

通过本命令可以配置 SSL 客户端策略支持的算法组合。例如，**rsa_des_cbc_sha** 表示 SSL 客户端支持的密钥交换算法为 RSA、数据加密算法为 DES_CBC、MAC 算法为 SHA。

SSL 客户端将本端支持的加密套件发送给 SSL 服务器，SSL 服务器将自己支持的加密套件与 SSL 客户端支持的加密套件比较。如果 SSL 服务器支持的加密套件中存在 SSL 客户端支持的加密套件，则加密套件协商成功；否则，加密套件协商失败。

执行本命令时，一次最多可以指定 11 个加密套件。如果多次执行本命令，那么 SSL 客户端策略支持的加密套件是指定的加密套件的合集。

【举例】

配置 SSL 客户端策略支持的加密套件为：密钥交换算法采用 RSA、数据加密算法采用 128 位 AES_CBC、MAC 算法采用 SHA。

```
<Sysname> system-view
```

```
[Sysname] ssl client-policy policy1
```

```
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

【相关命令】

- **ciphersuite**
- **display ssl client-policy**

1.1.9 server-verify enable

server-verify enable 命令用来配置对服务器端进行基于数字证书的身份验证。

undo server-verify enable 命令用取消对服务器端进行基于数字证书的身份验证，默认 SSL 服务器身份合法。

【命令】

```
server-verify enable
undo server-verify enable
```

【缺省情况】

SSL 客户端需要对 SSL 服务器端进行基于数字证书的身份验证。

【视图】

SSL 客户端策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

SSL 通过数字证书实现对对端的身份进行验证。数字证书的详细介绍，请参见“安全配置指导”中的“PKI”。

如果执行了 **server-verify enable** 命令，则 SSL 服务器端需要将自己的数字证书提供给客户端，以便客户端对服务器端进行基于数字证书的身份验证。只有身份验证通过后，SSL 客户端才会访问该 SSL 服务器。

【举例】

```
# 配置 SSL 客户端需要对 SSL 服务器端进行基于数字证书的身份验证。
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] server-verify enable
```

【相关命令】

- **display ssl client-policy**

1.1.10 session

session 命令用来配置 SSL 服务器上缓存的最大会话数目和 SSL 会话缓存的超时时间。

undo session 命令用来恢复缺省情况。

【命令】

```
session { cachesize size | timeout time } *
undo session { cachesize | timeout } *
```

【缺省情况】

SSL 服务器上缓存的最大会话数目为 500 个，SSL 会话缓存的超时时间为 3600 秒。

【视图】

SSL 服务器端策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

cache size *size*: 指定 SSL 服务器上缓存的最大会话数目。*size* 为缓存的最大会话数目，取值范围为 100~20480。

timeout *time*: 指定 SSL 会话缓存的超时时间。*time* 为会话缓存超时时间，取值范围为 1~4294967295，单位为秒。

【使用指导】

通过 SSL 握手协议协商会话参数并建立会话的过程比较复杂。为了简化 SSL 握手过程，SSL 允许重用已经协商出的会话参数建立会话。为此，SSL 服务器上需要保存已有的会话信息。保存的会话信息的数目和保存时间具有一定的限制：

- 如果缓存的会话数目达到最大值，SSL 将拒绝缓存新协商出的会话。
- 会话保存的时间超过设定的时间后，SSL 将删除该会话的信息。

【举例】

配置 SSL 服务器上缓存的最大会话数目为 600 个，SSL 会话缓存超时时间为 1800 秒。

```
<Sysname> system-view
```

```
[Sysname] ssl server-policy policy1
```

```
[Sysname-ssl-server-policy-policy1] session cache size 600 timeout 1800
```

【相关命令】

- **display ssl server-policy**

1.1.11 ssl client-policy

ssl client-policy 命令用来创建 SSL 客户端策略，并进入 SSL 客户端策略视图。如果指定的 SSL 客户端策略已经存在，则直接进入 SSL 客户端策略视图。

undo ssl client-policy 命令用来删除指定的 SSL 客户端策略。

【命令】

```
ssl client-policy policy-name
```

```
undo ssl client-policy policy-name
```

【缺省情况】

不存在 SSL 客户端策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: SSL 客户端策略名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

SSL 客户端策略视图下可以配置 SSL 客户端启动时使用的 SSL 参数，如使用的 PKI 域、支持的加密套件等。只有与应用层协议，如 DDNS（Dynamic Domain Name System，动态域名系统），关联后，SSL 客户端策略才能生效。

【举例】

```
# 创建 SSL 客户端策略 policy1，并进入 SSL 客户端策略视图。  
<Sysname> system-view  
[Sysname] ssl client-policy policy1  
[Sysname-ssl-client-policy-policy1]
```

【相关命令】

- **display ssl client-policy**

1.1.12 ssl renegotiation disable

ssl renegotiation disable 命令用来关闭 SSL 重协商。

undo ssl renegotiation disable 命令用来恢复缺省情况。

【命令】

```
ssl renegotiation disable  
undo ssl renegotiation disable
```

【缺省情况】

允许 SSL 重协商。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

关闭 SSL 重协商是指，不允许复用已有的 SSL 会话进行 SSL 快速协商，每次 SSL 协商必须进行完整的 SSL 握手过程。关闭 SSL 重协商会导致系统付出更多的计算开销，但可以避免潜在的风险，安全性更高。

通常情况下，不建议关闭 SSL 重协商。本命令仅用于用户明确要求关闭重协商的场景。

【举例】

```
# 关闭 SSL 重协商。  
<Sysname> system-view  
[Sysname] ssl renegotiation disable
```

1.1.13 ssl server-policy

ssl server-policy 命令用来创建 SSL 服务器端策略，并进入 SSL 服务器端策略视图。如果指定的 SSL 服务器端策略已经存在，则直接进入 SSL 服务器端策略视图。

undo ssl server-policy 命令用来删除指定的 SSL 服务器端策略。

【命令】

```
ssl server-policy policy-name  
undo ssl server-policy policy-name
```

【缺省情况】

不存在 SSL 服务器端策略。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: SSL 服务器端策略名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

SSL 服务器端策略视图下可以配置 SSL 服务器启动时使用的 SSL 参数，如使用的 PKI 域、支持的加密套件等。只有与 HTTPS 等应用关联后，SSL 服务器端策略才能生效。

【举例】

```
# 创建 SSL 服务器端策略 policy1，并进入 SSL 服务器端策略视图。  
<Sysname> system-view  
[Sysname] ssl server-policy policy1  
[Sysname-ssl-server-policy-policy1]
```

【相关命令】

- **display ssl server-policy**

1.1.14 ssl version disable

ssl version disable 命令用来禁止 SSL 服务器使用指定的 SSL 版本进行 SSL 协商。

undo ssl version disable 命令用来恢复缺省情况。

【命令】

```
ssl version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 } * disable  
undo ssl version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 } * disable
```

【缺省情况】

SSL 服务器允许使用 SSL3.0、TLS1.0、TLS1.1 和 TLS1.2 版本进行协商。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ssl3.0: SSL 协商的版本为 SSL3.0。

tls1.0: SSL 协商的版本为 TLS1.0。

tls1.1: SSL 协商的版本为 TLS1.1。

tls1.2: SSL 协商的版本为 TLS1.2。

【使用指导】

当对系统安全性有较高要求时可以禁止服务器端策略使用指定版本进行协商。

通过本命令禁止 SSL 服务器使用的 SSL 版本时，请至少允许 SSL 服务器使用一个 SSL 版本进行协商。

同时配置本命令和 SSL 服务器端策略视图下的 **version disable** 命令时，系统视图的配置对所有 SSL 服务器端策略都有效，而 SSL 服务器端策略内的配置只对当前 SSL 服务器端策略有效。对于一个 SSL 服务器端策略来说，优先采用该 SSL 服务器端策略内的配置，只有该 SSL 服务器端策略内未进行配置时，才采用全局的配置。

需要注意的是，如果通过本命令关闭了指定版本的 SSL 协商功能，并不会同时关闭比其更低版本的 SSL 协商功能，例如，**ssl version tls1.1 disable** 命令仅表示关闭了 TLS1.1 版本的 SSL 协商功能，不会同时关闭 TLS1.0 版本。

【举例】

关闭 TLS1.0。

```
<Sysname> system-view
```

```
[Sysname] ssl version tls1.0 disable
```

【相关命令】

- **version disable**

1.1.15 version

version 命令用来配置 SSL 客户端策略使用的 SSL 协议版本。

undo version 命令恢复缺省情况。

【命令】

```
version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 }
```

```
undo version
```

【缺省情况】

SSL 客户端策略使用的 SSL 协议版本为 TLS 1.0。

【视图】

SSL 客户端策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ssl3.0: SSL 客户端策略使用的 SSL 协议版本为 SSL3.0。
tls1.0: SSL 客户端策略使用的 SSL 协议版本为 TLS1.0。
tls1.1: SSL 客户端策略使用的 SSL 协议版本为 TLS1.1。
tls1.2: SSL 客户端策略使用的 SSL 协议版本为 TLS1.2。

【使用指导】

对安全性要求较高的环境下，建议为不要为 SSL 客户端指定 SSL3.0 版本。
多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 配置 SSL 客户端策略使用的 SSL 协议版本为 TLS 1.0。
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] version tls1.0
```

【相关命令】

- **display ssl client-policy**

1.1.16 version disable

version disable 命令用来禁止 SSL 服务器使用指定的 SSL 版本进行 SSL 协商。
undo version disable 命令用来恢复缺省情况。

【命令】

```
version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 } * disable  
undo version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 } * disable
```

【缺省情况】

SSL 服务器采用的 SSL 协商版本与全局采用的 SSL 协商版本一致。

【视图】

SSL 服务器端策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

ssl3.0: SSL 协商的版本为 SSL3.0。
tls1.0: SSL 协商的版本为 TLS1.0。
tls1.1: SSL 协商的版本为 TLS1.1。
tls1.2: SSL 协商的版本为 TLS1.2。

【使用指导】

当用户需要灵活控制 SSL 服务器支持的 SSL 版本时，可以在 SSL 服务端策略视图下执行本命令禁止 SSL 服务器使用指定版本进行协商。

通过本命令禁止 SSL 服务器使用的 SSL 版本时，请至少允许 SSL 服务器使用一个 SSL 版本进行协商。

同时配置本命令和系统视图下的 **ssl version disable** 命令时，系统视图的配置对所有 SSL 服务器端策略都有效，而 SSL 服务器端策略内的配置只对当前 SSL 服务器端策略有效。对于一个 SSL 服务器端策略来说，优先采用该 SSL 服务器端策略内的配置，只有该 SSL 服务器端策略内未进行配置时，才采用全局的配置。

如果通过本命令关闭了指定版本的 SSL 协商功能，并不会同时关闭比其更低版本的 SSL 协商功能，例如，**version tls1.0 disable** 命令仅表示关闭了 TLS1.0 版本的 SSL 协商功能，不会同时关闭其他 SSL 版本。

【举例】

配置 SSL 服务端策略禁止使用 TLS 1.0。

```
<Sysname> system-view
```

```
[Sysname] ssl server-policy policy1
```

```
[Sysname-ssl-server-policy-policy1] version tls1.0 disable
```

【相关命令】

- **ssl version disable**

目 录

1 ASPF	1-1
1.1 ASPF配置命令	1-1
1.1.1 aspf apply policy	1-1
1.1.2 aspf icmp-error reply	1-2
1.1.3 aspf log sending-realtime enable	1-2
1.1.4 aspf policy	1-3
1.1.5 detect	1-4
1.1.6 display aspf all	1-6
1.1.7 display aspf policy	1-7
1.1.8 display aspf session	1-8
1.1.9 icmp-error drop	1-11
1.1.10 reset aspf session	1-12
1.1.11 tcp syn-check	1-12

1 ASPF

1.1 ASPF配置命令

1.1.1 aspf apply policy

aspf apply policy 命令用来在安全域间实例上应用 ASPF 策略。

undo aspf apply policy 命令用来取消应用在安全域间实例上的指定 ASPF 策略。

【命令】

```
aspf apply policy aspf-policy-number
undo aspf apply policy aspf-policy-number
```

【缺省情况】

安全域间实例上应用了一个缺省的 ASPF 策略。

【视图】

安全域间实例视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

aspf-policy-number: ASPF 策略号，取值范围为 1~256。

【使用指导】

创建安全域间实例时，系统默认为该实例应用一个缺省的 ASPF 策略。该策略支持对所有传输层协议和 FTP 协议报文进行 ASPF 检测，但是 ICMP 差错报文检查功能和非 SYN 的 TCP 首报文丢弃功能处于关闭状态，并且默认的策略不可改变，如果需要调整 ASPF 策略，需要自定义一个 ASPF 策略，并在安全域间实例上引用。

多次执行本命令，最后一次执行的命令生效。

【举例】

在安全域间实例上应用 ASPF 策略。

```
<Sysname> system-view
[Sysname] security-zone name trust
[Sysname-security-zone-Trust] import interface gigabitethernet 1/0/1
[Sysname-security-zone-Trust] quit
[Sysname] security-zone name untrust
[Sysname-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Sysname-security-zone-Untrust] quit
[Sysname] zone-pair security source trust destination untrust
[Sysname-zone-pair-security-Trust-Untrust] aspf apply policy 1
```

【相关命令】

- **aspf policy**
- **display aspf all**
- **zone-pair security**（安全命令参考/安全域）

1.1.2 aspf icmp-error reply

aspf icmp-error reply 命令用来开启设备在域间策略丢包时，发送 ICMP 差错报文功能。
undo aspf icmp-error reply 命令用来恢复缺省情况。

【命令】

aspf icmp-error reply
undo aspf icmp-error reply

【缺省情况】

在域间策略丢包时，设备不发送 ICMP 差错报文。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

缺省情况下，设备在安全域间实例下配置安全域间策略，丢弃不符合策略的报文，但不发送 ICMP 差错报文，这样可以减少网络上的无用报文，节约带宽。

使用 **traceroute** 功能时，需要用到 ICMP 差错报文，需要开启发送 ICMP 差错报文的功能。

【举例】

```
# 开启设备在域间策略丢包时，发送 ICMP 差错报文功能。  
<Sysname> system-view  
[Sysname] aspf icmp-error reply
```

1.1.3 aspf log sending-realtime enable

aspf log sending-realtime enable 命令用来开启日志的实时发送功能。
undo aspf log sending-realtime enable 命令用来关闭日志的实时发送功能。

【命令】

aspf log sending-realtime enable
undo aspf log sending-realtime enable

【缺省情况】

日志的实时发送功能处于关闭状态，使用缓存方式发送。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

日志实时发送功能仅对安全策略和包过滤模块的日志发送有效。

日志的发送方式支持如下两种：

- 缓存发送方式：同一数据流的首报文匹配相关策略生成并发送日志后，设备缓存此日志，同时启动发送日志的时间间隔定时器，只有时间间隔到达后，才会判断是否继续发送此日志。在此时间间隔内若有流量匹配此日志，则发送日志，若没有则删除缓存的此日志。日志缓存数目达到上限后，续新增数据流匹配相关策略时不能生成日志。日志发送时间间隔缺省为 5 分钟，且不能修改。
- 实时发送方式：同一数据流的首报文匹配相关策略生成并发送日志后，设备不缓存此日志，因此这种方式无日志数目的限制。对于一条不间断的流量，若匹配的策略允许报文通过，则设备仅发送一次日志，若匹配的策略拒绝报文通过，则设备将对此条数据流的每个报文均发送一次日志。

有关安全策略和包过滤开启记录日志功能的详细介绍，请参见各自模块的相关配置介绍。

【举例】

开启日志的实时发送功能。

```
<Sysname> system-view
```

```
[Sysname] aspf log sending-realtime enable
```

【相关命令】

- **logging enable**（安全命令参考/安全策略）
- **rule rule-id logging**（ACL 命令参考/ACL）

1.1.4 aspf policy

aspf policy 命令用来创建 ASPF 策略，并进入 ASPF 策略视图。如果指定的 ASPF 策略已经存在，则直接进入 ASPF 策略视图。

undo aspf policy 命令用来删除指定的 ASPF 策略。

【命令】

```
aspf policy aspf-policy-number
```

```
undo aspf policy aspf-policy-number
```

【缺省情况】

不存在 ASPF 策略。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

aspf-policy-number: ASPF 策略号，取值范围为 1~256。

【举例】

创建 ASPF 策略 1，并进入该 ASPF 策略视图。

```
<Sysname> system-view  
[Sysname] aspf policy 1  
[Sysname-aspf-policy-1]
```

【相关命令】

- **display aspf all**
- **display aspf policy**

1.1.5 detect

detect 命令用来为应用层协议配置 ASPF 检测。

undo detect 命令用来恢复缺省情况。

【命令】

```
detect { dns [ action { drop | logging } * ] | { ftp | h323 | http | sccp |  
sip | smtp } [ action drop ] | gtp | ils | mgcp | nbt | pptp | rsh | rtsp | sqlnet  
| tftp | xdmcp }  
undo detect { dns | ftp | gtp | h323 | http | ils | mgcp | nbt | pptp | rsh  
| rtsp | sccp | sip | smtp | sqlnet | tftp | xdmcp }
```

【缺省情况】

对传输层协议和应用层协议 FTP 进行 ASPF 检测。

【视图】

ASPF 策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

dns: 表示 DNS 协议，属于应用层协议。

ftp: 表示 FTP 协议，属于应用层协议。

gtp: 表示 GTP（GPRS Tunneling Protocol，GPRS 隧道协议）协议，属于应用层协议。

h323: 表示 H.323 协议族，属于应用层协议。

http: 表示 HTTP 协议，属于应用层协议。

ils: 表示 ILS（Internet Locator Service，互联网定位服务）协议，属于应用层协议。

mgcp: 表示 MGCP（Media Gateway Control Protocol，媒体网关控制协议）协议，属于应用层协议。

nbt: 表示 NBT（NetBIOS over TCP/IP，基于 TCP/IP 的网络基本输入输出系统）协议，属于应用层协议。

pptp: 表示 PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议）协议，属于应用层协议。

rsh: 表示 RSH（Remote Shell，远程外壳）协议，属于应用层协议。

rtsp: 表示 RTSP（Real Time Streaming Protocol，实时流协议）协议，属于应用层协议。

sccp: 表示 SCCP（Skinny Client Control Protocol，瘦小客户端控制协议）协议，属于应用层协议。

sip: 表示 SIP（Session Initiation Protocol，会话初始化协议）协议，属于应用层协议。

smtp: 表示 SMTP 协议，属于应用层协议。

sqlnet: 表示 SQLNET 协议，属于应用层协议。

tftp: 表示 TFTP 协议，属于应用层协议。

xmcp: 表示 XDMCP（X Display Manager Control Protocol，X 显示监控）协议，属于应用层协议。

action: 设置对检测到的非法报文的处理行为。若不指定该参数，则表示放行报文。

drop: 表示丢弃报文。

logging: 表示生成日志信息。

【使用指导】

若配置了此命令，则对报文的应用层协议进行 ASPF 检查；若没有配置此命令，则仅对报文的传输层协议进行 ASPF 检查。

如果设备上其他业务模块开启 ALG 功能时，即便未配置多通道应用层协议的 ASPF 检测，多通道协议的数据连接也可以建立成功。例如：开启 DPI 相关业务功能时会打开 ALG 功能，此时 DPI 处理的多通道协议（如 SIP 等）报文进行 ASPF 处理时，即便未配置 SIP 协议的 ASPF 检测，SIP 协议的数据连接也可以建立成功。但是在设备上未配置 DPI（Deep Packet Inspection，深度报文检测）相关业务功能只配置了 ASPF 功能的情况下，必须配置此命令，否则会导致数据连接无法建立。此命令支持的应用层协议中除 HTTP、SMTP 和 TFTP 之外的所有应用层协议均为多通道应用层协议。

可通过多次执行本命令配置多种协议类型的 ASPF 检测。

ASPF 策略默认已经开启对传输层协议的检测，无需进行配置，也不能修改。检测的传输层协议包括：TCP 协议、UDP 协议、UDP-Lite 协议、SCTP 协议、Raw IP 协议、ICMP 协议、ICMPv6 协议和 DCCP 协议。

ASPF 策略可以根据需要配置应用层协议的检测。目前，设备对支持 **action** 参数的应用层协议（DNS、FTP、H323、HTTP、SCCP、SIP、SMTP）进行协议状态合法性检查，对不符合协议状态的报文根据 **action** 参数的配置进行丢弃处理。对于其它应用层协议，仅进行连接状态信息的维护，不做协议状态合法性检查。

【举例】

配置对 FTP 协议报文进行 ASPF 检测。

```
<Sysname> system-view
[Sysname] aspf policy 1
```



```
[Sysname-aspf-policy-1] detect ftp
# 配置对 DNS 协议进行应用层协议检测，丢弃不符合协议状态的报文，并生成日志信息。
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1] detect dns action drop logging
```

【相关命令】

- **display aspf policy**

1.1.6 display aspf all

display aspf all 命令用来查看 ASPF 策略配置信息及应用 ASPF 策略的信息。

【命令】

```
display aspf all
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 查看所有的 ASPF 策略配置信息。
<Sysname> display aspf all
ASPF policy configuration:
  Policy default:
    ICMP error message check: Disabled
    TCP SYN packet check: Disabled
    Inspected protocol      Action
    FTP                     None
  Policy number: 1
    ICMP error message check: Disabled
    TCP SYN packet check: Disabled
    Inspected protocol      Action
    FTP                     None

Zone-pair security application:
  Source Trust destination Untrust
  Apply ASPF policy: default
```

表1-1 display aspf all 命令显示信息描述表

字段	描述
ASPF policy configuration	ASPF策略的配置信息

字段	描述
Policy default	缺省ASPF策略
Policy number	ASPF策略号
ICMP error message check	ICMP差错报文检测功能的开启状态
TCP SYN packet check	非SYN的TCP首报文丢弃功能的开启状态
Inspected protocol	需要检测的应用层协议
Action	对检测到的非法协议报文的处理行为 • Drop: 丢弃 • Log: 生成日志信息 • None: 不做处理, 放行 “-”表示该协议不支持此配置项
Zone-pair security application	安全域间实例
Source XXX destination XXX	安全域间实例中的源安全域和目的安全域
Apply ASPF policy	在安全域间实例上应用的ASPF策略编号

【相关命令】

- **aspf apply policy**
- **aspf policy**
- **display aspf policy**

1.1.7 display aspf policy

display aspf policy 命令用来查看 ASPF 策略的配置信息。

【命令】

display aspf policy { *aspf-policy-number* | default }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

aspf-policy-number: ASPF 策略号, 取值范围为 1~256。

default: 缺省 ASPF 策略。

【举例】

查看策略号为 1 的 ASPF 策略的配置信息。

```
<Sysname> display aspf policy 1
ASPF policy configuration:
  Policy number: 1
    ICMP error message check: Disabled
    TCP SYN packet check: Enabled
  Inspected protocol  Action
    FTP                Drop
    HTTP               None
    RSH                -
```

表1-2 display aspf policy 命令显示信息描述表

字段	描述
ASPF policy configuration	ASPF策略的配置信息
Policy number	ASPF策略号
ICMP error message check	ICMP差错报文检测功能的开启状态
TCP SYN packet check	非SYN的TCP首报文丢弃功能的开启状态
Inspected protocol	需要检测的应用层协议
Action	对检测到的非法报文的处理行为 - Drop: 丢弃 - Log: 生成日志信息 - None: 不做处理，放行 “-”表示该协议不支持此配置项

【相关命令】

- aspf policy

1.1.8 display aspf session

display aspf session 命令用来查看 ASPF 的会话表信息。

【命令】

```
display aspf session [ ipv4 | ipv6 ] [ slot slot-number ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

ipv4: 查看 ASPF 创建的 IPv4 会话表。

ipv6: 查看 ASPF 创建的 IPv6 会话表。

slot slot-number: 显示指定成员设备上的 ASPF 会话表, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 显示所有成员设备上的 ASPF 会话表。

verbose: 查看 ASPF 会话表的详细信息。若不指定该参数, 则表示查看 ASPF 会话表的概要信息。

【使用指导】

不指定 **ipv4** 和 **ipv6** 参数时, 表示查看所有的 ASPF 会话表信息。

【举例】

显示 ASPF 创建的 IPv4 会话表的概要信息。

```
<Sysname> display aspf session ipv4
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Initiator:
  Source      IP/port: 192.168.1.18/1792
  Destination IP/port: 192.168.1.55/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
```

Total sessions found: 2

显示 IPv4 ASPF 会话的详细信息。

```
<Sysname> display aspf session ipv4 verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
  Source security zone: SrcZone
Responder:
  Source      IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.18/1877
  DS-Lite tunnel peer: -
```

```

VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/2
Source security zone: DestZone
State: TCP_SYN_SENT
Application: SSH
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:          1 packets          48 bytes
Responder->Initiator:          0 packets          0 bytes

Initiator:
Source      IP/port: 192.168.1.18/1792
Destination IP/port: 192.168.1.55/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet1/0/1
Source security zone: SrcZone
Responder:
Source      IP/port: 192.168.1.55/1792
Destination IP/port: 192.168.1.18/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet1/0/2
Source security zone: DestZone
State: ICMP_REQUEST
Application: OTHER
Start time: 2011-07-29 19:12:33  TTL: 55s
Initiator->Responder:          1 packets          6048 bytes
Responder->Initiator:          0 packets          0 bytes

Total sessions found: 2

```

表1-3 display aspf session 命令显示信息描述表

字段	描述
Initiator	发起方到响应方的连接对应的会话信息
Responder	响应方到发起方的连接对应的会话信息
Source IP/port	源IP地址/端口号
Destination IP/port	目的IP地址/端口号
DS-Lite tunnel peer	DS-Lite隧道对端地址。会话不属于任何DS-Lite隧道时，本字段显示为“-”
VPN-instance/VLAN ID/Inline ID	会话所属的MPLS L3VPN/二层转发时会话所属的VLAN ID/二层转发时会话所属的INLINE。未指定的参数则显示为“-”

字段	描述
Protocol	传输层协议类型，取值包括：DCCP、ICMP、ICMPv6、Raw IP、SCTP、TCP、UDP、UDP-Lite 括号中的数字表示协议号
Inbound interface	报文的入接口
Source security zone	源安全域，即入接口所属的安全域。若接口不属于任何安全域，则显示为“-”
State	会话的协议状态
Application	应用层协议类型，取值包括：FTP、DNS等，OTHER表示未知协议类型，其对应的端口为非知名端口
Start time	会话的创建时间
TTL	会话剩余存活时间，单位为秒
Initiator->Responder	发起方到响应方的报文数、报文字节数
Responder->Initiator	响应方到发起方的报文数、报文字节数
Total sessions found	当前查找到的会话总数

【相关命令】

- **reset aspf session**

1.1.9 icmp-error drop

icmp-error drop 命令用来开启 ICMP 差错报文检测功能。

undo icmp-error drop 命令用来关闭 ICMP 差错报文检测功能。

【命令】

icmp-error drop

undo icmp-error drop

【缺省情况】

ICMP 差错报文检测功能处于关闭状态。

【视图】

ASPF 策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

正常 ICMP 差错报文中均携带有本报文对应连接的相关信息，根据这些信息可以匹配到相应的连接。如果匹配失败，则根据当前配置决定是否丢弃该 ICMP 报文。

【举例】

```
# 设置 ASPF 策略 1 丢弃非法的 ICMP 差错报文。
<Sysname> system-view
[Sysname] aspf policy 1
[Sysname-aspf-policy-1] icmp-error drop
```

【相关命令】

- **aspf policy**
- **display aspf policy**

1.1.10 reset aspf session

reset aspf session 命令用来删除 ASPF 的会话表项。

【命令】

```
reset aspf session [ ipv4 | ipv6 ] [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ipv4: 删除 ASPF 创建的 IPv4 会话表项。

ipv6: 删除 ASPF 创建的 IPv6 会话表项。

slot slot-number: 删除指定成员设备上的所有 ASPF 创建的会话表项, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 删除所有成员设备上的所有 ASPF 创建的会话表项。

【使用指导】

如果不指定 **ipv4** 和 **ipv6** 参数, 则表示删除 ASPF 创建的所有会话表项。

【举例】

```
# 清除 ASPF 创建的所有会话表项。
<Sysname> reset aspf session
```

【相关命令】

- **display aspf session**

1.1.11 tcp syn-check

tcp syn-check 命令用来开启非 SYN 的 TCP 首报文丢弃功能。

undo tcp syn-check 命令用来关闭非 SYN 的 TCP 首报文丢弃功能。

【命令】

```
tcp syn-check
undo tcp syn-check
```

【缺省情况】

非 SYN 的 TCP 首报文丢弃功能处于关闭状态。

【视图】

ASPF 策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

ASPF 对 TCP 连接的首报文进行检测，查看是否为 SYN 报文，如果不是 SYN 报文则根据当前配置决定是否丢弃该报文。

当设备首次加入网络时，网络中原有 TCP 连接的非首包在经过新加入的设备时如果被丢弃，会中断已有的连接，造成不好的用户体验，因此建议暂且不丢弃非 SYN 首包，等待网络拓扑稳定后，再开启非 SYN 首包丢弃功能。

【举例】

设置 ASPF 策略 1 丢弃非 SYN 的 TCP 首报文。

```
<Sysname> system-view
```

```
[Sysname] aspf policy 1
```

```
[Sysname-aspf-policy-1] tcp syn-check
```

【相关命令】

- **aspf policy**

目 录

1 APR.....	1-1
1.1 APR配置命令	1-1
1.1.1 app-group	1-1
1.1.2 application statistics enable	1-1
1.1.3 apr set detectlen.....	1-3
1.1.4 apr signature auto-update.....	1-3
1.1.5 apr signature auto-update-now	1-4
1.1.6 apr signature rollback	1-5
1.1.7 apr signature update	1-5
1.1.8 copy app-group	1-7
1.1.9 description (application group view)	1-8
1.1.10 description (NBAR view).....	1-9
1.1.11 destination.....	1-9
1.1.12 detection	1-10
1.1.13 direction.....	1-11
1.1.14 disable.....	1-12
1.1.15 display app-group	1-13
1.1.16 display application.....	1-14
1.1.17 display application statistics	1-17
1.1.18 display application statistics top.....	1-19
1.1.19 display apr signature library.....	1-21
1.1.20 display port-mapping pre-defined.....	1-22
1.1.21 display port-mapping user-defined	1-23
1.1.22 include application.....	1-24
1.1.23 nbar application	1-25
1.1.24 override-current	1-26
1.1.25 port-mapping.....	1-26
1.1.26 port-mapping acl.....	1-28
1.1.27 port-mapping host	1-29
1.1.28 port-mapping subnet.....	1-30
1.1.29 reset application statistics	1-32
1.1.30 risk	1-32
1.1.31 service-port.....	1-33

1.1.32 signature	1-34
1.1.33 source	1-35
1.1.34 update schedule	1-36
1.1.35 user-defined-application	1-37

1 APR

1.1 APR配置命令

1.1.1 app-group

app-group 命令用来创建应用组，并进入应用组视图。如果指定的应用组已经存在，则直接进入应用组视图。

undo app-group 命令用来删除指定的应用组。

【命令】

app-group *group-name*

undo app-group *group-name*

【缺省情况】

不存在应用组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name: 应用组的名称，为 1~63 个字符的字符串，不区分大小写，不允许为系统保留的“invalid”或“other”。

【使用指导】

系统中最多可以定义 1000 个应用组。

【举例】

创建名称为 **aaa** 的应用组，并进入应用组视图。

```
<Sysname> system-view
```

```
[Sysname] app-group aaa
```

```
[Sysname-app-group-aaa]
```

【相关命令】

- **copy app-group**
- **description**
- **include application**

1.1.2 application statistics enable

application statistics enable 命令用来开启接口指定方向上的应用统计功能。

undo application statistics enable 命令用来关闭接口指定方向上的应用统计功能。

【命令】

```
application statistics enable [ inbound | outbound ]  
undo application statistics enable [ inbound | outbound ]
```

【缺省情况】

接口入方向和出方向上的应用统计功能处于关闭状态。

【视图】

二层接口视图/三层接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

inbound: 在接口的入方向上开启应用统计功能。

outbound: 在接口的出方向上开启应用统计功能。

【使用指导】

如果不指定任何参数，则表示同时开启接口出方向和入方向上的应用统计功能。

在接口上开启应用统计功能之后，设备能够对接口上收到或者发送的报文数目、速率按照应用协议分别进行统计，生成的统计信息可以通过 **display application statistics** 命令查看。

接口的应用统计功能会消耗大量系统内存。当系统出现内存告警时，请关闭接口的应用统计功能。

【举例】

在接口 GigabitEthernet1/0/1 上开启入方向应用统计功能。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] application statistics enable inbound
```

在接口 GigabitEthernet1/0/2 上开启出方向应用统计功能。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/2  
[Sysname-GigabitEthernet1/0/2] application statistics enable outbound
```

在接口 GigabitEthernet1/0/3 上开启所有方向应用统计功能。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/3  
[Sysname-GigabitEthernet1/0/3] application statistics enable
```

在接口 Vlan-interface 2 上开启入方向应用统计功能。

```
<Sysname> system-view  
[Sysname] interface Vlan-interface 2  
[Sysname-Vlan-interface2] application statistics enable inbound
```

【相关命令】

- **display application statistics**

1.1.3 apr set detectlen

apr set detectlen 命令用来配置 NBAR 规则的最大检测字节数。

undo apr set detectlen 命令用来恢复缺省情况。

【命令】

apr set detectlen bytes

undo apr set detectlen

【缺省情况】

未配置 NBAR 规则的最大检测字节数。

【视图】

NBAR 规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

bytes: 表示 NBAR 规则的最大检测长度，取值范围为 0~4294967295，单位为字节。

【使用指导】

当设备识别出应用时，若不配置最大检测字节数，设备将继续检测后续报文是否存在应用，这将对设备的性能产生影响；若配置最大检测字节数，设备将从识别出应用的位置开始，判断当前已检测的字节长度是否超出配置的最大检测字节数，若超出，则后续不进行检测，若未超出，则继续检测后续报文。请管理员根据设备的实际情况配置此参数。

多次执行本命令，最后一次执行的命令生效。

【举例】

为 NBAR 规则 abcd 配置最大检测字节数为 100000。

```
<Sysname> system-view
```

```
[Sysname] nbar application abcd protocol http
```

```
[Sysname-nbar-application-abcd] apr set detectlen 100000
```

【相关命令】

- **nbar application**

1.1.4 apr signature auto-update

apr signature auto-update 命令用来开启定期自动在线升级 APR 特征库功能，并进入自动升级配置视图。

undo apr signature auto-update 命令用来关闭定期自动在线升级 APR 特征库功能。

【命令】

apr signature auto-update

undo apr signature auto-update

【缺省情况】

定期自动在线升级 APR 特征库功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果设备可以访问官方网站上的特征库服务专区，可以采用定期自动在线升级方式来对设备上的 APR 特征库进行升级。

【举例】

开启定期自动在线升级 APR 特征库功能，并进入自动升级配置视图。

```
<Sysname> system-view
[Sysname] apr signature auto-update
[Sysname-apr-autoupdate]
```

【相关命令】

- **override-current**
- **update schedule**

1.1.5 apr signature auto-update-now

apr signature auto-update-now 命令用来立即自动在线升级 APR 特征库。

【命令】

apr signature auto-update-now

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

执行此命令后，将立即自动在线升级设备上的 APR 特征库，且会备份当前的 APR 特征库文件。此命令的生效与否，与是否开启了定期自动在线升级 APR 特征库功能无关。

当管理员发现官方网站上的特征库服务专区中的 APR 特征有更新时，可以选择立即自动在线升级方式来及时升级 APR 特征库版本。

【举例】

立即自动升级 APR 特征库。

```
<Sysname> system-view
[Sysname] apr signature auto-update-now
```

1.1.6 apr signature rollback

apr signature rollback 命令用来回滚 APR 特征库版本。

【命令】

apr signature rollback { factory | last }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

factory: 表示把 APR 特征库回滚到出厂版本。

last: 表示把 APR 特征库回滚到上一版本。

【使用指导】

设备使用当前 APR 特征库版本进行识别应用时，如果管理员发现设备识别应用的误报率较高或出现异常情况，则可以对当前 APR 特征库版本进行回滚。

APR 特征库版本每次回滚前，设备都会备份当前版本。多次回滚上一版本将会在当前版本和上一版本之间反复切换。例如当前 APR 特征库版本是 V2，上一版本是 V1，第一次执行回滚到上一版本的操作后，特征库替换成 V1 版本，再执行回滚到上一版本的操作则特征库重新变为 V2 版本。

升级 APR 特征库时，如果没有备份当前特征库文件，则回滚 APR 特征库到上一版本会失败。

【举例】

配置 APR 特征库回滚到上一版本。

```
<Sysname> system-view
```

```
[Sysname] apr signature rollback last
```

1.1.7 apr signature update

apr signature update 命令用来手动离线升级 APR 特征库。

【命令】

apr signature update [override-current] file-path

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

override-current: 表示覆盖当前版本的特征库文件。如果不指定本参数，则表示当前特征库在升级之后作为备份特征库保存在设备上。

file-path: 指定特征库文件的路径，为 1~255 个字符的字符串。

【使用指导】

如果设备不能访问官方网站上的特征库服务专区，管理员可以采用如下几种方式手动离线升级 APR 特征库版本。

- 本地升级：使用本地保存的特征库文件升级系统上的 APR 特征库版本。
- FTP/TFTP 升级：通过 FTP 或 TFTP 方式下载远程服务器上保存的特征库文件，并升级系统上的 APR 特征库版本。

使用本地升级方式离线升级 APR 特征库版本时，特征库文件只能存储在当前主用设备上，否则设备升级特征库会失败。

参数 *file-path* 的取值与手动离线升级的操作方式有关。本地升级时参数 *file-path* 取值请参见 [表 1-1](#)；FTP/TFTP 升级时参数 *file-path* 取值请参见 [表 1-2](#)。

表1-1 本地升级时参数 *file-path* 取值说明表

升级场景	参数 <i>file-path</i> 取值	说明
特征库文件的存储位置与当前工作路径一致	<i>filename</i>	可以执行 pwd 命令查看当前工作路径 有关 pwd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不一致，且在相同存储介质上	<i>filename</i>	需要先执行 cd 命令将工作路径切换至特征库文件所在目录下 有关 cd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不在相同存储介质上	<i>path/ filename</i>	需要先执行 cd 命令将工作路径切换至特征库文件所在存储介质的根目录下，再指定特征库文件的相对路径 有关 cd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”

表1-2 FTP/TFTP 升级时参数 *file-path* 取值说明表

升级场景	参数 <i>file-path</i> 取值	说明
特征库文件存储在开启 FTP 服务的远程服务器上	<i>ftp://username:password@server/filename</i>	<i>username</i> 为登录 FTP 服务器的用户名， <i>password</i> 为登录 FTP 服务器的密码， <i>server</i> 为 FTP 服务器的 IP 地址或主机名 当 FTP 的用户名和密码中使用了“.”、“@”和“/”三种特殊字符时，需要将这三种特殊字符替换为其对应的转义字符。“.”、“@”和“/”三种特殊字符对应的转义字符分别为“%3A”或“%3a”、“%40”和“%2F”或“%2f”
特征库文件存储在开启 TFTP 服务的远程服务器上	<i>tftp://server/filename</i>	<i>server</i> 为 TFTP 服务器的 IP 地址或主机名



说明

当采用 FTP/TFTP 方式升级特征库时，如果指定的是服务器的主机名，则需要确保设备能通过静态或动态域名解析方式获得 FTP/TFTP 服务器的 IP 地址，并与之路由可达。否则设备升级特征库会失败。有关域名解析功能的详细配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

【举例】

配置手动离线升级 APR 特征库，且采用 TFTP 方式，APR 特征库文件的远程路径为 tftp://192.168.0.10/apr-1.0.2-en.dat。

```
<Sysname> system-view
[Sysname] apr signature update tftp://192.168.0.10/apr-1.0.2-en.dat
```

配置手动离线升级 APR 特征库，且采用 FTP 方式，APR 特征库文件的远程路径为 ftp://192.168.0.10/apr-1.0.2-en.dat，用户名为 user:123，密码为 user@abc/123。

```
<Sysname> system-view
[Sysname] apr signature update
ftp://user%3A123:user%40abc%2F123@192.168.0.10/apr-1.0.2-en.dat
```

配置手动离线升级 APR 特征库，且采用本地方式，APR 特征库文件的本地路径为 cfa0:/apr-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> system-view
[Sysname] apr signature update apr-1.0.23-en.dat
```

配置手动离线升级 APR 特征库，且采用本地方式，APR 特征库文件的本地路径为 cfa0:/dpi/apr-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> cd dpi
<Sysname> system-view
[Sysname] apr signature update apr-1.0.23-en.dat
```

配置手动离线升级 APR 特征库，且采用本地方式，APR 特征库文件的本地路径为 cfb0:/dpi/apr-1.0.23-en.dat，当前工作路径为 cfa0:。

```
<Sysname> cd cfb0:/
<Sysname> system-view
[Sysname] apr signature update dpi/apr-1.0.23-en.dat
```

1.1.8 copy app-group

copy app-group 命令用来在应用组中复制另一个应用组中的所有应用。

【命令】

copy app-group group-name

【视图】

应用组视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name: 要复制应用组的名称，为 1~63 个字符的字符串，不区分大小写，不允许为系统保留的 “invalid” 和 “other”。

【使用指导】

可多次执行本命令复制多个应用组里的应用。

【举例】

在应用组 abc 中复制应用组 bcd 中的所有应用。

```
<Sysname> system-view
[Sysname] app-group abc
[Sysname-app-group-abc] copy app-group bcd
```

【相关命令】

- **app-group**
- **include application**

1.1.9 description (application group view)

description 命令用来配置自定义应用组的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

自定义应用组的描述信息为 “User-defined application group”。

【视图】

应用组视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

text: 应用组的描述信息，为 1~127 个字符的字符串，区分大小写，当有空格时，必须用双引号把所有字符串引起来。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别该应用组的作用，有利于后期维护。

【举例】

配置名称为 aaa 的自定义应用组描述信息为 “User defined aaa group”。

```
<Sysname> system-view
[Sysname] app-group aaa
[Sysname-app-group-aaa] description "User defined aaa group"
```

【相关命令】

- **app-group**

1.1.10 description (NBAR view)

description 命令用来配置自定义 NBAR 规则的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

自定义 NBAR 规则的描述信息为 “User defined application”。

【视图】

NBAR 规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: NBAR 规则的描述信息，为 1~127 个字符的字符串，区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别本条 NBAR 规则的作用，有利于后期维护。

【举例】

配置自定义 NBAR 规则 abcd 的描述信息为 “A user-defined application based on HTTP”。

```
<Sysname> system-view
```

```
[Sysname] nbar application abcd protocol http
```

```
[Sysname-nbar-application-abcd] description "A user-defined application based on HTTP"
```

【相关命令】

- **nbar application**

1.1.11 destination

destination 命令用来配置自定义 NBAR 规则匹配的目的 IP 地址网段。

undo destination 命令用来恢复缺省情况。

【命令】

destination ip *ipv4-address* [*mask-length*]

undo destination

【缺省情况】

NBAR 规则匹配所有目的 IP 地址网段。

【视图】

NBAR 规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip ipv4-address: 指定匹配的目的 IPv4 地址或网段，为点分十进制格式。

mask-length: 子网掩码长度，取值范围为 0~32。如果未指定本参数，则默认子网掩码长度为 32。

【使用指导】

在同一个 NBAR 规则视图下多次执行本命令，最后一次执行的命令生效。

【举例】

配置 NBAR 规则 abcd 匹配的目的 IP 地址网段为 192.168.1.0/24。

```
<Sysname> system-view
```

```
[Sysname] nbar application abcd protocol http
```

```
[Sysname-nbar-application-abcd] destination ip 192.168.1.0 24
```

【相关命令】

- **nbar application**

1.1.12 detection

detection 命令用来配置自定义 NBAR 规则特征的检查项。

undo detection 命令用来删除自定义 NBAR 规则特征的检查项。

【命令】

```
detection detection-id field field-name match-type { exclude | include }  
{ hex hex-vector | regex regex-pattern | text text-string } [ offset  
offset-value [ depth depth-value ] | relative-offset relative-offset-value  
[ relative-depth relative-depth-value ] ]
```

```
undo detection { all | detection-id }
```

【缺省情况】

未配置自定义 NBAR 规则特征的检查项。

【视图】

NBAR 规则特征视图

【缺省用户角色】

network-admin

context-admin

【参数】

detection-id: 表示检查项的 ID，取值范围为 1~255。

field *field-name*: 表示在指定的协议域中匹配检查项, *field-name* 表示协议域名称, 取值范围为 1~31 个字符, 区分大小写, 可通过输入 “?” 获取支持的协议域。

match-type { **exclude** | **include** }: 表示检查项和检查内容的匹配方式。

- **exclude**: 不包含。
- **include**: 包含。

hex *hex-vector*: 指定匹配检查项的 16 进制向量。取值范围为 8~256 个字符的字符串, 且字符个数必须为偶数, 输入参数必须在两个竖杠 (|) 之间, 例如|123456|。

regex *regex-pattern*: 指定匹配检查项的正则表达式, 为 3~253 个字符的字符串, 支持所有可输入字符, 区分大小写。

text *text-string*: 指定匹配检查项的字符串, 为 3~256 个字符的字符串, 支持所有可输入字符, 区分大小写。

offset *offset-value*: 表示检查项的绝对偏移量, 设备将在协议域起始位置偏移指定字节后的内容中去匹配检查项, *offset-value* 表示字节偏移量, 取值范围为 0~65535, 单位为字节。如果未指定本参数, 将从协议域起始位置后的所有内容中去匹配检查项。

depth *depth-value*: 表示检查项的检测深度, 取值范围为 3~65535, 单位为字节。

relative-offset *relative-offset-value*: 表示检查项之间的相对偏移量, 取值范围为 -32767~32767, 单位为字节。如果取值为负数, 则表示指定的检查项在上一个检查项之前。

relative-depth *relative-depth-value*: 表示检查项之间的相对深度, 取值范围为 3~65535, 单位为字节。

【使用指导】

一个 NBAR 规则特征下可以配多个检查项, 检查项之间为逻辑与的关系, 匹配顺序为配置顺序, 仅当特征的所有检查项均匹配成功时, 该特征才可以匹配成功。配置检查项匹配的协议字段时, 建议依据 HTTP 协议中各头域顺序进行配置, 否则可能会影响设备的检测结果。

【举例】

在名为 app_http 的自定义 NBAR 规则中, 配置编号为 1 的检查项, 检测的协议域为 http-uri、检测内容为文本 abc、偏移量为 10 字节、检测深度为 50 字节。

```
<Sysname> system-view
[Sysname] nbar application app_ protocol http
[Sysname-nbar-application-app_http] signature 1 filed uri string abcdefg
[Sysname-nbar-application-signature-app_http-1] detection 1 field uri match-type include text
abc offset 10 depth 50
```

1.1.13 direction

direction 命令用来配置 NBAR 规则的匹配方向。

undo direction 命令用来恢复缺省情况。

【命令】

```
direction { to-client | to-server }
undo direction
```

【缺省情况】

NBAR 规则的匹配方向是双向的。

【视图】

NBAR 规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

to-client: 表示对 Server 访问 Client 的流量进行基于 NBAR 规则的应用识别。

to-server: 表示对 Client 访问 Server 的流量进行基于 NBAR 规则的应用识别。

【使用指导】

在同一个 NBAR 规则视图下多次执行本命令，最后一次执行的命令生效。

【举例】

配置 NBAR 规则 abcd 的匹配方向为 Client 访问 Server。

```
<Sysname> system-view
```

```
[Sysname] nbar application abcd protocol http
```

```
[Sysname-nbar-application-abcd] direction to-server
```

【相关命令】

- **nbar application**

1.1.14 disable

disable 命令用来禁用自定义 NBAR 规则。

undo disable 命令用来恢复缺省情况。

【命令】

disable

undo disable

【缺省情况】

自定义 NBAR 规则处于生效状态。

【视图】

NBAR 规则视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

当在某些网络环境中，如果一些 NBAR 规则暂时不会被用到，而且又不想将其从设备上删除时，可以执行本命令来禁用这些规则。

【举例】

```
# 禁用自定义 NBAR 规则 abcd。
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd] disable
```

【相关命令】

- **nbar application**

1.1.15 display app-group

display app-group 命令用来显示应用组信息。

【命令】

```
display app-group [ name group-name ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

name group-name: 显示指定名称的应用组信息。*group-name* 表示应用组的名称，为 1~63 个字符的字符串，不区分大小写，不允许为系统保留的“invalid”和“other”。

【使用指导】

若不指定任何参数，则表示显示所有应用组信息。

【举例】

```
# 显示系统所有应用组的信息。
<Sysname> display app-group
User-defined count:3
Group Name                Type                Group ID
6767                      User-defined       0x00800002
er                         User-defined       0x00800001
hbc                       User-defined       0x00800003
# 显示自定义应用组名称为 er 的应用组的信息。
<Sysname> display app-group name er
Group English name: er
Group Chinese name: er
Group ID:                0x00800001
Type:                    User-defined

Application count: 2
```

```
Include application list:
Application name      Type      App ID
114Travel            Pre-defined  0x0000542c
banc                 User-defined 0x00800001
```

```
pre-defined app-group count:0
Include pre-defined app-group list:
App-group name      Type      App-group ID
```

表1-3 display app-group 命令显示信息描述表

字段	描述
User-defined count	自定义应用组的个数
Group Name	自定义应用组的名称
Group English name	应用组的英文名称
Group Chinese name	应用组的中文名称
Group ID	应用组的ID号
Type	类型
Application count	应用组下包含的应用的个数
Include application list	包含的应用列表
Application name	应用组中添加应用名
App ID	应用组中添加应用的ID号
pre-defined app-group count	应用组中包含的预定义应用组的个数（暂不支持）
Include pre-defined app-group list	包含的预定义应用组列表（暂不支持）
App-group name	应用组中添加的预定义应用组名（暂不支持）
App-group ID	应用组中添加的预定义应用组的ID号（暂不支持）

【相关命令】

- **app-group**
- **include**

1.1.16 display application

display application 命令用来显示应用信息。

【命令】

display application [name *application-name* | **pre-defined** | **user-defined**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

name *application-name*: 显示指定名称的应用信息。*application-name* 表示应用的名称，为 1~63 个字符的字符串，不区分大小写，不允许为系统保留的“invalid”和“other”。

pre-defined: 显示系统预定义的应用列表。

user-defined: 显示用户自定义的应用列表。

【使用指导】

若不指定任何参数，则表示显示所有的应用信息。

【举例】

显示系统预定义的应用列表。

```
<Sysname> display application pre-defined  
Pre-defined count: 817
```

Application name	Type	App ID	Tunnel	Encrypted	DetectLen
12530WAP_Application_Web_HTTP	Pre-defined	0x000003ac	No	No	0
12580_Application_HTTP	Pre-defined	0x00000312	No	No	0
126_Web_Email_Download_HTTP	Pre-defined	0x000002b7	No	No	0
126_Web_Email_Login_HTTP	Pre-defined	0x000002b3	No	No	0
126_Web_Email_Read_Email_HTTP	Pre-defined	0x000002b4	No	No	0
126_Web_Email_Receive_Email_HTTP	Pre-defined	0x000002b6	No	No	0
126_Web_Email_Send_Email_HTTP	Pre-defined	0x000002b5	No	No	0
126_Web_Email_Upload_HTTP	Pre-defined	0x000002b8	No	No	0
139_mobile_weibo_comment_HTTP	Pre-defined	0x000001da	No	No	0
139_mobile_weibo_login_HTTP	Pre-defined	0x000001d9	No	No	0
139_mobile_weibo_login_HTTP	Pre-defined	0x00000444	No	No	0

---- More ----

显示用户自定义的应用列表。

```
<Sysname> display application user-defined  
User-defined count: 4
```

Application name	Type	App ID	Tunnel	Encrypted	DetectLen
def	User-defined	0x00800002	No	No	0
dfer	User-defined	0x00800003	No	No	0
efer	User-defined	0x00800004	No	No	0
fdfad	User-defined	0x00800001	No	No	0

显示所有应用列表。

<Sysname> display application

Total count: 821

Pre-defined count: 817

User-defined count: 4

Application name	Type	App ID	Tunnel	Encrypted	DetectLen
12530WAP_Application_Web_HTTP	Pre-defined	0x000003ac	No	No	0
12580_Application_HTTP	Pre-defined	0x00000312	No	No	0
126_Web_Email_Download_HTTP	Pre-defined	0x000002b7	No	No	0
126_Web_Email_Login_HTTP	Pre-defined	0x000002b3	No	No	0
126_Web_Email_Read_Email_HTTP	Pre-defined	0x000002b4	No	No	0
126_Web_Email_Receive_Email_HTTP	Pre-defined	0x000002b6	No	No	0
126_Web_Email_Send_Email_HTTP	Pre-defined	0x000002b5	No	No	0
126_Web_Email_Upload_HTTP	Pre-defined	0x000002b8	No	No	0
139_mobile_weibo_comment_HTTP	Pre-defined	0x000001da	No	No	0
139_mobile_weibo_login_HTTP	Pre-defined	0x000001d9	No	No	0
139_mobile_weibo_login_HTTPS	Pre-defined	0x00000444	No	No	0
139Mail_Login_HTTP	Pre-defined	0x000001cb	No	No	0
139Mail_Login_HTTPS	Pre-defined	0x0000038c	No	No	0
139Mail_Login_TCP	Pre-defined	0x0000044b	No	No	0
163TV_HTTP	Pre-defined	0x000004c3	No	No	0
17173_Application_HTTP	Pre-defined	0x00000350	No	No	0
178Game_Application_HTTP	Pre-defined	0x00000222	No	No	0
17K_fiction_Application_HTTP	Pre-defined	0x00000330	No	No	0
19lou_Login_http_stream	Pre-defined	0x000002c0	No	No	0
19lou_Publish_Or_Reply_http_stream1	Pre-defined	0x000002c2	No	No	0
19lou_Publish_Or_Reply_http_stream2	Pre-defined	0x000002c3	No	No	0

```

19lou_View_http_stream  Pre-defined  0x0000002c1  No    No    0
1ting_Music_Application Pre-defined  0x0000001bc  No    No    0
_Mobile_HTTP
21CN_Email_Read_HTTP   Pre-defined  0x0000003fb  No    No    0
21CN_Email_Send_HTTP   Pre-defined  0x0000003fc  No    No    0
---- More ----

```

显示名称为 telnet 的应用信息。

```

<Sysname> display application name telnet
Application English Name: telnet
Application Chinese Name: telnet
Application ID: 0x0000000e
Tunnel: No
Encrypted: No

```

表1-4 display application 命令显示信息描述表

字段	描述
Total count	应用总数
Pre-defined count	预定义应用总数
User-defined count	自定义应用总数
Application Name	应用名
Type	应用的类型，取值包括： - Pre-defined: 系统预定义 - User-defined: 用户自定义
App ID/Application ID	应用协议编号
Tunnel	应用是否为隧道类型（暂不支持）
Encrypted	应用是否为加密类型，例如HTTPS为一个加密类型的应用
DetectLen	检测长度，分为预定义的检测长度和自定义的检测长度
Application English Name	应用的英文名称
Application Chinese Name	应用的中文名称

【相关命令】

- app-group
- include

1.1.17 display application statistics

display application statistics 命令用来显示接口上的应用统计信息。

【命令】

```

display application statistics [ direction { inbound | outbound } | interface
interface-type interface-number [ slot slot-number ] | name
application-name ] *

```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

direction: 显示指定方向的应用统计信息。

inbound: 显示接口入方向的应用统计信息。

outbound: 显示接口出方向的应用统计信息。

interface interface-type interface-number: 显示指定接口的应用统计信息。
interface-type interface-number 表示要显示统计信息的接口类型和接口编号。

slot slot-number: 显示指定成员设备上全局接口的应用统计信息。*slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定显示全局接口（例如 VLAN 接口、Tunnel 接口）时可见。

name application-name: 显示指定名称的应用统计信息。*application-name* 表示应用的名称，为 1~63 个字符的字符串，不区分大小写，不允许为系统保留的“invalid”和“other”。

【使用指导】

如果不指定任何参数，则表示显示所有接口的应用统计信息。

只有在接口应用统计功能开启的情况下，接口才能产生相应的应用统计信息。因此，使用本命令查看接口统计信息之前，请确保接口的应用统计功能处于开启状态。

可以按应用名称、接口出方向、接口入方向、接口名称分别显示相应的应用统计信息，也可以通过指定多个参数，显示同时符合多个参数的应用统计信息。

【举例】

显示 GigabitEthernet1/0/1 接口上的所有应用统计信息。

```
<Sysname> display application statistics interface GigabitEthernet1/0/1
```

```
Interface : GigabitEthernet1/0/1
```

Application	In/Out	Packets	Bytes	PPS	BPS
Slot 1 :					
http	IN	275	78631	0	275
	OUT	357	255251	0	101
https	IN	403	39267	0	44
	OUT	681	623501	0	32
netbios-dgm	IN	3	729	0	32
	OUT	0	0	0	0
netbios-ns	IN	248	22816	2	1423
	OUT	0	0	0	0
telnet	IN	801	43374	10	4509
	OUT	1519	65388	20	6774

显示 Vlan-interface 2 接口上的所有应用统计信息。

```
<Sysname> display application statistics interface Vlan-interface 2
```

```

Interface : Vlan-interface2
Application  In/Out  Packets          Bytes          PPS          BPS
Slot 1 :
http         IN      275             78631          0            275
             OUT      357             255251         0            101
https        IN      403             39267          0            44
             OUT      681             623501         0            32
netbios-dgm  IN      3               729            0            32
             OUT      0               0              0            0
netbios-ns   IN      248             22816          2            1423
             OUT      0               0              0            0
telnet       IN      801             43374          10           4509
             OUT      1519            65388          20           6774

```

表1-5 display application statistics 命令显示信息描述表

字段	描述
Interface	接口的名称
Application	应用的名称
In/Out	入方向/出方向
Packets	接口上接收或发送的报文个数
Bytes	接口上接收或发送的字节数
PPS	每秒报文数
BPS	每秒比特数

【相关命令】

- **app-group**
- **application statistics enable**

1.1.18 display application statistics top

display application statistics top 命令用来按指定类型的统计排名显示接口应用统计信息。

【命令】

```

display application statistics top number { bps | bytes | packets | pps }
interface interface-type interface-number [ slot slot-number ]

```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin

```

context-operator

【参数】

number: 显示排名前 *number* 的应用统计信息，取值范围为 0~4294967295。

bytes: 显示接口字节数为前 *number* 的应用统计信息。

bps: 显示接口比特速率统计为前 *number* 的应用统计信息。

packets: 显示接口包数为前 *number* 的应用统计信息。

pps: 显示接口包速率统计为前 *number* 的应用统计信息。

interface interface-type interface-number: 显示指定接口的应用统计信息。
interface-type interface-number 指定要显示统计信息的接口类型和接口编号。

slot slot-number: 显示指定成员设备上全局接口的应用统计信息。*slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定显示全局接口（例如 VLAN 接口、Tunnel 接口）时可见。

【使用指导】

只有在接口应用统计功能开启的情况下，接口才能产生相应的应用统计信息。因此，使用本命令查看接口统计信息之前，请确保接口的应用统计功能处于开启状态。

系统以接口上某一个应用的出方向和入方向的统计值之和为依据对应用进行排名。统计值相同的应用，再按照应用名称的字母顺序排列。

【举例】

显示 GigabitEthernet1/0/1 接口上包数为前 3 的应用统计信息。

```
<Sysname> display application statistics top 3 packets interface gigabitethernet 1/0/1
Interface : GigabitEthernet1/0/1
Application  In/Out Packets          Bytes          PPS          BPS
Slot 1 :
telnet       IN      1389          75219          0            44
              OUT     2626          112745          0            54
https        IN      468           42830           0           123
              OUT     746           626101          0            91
netbios-ns   IN      965           88780           2           1411
              OUT      0              0              0             0
```

显示 Vlan-interface 2 接口上包数为前 3 的应用统计信息。

```
<Sysname> display application statistics top 3 packets interface Vlan-interface 2
Interface : Vlan-interface2
Application  In/Out Packets          Bytes          PPS          BPS
Slot 1 :
telnet       IN      1389          75219          0            44
              OUT     2626          112745          0            54
https        IN      468           42830           0           123
              OUT     746           626101          0            91
netbios-ns   IN      965           88780           2           1411
              OUT      0              0              0             0
```

表1-6 display application statistics top 命令显示信息描述表

字段	描述
Interface	接口的名称
Application	应用的名称
In/Out	入方向/出方向
Packets	接口上接收或发送的报文个数
Bytes	接口上接收或发送的字节数
PPS	每秒报文数
BPS	每秒比特数

【相关命令】

- **app-group**
- **application statistics enable**

1.1.19 display apr signature library

display apr signature library 命令用来显示当前 APR 特征库的版本信息。

【命令】

display apr signature library

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示当前特征库版本信息

```
<Sysname> display apr signature library
```

APR signature library information:

Type	SigVersion	ReleaseTime	Size
Current	1.0.49	Tue Sep 13 06:54:01 2016	659744
Last	1.0.52	Wed Nov 02 07:14:03 2016	702640
Factory	1.0.0	Fri Dec 31 16:00:00 1999	77040

表1-7 display apr signature library 命令显示信息描述表

字段	描述
Type	APR特征库版本，包括如下取值： • Current: 当前版本 • Last: 上一版本 • Factory: 出厂版本
SigVersion	APR特征库版本号
ReleaseTime	APR特征库发布时间
Size	APR特征库大小，单位是Bytes

1.1.20 display port-mapping pre-defined

display port-mapping pre-defined 命令用来显示预定义的端口映射信息。

【命令】

display port-mapping pre-defined

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示预定义的端口映射信息。

```
<Sysname> display port-mapping pre-defined
```

Application	Protocol	Port
afs3-kaserver	TCP	7004
	UDP	7004
aol	TCP	5190, 5191, 5192, 5193
	UDP	5190, 5191, 5192, 5193
appleqt	TCP	458
	UDP	458

表1-8 display port-mapping pre-defined 命令显示信息描述表

字段	描述
Application	进行端口映射的应用层协议
Protocol	传输层协议类型
Port	应用层协议的端口号

【相关命令】

- **display port-mapping**
- **port-mapping**

1.1.21 display port-mapping user-defined

display port-mapping user-defined 命令用来显示自定义的端口映射信息。

【命令】

display port-mapping user-defined [application *application-name* | port *port-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

application *application-name*: 显示指定端口映射的应用协议。*application-name* 表示应用协议名称, 为 1~63 个字符的字符串, 不区分大小写, 不允许为系统保留的“invalid”和“other”。该应用层协议名称必须标准且能够被设备识别。

port *port-number*: 显示指定应用层协议的端口。*port-number* 表示端口号, 取值范围为 0~65535。

【使用指导】

若不指定任何参数, 则表示显示所有的用户自定义端口映射信息。

【举例】

显示所有自定义的端口映射信息。

<Sysname> display port-mapping user-defined

Application	Port	Protocol	Match Type	Match Condition
FTP	21	TCP	---	---
FTP	21	UDP	IPv4 host	10.10.10.1(vpn1)
FTP	2121	UDP	IPv4 host	[11.10.10.1, 11.10.10.10](vpn2)
FTP	21	UDP	IPv4 subnet	10.10.10.1/24
FTP	21	SCTP	IPv6 host	2000:fdb8::1:00ab:853c:39ab
HTTP	899	TCP	IPv4 ACL	2002
HTTP	999	SCTP	IPv6 ACL	2002

表1-9 display port-mapping user-defined 命令显示信息描述表

字段	描述
Application	进行端口映射的应用层协议
Port	应用层协议映射的端口号
Protocol	传输层协议类型
Match Type	匹配方式，包括以下类型： • ---: 表示通配，即未指定匹配类型和匹配条件，所有报文都可以进行匹配 • IPv4 host: 表示基于报文的目的 IPv4 地址进行匹配 • IPv6 host: 表示基于报文的目的 IPv6 地址进行匹配 • IPv4 subnet: 表示基于报文的目的 IPv4 网段进行匹配 • IPv6 subnet: 表示基于报文的目的 IPv6 网段进行匹配 • IPv4 ACL: 表示基于 IPv4 ACL 进行匹配 • IPv6 ACL: 表示基于 IPv6 ACL 进行匹配
Match Condition	匹配条件，包括以下几种情况： • 对于 IPv4 host/IPv6 host 匹配方式，显示为主机报文的目的 IP 地址 • 对于 IPv4 subnet/IPv6 subnet 匹配方式，显示为主机报文的目的网段地址 • 对于 IPv4 ACL/IPv6 ACL 匹配方式，显示为 ACL 编号 对于host和subnet类型的端口映射配置，如果指定了主机所属的VPN，则还会显示其所属的MPLS L3VPN的VPN实例名称

1.1.22 include application

include application 命令用来在应用组中添加应用。
undo include application 命令用来在应用组中删除应用。

【命令】

include application *application-name*
undo include application *application-name*

【缺省情况】

应用组中不存在应用。

【视图】

应用组视图

【缺省用户角色】

network-admin
context-admin

【参数】

application-name: 向应用组中添加的应用的名称, 为 1~63 个字符的字符串, 不区分大小写, 不允许为系统保留的 **invalid** 或 **other**。

【使用指导】

可多次执行本命令为一个应用组中添加多个预定义应用和自定义应用, 每个组里可以包含的应用个数不限制。

向应用组中添加应用时, 如果对应的应用不存在就会创建这个应用, 但该应用的报文是否能被识别, 取决于系统中是否定义了相应的识别规则, 比如端口映射配置。

【举例】

```
# 在应用组 abc 中增加应用 HTTP 和 FTP。
<Sysname> system-view
[Sysname] app-group abc
[Sysname-app-group-abc] include application http
[Sysname-app-group-abc] include application ftp
```

【相关命令】

- **app-group**
- **copy app-group**

1.1.23 nbar application

nbar application 命令用来创建自定义 NBAR 规则, 并进入 NBAR 规则视图。如果指定的 NBAR 规则已经存在, 则直接进入 NBAR 规则视图。

undo nbar application 命令用来删除指定的自定义 NBAR 规则。

【命令】

```
nbar application application-name protocol { http | tcp | udp }
undo nbar application application-name
```

【缺省情况】

不存在自定义 NBAR 规则。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

application-name: 指定自定义 NBAR 规则的名称, 为 1~63 个字符的字符串, 不区分大小写, 不允许为系统保留的 “invalid”、“other” 和系统预定义应用的名称。

http: 表示该规则用于识别基于 HTTP 协议的报文。

tcp: 表示该规则用于识别基于 TCP 协议的报文。

udp: 表示该规则用于识别基于 UDP 协议的报文。

【使用指导】

如果 APR 特征库中预定义的应用规则不能满足用户需求，可以使用本命令自定义 NBAR 规则，以及配置该规则的属性和特征。但不能对预定义的 NBAR 规则进行删除和修改。

【举例】

```
# 创建名称为 abcd 的自定义 NBAR 规则，并指定该规则用于识别基于 HTTP 协议的报文。  
<Sysname> system-view  
[Sysname] nbar application abcd protocol http  
[Sysname-nbar-application-abcd]
```

1.1.24 override-current

override-current 命令用来配置定期自动在线升级 APR 特征库时覆盖当前的特征文件。

undo override-current 命令用来恢复缺省情况。

【命令】

```
override-current  
undo override-current
```

【缺省情况】

定期自动在线升级 APR 特征库时不会覆盖当前的特征库文件，而是同时备份当前的特征库文件。

【视图】

自动升级配置视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

可以通过开启此功能解决升级 APR 特征库时设备内存不足的问题。在设备剩余内存充裕的情况下，不建议配置该功能，因为 APR 特征库升级时，如果没有备份当前特征库文件，则不能回滚到上一版本。

【举例】

```
# 配置定期自动在线升级 APR 特征库时覆盖当前的特征文件。  
<Sysname> system-view  
[Sysname] apr signature auto-update  
[Sysname-apr-autoupdate] override-current
```

【相关命令】

- **apr signature auto-update**

1.1.25 port-mapping

port-mapping 命令用来配置通用端口映射。

undo port-mapping 命令用来删除指定的通用端口映射。

【命令】

```
port-mapping application application-name port port-number [ protocol  
protocol-name ]
```

```
undo port-mapping application application-name port port-number [ protocol  
protocol-name ]
```

【缺省情况】

各应用层协议与其对应的常用的端口号映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

application *application-name*: 指定端口映射的应用层协议。*application-name* 表示应用协议名称。为 1~63 个字符的字符串, 不区分大小写, 不允许为系统保留的“invalid”和“other”。该应用层协议名称必须标准且能够被设备识别。

port *port-number*: 指定与应用层协议映射的端口。*port-number* 表示端口号, 取值范围为 0~65535。

protocol *protocol-name*: 指定应用层协议使用的传输层协议名称, 其取值及含义如下:

- **dccp**: 表示 DCCP (Datagram Congestion Control Protocol, 数据报拥塞控制协议) 协议。
- **sctp**: 表示 SCTP (Stream Control Transmission Protocol, 流控制传输协议) 协议。
- **tcp**: 表示 TCP 协议。
- **udp**: 表示 UDP 协议。
- **udp-lite**: 表示 UDP-Lite 协议。

【使用指导】

若不指定 **protocol** 参数, 则表示所有传输层协议的指定报文均可被识别为指定应用层协议的报文。

如果报文的目的端口号与某个通用端口映射匹配, 则该报文将被识别为相应的应用层协议报文。

指定传输层协议名称的映射优先级高于不指定传输层协议名称的映射。

应用层协议名称不同, 其他参数相同时, 多次执行本命令, 最后一次执行的命令生效。

不能通过重复执行本命令来修改与应用层协议映射的端口号。如需修改端口号, 请先通过 **undo port-mapping application** 命令删除通用端口映射, 再执行 **port-mapping application** 命令。

【举例】

建立端口 3456 到 FTP 协议的通用端口映射。

```
<Sysname> system-view
```

```
[Sysname] port-mapping application ftp port 3456
```

【相关命令】

- **display port-mapping user-defined**

1.1.26 port-mapping acl

port-mapping acl 命令用来配置基于 ACL 的主机端口映射。

undo port-mapping acl 命令用来删除指定的主机端口映射。

【命令】

port-mapping application *application-name* **port** *port-number* [**protocol** *protocol-name*] **acl** [**ipv6**] *acl-number*

undo port-mapping application *application-name* **port** *port-number* [**protocol** *protocol-name*] **acl** [**ipv6**] *acl-number*

【缺省情况】

各应用层协议与其对应的常用的端口号映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

application *application-name*: 指定端口映射的应用层协议。*application-name* 表示应用层协议名称。为 1~63 个字符的字符串,不区分大小写,不允许为系统保留的“invalid”和“other”。该应用层协议名称必须标准且能够被设备识别。

port *port-number*: 指定与应用层协议映射的端口。*port-number* 表示端口号,取值范围为 0~65535。

protocol *protocol-name*: 指定应用层协议使用的传输层协议名称,其取值及含义如下:

- **dccp**: 表示 DCCP (Datagram Congestion Control Protocol, 数据报拥塞控制协议) 协议。
- **sctp**: 表示 SCTP (Stream Control Transmission Protocol, 流控制传输协议) 协议。
- **tcp**: 表示 TCP 协议。
- **udp**: 表示 UDP 协议。
- **udp-lite**: 表示 UDP-Lite 协议。

acl [**ipv6**] *acl-number*: ACL 编号,取值范围为 2000~2999。如果指定 **ipv6**,则表示 IPv6 ACL,否则表示 IPv4 ACL。即使指定的 ACL 中开启统计功能后,此 ACL 也不会统计匹配此 PBAR 的流量。

【使用指导】

若不指定 **protocol** 参数,则表示所有传输层协议的指定报文均可被识别为指定应用层协议的报文。对于匹配指定 ACL 的报文(其目的 IP 地址与 ACL 中某规则指定的源 IP 地址参数相匹配),如果报文的目的端口号与某个映射关系匹配,则该报文将被识别为对应的应用层协议报文。

应用层协议名称不同，其他参数相同时，多次执行本命令，最后一次执行的命令生效。
指定传输层协议名称的映射优先级高于不指定传输层协议名称的映射。

【举例】

为匹配 ACL 2000 的报文，建立端口 3456 到 FTP 协议的映射。

```
<Sysname> system-view
```

```
[Sysname] port-mapping application ftp port 3456 acl 2000
```

【相关命令】

- **display port-mapping user-defined**

1.1.27 port-mapping host

port-mapping host 命令用来设置基于 IP 地址的主机端口映射。

undo port-mapping host 命令用来删除指定 IP 地址的主机端口映射。

【命令】

```
port-mapping application application-name port port-number [ protocol  
protocol-name ] host { ip | ipv6 } start-ip-address [ end-ip-address ]  
[ vpn-instance vpn-instance-name ]
```

```
undo port-mapping application application-name port port-number [ protocol  
protocol-name ] host { ip | ipv6 } start-ip-address [ end-ip-address ]  
[ vpn-instance vpn-instance-name ]
```

【缺省情况】

各应用层协议与其对应的常用的端口号映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

application *application-name*: 指定端口映射的应用层协议。*application-name* 表示应用层协议名称，为 1~63 个字符的字符串，不区分大小写，不允许为系统保留的“invalid”和“other”。该应用层协议名称必须标准且能够被设备识别。

port *port-number*: 指定与应用层协议映射的端口。*port-number* 表示端口号，取值范围为 0~65535。

protocol *protocol-name*: 指定应用层协议使用的传输层协议名称，其取值及含义如下：

- **dccp**: 表示 DCCP（Datagram Congestion Control Protocol，数据报拥塞控制协议）协议。
- **sctp**: 表示 SCTP（Stream Control Transmission Protocol，流控制传输协议）协议。
- **tcp**: 表示 TCP 协议。
- **udp**: 表示 UDP 协议。
- **udp-lite**: 表示 UDP-Lite 协议。

ip: 指定基于 IPv4 地址的主机端口映射。

ipv6: 指定基于 IPv6 地址的主机端口映射。

start-ip-address [**end-ip-address**]: 表示 IPv4 地址范围或 IPv6 地址范围。**start-ip-address** 表示起始 IP 地址, **end-ip-address** 表示终止 IP 地址。如果仅配置 **start-ip-address**, 则表示单个主机; 如果同时配置 **start-ip-address** 和 **end-ip-address**, 则表示位于 **start-ip-address** 和 **end-ip-address** 范围内的所有主机, 其中的 **end-ip-address** 必须大于等于 **start-ip-address**。

vpn-instance vpn-instance-name: 表示报文所属的 VPN。**vpn-instance-name** 为 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果不指定该参数, 则表示报文属于公网。

【使用指导】

若不指定 **protocol** 参数, 则表示所有传输层协议的指定报文均可被识别为指定应用层协议的报文。对于目的地址为指定地址或指定范围的地址的报文, 如果报文的目的端口号与某个映射关系匹配, 则该报文将被识别为对应的应用层协议报文。

对于应用协议、端口号、传输层协议参数均相同的配置, 要求各配置中指定的 IP 地址或者 IP 地址范围不能重叠。

应用层协议名称不同, 其他参数相同时, 多次执行本命令, 最后一次执行的命令生效。

指定传输层协议名称的映射优先级高于不指定传输层协议名称的映射。

【举例】

为目的 IP 地址范围为 1.1.1.1~1.1.1.10 的 IPv4 报文, 建立端口 3456 到 FTP 协议的映射。

```
<Sysname> system-view
```

```
[Sysname] port-mapping application ftp port 3456 host ip 1.1.1.1 1.1.1.10
```

为目的 IP 地址为 1::1 的 IPv6 报文, 建立端口 3456 到 FTP 协议的映射。

```
<Sysname> system-view
```

```
[Sysname] port-mapping application ftp port 3456 host ipv6 1::1
```

【相关命令】

- **display port-mapping user-defined**

1.1.28 port-mapping subnet

port-mapping subnet 命令用来配置基于网段的主机端口映射。

undo port-mapping subnet 命令用来删除指定网段的主机端口映射。

【命令】

```
port-mapping application application-name port port-number [ protocol  
protocol-name ] subnet { ip ipv4-address { mask-length | mask } | ipv6  
ipv6-address prefix-length } [ vpn-instance vpn-instance-name ]
```

```
undo port-mapping application application-name port port-number [ protocol  
protocol-name ] subnet { ip ipv4-address { mask-length | mask } | ipv6  
ipv6-address prefix-length } [ vpn-instance vpn-instance-name ]
```


【缺省情况】

各应用层协议与其对应的常用的端口号映射。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

application *application-name*: 指定端口映射的应用层协议。*application-name* 表示应用层协议名称。为 1~63 个字符的字符串,不区分大小写,不允许为系统保留的“invalid”和“other”。该应用层协议名称必须标准且能够被设备识别。

port *port-number*: 指定与应用层协议映射的端口。*port-number* 表示端口号,取值范围为 0~65535。

protocol *protocol-name*: 指定应用层协议使用的传输层协议名称,其取值及含义如下:

- **dccp**: 表示 DCCP (Datagram Congestion Control Protocol, 数据报拥塞控制协议)。
- **sctp**: 表示 SCTP (Stream Control Transmission Protocol, 流控制传输协议)。
- **tcp**: 表示 TCP 协议。
- **udp**: 表示 UDP 协议。
- **udp-lite**: 表示 UDP-Lite 协议。

ip *ipv4-address* { *mask-length* | *mask* }: 指定 IPv4 网段。其中, *ipv4-address* 表示 IPv4 地址; *mask-length* 表示子网掩码长度,取值范围为 1~32; *mask* 表示子网掩码,为点分十进制格式。

ipv6 *ipv6-address* *prefix-length*: 指定 IPv6 网段。其中, *ipv6-address* 表示 IPv6 地址; *prefix-length* 表示 IPv6 前缀长度,取值范围为 1~128。

vpn-instance *vpn-instance-name*: 表示主机所属的 VPN。*vpn-instance-name* 为 MPLS L3VPN 的 VPN 实例名称,为 1~31 个字符的字符串,区分大小写。如果不指定该参数,则表示主机属于公网。

【使用指导】

若不指定 **protocol** 参数,则表示所有传输层协议的指定端口的报文均被识别为指定应用层协议的报文。

对于目的地址为指定网段的报文,如果报文的目的端口号与某个映射关系匹配,则该报文将被识别为对应的应用层协议报文。

PBAR 以最精确的网络范围对报文进行匹配,即如果配置了多条网段映射关系,且各映射关系中指定的网段范围互相包含,则使用网络范围最小的映射配置进行匹配。

应用层协议名称不同,其他参数相同时,多次执行本命令,最后一次执行的命令生效。

指定传输层协议名称的映射优先级高于不指定传输层协议名称的映射。

【举例】

为目的网段地址为 1.1.1.0/24 的 IPv4 主机报文,建立端口 3456 到 FTP 协议的映射。

```
<Sysname> system-view
[Sysname] port-mapping application ftp port 3456 subnet ip 1.1.1.0 24
# 为目的网段地址为 1::/120 的 IPv6 主机报文，建立端口 3456 到 FTP 协议的映射。
<Sysname> system-view
[Sysname] port-mapping application ftp port 3456 subnet ipv6 1:: 120
```

【相关命令】

- **display port-mapping user-defined**

1.1.29 reset application statistics

reset application statistics 命令用来清除指定接口或所有接口的应用统计信息。

【命令】

reset application statistics [**interface** *interface-type interface-number*]

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface *interface-type interface-number*：清除指定接口上的应用统计信息。
interface-type interface-number 表示接口类型和接口编号。如果不指定此参数，则表示清除所有接口上的应用统计信息。

【举例】

```
# 清除所有接口的应用统计信息。
<Sysname> reset application statistics
```

【相关命令】

- **application statistics enable**
- **display application statistics**

1.1.30 risk

risk type 命令用来配置自定义应用的风险类型。

undo risk type 命令用来删除自定义应用的风险类型。

【命令】

```
risk type risk-type
undo risk type [ risk-type ]
```

【缺省情况】

未配置自定义应用的风险类型。

【视图】

自定义应用视图

【缺省用户角色】

network-admin

context-admin

【参数】

risk-type: 表示风险类型的名称，不区分大小写，可通过输入“？”来获取支持的风险类型名称。

【使用指导】

多次执行本命令，可为一个自定义应用配置多个风险类型。所属的风险类型越多，表示该应用的风险级别越高。管理员可根据应用的风险级别配置相应的防护策略（例如安全策略），保护内网安全。在执行 **undo risk type** 命令时，如果不指定风险类型，将删除该自定义应用的所有风险类型。

【举例】

```
# 配置自定义应用 app1 的风险类型为 Tunneling 和 Misoperation.  
<sysname> system-view  
[sysname] user-defined-application app1  
[sysname-user-defined-app-app1] risk type Tunneling  
[sysname-user-defined-app-app1] risk type Misoperation
```

1.1.31 service-port

service-port 命令用来配置自定义 NBAR 规则匹配的端口号。

undo service-port 命令用来恢复缺省情况。

【命令】

```
service-port { port-num | range start-port end-port }  
undo service-port
```

【缺省情况】

NBAR 规则匹配所有端口号。

【视图】

NBAR 规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

port-num: 指定规则匹配的端口号，取值范围为 0～65535。

range: 指定规则匹配的端口号范围。

start-port: 表示起始端口号，取值范围为 0～65535。

end-port: 表示终止端口号，取值范围为 0～65535。

【使用指导】

本命令配置的端口号用来匹配报文的源端口和目的端口。首先匹配报文的目的端口，当目的端口匹配失败后，再匹配源端口，只要其中一类端口与配置的端口号匹配成功就算此报文与此条件匹配成功。

在同一个 NBAR 规则视图下多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 配置 NBAR 规则 abcd 的端口号范围为 2001~2004。
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd] service-port range 2001 2004
```

【相关命令】

- **direction**

1.1.32 signature

signature 命令用来创建自定义 NBAR 规则的特征，并进入 NBAR 规则特征视图。如果指定的 NBAR 规则特征已存在，则直接进入 NBAR 规则特征视图。

undo signature 命令用来删除自定义 NBAR 规则的特征。

【命令】

```
signature [ signature-id ] [ field field-name ] [ offset offset-value ] { hex
hex-vector | regex regex-pattern | string string }
undo signature signature-id
```

【缺省情况】

未配置自定义 NBAR 规则的特征。

【视图】

NBAR 规则视图

【缺省用户角色】

network-admin
context-admin

【参数】

signature-id: 指定 NBAR 规则特征的编号。取值范围为 1~65535。若未指定本参数，系统将按照步长从 5 开始，自动分配规则中不存在的 5 的最小整倍数作为 ID，步长为 5。例如，现有规则的最大编号为 28，上次自动分配的编号是 5，接着手动配置一条编号为 10 的规则，再自动配置一条规则，此规则自动分配的编号是 15。

field field-name: 表示在指定的协议域中匹配特征，**field-name** 表示协议域名称，且这些协议域是系统预定义的，不可自定义。只有基于 HTTP 协议的 NBAR 规则中的特征才能指定协议域，不指定协议域表示在整个 HTTP 报文中匹配特征。

offset *offset-value*: 表示在数据起始位置的偏移指定字节后的内容中去匹配特征，*offset-value* 表示字节偏移量，取值范围为 0~65535，单位为字节。如果未指定本参数，将从数据起始位置后的所有内容中去匹配特征。如果指定了协议域，则偏移值从协议域的起始位置计算。

hex *hex-vector*: 指定 16 进制向量特征。取值范围为 8~256 个字符的字符串，且字符个数必须为偶数，输入参数必须在两个竖杠（|）之间。

regex *regex-pattern*: 指定正则表达式特征，为 3~253 个字符的字符串，支持所有可输入字符，区分大小写。

string *string*: 指定字符串特征，为 3~256 个字符的字符串，支持所有可输入字符，区分大小写。

【使用指导】

对于一个自定义应用，允许配置多个特征（特征编号不同），特征可以是字符串、16 进制向量或者正则表达式，不同特征之间是逻辑或的关系。

特征编号相同时，多次执行本命令，最后一次执行的命令生效。

正则表达式有如下限制：

- 正则表达式中，总的分支不能超过四个。例如'abc(c|d|e|\x3D)'有效，'abc(c|onreset|onselect|onchange|style\x3D)'无效。
- 正则表达式中，括号不能嵌套，即括号中不能有括号。例如'ab((abcs*?))'无效。
- 正则表达式中，分支不支持串联，即分支后面不能有分支。例如'ab(a|b)(c|d)^\r\n]+?'无效。
- 正则表达式中，零次重复量词'*'和'?'前面必须有四个确定字符。例如'abc*'无效，'abcd*DoS\x2d\d{5}\x20\x2bxi\r\nJOIN'有效。

【举例】

在名为 abcd 的自定义 NBAR 规则中创建编号为 1 的自定义 NBAR 规则特征，配置字符串特征为 abcdefg，并进入 NBAR 规则特征视图。

```
<Sysname> system-view
[Sysname] nbar application abcd protocol http
[Sysname-nbar-application-abcd] signature 1 string abcdefg
[Sysname-nbar-application-abcd-signature-1]
```

在名为 ddd 的自定义 NBAR 规则中创建编号为 2 的自定义 NBAR 规则特征，配置 16 进制向量特征为 123456。

```
<Sysname> system-view
[Sysname] nbar application ddd protocol http
[Sysname-nbar-application-ddd] signature 2 hex |123456|
[Sysname-nbar-application-ddd-signature-2]
```

【相关命令】

- **detection**

1.1.33 source

source 命令用来配置自定义 NBAR 规则匹配的源 IP 地址网段。

undo source 命令用来恢复缺省情况。

【命令】

```
source ip ipv4-address [ mask-length ]  
undo source
```

【缺省情况】

NBAR 规则匹配所有源 IP 地址网段。

【视图】

NBAR 规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

ip *ipv4-address*: 指定匹配的源 IPv4 地址或网段，为点分十进制格式。
mask-length: 子网掩码长度，取值范围为 0~32。

【使用指导】

在同一个 NBAR 规则视图下多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 配置应用 abcd 的源网段。  
<Sysname> system-view  
[Sysname] nbar application abcd protocol http  
[Sysname-nbar-application-abcd] source ip 192.168.2.0 24
```

【相关命令】

- **nbar application**

1.1.34 update schedule

update schedule 命令用来配置定期自动升级 APR 特征库的时间。

undo update schedule 命令用来恢复缺省情况。

【命令】

```
update schedule { daily | weekly { fri | mon | sat | sun | thu | tue | wed } }  
start-time time tingle minutes  
undo update schedule
```

【缺省情况】

设备会在每天 02:01:00 至 04:01:00 之间自动升级 APR 特征库。

【视图】

自动升级配置视图

【缺省用户角色】

```
network-admin
```

context-admin

【参数】

daily: 表示自动升级周期为每天。

weekly: 表示以一周为周期，在指定一天进行自动升级。

fri: 表示星期五。

mon: 表示星期一。

sat: 表示星期六。

sun: 表示星期日。

thu: 表示星期四。

tue: 表示星期二。

wed: 表示星期三。

start-time time: 指定自动升级开始时间，*time* 的格式为 hh:mm:ss，取值范围为 00:00～23:59:59。

tingle minutes: 指定抖动时间，即实际自动升级开始时间的偏差范围，取值范围为 0～120，单位为分钟。在 **start-time** 指定时间的前后各偏移抖动时间的一半作为自动升级的时间范围，例如，指定自动升级的开始时间为 01:00:00，抖动时间为 60 分钟，则自动升级的时间范围为 00:30:00 至 01:30:00。

【举例】

配置定期自动升级 APR 特征库的时间为每周一的 23:10:00，抖动时间为 10 分钟。

```
<Sysname> system-view
```

```
[Sysname] apr signature auto-update
```

```
[Sysname-apr-autoupdate] update schedule weekly mon start-time 23:10:00 tingle 10
```

【相关命令】

- **apr signature auto-update**

1.1.35 user-defined-application

user-defined-application 命令用来进入自定义应用视图。

undo user-defined-application 命令用来删除指定自定义应用的配置。

【命令】

```
user-defined-application application-name
```

```
undo user-defined-application application-name
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

application-name: 指定自定义应用的名称，为 1~63 个字符的字符串，不区分大小写，不允许为系统保留的“invalid”、“other”和系统预定义应用的名称。

【使用指导】

进入自定义应用视图后，可为 NBAR 类型和 PBAR 类型的自定义应用配置风险类型。指定的自定义应用必须已存在。

【举例】

```
# 进入名为 app1 的自定义应用视图。  
<sysname> system-view  
[sysname] user-defined-application app1  
[sysname-user-defined-app-app1]
```

【相关命令】

- **nbar application**
- **port-mapping**
- **port-mapping acl**
- **port-mapping host**
- **port-mapping subnet**

目 录

1 会话管理.....	1-1
1.1 会话管理配置命令.....	1-1
1.1.1 display session aging-time application.....	1-1
1.1.2 display session aging-time state.....	1-2
1.1.3 display session relation-table	1-3
1.1.4 display session statistics	1-5
1.1.5 display session statistics ipv4	1-9
1.1.6 display session statistics ipv6	1-12
1.1.7 display session statistics multicast.....	1-16
1.1.8 display session table ipv4	1-17
1.1.9 display session table ipv6	1-20
1.1.10 display session table multicast ipv4.....	1-24
1.1.11 display session table multicast ipv6.....	1-27
1.1.12 display session top-statistics.....	1-30
1.1.13 reset session relation-table	1-32
1.1.14 reset session statistics	1-33
1.1.15 reset session statistics multicast.....	1-33
1.1.16 reset session table	1-34
1.1.17 reset session table ipv4	1-34
1.1.18 reset session table ipv6	1-35
1.1.19 reset session table multicast.....	1-36
1.1.20 reset session table multicast ipv4	1-37
1.1.21 reset session table multicast ipv6	1-38
1.1.22 session aging-time application	1-39
1.1.23 session aging-time state	1-41
1.1.24 session log { bytes-active packets-active }.....	1-42
1.1.25 session log enable	1-43
1.1.26 session log flow-begin.....	1-45
1.1.27 session log flow-end	1-45
1.1.28 session log time-active	1-46
1.1.29 session persistent acl.....	1-47
1.1.30 session statistics enable.....	1-48
1.1.31 session top-statistics enable.....	1-49

1 会话管理

1.1 会话管理配置命令

1.1.1 display session aging-time application

display session aging-time application 命令用来显示应用层协议或应用的会话老化时间。

【命令】

display session aging-time application

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示当前各应用层协议或应用的会话老化时间。

<Sysname> display session aging-time application

Application	Aging time(s)
bootpc	120
bootps	120
dns	1
ftp	3600
ftp-data	240
gprs-data	60
gprs-sig	60
gtp-control	60
gtp-user	60
h225	3600
h245	3600
https	600
ils	3600
l2tp	120
mgcp-callagent	60
mgcp-gateway	60
netbios-dgm	3600
netbios-ns	3600
netbios-ssn	3600
ntp	120

pptp	3600
qq	120
ras	300
rip	120
rsh	60
rtsp	3600
sccp	3600
sip	300
snmp	120
snmptrap	120
sqlnet	600
stun	600
syslog	120
tacacs-ds	120
tftp	60
who	120
xmcp	3600
others:	1200

表1-1 display session aging-time application 命令显示信息描述表

字段	描述
Application	应用层协议或应用的名称
Aging time(s)	会话老化时间，单位为秒
others: 1200	老化时间为1200秒的应用层协议或应用都显示为others

【相关命令】

- session aging-time application

1.1.2 display session aging-time state

display session aging-time state 命令用来显示各协议状态的会话老化时间。

【命令】

display session aging-time state

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示当前各协议状态的会话老化时间。

```
<Sysname> display session aging-time state
State                Aging Time(s)
SYN                  10
TCP-EST              3600
FIN                  10
UDP-OPEN             10
UDP-READY            30
ICMP-REQUEST         30
ICMP-REPLY           10
RAWIP-OPEN           30
RAWIP-READY          60
UDPLITE-OPEN         30
UDPLITE-READY        60
DCCP-REQUEST         30
DCCP-EST             3600
DCCP-CLOSEREQ        30
SCTP-INIT            30
SCTP-EST             3600
SCTP-SHUTDOWN        30
ICMPV6-REQUEST       60
ICMPV6-REPLY         30
TCP-TIME-WAIT         2
TCP-CLOSE            2
```

表1-2 display session aging-time state 命令显示信息描述表

字段	描述
State	各协议的状态类型
Aging Time(s)	会话老化时间，单位为秒

【相关命令】

- **session aging-time state**

1.1.3 display session relation-table

display session relation-table 命令用来显示关联表项信息。

【命令】

display session relation-table { ipv4 | ipv6 } [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin

context-operator

【参数】

ipv4: 显示 IPv4 关联表项。
ipv6: 显示 IPv6 关联表项。
slot slot-number: 显示指定成员设备上的关联表项信息，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，显示所有成员设备上的关联表项信息。

【举例】

```
# 显示所有的 IPv4 关联表项。
<Sysname> display session relation-table ipv4
Slot 1:
Source IP/port:      192.168.1.100/-
Destination IP/port: 192.168.2.100/99
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: 1/-/-
Protocol: TCP(6)     TTL: 1234s    App: FTP-DATA

Source IP/port:      -/-
Destination IP/port: 192.168.2.200/1212
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: 1/-/-
Protocol: TCP(6)     TTL: 3100s    App: H225

Total entries found: 2

# 显示所有的 IPv6 关联表项。
<Sysname> display session relation-table ipv6
Slot 1:
Source IP:           2011::0002
Destination IP/port: 2011::0008/1212
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)     TTL: 567s     App: FTP-DATA

Total entries found: 1
```

表1-3 display session relation-table 命令显示信息描述表

字段	描述
Source IP/port	会话的源IP地址和端口号。如果未指定则显示“-/-” IPv6会话无源端口号字段
Destination IP/port	会话的目的IP地址/端口号
DS-Lite tunnel peer	会话所属的DS-Lite隧道对端地址。未指定的参数则显示为“-”
VPN instance/VLAN ID/ Inline ID	关联表项所属的MPLS L3VPN/二层转发时会话所属的VLAN ID/二层转发时会话所属的INLINE。未指定的参数则显示为“-”
Protocol	传输层协议类型

字段	描述
TTL	关联表的剩余存活时间，单位为秒
App	应用层协议类型
Total entries found	当前查找到的关联表总数

1.1.4 display session statistics

display session statistics 命令用来显示单播会话统计信息。

【命令】

display session statistics [**history-max** | **summary**] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

history-max: 显示单播历史会话数最大值和历史新建会话速率最大值的统计信息。

summary: 显示会话单播统计信息的概要信息。不指定该参数时，显示单播会话统计信息的详细信息。

slot *slot-number*: 显示指定成员设备上的单播会话统计信息，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，显示所有成员设备上的单播会话统计信息。

【使用指导】

若不指定任何参数，则显示当前单播会话统计信息的详细信息。

【举例】

显示所有单播会话统计信息的详细信息。

```
<Sysname> display session statistics
```

```
Slot 1:
```

```
Current sessions: 3
```

```

      TCP sessions:          0
      UDP sessions:          0
      ICMP sessions:         3
      ICMPv6 sessions:       0
      UDP-Lite sessions:     0
      SCTP sessions:         0
      DCCP sessions:         0
      RAWIP sessions:        0
```

DNS sessions:	0
FTP sessions:	0
GTP sessions:	0
H323 sessions:	0
HTTP sessions:	0
ILS sessions:	0
MGCP sessions:	0
NBT sessions:	0
PPTP sessions:	0
RSH sessions:	0
RTSP sessions:	0
SCCP sessions:	0
SIP sessions:	0
SMTP sessions:	0
SQLNET sessions:	0
SSH sessions:	0
TELNET sessions:	0
TFTP sessions:	0
XDMCP sessions:	0

History average sessions per second:

Past hour: 1

Past 24 hours: 0

Past 30 days: 0

History average session establishment rate:

Past hour: 0/s

Past 24 hours: 0/s

Past 30 days: 0/s

Current relation-table entries: 0

Relation table establishment rate: 0/s

Session establishment rate: 0/s

TCP:	0/s
UDP:	0/s
ICMP:	0/s
ICMPv6:	0/s
UDP-Lite:	0/s
SCTP:	0/s
DCCP:	0/s
RAWIP:	0/s

Received TCP	:	0 packets	0 bytes
Received UDP	:	118 packets	13568 bytes
Received ICMP	:	105 packets	8652 bytes
Received ICMPv6	:	0 packets	0 bytes
Received UDP-Lite	:	0 packets	0 bytes


```

Received SCTP      :                0 packets                0 bytes
Received DCCP      :                0 packets                0 bytes
Received RAWIP     :                0 packets                0 bytes

```

表1-4 display session statistics 命令显示信息描述表

字段	描述
Current sessions	系统当前的总会话数
TCP sessions	系统当前的TCP会话数
UDP sessions	系统当前的UDP会话数
ICMP sessions	系统当前的ICMP会话数
ICMPv6 sessions	系统当前的ICMPv6会话数
UDP-Lite sessions	系统当前的UDP-Lite会话数
SCTP sessions	系统当前的SCTP会话数
DCCP sessions	系统当前的DCCP会话数
RAWIP sessions	系统当前的Raw IP会话数
DNS sessions	系统当前的DNS会话数
FTP sessions	系统当前的FTP会话数
GTP sessions	系统当前的GTP会话数
H323 sessions	系统当前的H323会话数
HTTP sessions	系统当前的HTTP会话数
ILS sessions	系统当前的ILS会话数
MGCP sessions	系统当前的MGCP会话数
NBT sessions	系统当前的NBT会话数
PPTP sessions	系统当前的PPTP会话数
RSH sessions	系统当前的RSH会话数
RTSP sessions	系统当前的RTSP会话数
SCCP sessions	系统当前的SCCP会话数
SIP sessions	系统当前的SIP会话数
SMTP sessions	系统当前的SMTP会话数
SQLNET sessions	系统当前的SQLNET会话数
SSH sessions	系统当前的SSH会话数
TELNET sessions	系统当前的TELNET会话数
TFTP sessions	系统当前的TFTP会话数
XDMCP sessions	系统当前的XDMCP会话数
History average sessions per second	会话数的历史统计信息，以当前时间为基准

Past hour	最近一小时内每秒钟系统会话数目的平均值
Past 24 hours	最近一天内每秒钟系统会话数目的平均值
Past 30 days	最近三十天内每秒钟系统会话数目的平均值
History average session establishment rate	新建会话速率的历史统计信息，以当前时间为基准
Past hour	最近一小时内系统新建会话速率的平均值
Past 24 hours	最近一天内系统新建会话速率的平均值
Past 30 days	最近三十天内系统新建会话速率的平均值
Current relation-table entries	总关联表项个数
Relation table establishment rate	关联表创建速率
Session establishment rate	系统创建会话的速率，以及创建各协议会话的速率
Received TCP	系统当前收到的TCP报文数、报文字节数
Received UDP	系统当前收到的UDP报文数、报文字节数
Received ICMP	系统当前收到的ICMP报文数、报文字节数
Received ICMPv6	系统当前收到的ICMPv6报文数、报文字节数
Received UDP-Lite	系统当前收到的UDP-Lite报文数、报文字节数
Received SCTP	系统当前收到的SCTP报文数、报文字节数
Received DCCP	系统当前收到的DCCP报文数、报文字节数
Received RAWIP	系统当前收到的Raw IP报文数、报文字节数

显示单播会话统计信息的概要信息。

```
<Sysname> display session statistics summary
```

```
Slot Sessions  TCP      UDP      Rate      TCP rate  UDP rate
1      3          0        0        0/s       0/s       0/s
```

表1-5 display session statistics summary 命令显示信息描述表

字段	描述
Sessions	系统当前的单播总会话数
TCP	系统当前的TCP单播会话数
UDP	系统当前的UDP单播会话数
Rate	系统创建单播会话的速率
TCP rate	系统创建TCP单播会话的速率
UDP rate	系统创建UDP单播会话的速率

显示单播会话历史会话数最大值和历史新建会话速率最大值的统计信息。

```
<Sysname> display session statistics history-max
```

```
Slot 1
```

Max sessions: 20084	Time: 2017-03-04 12:03:53
Max session establishment rate: 9080/s	Time: 2017-03-04 12:03:53
Max TCP sessions: 20084	Time: 2017-03-04 12:03:53
Max TCP session establishment rate: 9080/s	Time: 2017-03-04 12:03:53
Max UDP sessions: 0	Time: 2017-03-04 12:03:53
Max UDP session establishment rate: 0	Time: 2017-03-04 12:03:53

表1-6 display session statistics history-max 命令显示信息描述表

字段	描述
Max sessions	系统历史单播会话数目的最大值
Max session establishment rate	系统历史新建单播会话速率的最大值，单位为：个/秒
Max TCP sessions	系统历史TCP单播会话数目的最大值
Max TCP session establishment rate	系统历史新建TCP单播会话速率的最大值，单位为：个/秒
Max UDP sessions	系统历史UDP单播会话数目的最大值
Max UDP session establishment rate	系统历史新建UDP单播会话速率的最大值，单位为：个/秒

1.1.5 display session statistics ipv4

display session statistics ipv4 命令用来根据五元组显示 IPv4 单播会话统计信息。

【命令】

```
display session statistics ipv4 [ [ responder ] { application
application-name | destination-ip destination-ip | destination-port
destination-port | destination-zone destination-zone-name | interface
interface-type interface-number | protocol { dccp | dns | ftp | gtp | h323 |
http | icmp | ils | mgcp | nbt | pptp | raw-ip | rsh | rtsp | sccp | sctp | sip | smtp
| sqlnet | ssh | tcp | telnet | tftp | udp | udp-lite | xdmcp } |
security-policy-rule rule-name | source-ip source-ip | source-port
source-port | source-zone source-zone-name | state { dccp-closereq |
dccp-closing | dccp-open | dccp-partopen | dccp-request | dccp-respond |
dccp-timewait | icmp-reply | icmp-request | rawip-open | rawip-ready |
sctp-closed | sctp-cookie-echoed | sctp-cookie-wait | sctp-established |
sctp-shutdown-ack-sent | sctp-shutdown-recd | sctp-shutdown-sent |
tcp-close | tcp-close-wait | tcp-est | tcp-fin-wait | tcp-last-ack |
tcp-syn-recv | tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-open |
udp-ready | udplite-open | udplite-ready } | vpn-instance vpn-instance-name }
* ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

responder: 表示以响应方的信息筛选显示 IPv4 单播会话统计信息。若不指定该参数时, 则以发起方的信息筛选显示 IPv4 单播会话统计信息。

application *application-name*: 显示指定应用的 IPv4 单播会话统计信息。
application-name 表示应用的名称, 为 1~63 个字符的字符串, 不区分大小写, 不允许为系统保留的 “invalid” 和 “other”。

destination-ip *destination-ip*: 显示指定目的 IPv4 地址的单播会话统计信息。其中, *destination-ip* 表示 IPv4 地址。

destination-port *destination-port*: 显示指定目的端口号的 IPv4 单播会话表项。其中, *destination-port* 表示端口号, 取值为 0~65535。

destination-zone *destination-zone-name*: 显示指定目的安全域的 IPv4 单播会话统计信息。其中 *destination-zone-name* 表示安全域的名称, 安全域的名称为 1~31 个字符的字符串, 不区分大小写。

interface *interface-type interface-num*: 显示指定接口的 IPv4 单播会话统计信息。
interface-type interface-number 表示接口类型和接口编号。

protocol { *dccp* | *dns* | *ftp* | *gtp* | *h323* | *http* | *icmp* | *ils* | *mgcp* | *nbt* | *pptp* | *raw-ip* | *rsh* | *rtsp* | *sccp* | *sctp* | *sip* | *smtp* | *sqlnet* | *ssh* | *tcp* | *telnet* | *tftp* | *udp* | *udp-lite* | *xmcp* }: 显示指定协议类型的 IPv4 单播会话表项。

security-policy-rule *rule-name*: 显示与指定安全策略规则匹配的 IPv4 单播会话统计信息。
rule-name 表示安全策略规则名称, 为 1~127 个字符的字符串, 区分大小写。

source-ip *source-ip*: 显示指定源 IP 地址的单播会话统计信息。其中, *source-ip* 表示 IPv4 地址。

source-port *source-port*: 显示指定源端口号的 IPv4 单播会话表项。其中, *source-port* 表示端口号, 取值为 0~65535。

source-zone *source-zone-name*: 显示指定源安全域的 IPv4 单播会话统计信息。其中 *source-zone-name* 表示安全域的名称, 安全域的名称为 1~31 个字符的字符串, 不区分大小写。

state { *dccp-closereq* | *dccp-closing* | *dccp-open* | *dccp-partopen* | *dccp-request* | *dccp-respond* | *dccp-timewait* | *icmp-reply* | *icmp-request* | *rawip-open* | *rawip-ready* | *sctp-closed* | *sctp-cookie-echoed* | *sctp-cookie-wait* | *sctp-established* | *sctp-shutdown-ack-sent* | *sctp-shutdown-recd* | *sctp-shutdown-sent* | *tcp-close* | *tcp-close-wait* | *tcp-est* | *tcp-fin-wait* | *tcp-last-ack* | *tcp-syn-recv* | *tcp-syn-sent* | *tcp-syn-sent2* | *tcp-time-wait* | *udp-open* | *udp-ready* | *udplite-open* | *udplite-ready* }: 显示指定状态的 IPv4 单播会话统计信息。

vpn-instance *vpn-instance-name*: 显示指定 VPN 实例的 IPv4 单播会话统计信息。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。若不指定此参数, 则显示公网的 IPv4 单播会话统计信息。

slot slot-number: 显示指定成员设备上的单播会话统计信息，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，显示所有成员设备上的单播会话统计信息。

【使用指导】

如果不指定任何参数，则显示所有的 IPv4 单播会话统计信息。

【举例】

```
# 根据源 IP 地址 111.15.111.66 显示单播会话统计信息的详细信息。
<Sysname> display session statistics ipv4 source-ip 111.15.111.66
Slot 1:
Current sessions: 3
    TCP sessions:          0
    UDP sessions:          0
    ICMP sessions:         3
    UDP-Lite sessions:     0
    SCTP sessions:         0
    DCCP sessions:         0
    RAWIP sessions:        0

    DNS sessions:          0
    FTP sessions:          0
    GTP sessions:          0
    H323 sessions:         0
    HTTP sessions:         0
    ILS sessions:          0
    MGCP sessions:         0
    NBT sessions:          0
    PPTP sessions:         0
    RSH sessions:          0
    RTSP sessions:         0
    SCCP sessions:         0
    SIP sessions:          0
    SMTP sessions:         0
    SQLNET sessions:       0
    SSH sessions:          0
    TELNET sessions:       0
    TFTP sessions:         0
    XDMCP sessions:        0
```

```
# 根据 TCP 协议显示单播会话统计信息的详细信息。
<Sysname> display session statistics ipv4 protocol tcp
Slot 1:
Current sessions: 3
    TCP sessions:          3
```

表1-7 display session statistics ipv4 命令显示信息描述表

字段	描述
Current sessions	系统当前的总会话数

字段	描述
TCP sessions	系统当前的TCP会话数
UDP sessions	系统当前的UDP会话数
ICMP sessions	系统当前的ICMP会话数
UDP-Lite sessions	系统当前的UDP-Lite会话数
SCTP sessions	系统当前的SCTP会话数
DCCP sessions	系统当前的DCCP会话数
RAWIP sessions	系统当前的Raw IP会话数
DNS sessions	系统当前的DNS会话数
FTP sessions	系统当前的FTP会话数
GTP sessions	系统当前的GTP会话数
H323 sessions	系统当前的H323会话数
HTTP sessions	系统当前的HTTP会话数
ILS sessions	系统当前的ILS会话数
MGCP sessions	系统当前的MGCP会话数
NBT sessions	系统当前的NBT会话数
PPTP sessions	系统当前的PPTP会话数
RSH sessions	系统当前的RSH会话数
RTSP sessions	系统当前的RTSP会话数
SCCP sessions	系统当前的SCCP会话数
SIP sessions	系统当前的SIP会话数
SMTP sessions	系统当前的SMTP会话数
SQLNET sessions	系统当前的SQLNET会话数
SSH sessions	系统当前的SSH会话数
TELNET sessions	系统当前的TELNET会话数
TFTP sessions	系统当前的TFTP会话数
XDMCP sessions	系统当前的XDMCP会话数

1.1.6 display session statistics ipv6

display session statistics ipv6 命令用来根据五元组显示 IPv6 单播会话统计信息。

【命令】

```
display session statistics ipv6 [ [ responder ] { application
application-name | destination-ip destination-ip | destination-port
```

```

destination-port | destination-zone destination-zone-name | interface
interface-type interface-number | protocol { dccp | dns | ftp | gtp | h323 |
http | icmpv6 | ils | mgcp | nbt | pptp | raw-ip | rsh | rtsp | sccp | sctp | sip |
smtp | sqlnet | ssh | tcp | telnet | tftp | udp | udp-lite | xmcp } |
security-policy-rule rule-name | source-ip source-ip | source-port
source-port | source-zone source-zone-name | state { dccp-closereq |
dccp-closing | dccp-open | dccp-partopen | dccp-request | dccp-respond |
dccp-timewait | icmpv6-reply | icmpv6-request | rawip-open | rawip-ready
| sctp-closed | sctp-cookie-echoed | sctp-cookie-wait | sctp-established
| sctp-shutdown-ack-sent | sctp-shutdown-recd | sctp-shutdown-sent |
tcp-close | tcp-close-wait | tcp-est | tcp-fin-wait | tcp-last-ack |
tcp-syn-recv | tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-open |
udp-ready | udplite-open | udplite-ready } | vpn-instance vpn-instance-name }
* ] [ slot slot-number ]

```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

responder: 表示以响应方的信息筛选显示 IPv6 单播会话统计信息。若不指定该参数时，则以发起方的信息筛选显示 IPv6 单播会话统计信息。

application *application-name*: 显示指定应用的 IPv6 单播会话统计信息。
application-name 表示应用的名称，为 1~63 个字符的字符串，不区分大小写，不允许为系统保留的“invalid”和“other”。

destination-ip *destination-ip*: 显示指定目的 IPv6 地址的单播会话统计信息。其中，*destination-ip* 表示 IPv6 地址。

destination-port *destination-port*: 显示指定目的端口号的 IPv6 单播会话表项。其中，*destination-port* 表示端口号，取值为 0~65535。

destination-zone *destination-zone-name*: 显示指定目的安全域的 IPv6 单播会话统计信息。其中 *destination-zone-name* 表示安全域的名称，安全域的名称为 1~31 个字符的字符串，不区分大小写。

interface *interface-type interface-num*: 显示指定接口的 IPv6 单播会话统计信息。
interface-type interface-number 表示接口类型和接口编号。

***protocol* { *dccp* | *dns* | *ftp* | *gtp* | *h323* | *http* | *icmpv6* | *ils* | *mgcp* | *nbt* | *pptp* | *raw-ip* | *rsh* | *rtsp* | *sccp* | *sctp* | *sip* | *smtp* | *sqlnet* | *ssh* | *tcp* | *telnet* | *tftp* | *udp* | *udp-lite* | *xmcp* }:** 显示指定协议类型的 IPv6 单播会话表项。

security-policy-rule rule-name: 显示与指定安全策略规则匹配的 IPv6 单播会话统计信息 *rule-name* 表示安全策略规则名称, 为 1~127 个字符的字符串, 区分大小写。

source-ip source-ip: 显示指定源 IP 地址的单播会话统计信息。其中, *source-ip* 表示 IPv6 地址。

source-port source-port: 显示指定源端口号的 IPv6 单播会话表项。其中, *source-port* 表示端口号, 取值为 0~65535。

source-zone source-zone-name: 显示指定源安全域名的 IPv6 单播会话统计信息。其中 *source-zone-name* 表示安全域的名称, 安全域的名称为 1~31 个字符的字符串, 不区分大小写。

state { dccp-closereq | dccp-closing | dccp-open | dccp-partopen | dccp-request | dccp-respond | dccp-timewait | icmpv6-reply | icmpv6-request | rawip-open | rawip-ready | sctp-closed | sctp-cookie-echoed | sctp-cookie-wait | sctp-established | sctp-shutdown-ack-sent | sctp-shutdown-recd | sctp-shutdown-sent | tcp-close | tcp-close-wait | tcp-est | tcp-fin-wait | tcp-last-ack | tcp-syn-recv | tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-open | udp-ready | udplite-open | udplite-ready }: 显示指定状态的 IPv6 单播会话统计信息。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的 IPv6 单播会话统计信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。若不指定此参数, 则显示公网的 IPv6 单播会话统计信息。

slot slot-number: 显示指定成员设备上的单播会话统计信息, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 显示所有成员设备上的单播会话统计信息。

【举例】

根据源 IPv6 地址 100::2 显示单播会话统计信息的详细信息。

```
<Sysname> display session statistics ipv6 source-ip 100::2
```

```
Slot 1:
```

```
Current sessions: 3
```

TCP sessions:	0
UDP sessions:	0
ICMPv6 sessions:	3
UDP-Lite sessions:	0
SCTP sessions:	0
DCCP sessions:	0
RAWIP sessions:	0
DNS sessions:	0
FTP sessions:	0
GTP sessions:	0
H323 sessions:	0
HTTP sessions:	0
ILS sessions:	0
MGCP sessions:	0
NBT sessions:	0
PPTP sessions:	0
RSH sessions:	0


```

RTSP sessions:          0
SCCP sessions:          0
SIP sessions:           0
SMTP sessions:          0
SQLNET sessions:        0
SSH sessions:           0
TELNET sessions:        0
TFTP sessions:          0
XDMCP sessions:         0

```

根据 TCP 协议显示单播会话统计信息的详细信息。

```
<Sysname> display session statistics ipv6 protocol tcp
```

Slot 1:

```
Current sessions: 3
```

```
TCP sessions:          3
```

表1-8 display session statistics ipv6 命令显示信息描述表

字段	描述
Current sessions	系统当前的总会话数
TCP sessions	系统当前的TCP会话数
UDP sessions	系统当前的UDP会话数
ICMPv6 sessions	系统当前的ICMPv6会话数
UDP-Lite sessions	系统当前的UDP-Lite会话数
SCTP sessions	系统当前的SCTP会话数
DCCP sessions	系统当前的DCCP会话数
RAWIP sessions	系统当前的Raw IP会话数
DNS sessions	系统当前的DNS会话数
FTP sessions	系统当前的FTP会话数
GTP sessions	系统当前的GTP会话数
H323 sessions	系统当前的H323会话数
HTTP sessions	系统当前的HTTP会话数
ILS sessions	系统当前的ILS会话数
MGCP sessions	系统当前的MGCP会话数
NBT sessions	系统当前的NBT会话数
PPTP sessions	系统当前的PPTP会话数
RSH sessions	系统当前的RSH会话数
RTSP sessions	系统当前的RTSP会话数
SCCP sessions	系统当前的SCCP会话数
SIP sessions	系统当前的SIP会话数

字段	描述
SMTP sessions	系统当前的SMTP会话数
SQLNET sessions	系统当前的SQLNET会话数
SSH sessions	系统当前的SSH会话数
TELNET sessions	系统当前的TELNET会话数
TFTP sessions	系统当前的TFTP会话数
XDMCP sessions	系统当前的XDMCP会话数

1.1.7 display session statistics multicast

display session statistics multicast 命令用来显示组播会话统计信息。

【命令】

display session statistics multicast [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备上的组播会话统计信息，*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示显示所有成员设备上的组播会话统计信息。

【举例】

显示组播会话统计信息。

```
<Sysname> display session statistics multicast
Slot 1:
Current sessions: 0
Session establishment rate: 0/s
History max sessions: 0                               Time: 2017-04-25 11:28:00
History max session establishment rate: 0/s            Time: 2017-04-25 11:28:00
Received:                0 packets                      0 bytes
Sent      :                0 packets                      0 bytes
```

表1-9 display session statistics multicast 命令显示信息描述表

字段	描述
Current sessions	系统当前为业务流量创建的组播会话数
Session establishment rate	系统创建组播会话的速率

History max sessions	系统历史组播会话数目的最大值
History max session establishment rate	系统创建组播会话历史速率的最大值
Time	各个最大值对应的时间
Received	系统当前收到的组播报文数、报文字节数
Sent	系统当前发出的组播报文数、报文字节数

1.1.8 display session table ipv4

display session table ipv4 命令用来显示 IPv4 单播会话表项信息。

【命令】

```
display session table ipv4 [ slot slot-number ] [ [ responder ] { application
application-name | destination-ip start-destination-ip
[ end-destination-ip ] | destination-port destination-port |
destination-zone destination-zone-name | interface interface-type
interface-number | protocol { dccp | icmp | raw-ip | sctp | tcp | udp | udp-lite }
| security-policy-rule rule-name | source-ip start-source-ip
[ end-source-ip ] | source-port source-port | source-zone source-zone-name |
state { dccp-closereq | dccp-closing | dccp-open | dccp-partopen |
dccp-request | dccp-respond | dccp-timewait | icmp-reply | icmp-request |
rawip-open | rawip-ready | sctp-closed | sctp-cookie-echoed |
sctp-cookie-wait | sctp-established | sctp-shutdown-ack-sent |
sctp-shutdown-recd | sctp-shutdown-sent | tcp-close | tcp-close-wait |
tcp-est | tcp-fin-wait | tcp-last-ack | tcp-syn-recv | tcp-syn-sent |
tcp-syn-sent2 | tcp-time-wait | udp-open | udp-ready | udplite-open |
udplite-ready } | vpn-instance vpn-instance-name } * ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备上的 IPv4 单播会话表项, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 显示所有成员设备上的 IPv4 单播会话表项。

responder: 表示以响应方的信息筛选显示 IPv4 单播会话表项。若不指定该参数时, 则以发起方的信息筛选显示 IPv4 单播会话表项。

application *application-name*: 显示指定应用的 IPv4 单播会话表项。*application-name* 表示应用的名称, 为 1~63 个字符的字符串, 不区分大小写, 不允许为系统保留的“invalid”和“other”。

destination-ip *start-destination-ip* [*end-destination-ip*]: 显示指定目的 IPv4 地址的单播会话表项。其中, *start-destination-ip* 表示目的 IPv4 地址范围的起始地址, *end-destination-ip* 目的 IPv4 地址范围的结束地址。

destination-port *destination-port*: 显示指定目的端口号的 IPv4 单播会话表项。其中, *destination-port* 表示目的端口号, 取值为 0~65535。

destination-zone *destination-zone-name*: 显示指定目的安全域的 IPv4 单播会话表项。其中 *destination-zone-name* 表示安全域的名称, 安全域的名称为 1~31 个字符的字符串, 不区分大小写。

interface *interface-type interface-number*: 显示指定接口的 IPv4 单播会话表项。*interface-type interface-number* 表示接口类型和接口编号。

protocol { *dccp* | *icmp* | *raw-ip* | *sctp* | *tcp* | *udp* | *udp-lite* }: 显示指定协议类型的 IPv4 单播会话表项。其中, IPv4 传输层协议类型可包括: DCCP、ICMP、RawIP、SCTP、TCP、UDP 和 UDP-Lite。

security-policy-rule *rule-name*: 显示与指定安全策略规则匹配的 IPv4 单播会话表项。*rule-name* 为安全策略规则的名称, 为 1~127 个字符的字符串, 区分大小写。

source-ip *start-source-ip* [*end-source-ip*]: 显示指定源 IP 地址的单播会话表项。其中, *start-source-ip* 表示源 IPv4 地址范围的起始地址, *end-source-ip* 表示源 IPv4 地址范围的结束地址。

source-port *source-port*: 显示指定源端口号的 IPv4 单播会话表项。其中, *source-port* 表示源端口号, 取值为 0~65535。

source-zone *source-zone-name*: 显示指定源安全域的 IPv4 单播会话表项。其中 *source-zone-name* 表示安全域的名称, 安全域的名称为 1~31 个字符的字符串, 不区分大小写。

state { *dccp-closereq* | *dccp-closing* | *dccp-open* | *dccp-partopen* | *dccp-request* | *dccp-respond* | *dccp-timewait* | *icmp-reply* | *icmp-request* | *rawip-open* | *rawip-ready* | *sctp-closed* | *sctp-cookie-echoed* | *sctp-cookie-wait* | *sctp-established* | *sctp-shutdown-ack-sent* | *sctp-shutdown-recd* | *sctp-shutdown-sent* | *tcp-close* | *tcp-close-wait* | *tcp-est* | *tcp-fin-wait* | *tcp-last-ack* | *tcp-syn-recv* | *tcp-syn-sent* | *tcp-syn-sent2* | *tcp-time-wait* | *udp-open* | *udp-ready* | *udplite-open* | *udplite-ready* }: 显示指定状态的 IPv4 单播会话表项。

vpn-instance *vpn-instance-name*: 显示指定 VPN 实例的 IPv4 单播会话表项。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。若不指定此参数, 则显示公网的 IPv4 单播会话表项。

verbose: 显示 IPv4 单播会话表项的详细信息。不指定该参数时, 显示 IPv4 单播会话表项的概要信息。

【使用指导】

如果不指定任何参数, 则显示所有的 IPv4 单播会话表项。

【举例】

```
# 显示所有的 IPv4 单播会话表项的概要信息。
<Sysname> display session table ipv4
Slot 1:
Initiator:
    Source      IP/port: 192.168.1.18/1877
    Destination IP/port: 192.168.1.55/22
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/1
    Source security zone: Trust
Total sessions found: 1
# 显示所有的 IPv4 单播会话表项的详细信息。
<Sysname> display session table ipv4 verbose
Slot 1:
Initiator:
    Source      IP/port: 192.168.1.18/1877
    Destination IP/port: 192.168.1.55/22
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/1
    Source security zone: Trust
Responder:
    Source      IP/port: 192.168.1.55/22
    Destination IP/port: 192.168.1.18/1877
    DS-Lite tunnel peer: -
    VPN instance/VLAN ID/Inline ID: -/-/-
    Protocol: TCP(6)
    Inbound interface: GigabitEthernet1/0/2
    Source security zone: Local
State: TCP_SYN_SENT
Application: SSH
Rule ID: 1
Rule name: test
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:          1 packets          48 bytes
Responder->Initiator:          0 packets          0 bytes
Total sessions found: 1
```

表1-10 display session table 命令显示信息描述表

字段	描述
Initiator	发起方到响应方的连接对应的会话信息
Responder	响应方到发起方的连接对应的会话信息
Source IP/port	源IP地址/端口号

字段	描述
Destination IP/port	目的IP地址/端口号
DS-Lite tunnel peer	DS-Lite隧道对端地址。会话不属于任何DS-Lite隧道时，本字段显示为“-”
VPN instance/VLAN ID/Inline ID	会话所属的MPLS L3VPN/二层转发时会话所属的VLAN ID/二层转发时会话所属的INLINE。未指定的参数则显示为“-”
Protocol	传输层协议类型，取值包括：DCCP、ICMP、ICMPv6、Raw IP、SCTP、TCP、UDP、UDP-Lite 括号中的数字表示协议号
Inbound interface	报文的入接口
Source security zone	源安全域，即入接口所属的安全域。若接口不属于任何安全域，则显示为“-”
State	会话状态
Application	应用层协议类型，取值包括：FTP、DNS等，OTHER表示未知协议类型，其对应的端口为非知名端口
Rule ID	安全策略规则的ID
Rule name	安全策略规则的名称
Start time	会话创建时间
TTL	会话剩余存活时间，单位为秒
Initiator->Responder	发起方到响应方的报文数、报文字节数
Responder->Initiator	响应方到发起方的报文数、报文字节数
Total sessions found	当前查找到的会话表项总数

1.1.9 display session table ipv6

display session table ipv6 命令用来显示 IPv6 单播会话表项信息。

【命令】

```
display session table ipv6 [ slot slot-number ] [ [ responder ] { application
application-name          | destination-ip      start-destination-ip
[ end-destination-ip ]    | destination-port destination-port |
destination-zone destination-zone-name | interface interface-type
interface-number | protocol { dccp | icmpv6 | raw-ip | sctp | tcp | udp |
udp-lite } | security-policy-rule rule-name | source-ip start-source-ip
[ end-source-ip ] | source-port source-port | source-zone source-zone-name |
state { dccp-closereq | dccp-closing | dccp-open | dccp-partopen |
dccp-request | dccp-respond | dccp-timewait | icmpv6-reply | icmpv6-request
| rawip-open | rawip-ready | sctp-closed | sctp-cookie-echoed |
sctp-cookie-wait | sctp-established | sctp-shutdown-ack-sent |
```

```
sctp-shutdown-recd | sctp-shutdown-sent | tcp-close | tcp-close-wait |  
tcp-est | tcp-fin-wait | tcp-last-ack | tcp-syn-recv | tcp-syn-sent |  
tcp-syn-sent2 | tcp-time-wait | udp-open | udp-ready | udplite-open |  
udplite-ready } | vpn-instance vpn-instance-name } * ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot *slot-number*: 显示指定成员设备上的 IPv6 单播会话表项, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 显示所有成员设备上的 IPv6 单播会话表项。

responder: 表示以响应方的信息筛选显示 IPv6 单播会话表项。若不指定该参数时, 则以发起方的信息筛选显示 IPv6 单播会话表项。

application *application-name*: 显示指定应用的 IPv6 单播会话表项。*application-name* 表示应用的名称, 为 1~63 个字符的字符串, 不区分大小写, 不允许为系统保留的“invalid”和“other”。

destination-ip *start-destination-ip* [*end-destination-ip*]: 显示指定目的 IPv6 地址的单播会话表项。其中, *start-destination-ip* 表示目的 IPv6 地址范围的起始地址, *end-destination-ip* 目的 IPv6 地址范围的结束地址。

destination-port *destination-port*: 显示指定目的端口号的 IPv6 单播会话表项。其中, *destination-port* 表示目的端口号, 取值为 0~65535。

destination-zone *destination-zone-name*: 显示指定目的安全域的 IPv6 单播会话表项。其中 *destination-zone-name* 表示安全域的名称, 安全域的名称为 1~31 个字符的字符串, 不区分大小写。

interface *interface-type interface-number*: 显示指定接口的 IPv6 单播会话表项。*interface-type interface-number* 表示接口类型和接口编号。

protocol { *dccp* | *icmp* | *raw-ip* | *sctp* | *tcp* | *udp* | *udp-lite* }: 显示指定协议类型的 IPv6 单播会话表项。其中, IPv6 传输层协议类型可包括: DCCP、ICMP、RawIP、SCTP、TCP、UDP 和 UDP-Lite。

security-policy-rule *rule-name*: 显示与指定安全策略规则匹配的 IPv6 单播会话表项。*rule-name* 为安全策略规则的名称, 为 1~127 个字符的字符串, 区分大小写。

source-ip *start-source-ip* [*end-source-ip*]: 显示指定源 IP 地址的单播会话表项。其中, *start-source-ip* 表示源 IPv6 地址范围的起始地址, *end-source-ip* 表示源 IPv6 地址范围的结束地址。

source-port *source-port*: 显示指定源端口号的 IPv6 单播会话表项。其中, *source-port* 表示源端口号, 取值为 0~65535。

source-zone *source-zone-name*: 显示指定源安全域的 IPv6 单播会话表项。其中 *source-zone-name* 表示安全域的名称,安全域的名称为 1~31 个字符的字符串,不区分大小写。

state { **dccp-closereq** | **dccp-closing** | **dccp-open** | **dccp-partopen** | **dccp-request** | **dccp-respond** | **dccp-timewait** | **icmpv6-reply** | **icmpv6-request** | **rawip-open** | **rawip-ready** | **sctp-closed** | **sctp-cookie-echoed** | **sctp-cookie-wait** | **sctp-established** | **sctp-shutdown-ack-sent** | **sctp-shutdown-recd** | **sctp-shutdown-sent** | **tcp-close** | **tcp-close-wait** | **tcp-est** | **tcp-fin-wait** | **tcp-last-ack** | **tcp-syn-recv** | **tcp-syn-sent** | **tcp-syn-sent2** | **tcp-time-wait** | **udp-open** | **udp-ready** | **udplite-open** | **udplite-ready** }: 显示指定状态的 IPv6 单播会话表项。

vpn-instance *vpn-instance-name*: 显示指定 VPN 实例的 IPv6 单播会话表项。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称,为 1~31 个字符的字符串,区分大小写。若不指定此参数,则显示公网的 IPv6 单播会话表项。

verbose: 显示 IPv6 单播会话表项的详细信息。不指定该参数时,显示 IPv6 单播会话表项的概要信息。

【使用指导】

如果不指定任何参数,则显示所有的 IPv6 单播会话表项。

【举例】

显示所有的 IPv6 单播会话表项的概要信息。

```
<Sysname> display session table ipv6
```

Slot 1:

Initiator:

```
Source      IP/port: 2011::2/58473
Destination IP/port: 2011::8/32768
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: IPV6-ICMP(58)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
```

Total sessions found: 1

显示所有的 IPv6 单播会话表项的详细信息。

```
<Sysname> display session table ipv6 verbose
```

Slot 1:

Initiator:

```
Source      IP/port: 2011::2/58473
Destination IP/port: 2011::8/32768
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: IPV6-ICMP(58)
Inbound interface: GigabitEthernet1/0/1
Source security zone: Trust
```

Responder:

```
Source      IP/port: 2011::8/58473
```



```

Destination IP/port: 2011::2/33024
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: IPV6-ICMP(58)
Inbound interface: GigabitEthernet1/0/2
Source security zone: Local
State: ICMPV6_REQUEST
Application: OTHER
Rule ID: 1
Rule name: test
Start time: 2011-07-29 19:23:41  TTL: 55s
Initiator->Responder:          1 packets          104 bytes
Responder->Initiator:          0 packets           0 bytes

Total sessions found: 1

```

表1-11 display session table 命令显示信息描述表

字段	描述
Initiator	发起方到响应方的连接对应的会话信息
Responder	响应方到发起方的连接对应的会话信息
Source IP/port	源IP地址/端口号
Destination IP/port	目的IP地址/端口号
DS-Lite tunnel peer	DS-Lite隧道对端地址。会话不属于任何DS-Lite隧道时，本字段显示为“-”
VPN instance/VLAN ID/Inline ID	会话所属的MPLS L3VPN/二层转发时会话所属的VLAN ID/二层转发时会话所属的INLINE。未指定的参数则显示为“-”
Protocol	传输层协议类型，取值包括：DCCP、ICMP、ICMPv6、Raw IP、SCTP、TCP、UDP、UDP-Lite 括号中的数字表示协议号
Inbound interface	报文的入接口
Source security zone	源安全域，即入接口所属的安全域。若接口不属于任何安全域，则显示为“-”
State	会话状态
Application	应用层协议类型，取值包括：FTP、DNS等，OTHER表示未知协议类型，其对应的端口为非知名端口
Rule ID	安全策略规则的ID
Rule name	安全策略规则的名称
Start time	会话创建时间
TTL	会话剩余存活时间，单位为秒
Initiator->Responder	发起方到响应方的报文数、报文字节数
Responder->Initiator	响应方到发起方的报文数、报文字节数

字段	描述
Total sessions found	当前查找到的会话表项总数

1.1.10 display session table multicast ipv4

display session table multicast ipv4 命令用来显示 IPv4 组播会话表项信息。

【命令】

```
display session table multicast ipv4 [ slot slot-number ] [ [ responder ]
{ destination-ip start-destination-ip [ end-destination-ip ] |
destination-port destination-port | protocol { dccp | icmp | raw-ip | sctp |
tcp | udp | udp-lite } | source-ip start-source-ip [ end-source-ip ] |
source-port source-port } * ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot *slot-number*: 显示指定成员设备上的 IPv4 组播会话表项, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 显示所有成员设备上的 IPv4 组播会话表项。

responder: 表示以响应方的信息筛选显示 IPv4 组播会话表项。若不指定该参数时, 则以发起方的信息筛选显示 IPv4 组播会话表项。

destination-ip *start-destination-ip* [*end-destination-ip*]: 显示指定目的 IPv4 地址的组播会话表项。其中, *start-destination-ip* 表示目的 IPv4 地址范围的起始地址, *end-destination-ip* 目的 IPv4 地址范围的结束地址。

destination-port *destination-port*: 显示指定目的端口号的 IPv4 组播会话表项。其中, *destination-port* 表示端口号, 取值为 0~65535。

protocol { **dccp** | **icmp** | **raw-ip** | **sctp** | **tcp** | **udp** | **udp-lite** }: 显示指定协议类型的 IPv4 组播会话表项。

source-ip *start-source-ip* [*end-source-ip*]: 显示指定源 IP 地址的组播会话表项。其中, *start-source-ip* 表示源 IPv4 地址范围的起始地址, *end-source-ip* 表示源 IPv4 地址的结束地址。

source-port *source-port*: 显示指定源端口号的 IPv4 组播会话表项。其中, *source-port* 表示源端口号, 取值为 0~65535。

verbose: 显示 IPv4 组播会话表项的详细信息。不指定该参数时, 显示 IPv4 组播会话表项的概要信息。

【使用指导】

如果不指定任何参数，则显示所有的 IPv4 组播会话表项。

【举例】

显示所有的 IPv4 组播会话表项的概要信息。

```
<Sysname> display session table multicast ipv4
```

Slot 1:

Inbound initiator:

```
Source      IP/port: 3.3.3.4/1609
Destination IP/port: 232.0.0.1/1025
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)
```

Inbound interface: GigabitEthernet1/0/1

Outbound interface list:

```
GigabitEthernet1/0/2
GigabitEthernet1/0/3
```

Totalsessions found: 1

显示所有的 IPv4 组播会话表项的详细信息。

```
<Sysname> display session table multicast ipv4 verbose
```

Slot 1:

Inbound initiator:

```
Source      IP/port: 3.3.3.4/1609
Destination IP/port: 232.0.0.1/1025
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)
```

Inbound responder:

```
Source      IP/port: 232.0.0.1/1025
Destination IP/port: 3.3.3.4/1609
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)
```

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

State: UDP_OPEN

Application: OTHER

Start time: 2014-03-03 15:59:22 TTL: 18s

Initiator->Responder: 1 packets 84 bytes

Outbound initiator:

```
Source      IP/port: 3.3.3.4/1609
Destination IP/port: 232.0.0.1/1025
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)
```

Outbound responder:

Source IP/port: 232.0.0.1/1025
 Destination IP/port: 3.3.3.4/1609
 DS-Lite tunnel peer: -
 VPN instance/VLAN ID/Inline ID: -/-/-
 Protocol: UDP(17)
 Outbound interface: GigabitEthernet1/0/2
 Destination security zone: aaa
 State: UDP_OPEN
 Application: OTHER
 Start time: 2014-03-03 15:59:22 TTL: 18s
 Initiator->Responder: 1 packets 84 bytes

Outbound initiator:
 Source IP/port: 3.3.3.4/1609
 Destination IP/port: 232.0.0.1/1025
 DS-Lite tunnel peer: -
 VPN instance/VLAN ID/Inline ID: -/-/-
 Protocol: UDP(17)

Outbound responder:
 Source IP/port: 232.0.0.1/1025
 Destination IP/port: 3.3.3.4/1609
 DS-Lite tunnel peer: -
 VPN instance/VLAN ID/Inline ID: -/-/-
 Protocol: UDP(17)
 Outbound interface: GigabitEthernet1/0/3
 Destination security zone: bbb
 State: UDP_OPEN
 Application: OTHER
 Start time: 2014-03-03 15:59:22 TTL: 18s
 Initiator->Responder: 1 packets 84 bytes

Total sessions found: 3

表1-12 display session table multicast ipv4 命令显示信息描述表

字段	描述
Inbound initiator	入接口上发起方到响应方的连接对应的组播会话信息
Inbound responder	入接口上响应方到发起方的连接对应的组播会话信息
Outbound initiator	出接口上发起方到响应方的连接对应的组播会话信息
Outbound responder	出接口上响应方到发起方的连接对应的组播会话信息
Source IP/port	源IP地址/端口号
Destination IP/port	目的IP地址/端口号
DS-Lite tunnel peer	DS-Lite隧道对端地址。会话不属于任何DS-Lite隧道时，本字段显示为“-”
VPN instance/VLAN ID/Inline ID	组播会话所属的MPLS L3VPN/二层转发时会话所属的VLAN ID/二层转发时会话所属的INLINE。未指定的参数则显示为“-”

字段	描述
Protocol	传输层协议类型，取值包括：DCCP、ICMP、Raw IP、SCTP、TCP、UDP、UDP-Lite，括号中的数字表示协议号
State	组播会话状态
Application	应用层协议类型，取值包括：FTP、DNS等，OTHER表示未知协议类型，其对应的端口为非知名端口
Start time	组播会话创建时间
TTL	组播会话剩余存活时间，单位为秒
Inbound interface	发起方到响应方首报文的入接口
Outbound interface	发起方到响应方首报文的出接口
Outbound interface list	发起方到响应方首报文的出接口列表
Source security zone	源安全域，即入接口所属的安全域。若接口不属于任何安全域，则显示为“-”
Destination security zone	目的安全域，即出接口所属的安全域。若接口不属于任何安全域，则显示为“-”
Initiator->Responder	发起方到响应方的报文数、报文字节数
Total sessions found	当前查找到的组播会话表项总数

1.1.11 display session table multicast ipv6

display session table multicast ipv6 命令用来显示 IPv6 组播会话表项信息。

【命令】

```
display session table multicast ipv6 [ slot slot-number ] [ [ responder ]
{ destination-ip start-destination-ip [ end-destination-ip ] |
destination-port destination-port | protocol { dccp | icmpv6 | raw-ip | sctp |
tcp | udp | udp-lite } | source-ip start-source-ip [ end-source-ip ] |
source-port source-port } * ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备上的 IPv6 组播会话表项，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，显示所有成员设备上的 IPv6 组播会话表项。

responder: 表示以响应方的信息筛选显示 IPv4 组播会话表项。若不指定该参数时，则以发起方的信息筛选显示 IPv4 组播会话表项。

destination-ip start-destination-ip [end-destination-ip]: 显示指定目的 IPv6 地址的组播会话表项。其中，*start-destination-ip* 表示目的 IPv6 地址的起始地址，*end-destination-ip* 表示目的 IPv6 地址的结束地址。

destination-port destination-port: 显示指定目的端口号的 IPv6 组播会话表项。其中，*destination-port* 表示端口号，取值为 0~65535。

protocol { dccp | icmpv6 | raw-ip | sctp | tcp | udp | udp-lite }: 显示指定协议类型的 IPv6 组播会话表项。

source-ip start-source-ip [end-source-ip]: 显示指定源 IPv6 地址的组播会话表项。其中，*start-source-ip* 表示源 IPv6 地址的起始地址，*end-source-ip* 表示源 IPv6 地址的结束地址。

source-port source-port: 显示指定源端口号的 IPv6 组播会话表项。其中，*source-port* 表示端口号，取值为 0~65535。

verbose: 显示 IPv6 组播会话表项的详细信息。不指定该参数时，显示 IPv6 组播会话表项的概要信息。

【使用指导】

如果不指定任何参数，则显示所有的 IPv6 组播会话表项。

【举例】

显示所有的 IPv6 组播会话表项的概要信息。

```
<Sysname> display session table multicast ipv6
```

Slot 1:

Inbound initiator:

Source IP/port: 3::4/1617

Destination IP/port: FF0E::1/1025

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: UDP(17)

Inbound interface: GigabitEthernet1/0/1

Outbound interface list:

GigabitEthernet1/0/2

GigabitEthernet1/0/3

Total sessions found: 3

显示所有的 IPv6 组播会话表项的详细信息。

```
<Sysname> display session table multicast ipv6 verbose
```

Slot 1:

Inbound initiator:

Source IP/port: 3::4/1617

Destination IP/port: FF0E::1/1025

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: UDP(17)

Inbound responder:

Source IP/port: FF0E::1/1025
Destination IP/port: 3::4/1617
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)

Inbound interface: GigabitEthernet1/0/1

Source security zone: Trust

State: UDP_OPEN

Application: OTHER

Start time: 2014-03-03 16:10:58 TTL: 23s

Initiator->Responder: 5 packets 520 bytes

Outbound initiator:

Source IP/port: 3::4/1617
Destination IP/port: FF0E::1/1025
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)

Outbound responder:

Source IP/port: FF0E::1/1025
Destination IP/port: 3::4/1617
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)

Outbound interface: GigabitEthernet1/0/2

Destination security zone: bbb

State: UDP_OPEN

Application: OTHER

Start time: 2014-03-03 16:10:58 TTL: 23s

Initiator->Responder: 5 packets 520 bytes

Outbound initiator:

Source IP/port: 3::4/1617
Destination IP/port: FF0E::1/1025
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)

Outbound responder:

Source IP/port: FF0E::1/1025
Destination IP/port: 3::4/1617
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: UDP(17)

Outbound interface: GigabitEthernet1/0/3

Destination security zone: ccc

State: UDP_OPEN

Application: OTHER

Start time: 2014-03-03 16:10:58 TTL: 23s
Initiator->Responder: 5 packets 520 bytes

Total sessions found: 3

表1-13 display session table multicast ipv6 命令显示信息描述表

字段	描述
Inbound initiator	入接口上发起方到响应方的连接对应的组播会话信息
Inbound responder	入接口上响应方到发起方的连接对应的组播会话信息
Outbound initiator	出接口上发起方到响应方的连接对应的组播会话信息
Outbound responder	出接口上响应方到发起方的连接对应的组播会话信息
Source IP/port	源IP地址/端口号
Destination IP/port	目的IP地址/端口号
DS-Lite tunnel peer	DS-Lite隧道对端地址。会话不属于任何DS-Lite隧道时，本字段显示为“-”
VPN instance/VLAN ID/Inline ID	组播会话所属的MPLS L3VPN/二层转发时会话所属的VLAN ID/二层转发时会话所属的INLINE。未指定的参数则显示为“-”
Protocol	传输层协议类型，取值包括：DCCP、ICMPv6、Raw IP、SCTP、TCP、UDP、UDP-Lite，括号中的数字表示协议号
State	组播会话状态
Application	应用层协议类型，取值包括：FTP、DNS等，OTHER表示未知协议类型，其对应的端口为非知名端口
Start time	组播会话创建时间
TTL	组播会话剩余存活时间，单位为秒
Inbound interface	发起方到响应方首报文的入接口
Outbound interface	发起方到响应方首报文的出接口
Outbound interface list	发起方到响应方首报文的出接口列表
Source security zone	源安全域，即入接口所属的安全域。若接口不属于任何安全域，则显示为“-”
Destination security zone	目的安全域，即出接口所属的安全域。若接口不属于任何安全域，则显示为“-”
Initiator->Responder	发起方到响应方的报文数、报文字节数
Total sessions found	当前查找到的组播会话表项总数

1.1.12 display session top-statistics

display session top-statistics 命令用来显示会话数目的 Top 10 排名统计信息。

【命令】

```
display session top-statistics { last-1-hour | last-24-hours | last-30-days }
```


【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

last-1-hour: 显示最近 1 小时的会话数目的 Top 10 排名统计信息。

last-24-hours: 显示最近 24 小时的会话数目的 Top 10 排名统计信息。

last-30-days: 显示最近 30 天的会话数据的 Top 10 排名统计信息。

【使用指导】

未开启会话数目的 Top 排名统计功能时，统计信息为空。

【举例】

显示最近 1 小时的会话数目 Top 10 的排名统计信息。

```
<Sysname> display session top-statistics last-1-hour
```

Counting by source addresses:

No.	Source address	Sessions
1	10.1.2.3	50004302
2	10.1.2.2	40123255
3	10.2.2.10	26664302
4	10.1.2.11	7123255
5	10.1.2.12	424302
6	10.1.2.13	253255
7	10.1.2.14	55302
8	10.1.2.15	50025
9	10.1.2.16	3555
10	10.1.2.1	995

Counting by destination addresses:

No.	Destination address	Sessions
1	20.1.2.3	50004302
2	20.1.2.2	40123255
3	20.2.2.10	26664302
4	20.1.2.11	7123255
5	20.1.2.12	424302
6	20.1.2.13	325325
7	20.1.2.14	55530
8	20.1.2.15	50025
9	20.1.2.16	3555
10	20.1.2.1	995

表1-14 display session top-statistics 命令显示信息描述表

字段	描述
Counting by source addresses	基于源IP地址的新建会话数目Top 10的排名统计信息
Counting by destination addresses	基于目的IP地址的新建会话数目Top 10的排名统计信息
No.	Top 10排名
Source address	会话的源IP地址
Destination address	会话的目的IP地址
Sessions	会话数目

【相关命令】

- **session top-statistics enable**

1.1.13 reset session relation-table

reset session relation-table 命令用来删除关联表项。

【命令】

reset session relation-table [ipv4 | ipv6] [slot slot-number]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4: 删除 IPv4 关联表项。

ipv6: 删除 IPv6 关联表项。

slot slot-number: 删除指定成员设备上的关联表项, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 删除所有成员设备上的关联表项。

【使用指导】

如果不指定任何参数, 则删除所有关联表项。

【举例】

删除所有的 IPv4 关联表项。

```
<Sysname> reset session relation-table ipv4
```

【相关命令】

- **display session relation-table**

1.1.14 reset session statistics

reset session statistics 命令用来清除单播会话统计信息。

【命令】

```
reset session statistics [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number: 清除指定成员设备上的单播会话统计信息, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 清除所有成员设备上的单播会话统计信息。

【举例】

```
# 清除所有的单播会话统计信息。  
<Sysname> reset session statistics
```

【相关命令】

- **display session statistics**

1.1.15 reset session statistics multicast

reset session statistics multicast 命令用来清除组播会话统计信息。

【命令】

```
reset session statistics multicast [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number: 清除指定成员设备上的组播会话统计信息, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 清除所有成员设备上的组播会话统计信息。

【举例】

```
# 清除所有的组播会话统计信息。  
<Sysname> reset session statistics multicast
```

【相关命令】

- **display session statistics multicast**

1.1.16 reset session table

reset session table 命令用来删除所有 IP 类型的单播会话表项。

【命令】

```
reset session table [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number: 删除指定成员设备上的所有单播会话表项, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 删除所有成员设备上的所有单播会话表项。

【举例】

```
# 删除所有单播会话表项。  
<Sysname> reset session table
```

【相关命令】

- **display session table ipv4**
- **display session table ipv6**

1.1.17 reset session table ipv4

reset session table ipv4 命令用来删除 IPv4 单播会话表项。

【命令】

```
reset session table ipv4 [ slot slot-number ] [ source-ip source-ip ]  
[ destination-ip destination-ip ] [ protocol { dccp | icmp | raw-ip | sctp | tcp  
| udp | udp-lite } ] [ source-port source-port ] [ destination-port  
destination-port ] [ vpn-instance vpn-instance-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number: 删除指定成员设备上的 IPv4 单播会话表项, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 删除所有成员设备上的 IPv4 单播会话表项。

source-ip source-ip: 删除指定源 IP 地址的 IPv4 单播会话表项。其中, *source-ip* 表示发起方到响应方会话的源 IPv4 地址。

destination-ip destination-ip: 删除指定目的 IP 地址的 IPv4 单播会话表项。其中，*destination-ip* 表示发起方到响应方会话的目的 IPv4 地址。

protocol { dccp | icmp | raw-ip | sctp | tcp | udp | udp-lite }: 删除指定协议类型的单播会话表项。其中，IPv4 传输层协议类型可包括：DCCP、ICMP、RawIP、SCTP、TCP、UDP 和 UDP-Lite。

source-port source-port: 删除指定源端口号的 IPv4 单播会话表项。其中，*source-port* 表示发起方到响应方会话的源端口号，取值为 0~65535。

destination-port destination-port: 删除指定目的端口号的 IPv4 单播会话表项。其中，*destination-port* 表示发起方到响应方会话的目的端口号，取值为 0~65535。

vpn-instance vpn-instance-name: 删除指定 VPN 实例的 IPv4 单播会话表项。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。不指定该参数时，删除公网中的 IPv4 单播会话表项。

【使用指导】

如果不指定任何参数，则删除所有公网中的 IPv4 单播会话表项。

【举例】

删除所有 IPv4 单播会话表项。

```
<Sysname> reset session table ipv4
```

删除所有发起方源 IP 地址为 10.10.10.10 的 IPv4 单播会话表项。

```
<Sysname> reset session table ipv4 source-ip 10.10.10.10
```

【相关命令】

- **display session table ipv4**

1.1.18 reset session table ipv6

reset session table ipv6 命令用来删除 IPv6 单播会话表项。

【命令】

```
reset session table ipv6 [ slot slot-number ] [ source-ip source-ip ]  
[ destination-ip destination-ip ] [ protocol { dccp | icmpv6 | raw-ip | sctp |  
tcp | udp | udp-lite } ] [ source-port source-port ] [ destination-port  
destination-port ] [ vpn-instance vpn-instance-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot slot-number: 删除指定成员设备上的 IPv6 单播会话表项，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，删除所有成员设备上的 IPv6 单播会话表项。

source-ip source-ip: 删除指定源 IP 地址的 IPv6 单播会话表项。其中，*source-ip* 表示发起方到响应方会话的源 IPv6 地址。

destination-ip destination-ip: 删除指定目的 IP 地址的 IPv6 单播会话表项。其中，*destination-ip* 表示发起方到响应方会话的目的 IPv6 地址。

protocol { dccp | icmpv6 | raw-ip | sctp | tcp | udp | udp-lite }: 删除指定协议类型的 IPv6 单播会话表项。其中，IPv6 传输层协议类型可包括：DCCP、ICMPv6、RawIP、SCTP、TCP、UDP 和 UDP-Lite。

source-port source-port: 删除指定源端口号的 IPv6 单播会话表项。其中，*source-port* 表示发起方到响应方会话的源端口号，取值为 0~65535。

destination-port destination-port: 删除指定目的端口号的 IPv6 单播会话表项。其中，*destination-port* 表示发起方到响应方会话的目的端口号，取值为 0~65535。

vpn-instance vpn-instance-name: 删除指定 VPN 实例的 IPv6 单播会话表项。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。不指定该参数时，删除公网中的 IPv6 单播会话表项。

【使用指导】

如果不指定任何参数，则删除所有公网中的 IPv6 单播会话表项。

【举例】

```
# 删除所有 IPv6 单播会话表项。
<Sysname> reset session table ipv6
# 删除所有发起方源 IP 地址为 2011::0002 的 IPv6 单播会话表项。
<Sysname> reset session table ipv6 source-ip 2011::0002
```

【相关命令】

- **display session table ipv6**

1.1.19 reset session table multicast

reset session table multicast 命令用来删除所有 IP 类型的组播会话表项。

【命令】

```
reset session table multicast [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

slot slot-number: 删除指定成员设备上的所有组播会话表项，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，删除所有成员设备上的所有组播会话表项。

【举例】

```
# 删除所有组播会话表项。
```

<Sysname> reset session table multicast

【相关命令】

- **display session table multicast ipv4**
- **display session table multicast ipv6**

1.1.20 reset session table multicast ipv4

reset session table multicast ipv4 命令用来删除 IPv4 组播会话表项。

【命令】

```
reset session table multicast ipv4 [ slot slot-number ] [ source-ip source-ip ]  
[ destination-ip destination-ip ] [ protocol { dccp | icmp | raw-ip | sctp | tcp  
| udp | udp-lite } ] [ source-port source-port ] [ destination-port  
destination-port ] [ vpn-instance vpn-instance-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number: 删除指定成员设备上的 IPv4 组播会话表项, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 删除所有成员设备上的 IPv4 组播会话表项。

source-ip source-ip: 删除指定源 IP 地址的 IPv4 组播会话表项。其中, *source-ip* 表示发起方到响应方组播会话的源 IPv4 地址。

destination-ip destination-ip: 删除指定目的 IP 地址的 IPv4 组播会话表项。其中, *destination-ip* 表示发起方到响应方组播会话的目的 IPv4 地址。

protocol { dccp | icmp | raw-ip | sctp | tcp | udp | udp-lite }: 删除指定协议类型的组播会话表项。其中, IPv4 传输层协议类型可包括: DCCP、ICMP、RawIP、SCTP、TCP、UDP 和 UDP-Lite。

source-port source-port: 删除指定源端口号的 IPv4 组播会话表项。其中, *source-port* 表示发起方到响应方组播会话的源端口号, 取值为 0~65535。

destination-port destination-port: 删除指定目的端口号的 IPv4 组播会话表项。其中, *destination-port* 表示发起方到响应方组播会话的目的端口号, 取值为 0~65535。

vpn-instance vpn-instance-name: 删除指定 VPN 实例的 IPv4 组播会话表项。其中, *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。不指定该参数时, 删除公网中的 IPv4 组播会话表项。

【使用指导】

如果不指定任何参数, 则删除所有公网中的 IPv4 组播会话表项。

【举例】

删除所有 IPv4 组播会话表项。

```
<Sysname> reset session table multicast ipv4
# 删除所有发起方源 IP 地址为 10.10.10.10 的 IPv4 组播会话表项。
<Sysname> reset session table multicast ipv4 source-ip 10.10.10.10
```

【相关命令】

- **display session table multicast ipv4**

1.1.21 reset session table multicast ipv6

reset session table multicast ipv6 命令用来删除 IPv6 组播会话表项。

【命令】

```
reset session table multicast ipv6 [ slot slot-number ] [ source-ip source-ip ]
[ destination-ip destination-ip ] [ protocol { dccp | icmpv6 | raw-ip | sctp |
tcp | udp | udp-lite } ] [ source-port source-port ] [ destination-port
destination-port ] [ vpn-instance vpn-instance-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number: 删除指定成员设备上的 IPv6 组播会话表项, *slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时, 删除所有成员设备上的 IPv6 组播会话表项。

source-ip source-ip: 删除指定源 IP 地址的 IPv6 组播会话表项。其中, *source-ip* 表示发起方到响应方组播会话的源 IPv6 地址。

destination-ip destination-ip: 删除指定目的 IP 地址的 IPv6 组播会话表项。其中, *destination-ip* 表示发起方到响应方组播会话的目的 IPv6 地址。

protocol { dccp | icmpv6 | raw-ip | sctp | tcp | udp | udp-lite }: 删除指定协议类型的 IPv6 组播会话表项。其中, IPv6 传输层协议类型可包括: DCCP、ICMPv6、RawIP、SCTP、TCP、UDP 和 UDP-Lite。

source-port source-port: 删除指定源端口号的 IPv6 组播会话表项。其中, *source-port* 表示发起方到响应方组播会话的源端口号, 取值为 0~65535。

destination-port destination-port: 删除指定目的端口号的 IPv6 组播会话表项。其中, *destination-port* 表示发起方到响应方组播会话的目的端口号, 取值为 0~65535。

vpn-instance vpn-instance-name: 删除指定 VPN 实例的 IPv6 组播会话表项。其中, *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。不指定该参数时, 删除公网中的 IPv6 组播会话表项。

【使用指导】

如果不指定任何参数, 则删除所有公网中的 IPv6 组播会话表项。

【举例】

删除所有 IPv6 组播会话表项。

```
<Sysname> reset session table multicast ipv6
```

删除所有发起方源 IP 地址为 2011::0002 的 IPv6 组播会话表项。

```
<Sysname> reset session table multicast ipv6 source-ip 2011::0002
```

【相关命令】

- **display session table multicast ipv6**

1.1.22 session aging-time application

session aging-time application 命令用来设置应用层协议或应用的会话老化时间。

undo session aging-time application 命令用来恢复缺省情况。如果不指定应用层协议或应用的名称，则将所有应用层协议和应用的会话老化时间都恢复为缺省情况。

【命令】

```
session aging-time application application-name time-value
```

```
undo session aging-time application [ application-name ]
```

【缺省情况】

部分应用层协议或应用的会话老化时间如下，单位为秒：

- DNS: 1
- FTP: 3600
- GTP-CONTROL: 60
- GTP-USER: 60
- GPRS-DATA: 60
- GPRS-SIG: 60
- H225: 3600
- H245: 3600
- RAS: 300
- RTSP: 3600
- SIP: 300
- TFTP: 60
- ILS: 3600
- MGCP-CALLAGENT: 60
- MGCP-GATEWAY: 60
- PPTP: 3600
- RSH: 60
- SCCP: 3600
- SQLNET: 600
- XDMCP: 3600
- BOOTPC: 120

- BOOTPS: 120
- FTP-DATA: 240
- HTTPS: 600
- L2TP: 120
- NETBIOS-DGM: 3600
- NETBIOS-NS: 3600
- NETBIOS-SSN: 3600
- NTP: 120
- QQ: 120
- RIP: 120
- SNMP: 120
- SNMPTRAP: 120
- STUN: 600
- SYSLOG: 120
- TACACS-DS: 120
- WHO: 120

除以上列举的之外，系统中其他的所有应用层协议或应用的会话老化时间均为 1200 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

application-name: 表示应用协议或应用的名称，为 1~63 个字符的字符串，不区分大小写，可以为数字、字母、连字符、下划线，但不允许为系统保留的“invalid”和“other”。该应用层协议或应用必须在设备上已存在。

time-value: 指定的老化时间，取值范围为 1~100000，单位为秒。

【使用指导】

应用层协议的会话老化时间仅在会话进入稳态时生效（TCP 会话的稳态为 TCP-EST，UDP 会话的稳态为 UDP-READY）。

会话进入稳态后，如果该会话属于本命令中指定的一种应用层协议或应用，则此会话的老化时间为指定的应用层协议或应用老化时间；否则为传输层协议状态的老化时间（由 **session aging-time state** 命令配置）。

对 TCP 会话来说，如果会话符合长连接会话的规则，那么该会话稳态的老化时间为长连接老化时间（由 **session persistent acl** 命令配置）。

此命令中的应用层协议或应用由 APR 模块定义，有关 APR 功能的详细介绍请参见“安全配置指导”中的“APR”。

【举例】

```
# 设置 FTP 协议的会话老化时间为 1800 秒。
<Sysname> system-view
[Sysname] session aging-time application ftp 1800
# 设置应用 126WebEmail 的会话老化时间为 1800 秒。
<Sysname> system-view
[Sysname] session aging-time application 126WebEmail 1800
```

【相关命令】

- **display session aging-time application**
- **nbar application**（安全命令参考/APR）
- **port-mapping**（安全命令参考/APR）
- **session aging-time state**
- **session persistent acl**

1.1.23 session aging-time state

session aging-time state 命令用来设置各协议状态的会话老化时间。

undo session aging-time state 命令用来恢复缺省情况，如果不指定任何参数，则将所有协议状态的会话老化时间都恢复为缺省情况。

【命令】

```
session aging-time state { fin | icmp-reply | icmp-request | rawip-open |
rawip-ready | syn | tcp-close | tcp-est | tcp-time-wait | udp-open | udp-ready }
time-value
undo session aging-time state [ fin | icmp-reply | icmp-request | rawip-open
| rawip-ready | syn | tcp-close | tcp-est | tcp-time-wait | udp-open |
udp-ready ]
```

【缺省情况】

各协议状态的会话老化时间为：

- FIN: 30 秒
- ICMP-REPLAY: 30 秒
- ICMP-REQUEST: 60 秒
- RAWIP-OPEN: 30 秒
- RAWIP-READY: 60 秒
- SYN: 30 秒
- TCP-CLOSE: 2 秒
- TCP-EST: 3600 秒
- TCP-TIME-WAIT: 2 秒
- UDP-OPEN: 30 秒
- UDP-READY: 60 秒

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

fin: 表示 TCP 协议 FIN-WAIT 状态的会话老化时间。

icmp-reply: 表示 ICMP 协议 REPLY 状态的会话老化时间。

icmp-request: 表示 ICMP 协议 REQUEST 状态的会话老化时间。

rawip-open: 表示 RAWIP-OPEN 状态的会话老化时间。

rawip-ready: 表示 RAWIP-READY 状态的会话老化时间。

syn: 表示 TCP 协议 SYN-SENT 和 SYN-RCV 状态的会话老化时间。

tcp-close: 表示 TCP 协议 CLOSE 状态的会话老化时间。

tcp-est: 表示 TCP 协议 ESTABLISHED 状态的会话老化时间。

tcp-time-wait: 表示 TCP 协议 TIME-WAIT 状态的会话老化时间。

udp-open: 表示 UDP 协议 OPEN 状态的会话老化时间。

udp-ready: 表示 UDP 协议 READY 状态的会话老化时间。

time-value: 指定的老化时间，取值范围为 1~100000，单位为秒。

【使用指导】

会话进入稳态后，如果该会话属于 **session aging-time application** 命令中指定的一种应用层协议，则此会话的老化时间为指定的应用层协议老化时间；否则为四层协议状态的老化时间（由 **session aging-time state** 命令配置）。

对 TCP 会话来说，如果会话符合长连接会话的规则，那么该会话稳态的老化时间为长连接老化时间（由 **session persistent acl** 命令配置）。

【举例】

设置 TCP 协议 SYN-SENT 和 SYN-RCV 状态的老化时间为 60 秒。

```
<Sysname> system-view
```

```
[Sysname] session aging-time state syn 60
```

【相关命令】

- **display session aging-time state**
- **session aging-time application**
- **session persistent acl**

1.1.24 session log { bytes-active | packets-active }

session log { bytes-active | packets-active }命令用来配置输出会话日志的流量阈值。

undo session log { bytes-active | packets-active }命令用来恢复缺省情况。

【命令】

```
session log { bytes-active bytes-value | packets-active packets-value }  
undo session log { bytes-active | packets-active }
```

【缺省情况】

未配置输出会话日志的流量阈值。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

bytes-value: 表示字节数阈值，取值范围为 1~100000，单位为兆字节。

packets-value: 表示报文数阈值，取值范围为 1~100000，单位为兆包。

【使用指导】

如果设置的流量阈值为 *n*，则一个会话每传输 *n* 兆个字节整数倍时或 *n* 兆个报文，设备就输出一相应的会话日志。

配置的流量阈值在软件快速转发的会话统计功能处于开启的状态下才能生效。否则，会话由于无法统计报文的流量信息而不能通过流量阈值触发输出会话日志。

同时配置了时间阈值和流量阈值的情况下，只要有一个阈值到达，就会输出相应的会话日志，并将所有的阈值统计信息清零。

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 设置输出会话日志的流量阈值为 10 兆包。  
<Sysname> system-view  
[Sysname] session statistics enable  
[Sysname] session log packets-active 10
```

【相关命令】

- **session log enable**
- **session statistics enable**

1.1.25 session log enable

session log enable 命令用来开启会话日志功能。

undo session log enable 命令用来关闭会话日志功能。

【命令】

```
session log enable { ipv4 | ipv6 } [ acl acl-number ] { inbound | outbound }  
undo session log enable { ipv4 | ipv6 } [ acl acl-number ] { inbound |  
outbound }
```

【缺省情况】

会话日志功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4: 表示 IPv4 会话日志。

ipv6: 表示 IPv6 会话日志。

acl *acl-number*: 对与指定 ACL 相匹配的会话输出会话日志，其中 *acl-number* 表示 ACL 的编号，取值范围为 2000~3999。如果不指定 ACL，则表示允许输出经过接口的所有 IPv4 或 IPv6 会话的日志。

inbound: 指定输出方向的会话日志。

outbound: 指定输出方向的会话日志。

【使用指导】

可配置仅输出单方向的会话日志，也可以配置输出双向的会话日志。每个方向上最多可以配置一个 IPv4 ACL 规则和一个 IPv6 ACL 规则。

开启会话日志功能后，若指定了相关阈值（流量阈值、时间阈值），则达到阈值条件时输出相应的会话日志。

开启会话日志功能后，若开启了新建会话日志功能和删除会话日志功能，则在会话表创建和删除时分别输出一次会话日志；否则在会话表创建和删除时不输出会话日志。

因为会话日志仅支持通过快速日志输出方式进行输出，开启会话日志功能后，必须配置快速日志输出的相关功能才能输出会话日志信息。有关快速日志输出模块的相关配置请参见“网络管理和监控配置指导”中的“快速日志输出”。

【举例】

在 GigabitEthernet1/0/1 接口下开启会话日志功能，指定输出此接口入方向上的所有 IPv4 会话日志。

```
<Sysname> system-view
[Sysname] session log flow-begin
[Sysname] session log flow-end
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] session log enable ipv4 inbound
```

在 GigabitEthernet1/0/2 接口下开启会话日志功能，指定输出此接口出方向上匹配 ACL 2050 的 IPv4 会话日志。

```
<Sysname> system-view
[Sysname] session log flow-begin
[Sysname] session log flow-end
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] session log enable ipv4 acl 2050 outbound
```

在 GigabitEthernet1/0/3 接口下开启会话日志功能，指定输出此接口出方向上匹配 ACL 2050 的 IPv6 会话日志。

```
<Sysname> system-view
[Sysname] session log flow-begin
[Sysname] session log flow-end
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] session log enable ipv6 acl 2050 outbound
```

【相关命令】

- **session log bytes-active**
- **session log flow-begin**
- **session log flow-end**
- **session log packets-active**
- **session log time-active**

1.1.26 session log flow-begin

session log flow-begin 命令用来开启新建会话日志功能，即新建会话时输出会话日志。

undo session log flow-begin 命令用来关闭新建会话日志功能。

【命令】

```
session log flow-begin
undo session log flow-begin
```

【缺省情况】

新建会话日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

只有同时开启了会话日志功能和新建会话日志功能，新建会话时才会输出会话日志。

【举例】

```
# 开启新建会话日志功能。
<Sysname> system-view
[Sysname] session log flow-begin
```

【相关命令】

- **session log enable**

1.1.27 session log flow-end

session log flow-end 命令用来开启删除会话日志功能，即删除会话时输出会话日志。

undo session log flow-end 命令用来关闭删除会话日志功能。

【命令】

```
session log flow-end
undo session log flow-end
```

【缺省情况】

删除会话日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

只有同时开启了会话日志功能和删除会话日志功能，删除会话时才会输出会话日志。

【举例】

```
# 开启删除会话日志功能。
<Sysname> system-view
[Sysname] session log flow-end
```

【相关命令】

- **session log enable**

1.1.28 session log time-active

session log time-active 命令用来配置输出会话日志的时间阈值。

undo session log time-active 用来恢复缺省情况。

【命令】

```
session log time-active time-value
undo session log time-active
```

【缺省情况】

不依据时间阈值发送会话日志。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

time-value: 表示发送会话日志的时间阈值，取值范围为 10~120，单位为分钟，只能为 10 的整数倍。

【使用指导】

如果设置的时间阈值为 n ，则每经过 n 分钟，设备就输出一次相应的会话日志。

同时配置了时间阈值和流量阈值的情况下，只要有一个阈值到达，就会输出相应的会话日志，并将所有的阈值统计信息清零。

【举例】

设置输出会话日志的时间阈值为 50 分钟。

```
<Sysname> system
[Sysname] session log time-active 50
```

【相关命令】

- **session log enable**
- **session log { bytes-active | packets-active }**

1.1.29 session persistent acl

session persistent acl 命令用来配置长连接会话规则。

undo session persistent acl 命令用来恢复缺省情况。

【命令】

```
session persistent acl [ ipv6 ] acl-number [ aging-time time-value ]
undo session persistent acl [ ipv6 ] acl-number
```

【缺省情况】

无长连接会话规则。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6: 指定 IPv6 ACL。如果没有指定本参数，则表示 IPv4 ACL。

acl-number: ACL 的编号，取值范围为 2000~3999。

aging-time time-value: 长连接会话的老化时间。其中，*time-value* 表示指定的老化时间，取值范围为 0~360，单位为小时，缺省值为 24。0 表示永不老化。

【使用指导】

长连接老化时间仅在 TCP 会话进入稳态（TCP-EST 状态）时生效。在 TCP 会话处于稳态时，长连接老化时间具有最高的优先级，其次为应用层协议老化时间，最后为协议状态老化时间。

对于长连接会话规则触发生成的长连接会话不会因为其配置的删除、修改或没有报文命中而被删除，只有当会话的发起方或响应方主动发起关闭连接请求、达到长连接会话老化时间或管理员使用 **reset session table** 命令手动删除该会话时，才会被删除。

长连接会话的配置仅影响后续生成的会话，对于已经生效的会话不产生作用。

可通过多次执行此命令来配置多条长连接会话规则。

【举例】

```
# 配置符合 ACL 2000 规则的 IPv4 会话为长连接，老化时间为 72 小时。
<Sysname> system-view
[Sysname] session persistent acl 2000 aging-time 72
# 配置符合 ACL 3000 规则的 IPv6 会话为长连接，老化时间为 100 小时。
<Sysname> system-view
[Sysname] session persistent acl ipv6 3000 aging-time 100
```

【相关命令】

- **session aging-time application**
- **session aging-time state**

1.1.30 session statistics enable

session statistics enable 命令用来开启软件快速转发的会话统计功能。

undo session statistics enable 命令用来关闭软件快速转发的会话统计功能。

【命令】

```
session statistics enable
undo session statistics enable
```

【缺省情况】

软件快速转发的会话统计功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启软件快速转发的会话统计功能之后，设备将对经软件快速转发收到和发送的基于会话的业务报文数目和报文字节数进行统计，基于会话的报文统计信息可以通过 **display session table** 命令查看，基于报文类型的报文统计信息可以通过 **display session statistics** 命令查看。

开启此功能后，会占用较多的 CPU 和内存资源，请只在需要时开启。

【举例】

```
# 开启软件快速转发的会话统计功能。
<Sysname> system-view
[Sysname] session statistics enable
```

【相关命令】

- **display session statistics**
- **display session table**

1.1.31 session top-statistics enable

session top-statistics enable 命令用来开启会话数目的 Top 排名统计功能。

undo session top-statistics enable 命令用来关闭会话数目的 Top 排名统计功能。

【命令】

```
session top-statistics enable
undo session top-statistics enable
```

【缺省情况】

会话数目的 Top 排名统计功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启会话数目的 Top 排名统计功能之后，设备将对基于会话的业务进行会话数目统计，分别基于源地址和目的地址对新建会话数目进行排序。会话数目的 Top 排名统计信息可以通过 **display session top-statistics** 命令查看。

【举例】

```
# 开启会话数目的 Top 排名统计功能。
<Sysname> system-view
[Sysname] session top-statistics enable
```

【相关命令】

- **display session top-statistics**

目 录

1 连接数限制	1-1
1.1 连接数限制配置命令	1-1
1.1.1 connection-limit	1-1
1.1.2 connection-limit apply	1-2
1.1.3 connection-limit apply global	1-2
1.1.4 description	1-3
1.1.5 display connection-limit	1-4
1.1.6 display connection-limit ipv6-stat-nodes	1-7
1.1.7 display connection-limit statistics	1-9
1.1.8 display connection-limit stat-nodes	1-10
1.1.9 limit	1-12
1.1.10 reset connection-limit statistics	1-15

1 连接数限制

1.1 连接数限制配置命令

1.1.1 connection-limit

connection-limit 命令用来创建连接数限制策略，并进入连接数限制策略视图。如果指定的连接数限制策略已经存在，则直接进入连接数限制策略视图。

undo connection-limit 命令用来删除连接数限制策略。

【命令】

```
connection-limit { ipv6-policy | policy } policy-id  
undo connection-limit { ipv6-policy | policy } policy-id
```

【缺省情况】

不存在连接数限制策略。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-policy: 指定 IPv6 连接数限制策略。

policy: 指定 IPv4 连接数限制策略。

policy-id: 连接数限制策略编号（IPv4、IPv6 连接数限制策略的编号空间各自独立），取值范围为 1~32。

【举例】

创建编号为 1 的 IPv4 连接数限制策略，并进入 IPv4 连接数限制策略视图。

```
<Sysname> system-view  
[Sysname] connection-limit policy 1  
[Sysname-connlmt-policy-1]
```

创建编号为 12 的 IPv6 连接数限制策略，并进入 IPv6 连接数限制策略视图。

```
<Sysname> system-view  
[Sysname] connection-limit ipv6-policy 12  
[Sysname-connlmt-ipv6-policy-12]
```

【相关命令】

- **connection-limit apply**
- **connection-limit apply global**
- **display connection-limit**

- **limit**

1.1.2 connection-limit apply

connection-limit apply 命令用来在接口上应用连接数限制策略。

undo connection-limit apply 命令用来在接口上取消应用的连接数限制策略。

【命令】

```
connection-limit apply { ipv6-policy | policy } policy-id
undo connection-limit apply { ipv6-policy | policy }
```

【缺省情况】

接口上未应用连接数限制策略。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-policy: 指定 IPv6 连接数限制策略。

policy: 指定 IPv4 连接数限制策略。

policy-id: 连接数限制策略编号，取值范围为 1~32。

【使用指导】

同一个接口上同时只能应用一个 IPv4 连接数限制策略和一个 IPv6 连接数限制策略，后配置的 IPv4 或 IPv6 连接数限制策略会覆盖已配置的对应该类型的策略。

【相关命令】

- **connection-limit**
- **limit**

1.1.3 connection-limit apply global

connection-limit apply global 命令用来在全局应用连接数限制策略。

undo connection-limit apply global 命令用来在全局取消应用的连接数限制策略。

【命令】

```
connection-limit apply global { ipv6-policy | policy } policy-id
undo connection-limit apply global { ipv6-policy | policy }
```

【缺省情况】

全局未应用连接数限制策略。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-policy: 指定 IPv6 连接数限制策略。
policy: 指定 IPv4 连接数限制策略。
policy-id: 连接数限制策略编号，取值范围为 1~32。

【使用指导】

全局最多只能应用一个 IPv4 连接数限制策略和一个 IPv6 连接数限制策略，后配置的 IPv4 或 IPv6 连接数限制策略会覆盖已配置的对应该类型的策略。

【举例】

```
# 在全局应用编号为 1 的 IPv4 连接数限制策略。
<Sysname> system-view
[Sysname] connection-limit apply global policy 1
# 在全局应用编号为 12 的 IPv6 连接数限制策略。
<Sysname> system-view
[Sysname] connection-limit apply global ipv6-policy 12
```

【相关命令】

- **connection-limit**
- **limit**

1.1.4 description

description 命令用来配置连接数限制策略的描述信息。
undo description 命令用来恢复缺省情况。

【命令】

description text
undo description

【缺省情况】

未配置描述信息。

【视图】

IPv4 连接数限制策略视图
IPv6 连接数限制策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

text: 表示连接数限制策略的描述信息，为 1~127 个字符的字符串，区分大小写。

【使用指导】

使用 **description** 命令时，如果当前连接数限制策略没有描述信息，则为其添加描述信息，否则修改其现有的描述信息。

【举例】

配置编号为 1 的 IPv4 连接数限制策略的描述信息为 CenterToA。

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1] description CenterToA
```

【相关命令】

- **display connection-limit**

1.1.5 display connection-limit

display connection-limit 命令用来显示连接数限制策略的配置信息。

【命令】

display connection-limit { ipv6-policy | policy } { policy-id | all }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ipv6-policy: 显示 IPv6 连接数限制策略。

policy: 显示 IPv4 连接数限制策略。

policy-id: 连接数限制策略编号，取值范围为 1~32。

all: 显示所有指定类型的连接数限制策略。

【举例】

显示所有 IPv4 连接数限制策略的配置信息。

```
<Sysname> display connection-limit policy all
```

3 policies in total:

Policy	Rule	Stat Type	HiThres	LoThres	Rate	PermitNew	ACL
0	1	Src-Dst-Port	2000	1800	10	No	3000
	12	Src-Dst	500	45	0	Yes	3001
	255	--	1000000	980000	0	No	2001
1	2	Dst-Port	800	70	0	Yes	3010
	3	Src-Dst	100	90	0	No	3000

	10	Src-Dst-Port	50	45	0	No	3003
	11	Src	200	200	0	No	3004
	200	--	500000	498000	0	No	2002
28	4	Port	1500	1400	0	No	3100
	5	Dst	3000	280	0	No	3101
	21	Src-Dst	200	180	0	No	3102
	25	Src-Port	50	35	0	No	3200

Description list:

Policy	Description

1	IPv4Description1
28	Description for IPv4 28

显示编号为 1 的 IPv4 连接数策略的配置信息。

<Sysname> display connection-limit policy 1

IPv4 connection limit policy 1 has been applied 5 times, and has 5 limit rules.

Description: IPv4Description1

Limit rule list:

Policy	Rule	Stat Type	HiThres	LoThres	Rate	PermitNew	ACL
1	2	Dst-Port	800	70	0	Yes	3010
	3	Src-Dst	100	90	0	No	3000
	10	Src-Dst-Port	50	45	0	No	3003
	11	Src	200	200	0	No	3004
	200	--	500000	498000	0	No	2002

Application list:

GigabitEthernet1/0/1
GigabitEthernet1/0/2
Vlan-interface2
Global

显示所有 IPv6 连接数限制策略的配置信息。

<Sysname> display connection-limit ipv6-policy all

2 policies in total:

Policy	Rule	Stat Type	HiThres	LoThres	Rate	PermitNew	ACL
3	1	Src-Dst	1000	800	10	Yes	3010
	2	Dst	500	450	0	Yes	3001
4	2	Src-Dst-Port	800	700	0	No	3010
	3	Src	100	90	0	No	3020
	200	--	100000	89000	0	No	2005

Description list:

Policy	Description

3	IPv6Description3
4	Description for IPv6 4

```
# 显示编号为 3 的 IPv6 连接数限制策略的配置信息。
<Sysname> display connection-limit ipv6-policy 3
IPv6 connection limit policy 3 has been applied 3 times, and has 2 limit rules.
Description: IPv6Description3
Limit rule list:
Policy  Rule      Stat Type  HiThres  LoThres  Rate      PermitNew  ACL
-----
      3      1      Src-Dst   1000     800     0          Yes      3010
              2          Dst     500     450     0          No       3001
Application list:
    GigabitEthernet1/0/1
    Vlan-interface2
```

表1-1 display connection-limit 命令显示信息描述表

字段	描述
Limit rule list	连接数限制策略信息列表
Policy	连接数限制策略编号
Rule	连接数限制规则编号
Stat Type	统计方式，有如下取值： • Src-Dst-Port：按源 IP—目的 IP—服务的组合进行统计和限制 • Src-Dst：按源 IP—目的 IP 的组合进行统计和限制 • Src-Port：按源 IP—服务的组合进行统计和限制 • Dst-Port：按目的 IP—服务的组合进行统计和限制 • Src：按源 IP 进行统计和限制 • Dst：按目的 IP 进行统计和限制 • Port：按服务进行统计和限制 • Dslite：按 DS-Lite 隧道的 B4 设备进行统计和限制（暂不支持） • --：不按照具体的 IP 地址、服务进行统计和限制，与本规则引用的 ACL 相匹配的所有连接将整体受到指定的阈值限制
HiThres	连接数上限
LoThres	连接数下限
Rate	每秒新建连接速率值
ACL	规则引用的ACL编号或ACL名称
PermitNew	连接数或者新建速率超过设定的上限时，允许用户继续新建连接
Application list	连接数限制策略应用列表，包括接口名称和Global，其中Global表示该连接数限制策略应用在全局
Description	连接数限制策略描述信息
Description list	连接数限制策略描述信息列表

【相关命令】

- **connection-limit**
- **connection-limit apply**
- **connection-limit apply global**
- **limit**

1.1.6 display connection-limit ipv6-stat-nodes

display connection-limit ipv6-stat-nodes 命令用来显示连接数限制在全局或接口的 IPv6 统计节点列表。

【命令】

```
display connection-limit ipv6-stat-nodes { global | interface  
interface-type interface-number } [ slot slot-number ] [ { deny-new |  
permit-new } | destination destination-ip | service-port port-number | source  
source-ip ] * [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

global: 显示全局的 IPv6 统计节点列表。

interface interface-type interface-number: 显示指定接口的 IPv6 统计节点列表，*interface-type interface-number* 表示接口类型和接口编号。

slot slot-number: 显示指定成员设备上全局或全局接口的 IPv6 统计节点列表，*slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定显示全局统计节点列表，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。

deny-new: 显示禁止创建新连接的 IPv6 统计节点列表。

permit-new: 显示允许创建新连接的 IPv6 统计节点列表。

destination destination-ip: 显示指定目的 IP 地址的 IPv6 统计节点列表。

service-port port-number: 显示指定服务端口号的 IPv6 统计节点列表。

source source-ip: 显示指定源 IP 地址的 IPv6 统计节点列表。

count: 显示 IPv6 统计节点的个数。如果配置本参数，将仅显示符合条件的（由 **count** 前面的参数决定）IPv6 统计节点的数量，而不显示 IPv6 统计节点的具体内容。如果不指定本参数，则显示符合条件的 IPv6 统计节点的具体内容。

【使用指导】

一个统计节点标识了连接数限制进行统计和限制的一个对象（一个连接或一类连接），包括该连接的报文特征（源/目的 IP 地址、服务端口号、传输层协议类型等）、对该连接所应用的连接限制策略、当前连接数目以及当前是否允许创建新的连接。

如果指定 **source**、**destination**、**service-port**、**deny-new**、**permit-new** 中的一个或多个参数，则表示将按照多个条件来显示统计节点列表，比如指定了 **source** 和 **destination**，则显示同时符合指定源 IP 地址和目的 IP 地址的统计节点列表。

如果不指定 **source**、**destination**、**service-port**、**deny-new**、**permit-new** 中任何一个参数，则表示显示所有的统计节点列表。

修改或删除连接数限制策略后，由该策略产生且已经生效的连接数限制统计节点不会受到影响。这些节点将在所统计的连接都断开后自动删除。

【举例】

显示 2 号成员设备上全局的 IPv6 连接数限制统计节点列表。

```
<Sysname> display connection-limit ipv6-stat-nodes global slot 2
```

Slot 2:

```
Src IP address      : Any
  VPN instance      : --
Dst IP address      : Any
  VPN instance      : --
DS-Lite tunnel peer : --
Service             : icmp/0
Limit rule ID       : 22(ACL: 3666)
Sessions threshold Hi/Lo: 3500/3000
Sessions count      : 3100
Sessions limit rate  : 0
New session flag     : Permit
```

显示 2 号成员设备上的 IPv6 连接数限制统计节点个数。

```
<Sysname> display connection-limit ipv6-stat-nodes global slot 2 count
```

Slot 2:

```
Current limit statistic nodes count is 0.
```

表1-2 display connection-limit stat-nodes 命令显示信息描述表

字段	描述
Src IP address	源IP地址
Dst IP address	目的IP地址
VPN instance	该地址所属的MPLS L3VPN的VPN实例名称，“--”表示属于公网
DS-Lite tunnel peer	（暂不支持）DS Lite隧道对端的IP地址，“--”表示不属于任何DS Lite Tunnel
Service	协议名及服务端口号。如果不是知名协议则显示为“unknown(xx)”，xx为协议编号，此时不显示服务端口号。其中，对于ICMP协议，括弧内的数字为ICMP的type和code字段组合表示的十六进制数所对应的十进制数
Limit rule ID	匹配的规则编号，括号里为匹配的ACL编号
Sessions threshold Hi/Lo	连接数限制的上限值及下限值

字段	描述
Sessions count	当前连接计数
Sessions limit rate	每秒新建连接的最大数目
New session flag	是否允许创建新连接，Permit表示允许创建，Deny表示不允许创建  说明 当连接数增长到上限值（max-amount）时，New session flag 仍显示为 Permit，但此时不允许创建新连接。只有连接数超过上限值，New session flag 才会显示为 Deny

【相关命令】

- `connection-limit apply global ipv6-policy`
- `connection-limit apply ipv6-policy`
- `connection-limit ipv6-policy`
- `limit`

1.1.7 display connection-limit statistics

`display connection-limit statistics` 命令用来显示连接数限制在全局或接口的统计信息。

【命令】

`display connection-limit statistics { global | interface interface-type interface-number } [ slot slot-number ]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

global：显示全局的连接数限制统计信息。

interface *interface-type* *interface-number*：显示指定接口的连接数限制统计信息，*interface-type* *interface-number* 表示接口类型和接口编号。

slot *slot-number*：显示指定成员设备上全局或全局接口的连接数限制统计信息，*slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定显示全局的连接数限制统计信息，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。

【举例】

显示 2 号成员设备上全局的连接数限制统计信息。

```
<Sysname> display connection-limit statistics global slot 2
Connection limit statistics (Global, slot 2):
```

Dropped IPv4 packets: 74213
Dropped IPv6 packets: 58174

表1-3 display connection-limit statistics 命令显示信息描述表

字段	描述
Dropped IPv4 packet	匹配全局或接口IPv4连接数限制策略，因连接数超过指定上限而被丢弃的报文个数
Dropped IPv6 packet	匹配全局或接口IPv6连接数限制策略，因连接数超过指定上限而被丢弃的报文个数

【相关命令】

- **connection-limit**
- **connection-limit apply**
- **connection-limit apply global**
- **limit**

1.1.8 display connection-limit stat-nodes

display connection-limit stat-nodes 命令用来显示连接数限制在全局或接口的 IPv4 统计节点列表。

【命令】

```
display connection-limit stat-nodes { global | interface interface-type  
interface-number } [ slot slot-number ] [ { deny-new | permit-new } |  
destination destination-ip | service-port port-number | source source-ip ] *  
[ count ]  
display connection-limit stat-nodes { global | interface interface-type  
interface-number } [ slot slot-number ] dslite-peer b4-address [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

global: 显示全局的 IPv4 统计节点列表。

interface interface-type interface-number: 显示指定接口的 IPv4 统计节点列表，*interface-type interface-number* 表示接口类型和接口编号。

slot slot-number: 显示指定成员设备上全局或全局接口的 IPv4 统计节点列表，*slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定显示全局统计节点列表，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。

deny-new: 显示禁止创建新连接的 IPv4 统计节点列表。

permit-new: 显示允许创建新连接的 IPv4 统计节点列表。

destination destination-ip: 显示指定目的 IP 地址的 IPv4 统计节点列表。

service-port port-number: 显示指定服务端口号的 IPv4 统计节点列表。

source source-ip: 显示指定源 IP 地址的 IPv4 统计节点列表。

dslite-peer b4-address: 显示指定 DS-Lite B4 设备的 IPv4 统计节点列表，*b4-address* 表示 B4 设备的 IPv6 地址。

count: 显示 IPv4 统计节点的个数。如果配置本参数，将仅显示符合条件的（由 **count** 前面的参数决定）IPv4 统计节点的数量，而不显示 IPv4 统计节点的具体内容。如果不指定本参数，则显示符合条件的 IPv4 统计节点的具体内容。

【使用指导】

一个统计节点标识了连接数限制进行统计和限制的一个对象（一个连接或一类连接），包括该连接的报文特征（源/目的 IP 地址、服务端口号、传输层协议类型等）、对该连接所应用的连接限制策略、当前连接数目的统计值，以及当前是否允许创建新的连接。

如果指定 **source**、**destination**、**service-port**、**deny-new**、**permit-new** 中的一个或多个参数，则表示将按照多个条件来显示统计节点列表，比如指定了 **source** 和 **destination**，则显示同时符合指定源 IP 地址和目的 IP 地址的统计节点列表。

如果不指定 **source**、**destination**、**service-port**、**deny-new**、**permit-new** 中任何一个参数，则表示显示所有的统计节点列表。

修改或删除连接数限制策略后，由该策略产生且已经生效的连接数限制统计节点不会受到影响。这些节点将在所统计的连接都断开后自动删除。

【举例】

显示 2 号成员设备上全局的 IPv4 连接数限制统计节点列表。

```
<Sysname> display connection-limit stat-nodes global slot 2
```

Slot 2:

Src IP address	: Any
VPN instance	: Vpn1
Dst IP address	: 202.113.16.117
VPN instance	: Vpn2
DS-Lite tunnel peer	: --
Service	: icmp/0
Limit rule ID	: 7(ACL: 3102)
Sessions threshold Hi/Lo:	4000/3800
Sessions count	: 1001
Sessions limit rate	: 0
New session flag	: Permit

显示 2 号成员设备上源 IP 地址为 1.1.1.1 的 IPv4 连接数限制统计节点个数。

```
<Sysname> display connection-limit stat-nodes global slot 2 source 1.1.1.1 count
```

Slot 2:

Current limit statistic nodes count is 0.

表1-4 display connection-limit stat-nodes 命令显示信息描述表

字段	描述
Src IP address	源IP地址
Dst IP address	目的IP地址
VPN instance	该地址所属的MPLS L3VPN的VPN实例名称，“--”表示不属于任何VPN
DS-Lite tunnel peer	（暂不支持）DS Lite隧道对端的IP地址，“--”表示不属于任何DS Lite Tunnel
Service	协议名及服务端口号。如果不是知名协议则显示为“unknown(xx)”，xx为协议编号，此时不显示服务端口号。其中，对于ICMP协议，括弧内的数字为ICMP的type和code字段组合表示的十六进制数所对应的十进制数
Limit rule ID	匹配的规则编号，括号里为匹配的ACL编号
Sessions threshold Hi/Lo	连接数限制的上限值及下限值
Sessions count	当前连接计数
Sessions limit rate	每秒新建连接的最大数目
New session flag	是否允许创建新连接，Permit表示允许创建，Deny表示不允许创建  说明 当连接数增长到上限值（max-amount）时，New session flag仍显示为Permit，但此时不允许创建新连接。只有连接数超过上限值，New session flag才会显示为Deny

【相关命令】

- **connection-limit policy**
- **connection-limit apply global policy**
- **connection-limit apply policy**
- **limit**

1.1.9 limit

limit 命令用来配置连接数限制规则。

undo limit 命令用来删除指定的连接数限制规则。

【命令】

IPv4 连接数限制策略视图：

```
limit limit-id acl { acl-number | name acl-name } [ per-destination | per-service | per-source ] * { amount max-amount min-amount | rate rate } * [ description text | permit-new ] *
```

```
limit limit-id acl ipv6 { acl-number | name acl-name } per-dslite-b4 { amount max-amount min-amount | rate rate } * [ description text | permit-new ] *
```

```
undo limit limit-id
```

IPv6 连接数限制策略视图：


```

limit limit-id acl ipv6 { acl-number | name acl-name } [ per-destination |
per-service | per-source ] * { amount max-amount min-amount | rate rate } *
[ description text | permit-new ] *
undo limit limit-id

```

【缺省情况】

不存在连接数限制规则。

【视图】

IPv4 连接数限制策略视图

IPv6 连接数限制策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

limit-id: 连接数限制规则编号，取值范围为 1~256。

acl: 指定用于匹配用户范围的 ACL。该连接限制规则仅对匹配 ACL 规则的用户连接数进行统计和限制。

ipv6: 表示引用 IPv6 ACL。若不指定该参数，则表示引用 IPv4 ACL。

acl-number: ACL 的编号，取值范围为 2000~3999。

name acl-name: ACL 的名称，为 1~63 个字符的字符串，不区分大小写，必须以英文字母 a~z 或 A~Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

per-destination: 表示按目的地址进行统计和限制。

per-service: 表示按服务（即按传输层协议和服务端口）进行统计和限制。

per-source: 表示按源地址进行统计和限制。

amount: 表示对连接数进行限制。

max-amount: 指定的连接数上限，取值范围为 1~4294967294。若不配置 **permit-new** 参数，当某范围或某种类型的连接数值超过此值时，用户将不能建立新的连接，直到连接数下降到 **min-amount** 指定的连接数下限之下时，才允许用户建立新的连接。

min-amount: 指定的连接数下限，取值范围为 1~4294967294，不能大于 **max-amount** 的取值。连接数的统计值降到此值之下时，允许用户建立新的连接。

rate: 表示对新建连接速率进行限制。

rate: 指定每秒新建连接的最大数目，取值范围为 5~10000000。若不配置 **permit-new** 参数，当某范围或某种类型的新建连接数速率超过此值时，用户将不能建立新的连接。

description text: 表示连接数限制规则的描述信息，其中，**text** 为 1~127 个字符的字符串，区分大小写。

permit-new: 当连接数或者新建速率超过设定的上限时，允许用户继续新建连接。设备将记录告警日志。

【使用指导】

每个连接数限制策略中可以定义多个规则，每个规则中需要指定引用的 ACL、规则的类型以及统计的上下门限值/新建速率限值。对于 **per-destination**、**per-source**、**per-service** 类型，可以在一条规则中单独指定其中之一或指定它们的组合。例如，同时指定 **per-destination** 和 **per-source**，就表示同时按照连接的报文源地址和目的地址进行统计和限制，具有相同源和目的的连接属于同一类连接，该类连接的数目将受到指定的阈值的限制。对于 **per-dslite-b4** 类型，只能在一条规则中单独指定。

对设备上建立的连接与某连接数限制策略进行匹配时，将按照规则编号从小到大的顺序依次遍历该策略中的所有规则，直到找到一条匹配的规则为止。

同一个连接数限制策略中的不同规则必须引用不同的 ACL。

当引用的 ACL 内容发生改变时，设备将按照新的连接数限制策略重新对已有连接进行统计和限制。

如果 **per-destination**、**per-service**、**per-source** 三个参数都不指定，则表示与本规则引用的 ACL 相匹配的所有连接将整体受到指定的阈值限制。

【举例】

在 IPv4 连接数限制策略 1 中创建一条规则，规则编号为 1，引用 ACL 3000，对匹配 ACL 3000 的连接同时按照报文的源地址和目的地址进行统计和限制，连接数的上限值为 2000、下限值为 1800。该规则用于限制 192.168.0.0/24 网段的每台主机最多只能同时向外网的同一个目的 IP 地址发起 2000 条连接，超过 2000 条时，需要等待连接数下降到 1800 以下之后，才允许新建连接，且每秒最多允许新建连接数为 10。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1] limit 1 acl 3000 per-destination per-source amount 2000 1800 rate 10
```

在 IPv4 连接数限制策略 1 中创建一条规则，规则编号为 1，引用 ACL 3000，对匹配 ACL 3000 的连接同时按照报文的源地址和目的地址进行统计和限制，连接数的上限值为 2000、下限值为 1800。该规则用于限制 192.168.0.0/24 网段的每台主机最多只能同时向外网的同一个目的 IP 地址发起 2000 条连接，超过 2000 条时，允许新建连接，但会产生告警日志，每秒最多允许新建连接数为 10，超过 10 时，允许新建连接，但会产生告警日志。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1] limit 1 acl 3000 per-destination per-source amount 2000 1800 rate 10 permit-new
```

在 IPv6 连接数限制策略 12 中创建一条规则，规则编号为 2，引用 ACL 2001，对匹配 ACL 2001 的连接按照报文的源地址进行统计和限制，连接数的上限值为 200、下限值为 100。该规则用于限制 2::1::/96 网段的主机最多只能同时向外网的同一个目的 IP 地址发起 200 条连接，超过 200 条时，需要等待连接数下降到 100 以下之后，才允许新建连接，且每秒最多允许新建连接数为 10。

```
<Sysname> system-view
```

```

[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2:1::/96
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] connection-limit ipv6-policy 12
[Sysname-connlmt-ipv6-policy-12] limit 2 acl ipv6 2001 per-destination amount 200 100 rate 10
# 在 IPv6 连接数限制策略 12 中创建一条规则，规则编号为 2，引用 ACL 2001，对匹配 ACL 2001 的连接按照报文的目的地址进行统计和限制，连接数的上限值为 200、下限值为 100。该规则用于限制 2:1::/96 网段的主机最多只能同时向外网的同一个目的 IP 地址发起 200 条连接，超过 200 条时，允许新建连接，但会产生告警日志，每秒最多允许新建连接数为 10，超过 10 时，允许新建连接，但会产生告警日志。
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2:1::/96
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] connection-limit ipv6-policy 12
[Sysname-connlmt-ipv6-policy-12] limit 2 acl ipv6 2001 per-destination amount 200 100 rate 10 permit-new

```

【相关命令】

- **connection-limit**
- **display connection-limit**

1.1.10 reset connection-limit statistics

reset connection-limit statistics 命令用来清除连接数限制在全局或接口的统计信息。

【命令】

```

reset connection-limit statistics { global | interface interface-type interface-number } [ slot slot-number ]

```

【视图】

用户视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

global: 清除全局的连接数限制统计信息。

interface *interface-type* *interface-number*: 清除指定接口上的连接数限制统计信息，*interface-type* *interface-number* 表示接口类型和接口编号。

slot *slot-number*: 清除指定成员设备上全局或全局接口应用的连接数限制统计信息，*slot-number* 表示设备在 IRF 中的成员编号。该参数仅在指定清除全局的连接数限制统计信息，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。

【举例】

清除 2 号成员设备上全局应用的连接数限制统计信息。

```
<Sysname> reset connection-limit statistics global slot 2
```

【相关命令】

- **display connection-limit statistics**

目 录

1 对象组	1-1
1.1 对象组配置命令	1-1
1.1.1 description	1-1
1.1.2 display object-group	1-1
1.1.3 mac	1-3
1.1.4 network (IPv4 address object group view)	1-4
1.1.5 network (IPv6 address object group view)	1-7
1.1.6 network exclude	1-9
1.1.7 object-group	1-10
1.1.8 object-group rename	1-11
1.1.9 security-zone	1-12
1.1.10 service(service object group view)	1-13

1 对象组

1.1 对象组配置命令

1.1.1 description

description 命令用来配置对象组的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

对象组未配置任何描述信息。

【视图】

对象组视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: 表示对象组的描述信息，为 1~127 个字符的字符串，区分大小写。

【举例】

配置对象组的描述信息为 “This is an IPv4 object-group”。

```
<Sysname> system-view
```

```
[Sysname] object-group ip address ipgroup
```

```
[Sysname-obj-grp-ip-ipgroup] description This is an IPv4 object-group
```

1.1.2 display object-group

display object-group 命令用来显示对象组的内容。

【命令】

display object-group [{ { **ip** | **ipv6** } **address** | **mac-address** | **service** }
[**default**] [**name** *object-group-name*] | **name** *object-group-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin
context-operator

【参数】

ip address: 指定对象组类型为 IPv4 地址对象组。

ipv6 address: 指定对象组类型为 IPv6 地址对象组。

mac-address: 指定对象组类型为 MAC 地址对象组。

service: 指定对象组类型为服务对象组。

default: 指定默认对象组。

name: 指定对象组名称。

object-group-name: 对象组的名称，为 1~31 个字符的字符串，不区分大小写。

【举例】

显示所有对象组。

```
<Sysname> display object-group
```

```
IP address object group obj1: 0 object(in use)
```

```
IP address object group obj2: 6 objects(out of use)
```

```
0 network host address 1.1.1.1
```

```
10 network host name host
```

```
20 network subnet 1.1.1.1 255.255.255.0
```

```
30 network range 1.1.1.1 1.1.1.2
```

```
40 network group-object obj1
```

```
50 network user-group group1
```

```
IPv6 address object-group obj3: 0 object(in use)
```

```
IPv6 address object-group obj4: 5 objects(out of use)
```

```
0 network host address 1::1:1
```

```
10 network host name host
```

```
20 network subnet 1::1:0 112
```

```
30 network range 1::1:1 1::1:2
```

```
40 network group-object obj3
```

```
Service object-group obj5: 0 object(in use)
```

```
Service object-group obj6: 6 objects(out of use)
```

```
0 service 200
```

```
10 service tcp source lt 50 destination range 30 40
```

```
20 service udp source range 30 40 destination gt 30
```

```
30 service icmp 20 20
```

```
40 service icmpv6 20 20
```

```
50 service group-object obj5
```

```
MAC object-group obj7: 0 object(in use)
```

```

MAC object-group obj8: 2 objects(out of use)
0 MAC address 0010-dc28-11ac
10 MAC group-object obj7
# 显示名称为 obj2 的对象组。
<Sysname> display object-group name obj2
IP address object-group obj2: 5 objects(out of use)
0 network host address 1.1.1.1
10 network host name host
20 network subnet 1.1.1.1 255.255.255.0
30 network range 1.1.1.1 1.1.1.2
40 network group-object obj1
# 显示所有 IPv4 地址对象组。
<Sysname> display object-group ip address
IP address object-group obj1: 0 object(in use)

IP address object-group obj2: 5 objects(out of use)
0 network host address 1.1.1.1
10 network host name host
20 network subnet 1.1.1.1 255.255.255.0
30 network range 1.1.1.1 1.1.1.2
40 network group-object obj1
# 显示名称为 obj4 的 IPv6 地址对象组。
<Sysname> display object-group ipv6 address name obj4
IPv6 address object-group obj4: 5 objects(out of use)
0 network host address 1::1:1
10 network host name host
20 network subnet 1::1:0 112
30 network range 1::1:1 1::1:2
40 network group-object obj3

```

表1-1 display object-group 命令显示信息描述表

字段	描述
in use	表明此对象组被引用，包括被ACL引用或被对象组嵌套引用
out of use	表明此对象组没有被引用

1.1.3 mac

mac 命令用来创建一个 MAC 地址对象。

undo mac 命令用来删除指定的 MAC 地址对象。

【命令】

```

[ object-id ] mac { mac-address | group-object object-group-name }
undo mac { mac-address | group-object object-group-name }
undo object-id

```


【缺省情况】

不存在 MAC 地址对象。

【视图】

MAC 地址对象组视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-id: 指定对象 ID，取值范围为 0~4294967294。若未指定本参数，系统将按照步长 10 从 0 开始，自动分配一个大于现有最大 ID 的最小 ID。譬如现有对象的最大 ID 为 22，那么自动分配的新 ID 将是 30。

mac-address: MAC 地址，格式为 H-H-H。

group-object object-group-name: 指定引用 MAC 地址对象组。**object-group-name** 表示 MAC 地址对象组名称，为 1~31 字符，不区分大小写。

【使用指导】

可通过多次执行本命令，在一个 MAC 地址对象组中配置多个 MAC 地址对象。

创建 MAC 地址对象时，需要注意的是：

- 如果指定 ID 的对象不存在，则表示创建一个新的对象。
- 如果指定 ID 的对象已存在，则表示对该对象进行修改。

在配置 **group-object** 参数时，需要注意的是：

- 如果指定名称的对象组不存在，则系统会创建此名称的 MAC 地址对象组。
- 如果指定名称的对象组存在，则对象组类型必须为 MAC 地址对象组。
- 引用的 MAC 地址对象组不能形成循环嵌套，譬如 MAC 地址对象组 a 引用 MAC 地址对象组 b，则 MAC 地址对象组 b 不能再引用 MAC 地址对象组 a。
- 引用的 MAC 对象组最大嵌套层次为 5 层，譬如 MAC 地址对象组 1、2、3、4 分别引用 MAC 地址对象组 2、3、4、5，则 MAC 地址对象组 5 不能再引用其他 MAC 地址对象组，MAC 地址对象组 1 也不能再被其他 MAC 地址对象组引用。

【举例】

为 MAC 地址对象组 groupmac，创建一个 MAC 地址对象 0010-dc28-a4e9。

```
<Sysname> system-view
```

```
[Sysname] object-group mac-address groupmac
```

```
[Sysname-obj-grp-mac-groupmac] mac 0010-dc28-a4e9
```

【相关命令】

- **display object-group**
- **object-group**

1.1.4 network (IPv4 address object group view)

network 命令用来创建一个 IPv4 地址对象。

undo network 命令用来删除指定的 IPv4 地址对象。

【命令】

```
[ object-id ] network { host { address ip-address | name host-name } | subnet  
ip-address { mask-length | mask | wildcard wildcard } | range ip-address1  
ip-address2 | group-object object-group-name | user user-name [ domain  
domain-name ] | user-group user-group-name [ domain domain-name ] }  
undo network { host { address ip-address | name host-name } | subnet  
ip-address { mask-length | mask | wildcard wildcard } | range ip-address1  
ip-address2 | group-object object-group-name | user user-name [ domain  
domain-name ] | user-group user-group-name [ domain domain-name ] }  
undo object-id
```

【缺省情况】

不存在 IPv4 地址对象。

【视图】

IPv4 地址对象组视图

【缺省用户角色】

network-admin
context-admin

【参数】

object-id: 指定对象 ID，取值范围为 0~4294967294。若未指定本参数，系统将按照步长 10 从 0 开始，自动分配一个大于现有最大 ID 的最小 ID。譬如现有对象的最大 ID 为 22，那么自动分配的新 ID 将是 30。

host: 指定主机 IPv4 地址或主机名称。

address ip-address: 指定主机 IPv4 地址。

name host-name: 指定主机名称。*host-name* 表示主机名称，为 1~60 字符，不区分大小写。支持模糊匹配主机名称，输入方式为*abc*或者*abc 或者 abc*，三种方式均表示主机名中包含指定的字符串即可。主机名称中间不能带“*”号。若输入的主机名中不存在“*”号，则表示精确匹配所配置的主机名。

subnet ip-address { mask-length | mask | wildcard wildcard }: 指定子网 IPv4 地址。*mask-length* 表示子网掩码长度，即掩码中连续“1”的个数，取值范围为 0~32。*mask* 表示接口 IPv4 地址相应的子网掩码，为点分十进制格式。**wildcard wildcard** 表示 IPv4 地址的通配符掩码（为 0 表示主机地址）。

range ip-address1 ip-address2: 指定范围 IPv4 地址。*ip-address1* 表示范围起始 IPv4 地址。*ip-address2* 表示范围结束 IPv4 地址。

group-object object-group-name: 指定引用 IPv4 地址对象组。*object-group-name* 表示 IPv4 地址对象组名称，为 1~31 字符，不区分大小写。

user user-name: 指定用户名称，为 1~55 字符，区分大小写。

user-group user-group-name: 指定用户组名称，为 1~32 字符，不区分大小写。

domain domain-name: 表示用户和用户组所属的身份识别域。*domain-name* 是身份识别域的名称, 为 1~255 个字符的字符串, 不区分大小写, 不能包括字符“?”。若不指定此参数, 则表示用户和用户组不属于任何身份识别域。

【使用指导】

创建对象时指定 ID, 如果指定 ID 的对象不存在, 则创建一条新的对象; 如果指定 ID 的对象已存在, 则对原对象进行修改。

新创建或修改的对象不能与已有对象的内容完全相同, 否则该命令执行失败, 并提示出错。

在配置 **subnet** 参数时, 如果指定 *mask-length* 为 32 或者 *mask* 为 255.255.255.255, 则该配置被视为主机地址对象配置。

在配置 **range** 参数时, 需要注意的是:

- 如果指定的 *ip-address1* 和 *ip-address2* 相同, 则该配置被视为主机地址对象配置。
- 如果指定的 *ip-address1* 和 *ip-address2* 是一个子网的起始地址和结束地址, 则该配置被视为子网地址对象配置。
- 如果指定的 *ip-address1* 比 *ip-address2* 大, 会自动调整范围为[*ip-address2*, *ip-address1*]。

在配置 **group-object** 参数时, 需要注意的是:

- 如果指定名称的对象组不存在, 则系统会创建此名称的 IP 地址对象组, 相反对象组类型必须为 IPv4 地址对象组。
- 引用的 IPv4 地址对象组不能形成循环, 譬如 IP 地址对象组 a 引用 IPv4 地址对象组 b, 则 IP 地址对象组 b 不能再引用 IP 地址对象组 a。
- 引用的 IPv4 地址对象组最大嵌套层次为 5 层, 譬如 IP 地址对象组 1、2、3、4 分别引用 IP 地址对象组 2、3、4、5, 则 IP 地址对象组 5 不能再引用其他 IPv4 地址对象组, IP 地址对象组 1 也不能再被其他 IP 地址对象组引用。

【举例】

配置地址为 192.168.0.1 的 IPv4 主机地址对象。

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network host address 192.168.0.1
```

配置匹配主机名称为 pc3 的 IPv4 主机地址对象。

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network host name pc3
```

配置模糊匹配主机名称为 abc 的 IPv4 主机地址对象。

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup1
[Sysname-obj-grp-ip-ipgroup1] network host name *abc*
```

配置地址为 192.167.0.0, 掩码长度为 24 的 IPv4 子网地址对象。

```
<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network subnet 192.167.0.0 24
```

配置地址为 192.166.0.0, 掩码为 255.255.0.0 的 IPv4 子网地址对象。

```

<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network subnet 192.166.0.0 255.255.0.0
# 配置地址范围为 192.165.0.100 到 192.165.0.200 的 IPv4 范围地址对象。

<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network range 192.165.0.100 192.165.0.200
# 配置引用 ipgroup2 对象组的地址对象。

<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network group-object ipgroup2
# 配置地址为 192.168.x.1 的不连续地址（通配符地址）对象，x 表示的地址内容可变。

<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network subnet 192.168.0.1 wildcard 0.0.255.0
# 配置引用用户名为 user1，身份识别域为 domain1 的用户。

<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network user user1 domain domain1
# 配置引用用户组名为 usergroup1，身份识别域为 domain1 的用户组。

<Sysname> system-view
[Sysname] object-group ip address ipgroup
[Sysname-obj-grp-ip-ipgroup] network user-group usergroup1 domain domain1

```

1.1.5 network (IPv6 address object group view)

network 命令用来创建一个 IPv6 地址对象。

undo network 命令用来删除指定的 IPv6 地址对象。

【命令】

```

[ object-id ] network { host { address ipv6-address | name host-name } | subnet
ipv6-address prefix-length | range ipv6-address ipv6-address2 |
group-object object-group-name | user user-name [ domain domain-name ] |
user-group user-group-name [ domain domain-name ] }
undo network { host { address ipv6-address | name host-name } | subnet
ipv6-address prefix-length | range ipv6-address1 ipv6-address2 |
group-object object-group-name | user user-name [ domain domain-name ] |
user-group user-group-name [ domain domain-name ] }
undo object-id

```

【缺省情况】

不存在 IPv6 地址对象。

【视图】

IPv6 地址对象组视图

【缺省用户角色】

network-admin
context-admin

【参数】

object-id: 指定对象 ID，取值范围为 0~4294967294。若未指定本参数，系统将按照步长 10 从 0 开始，自动分配一个大于现有最大 ID 的最小 ID。譬如现有对象的最大 ID 为 22，那么自动分配的新 ID 将是 30。

host: 指定主机 IPv6 地址或主机名称。

address ipv6-address: 指定主机 IPv6 地址。

name host-name: 指定主机名称。*host-name* 表示主机名称，为 1~60 字符，不区分大小写。支持模糊匹配主机名称，输入方式为*abc*或者*abc 或者 abc*，三种方式均表示主机名中包含指定的字符串即可。主机名称中间不能带“*”号。若输入的主机名中不存在“*”号，则表示精确匹配所配置的主机名。

subnet ipv6-address prefix-length: 指定子网 IPv6 地址。*prefix-length*: 指定 IPv6 地址的前缀长度，取值范围为 1~128。

range ipv6-address1 ipv6-address2: 指定范围 IPv6 地址。*ipv6-address1* 表示范围起始 IPv6 地址。*ipv6-address2* 表示范围结束 IPv6 地址。

group-object object-group-name: 指定引用 IPv6 地址对象组。*object-group-name* 表示 IPv6 地址对象组名称，为 1~31 字符，不区分大小写。

user user-name: 指定用户名称，为 1~55 字符，区分大小写。

user-group user-group-name: 指定用户组名称，为 1~32 字符，不区分大小写。

domain domain-name: 表示用户和用户组所属的身份识别域。*domain-name* 是身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包括字符“?”。若不指定此参数，则表示用户和用户组不属于任何身份识别域。

【使用指导】

创建对象时指定 ID，如果指定 ID 的对象不存在，则创建一条新的对象；如果指定 ID 的对象已存在，则对原对象进行修改。

新建或修改的对象不能与已有对象的内容完全相同，否则该命令执行失败，并提示出错。

在配置 **subnet** 参数时，如果指定掩码长度为 128，则该配置被视为主机地址对象配置。

在配置 **range** 参数时，需要注意的是：

- 如果指定的 *ipv6-address1* 和 *ipv6-address2* 相同，则该配置被视为主机地址对象配置。
- 如果指定的 *ipv6-address1* 和 *ipv6-address2* 是一个子网的起始地址和结束地址，则该配置被视为子网地址对象配置。
- 如果指定的 *ipv6-address1* 比 *ipv6-address2* 大，会自动调整范围为 [*ipv6-address2*, *ipv6-address1*]。

在配置 **group-object** 参数时，需要注意的是：

- 如果指定名称的对象组不存在，则系统会创建此名称的 IPv6 地址对象组。
- 如果指定名称的对象组存在，则对象组类型必须为 IPv6 地址对象组。

- 引用的 IPv6 地址对象组不能形成循环，譬如 IPv6 地址对象组 a 引用 IPv6 地址对象组 b，则 IPv6 地址对象组 b 不能再引用 IPv6 地址对象组 a。
- 引用的 IPv6 地址对象组最大嵌套层次为 5 层，譬如 IPv6 地址对象组 1、2、3、4 分别引用 IPv6 地址对象组 2、3、4、5，则 IPv6 地址对象组 5 不能再引用其他 IPv6 地址对象组，IPv6 地址对象组 1 也不能再被其他 IPv6 地址对象组引用。

【举例】

配置地址为 1::1 的 IPv6 主机地址对象。

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network host address 1::1
```

配置匹配主机名称为 pc3 的 IPv6 主机地址对象。

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network host name pc3
```

配置模糊匹配主机名称为 abc 的 IPv6 主机地址对象。

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group1
[Sysname-obj-grp-ipv6-ipv6group1] network host name *abc*
```

配置地址为 1:1:1::1，前缀长度为 24 的 IPv6 子网地址对象。

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network subnet 1:1:1::1 24
```

配置地址范围为 1:1:1::1 到 1:1:1::100 的 IPv6 范围地址对象。

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network range 1:1:1::1 1:1:1::100
```

配置引用 ipv6group2 对象组的地址对象。

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network group-object ipv6group2
```

配置引用用户名为 user1，身份识别域为 domain1 的用户。

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network user user1 domain domain1
```

配置引用用户组名为 usergroup1，身份识别域为 domain1 的用户组。

```
<Sysname> system-view
[Sysname] object-group ipv6 address ipv6group
[Sysname-obj-grp-ipv6-ipv6group] network user-group usergroup1 domain domain1
```

1.1.6 network exclude

network exclude 命令用来配置地址对象中排除的 IPv4/IPv6 地址。

undo network exclude 命令用来恢复缺省情况。

【命令】

```
object-id network exclude ip-address  
undo object-id network exclude ip-address
```

【缺省情况】

地址对象中不存在排除的 IPv4/IPv6 地址。

【视图】

IPv4 地址对象组
IPv6 地址对象组

【缺省用户角色】

network-admin
context-admin

【参数】

object-id: 指定对象 ID，取值范围为 0~4294967294，此对象 ID 必须已存在。
ip-address: 表示地址对象中排除的 IPv4/IPv6 地址。

【使用指导】

多次执行本命令，可在某个地址对象中排除多个 IPv4/IPv6 地址。

【举例】

```
# 配置地址为 192.166.0.0，掩码为 255.255.0.0 的 IPv4 子网地址对象，并配置此地址对象排除的  
IPv4 地址为 192.166.0.10。  
<Sysname> system-view  
[Sysname] object-group ip address ipgroup  
[Sysname-obj-grp-ip-ipgroup] 10 network subnet 192.166.0.0 255.255.0.0  
[Sysname-obj-grp-ip-ipgroup] 10 network exclude 192.166.0.10  
# 配置地址为 1:1:1::1，前缀长度为 24 的 IPv6 子网地址对象，并配置此地址对象排除的 IPv6 地址  
为 1:1:1::10  
<Sysname> system-view  
[Sysname] object-group ipv6 address ipv6group  
[Sysname-obj-grp-ipv6-ipv6group] 10 network subnet 1:1:1::1 24  
[Sysname-obj-grp-ipv6-ipv6group] 10 network exclude 1:1:1::10
```

1.1.7 object-group

object-group 命令用来创建一个对象组，并进入对象组视图。如果指定的对象组已经存在且类型一致，则直接进入对象组视图。

undo object-group 命令用来删除指定的对象组。

【命令】

```
object-group { { ip | ipv6 } address | mac-address | service }  
object-group-name  
undo object-group { { ip | ipv6 } address | mac-address | service }  
object-group-name
```


【缺省情况】

存在系统默认对象组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip address: 指定对象组类型为 IP 地址对象组。

ipv6 address: 指定对象组类型为 IPv6 地址对象组。

mac-address: 指定对象组类型为 MAC 地址对象组。

service: 指定对象组类型为服务对象组。

object-group-name: 对象组的名称，为 1~31 个字符的字符串，不区分大小写，且对象组的名称必须全局唯一。

【使用指导】

在配置 **object-group** 命令时，需要注意的是：

- 如果指定名称的对象组不存在，则创建对象组并进入其视图。
- 如果指定名称的对象组存在但类型不一致，命令执行失败，并提示出错。

在配置 **undo object-group** 命令时，需要注意的是：

- 如果指定名称的对象组不存在，处理结束。
- 如果指定名称的对象组存在但类型不一致，则命令执行失败，并提示出错。
- 要删除的对象组被 ACL 或者其他对象组引用，命令执行失败，并提示出错。
- 系统默认对象组不能被删除。

【举例】

配置名称为 ipgroup 的 IP 地址对象组。

```
<Sysname> system-view
```

```
[Sysname] object-group ip address ipgroup
```

配置名称为 ipv6group 的 IPv6 地址对象组。

```
<Sysname> system-view
```

```
[Sysname] object-group ipv6 address ipv6group
```

创建名称为 groupmac 的 MAC 地址对象组。

```
<Sysname> system-view
```

```
[Sysname] object-group mac-address groupmac
```

配置名称为 servicegroup 的服务对象组。

```
<Sysname> system-view
```

```
[Sysname] object-group service servicegroup
```

1.1.8 object-group rename

object-group rename 命令用来重命名对象组。

【命令】

object-group rename *old-object-group-name new-object-group-name*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

old-object-group-name: 被重命名对象组的名称，为 1~31 个字符的字符串，不区分大小写。

new-object-group-name: 重命名后的对象组名称，为 1~31 个字符的字符串，不区分大小写，且对象组的名称必须全局唯一。

【使用指导】

只能对用户创建的对象组进行重命名，系统缺省的对象组不能被重命名。

【举例】

重命名 IPv4 地址对象组 **ipgroup1** 的名称为 **ipgroup2**。

<Sysname> system-view

[Sysname] object-group rename ipgroup1 ipgroup2

【相关命令】

- **object-group**

1.1.9 security-zone

security-zone 命令用来配置地址对象组所属的安全域。

undo security-zone 命令用来恢复缺省情况。

【命令】

security-zone *security-zone-name*

【缺省情况】

未配置地址对象组所属的安全域。

【视图】

IPv4 地址对象组

IPv6 地址对象组

【缺省用户角色】

network-admin

context-admin

【参数】

security-zone-name: 安全域的名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”和“%”，不能是字符串“any”。

【使用指导】

将地址对象组加入安全域后，在使用 Web 方式配置安全策略的源/目的 IP 地址过滤条件时，只能从属于此次安全域和不属于任何安全域的地址对象组中选取，可达到快速选择地址对象组的目的。
一个对象组只能属于一个安全域。

【举例】

```
# 配置 IPv4 地址对象组 1 所属的安全域为 Local。  
<Sysname> system-view  
[Sysname] object-group ip address 1  
[Sysname-obj-grp-ip-1] security-zone Local
```

【相关命令】

- **object-group**

1.1.10 service(service object group view)

service 命令用来创建一个服务对象。

undo service 命令用来删除指定的服务对象。

【命令】

```
[ object-id ] service { protocol [ { source { { eq | lt | gt } port | range port1 port2 } | destination { { eq | lt | gt } port | range port1 port2 } } * | icmp-type icmp-code | icmpv6-type icmpv6-code ] | group-object object-group-name }  
undo service { protocol [ { source { { eq | lt | gt } port | range port1 port2 } | destination { { eq | lt | gt } port | range port1 port2 } } * | icmp-type icmp-code | icmpv6-type icmpv6-code ] | group-object object-group-name }  
undo object-id
```

【缺省情况】

不存在服务对象。

【视图】

服务对象组视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

object-id: 指定对象 ID，取值范围为 0~4294967294。若未指定本参数，系统将按照步长 10 从 0 开始，自动分配一个大于现有最大 ID 的最小 ID。譬如现有对象的最大 ID 为 22，那么自动分配的新 ID 将是 30。

protocol: 协议类型，可输入的形式如下：

- 数字：取值范围为 0~255；
- 名称：可选取 **tcp** (6)、**udp** (17)、**icmp** (1) 或 **icmpv6** (58)。

source: 指定源端口。只在 **protocol** 为 **tcp** 或 **udp** 时有效。

destination: 指定目的端口。只在 *protocol* 为 **tcp** 或 **udp** 时有效。

eq: 等于指定的端口号。

lt: 小于指定的端口号。

gt: 大于指定的端口号。

port: 指定端口号, 取值范围为 0~65535。

range port1 port2: 在指定的两个端口号范围内。*port1* 表示端口号 1, 取值范围为 0~65535。*port2* 表示端口号 2, 取值范围为 0~65535。

icmp-type: ICMP 消息类型, 取值范围为 0~255, 只在 *protocol* 为 **icmp** 时有效。

icmp-code: ICMP 消息码, 取值范围为 0~255。

icmpv6-type: ICMPv6 消息类型, 取值范围为 0~255, 只在 *protocol* 为 **icmpv6** 时有效。

icmpv6-code: ICMPv6 消息码, 取值范围为 0~255。

group-object: 指定引用服务对象组。*object-group-name* 表示服务对象组名称, 为 1~31 字符, 不区分大小写。

【使用指导】

创建对象时指定 ID, 如果指定 ID 的对象不存在, 则创建一条新的对象; 如果指定 ID 的对象已存在, 则对旧对象进行修改。

新创建或修改的对象不能与已有对象的内容完全相同, 否则该命令执行失败, 并提示出错。

在配置 **lt** 参数时, 需要注意的是:

- 不能指定 *port* 为 0。
- 如果指定 *port* 为 1, 则该配置被视为 **eq 0**。
- 如果指定 *port* 为 2~65535, 则实际生效的端口号为 [0, *port-1*]。

在配置 **gt** 参数时, 需要注意的是:

- 不能指定 *port* 为 65535。
- 如果指定 *port* 为 65534, 该配置被视为 **eq 65535**。
- 如果指定 *port* 为 0~65533, 则实际生效的端口号为 [*port+1*, 65535]。

在配置 **range** 参数时, 需要注意的是:

- 如果指定的 *port1* 和 *port2* 相同, 则该配置被视为等于指定的端口号。
- 如果指定 *port1* 为 0, 则该配置被视为 **lt** 配置, 譬如配置 **range 0 999**, 被视为 **lt 1000**。
- 如果指定 *port2* 为 65535, 则该配置被视为 **gt** 配置, 譬如配置 **range 50001 65535**, 被视为 **gt 50000**。
- 如果指定的 *port1* 比 *port2* 大, 会自动调整范围为 [*port2*, *port1*]。

在配置 **group-object** 参数时, 需要注意的是:

- 如果指定名称的对象组不存在, 则系统会创建此名称的服务对象组。
- 如果指定名称的对象组存在, 则对象组类型必须为服务对象组。
- 引用的服务对象组不能形成循环, 譬如服务对象组 **a** 引用服务对象组 **b**, 则服务对象组 **b** 不能再引用服务对象组 **a**。
- 引用的服务对象组最大嵌套层次为 5 层, 譬如服务对象组 1、2、3、4 分别引用服务对象组 2、3、4、5, 则服务对象组 5 不能再引用其他服务对象组, 服务对象组 1 也不能再被其他服务对象组引用。

【举例】

配置协议号等于 100 的服务对象。

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service 100
```

配置指定源端口和目的端口的 tcp 协议报文的服务对象。

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service tcp source eq 100 destination range 10 100
```

配置 icmp 协议的服务对象。

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service icmp 100 150
```

配置引用 servicegroup2 对象组的服务对象。

```
<Sysname> system-view
[Sysname] object-group service servicegroup
[Sysname-obj-grp-service-servicegroup] service group-object servicegroup2
```

目 录

1 攻击检测与防范	1-1
1.1 攻击检测与防范配置命令	1-1
1.1.1 ack-flood action	1-1
1.1.2 ack-flood detect	1-2
1.1.3 ack-flood detect non-specific	1-3
1.1.4 ack-flood threshold	1-4
1.1.5 attack-defense apply policy	1-5
1.1.6 attack-defense login block-timeout	1-6
1.1.7 attack-defense login enable	1-7
1.1.8 attack-defense login max-attempt	1-7
1.1.9 attack-defense login reauthentication-delay	1-8
1.1.10 attack-defense policy	1-9
1.1.11 attack-defense signature log non-aggregate	1-9
1.1.12 attack-defense top-attack-statistics enable	1-10
1.1.13 blacklist destination-ip	1-11
1.1.14 blacklist destination-ipv6	1-12
1.1.15 blacklist enable	1-13
1.1.16 blacklist global enable	1-14
1.1.17 blacklist ip	1-14
1.1.18 blacklist ipv6	1-15
1.1.19 blacklist logging enable	1-16
1.1.20 blacklist object-group	1-17
1.1.21 blacklist user	1-18
1.1.22 client-verify dns enable	1-19
1.1.23 client-verify dns-reply enable	1-19
1.1.24 client-verify http enable	1-20
1.1.25 client-verify sip enable	1-21
1.1.26 client-verify protected ip	1-22
1.1.27 client-verify protected ipv6	1-23
1.1.28 client-verify tcp enable	1-24
1.1.29 display attack-defense flood statistics ip	1-26
1.1.30 display attack-defense flood statistics ipv6	1-28
1.1.31 display attack-defense policy	1-30

1.1.32 display attack-defense policy ip	1-37
1.1.33 display attack-defense policy ipv6	1-39
1.1.34 display attack-defense scan attacker ip	1-41
1.1.35 display attack-defense scan attacker ipv6	1-42
1.1.36 display attack-defense statistics security-zone	1-44
1.1.37 display attack-defense top-attack-statistics	1-48
1.1.38 display blacklist destination-ip	1-50
1.1.39 display blacklist destination-ipv6	1-51
1.1.40 display blacklist ip	1-53
1.1.41 display blacklist ipv6	1-54
1.1.42 display blacklist user	1-56
1.1.43 display client-verify protected ip	1-57
1.1.44 display client-verify protected ipv6	1-59
1.1.45 display client-verify trusted ip	1-60
1.1.46 display client-verify trusted ipv6	1-62
1.1.47 display whitelist object-group	1-63
1.1.48 dns-flood action	1-64
1.1.49 dns-flood detect	1-65
1.1.50 dns-flood detect non-specific	1-67
1.1.51 dns-flood port	1-67
1.1.52 dns-flood threshold	1-68
1.1.53 dns-reply-flood action	1-69
1.1.54 dns-reply-flood detect	1-70
1.1.55 dns-reply-flood detect non-specific	1-72
1.1.56 dns-reply-flood port	1-73
1.1.57 dns-reply-flood threshold	1-74
1.1.58 exempt acl	1-75
1.1.59 fin-flood action	1-76
1.1.60 fin-flood detect	1-77
1.1.61 fin-flood detect non-specific	1-78
1.1.62 fin-flood threshold	1-79
1.1.63 http-flood action	1-80
1.1.64 http-flood detect	1-81
1.1.65 http-flood detect non-specific	1-83
1.1.66 http-flood port	1-84
1.1.67 http-flood threshold	1-85

1.1.68 icmp-flood action	1-86
1.1.69 icmp-flood detect ip	1-87
1.1.70 icmp-flood detect non-specific	1-88
1.1.71 icmp-flood threshold	1-89
1.1.72 icmpv6-flood action	1-90
1.1.73 icmpv6-flood detect ipv6	1-91
1.1.74 icmpv6-flood detect non-specific	1-92
1.1.75 icmpv6-flood threshold	1-93
1.1.76 reset attack-defense policy flood	1-94
1.1.77 reset attack-defense statistics security-zone	1-94
1.1.78 reset attack-defense top-attack-statistics	1-95
1.1.79 reset blacklist destination-ip	1-95
1.1.80 reset blacklist destination-ipv6	1-96
1.1.81 reset blacklist ip	1-97
1.1.82 reset blacklist ipv6	1-98
1.1.83 reset blacklist statistics	1-98
1.1.84 reset client-verify protected statistics	1-99
1.1.85 reset client-verify trusted	1-100
1.1.86 reset whitelist statistics	1-100
1.1.87 rst-flood action	1-101
1.1.88 rst-flood detect	1-102
1.1.89 rst-flood detect non-specific	1-103
1.1.90 rst-flood threshold	1-104
1.1.91 scan detect	1-105
1.1.92 signature { large-icmp large-icmpv6 } max-length	1-107
1.1.93 signature detect	1-108
1.1.94 signature level action	1-111
1.1.95 signature level detect	1-112
1.1.96 sip-flood action	1-113
1.1.97 sip-flood detect	1-114
1.1.98 sip-flood detect non-specific	1-116
1.1.99 sip-flood port	1-117
1.1.100 sip-flood threshold	1-118
1.1.101 syn-ack-flood action	1-118
1.1.102 syn-ack-flood detect	1-120
1.1.103 syn-ack-flood detect non-specific	1-121

1.1.104 syn-ack-flood threshold	1-122
1.1.105 syn-flood action	1-123
1.1.106 syn-flood detect	1-124
1.1.107 syn-flood detect non-specific	1-125
1.1.108 syn-flood threshold	1-126
1.1.109 threshold-learn apply	1-127
1.1.110 threshold-learn auto-apply enable	1-128
1.1.111 threshold-learn duration	1-129
1.1.112 threshold-learn enable	1-129
1.1.113 threshold-learn interval	1-130
1.1.114 threshold-learn mode	1-131
1.1.115 threshold-learn tolerance-value	1-132
1.1.116 udp-flood action	1-133
1.1.117 udp-flood detect	1-133
1.1.118 udp-flood detect non-specific	1-135
1.1.119 udp-flood threshold	1-136
1.1.120 whitelist enable	1-137
1.1.121 whitelist global enable	1-137
1.1.122 whitelist object-group	1-138

1 攻击检测与防范

1.1 攻击检测与防范配置命令

1.1.1 ack-flood action

ack-flood action 命令用来配置 ACK flood 攻击防范的全局处理行为。

undo ack-flood action 命令用来恢复缺省情况。

【命令】

```
ack-flood action { client-verify | drop | logging } *  
undo ack-flood action
```

【缺省情况】

不对检测到的 ACK flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

client-verify: 表示自动将受到攻击的 IP 地址添加到 TCP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ACK 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

本命令中 **client-verify** 参数的使用需要和 TCP 客户端验证功能配合。使能了 TCP 客户端验证功能的安全域检测到 ACK flood 攻击时，若本命令中指定了 **client-verify** 参数，则设备会将受攻击的 IP 地址动态添加到相应客户端验证的受保护 IP 列表中，并对与这些 IP 地址建立的连接进行代理。若安全域上未使能相应的代理功能，则不会对任何连接进行代理。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 atk-policy-1 中配置 ACK flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood action drop
```

【相关命令】

- **ack-flood threshold**
- **ack-flood detect**
- **ack-flood detect non-specific**
- **client-verify tcp enable**

1.1.2 ack-flood detect

ack-flood detect 命令用来开启对指定 IP 地址的 ACK flood 攻击防范检测，并配置 ACK flood 攻击防范的触发阈值和对 ACK flood 攻击的处理行为。

undo ack-flood detect 命令用来关闭对指定 IP 地址的 ACK flood 攻击防范检测。

【命令】

```
ack-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] [ threshold threshold-value ] [ action { { client-verify | drop | logging } * | none } ]
undo ack-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址开启 ACK flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为 255.255.255.255 或 0.0.0.0。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。该 IPv6 地址不能为组播地址或::。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold *threshold-value*: 指定 ACK flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 ACK 报文数目，取值范围为 1~1000000。

action: 设置对 ACK flood 攻击的处理行为。若未指定本参数，则表示采用 ACK flood 攻击防范的全局处理行为。

client-verify: 表示自动将被攻击的 IP 地址添加到 TCP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ACK 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

使能 ACK flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 ACK 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 ACK flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

每个攻击防范策略下可以同时多个 IP 地址配置 ACK flood 攻击防范检测。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **192.168.1.2** 的 ACK flood 攻击防范检测，并指定触发阈值为 **2000**。当设备监测到向该 IP 地址每秒发送的 ACK 报文数持续达到或超过 **2000** 时，启动 ACK flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **ack-flood action**
- **ack-flood detect non-specific**
- **ack-flood threshold**
- **client-verify tcp enable**

1.1.3 ack-flood detect non-specific

ack-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 ACK flood 攻击防范检测。

undo ack-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 ACK flood 攻击防范检测。

【命令】

```
ack-flood detect non-specific
undo ack-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 ACK flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

对所有未配置具体攻击防范策略的 IP 地址开启 ACK flood 攻击防范检测后, 设备将采用全局的阈值设置（由 **ack-flood threshold** 命令设置）和处理行为（由 **ack-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中, 对所有非受保护 IP 地址开启 ACK flood 攻击防范检测。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] ack-flood detect non-specific
```

【相关命令】

- **ack-flood action**
- **ack-flood detect**
- **ack-flood threshold**

1.1.4 ack-flood threshold

ack-flood threshold 命令用来配置 ACK flood 攻击防范的全局触发阈值。

undo ack-flood threshold 命令用来恢复缺省情况。

【命令】

ack-flood threshold *threshold-value*

undo ack-flood threshold

【缺省情况】

ACK flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 ACK 报文数目, 取值范围为 1~1000000。

【使用指导】

使能 ACK flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 ACK 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 ACK flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

对于未专门配置 ACK flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（HTTP 服务器或者 FTP 服务器）的 ACK 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 atk-policy-1 中配置 ACK flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 ACK 报文数持续达到或超过 100 时，启动 ACK flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] ack-flood threshold 100
```

【相关命令】

- **ack-flood action**
- **ack-flood detect**
- **ack-flood detect non-specific**

1.1.5 attack-defense apply policy

attack-defense apply policy 命令用来在安全域上应用攻击防范策略。

undo attack-defense apply policy 命令用来恢复缺省情况。

【命令】

```
attack-defense apply policy policy-name
undo attack-defense apply policy
```

【缺省情况】

安全域上未应用任何攻击防范策略。

【视图】

安全域视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

【使用指导】

一个安全域上只能应用一个攻击防范策略（多次执行本命令，最后一次执行的命令生效），但一个攻击防范策略可应用到多个安全域上。

【举例】

将攻击防范策略 **atk-policy-1** 应用到安全域 **DMZ** 上。

```
<Sysname> system-view
```

```
[Sysname] security-zone name dmz
```

```
[Sysname-security-zone-DMZ] attack-defense apply policy atk-policy-1
```

【相关命令】

- **attack-defense policy**
- **display attack-defense policy**

1.1.6 attack-defense login block-timeout

attack-defense login block-timeout 命令用来配置 Login 用户登录失败后阻断时长。

undo attack-defense login block-timeout 命令用来恢复缺省情况。

【命令】

attack-defense login block-timeout *minutes*

undo attack-defense login block-timeout

【缺省情况】

Login 用户登录失败后默认阻断时长为 60 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

minutes: 设备管理用户登录失败后阻断时长，取值范围为 1~2880，单位为分钟。

【使用指导】

Login 用户登录失败后，若用户的 IP 地址被加入黑名单，则设备将会丢弃来自该 IP 地址的报文，使得该用户不能在指定的阻断时长内进行登录操作。

【举例】

配置 Login 用户登录失败后阻断时长为 5 分钟。

```
<Sysname> system-view
```

```
[Sysname] attack-defense login block-timeout 5
```

【相关命令】

- **attack-defense login enable**
- **blacklist global enable**

1.1.7 attack-defense login enable

attack-defense login enable 命令用来开启 Login 用户攻击防范功能。

undo attack-defense login enable 命令用来关闭 Login 用户攻击防范功能。

【命令】

```
attack-defense login enable
undo attack-defense login enable
```

【缺省情况】

Login 用户攻击防范功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启 Login 用户攻击防范功能后，如果用户登录设备连续失败的次数达到指定次数，则此用户 IP 将被加入黑名单，并在指定时间内不能进行登录。

将 Login 用户加入黑名单进行阻断的功能必须在全局黑名单过滤功能处于开启状态时才能生效。

【举例】

```
# 开启 Login 用户攻击防范功能。
<Sysname> system-view
[Sysname] attack-defense login enable
```

【相关命令】

- **blacklist global enable**

1.1.8 attack-defense login max-attempt

attack-defense login max-attempt 命令用来配置 Login 用户登录失败的最大次数。

undo attack-defense login max-attempt 命令用来恢复缺省情况。

【命令】

```
attack-defense login max-attempt max-attempt
undo attack-defense login max-attempt
```

【缺省情况】

Login 用户登录失败的最大次数为 3 次。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

max-attempt: 用户登录连续失败的最大次数，取值为 1~60。

【使用指导】

Login 用户攻击防范功能处于开启状态时，如果用户登录设备连续失败的次数达到指定次数，则此用户 IP 地址将被加入黑名单，在全局黑名单功能开启的情况下，来自该 IP 地址的用户报文将被阻断指定的时长。

若用户成功登录或设备重启，用户登录失败次数会重新从零计数。

【举例】

```
# 配置 Login 用户登录失败的最大次数为 5 次。  
<Sysname> system-view  
[Sysname] attack-defense login max-attempt 5
```

【相关命令】

- **attack-defense login enable**

1.1.1.9 attack-defense login reauthentication-delay

attack-defense login reauthentication-delay 命令用来配置 Login 用户登录失败后重新进行认证的等待时长。

undo attack-defense login reauthentication-delay 命令用来恢复缺省情况。

【命令】

```
attack-defense login reauthentication-delay seconds  
undo attack-defense login reauthentication-delay
```

【缺省情况】

Login 用户登录失败后重新进行认证不需要等待。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

seconds: 设备管理用户登录失败后重新进行认证的等待时长，取值范围为 4~60，单位为秒。

【使用指导】

Login 用户登录失败后，若设备上配置了重新进行认证的等待时长，则系统将会延迟一定的时长之后再允许用户进行认证，可以避免设备受到字典式攻击。

Login 用户延迟认证功能与 Login 用户攻击防范功能无关，只要配置了延迟认证等待时间，即可生效。

【举例】

配置 Login 用户登录失败后重新进行认证的等待时长为 5 秒钟。

```
<Sysname> system-view
```

```
[Sysname] attack-defense login reauthentication-delay 5
```

1.1.10 attack-defense policy

attack-defense policy 命令用来创建一个攻击防范策略，并进入攻击防范策略视图。如果指定的攻击防范策略已经存在，则直接进入攻击防范策略视图。

undo attack-defense policy 命令用来删除指定的攻击防范策略。

【命令】

```
attack-defense policy policy-name
```

```
undo attack-defense policy policy-name
```

【缺省情况】

不存在任何攻击防范策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name：攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

【举例】

创建攻击防范策略 **atk-policy-1**，并进入攻击防范策略视图。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1]
```

【相关命令】

- **attack-defense apply policy**
- **display attack-defense policy**

1.1.11 attack-defense signature log non-aggregate

attack-defense signature log non-aggregate 命令用来指定对单包攻击防范日志非聚合输出。

undo attack-defense signature log non-aggregate 命令用来恢复缺省情况。

【命令】

```
attack-defense signature log non-aggregate
undo attack-defense signature log non-aggregate
```

【缺省情况】

单包攻击防范的日志信息经系统聚合后再输出。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

对日志进行聚合输出是指，在一定时间内，对在同一个安全域上检测到的相同攻击类型、相同攻击防范动作、相同的源/目的地址以及属于相同 VPN 的单包攻击的所有日志聚合成一条日志输出。通常不建议开启单包攻击防范的日志非聚合输出功能，因为在单包攻击较为频繁的情况下，它会导致大量日志信息输出，占用控制台的显示资源。

【举例】

```
# 开启对单包攻击防范日志的非聚合输出功能。
<Sysname> system-view
[Sysname] attack-defense signature log non-aggregate
```

【相关命令】

- **signature detect**

1.1.12 attack-defense top-attack-statistics enable

attack-defense top-attack-statistics enable 命令用来开启攻击排名的 Top 统计功能。
undo attack-defense top-attack-statistics enable 命令用来关闭攻击排名的 Top 统计功能。

【命令】

```
attack-defense top-attack-statistics enable
undo attack-defense top-attack-statistics enable
```

【缺省情况】

攻击排名的 Top 统计功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

可以通过 **display attack-defense top-attack-statistics** 命令查看攻击数目的 Top 排名统计信息。

【举例】

开启攻击排名的 Top 统计功能。

```
<Sysname> system-view
```

```
[Sysname] attack-defense top-attack-statistics enable
```

【相关命令】

- **display attack-defense top-attack-statistics**

1.1.13 blacklist destination-ip

blacklist destination-ip 命令用来添加目的 IPv4 黑名单表项。

undo blacklist destination-ip 命令用来删除指定的目的 IPv4 黑名单表项。

【命令】

```
blacklist destination-ip destination-ip-address [ vpn-instance  
vpn-instance-name ] [ timeout minutes ]
```

```
undo blacklist destination-ip destination-ip-address [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

不存在目的 IPv4 黑名单表项。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

destination-ip-address: 黑名单的 IPv4 地址，用于匹配报文的目的 IP 地址。

vpn-instance vpn-instance-name: 黑名单所属的 VPN 实例。其中，**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该黑名单属于公网。

timeout minutes: 黑名单表项的老化时间。其中，**minutes** 表示老化时间，取值范围为 1~10080，单位为分钟。若未指定本参数，则表示该黑名单表项永不老化，除非用户手动将其删除。

【使用指导】

通过执行 **undo blacklist destination-ip** 命令可以删除用户手工添加的目的 IPv4 黑名单表项，动态生成的目的 IPv4 黑名单表项需通过执行 **reset blacklist destination-ip** 命令删除。指定了老化时间的目的黑名单表项不会被保存在配置文件中，且保存配置重启后会被删除。

可通过执行 **display blacklist destination-ip** 命令查看当前所有生效的目的 IPv4 黑名单表项。

【举例】

将 IP 地址 192.168.1.2 加入目的 IPv4 黑名单，指定其老化时间为 20 分钟。

```
<Sysname> system-view
```

```
[Sysname] blacklist destination-ip 192.168.1.2 timeout 20
```

【相关命令】

- **blacklist enable**
- **blacklist global enable**
- **display blacklist destination-ip**

1.1.14 blacklist destination-ipv6

blacklist destination-ipv6 命令用来添加目的 IPv6 黑名单表项。

undo blacklist destination-ipv6 命令用来删除指定的目的 IPv6 黑名单表项。

【命令】

```
blacklist destination-ipv6 destination-ipv6-address [ vpn-instance  
vpn-instance-name ] [ timeout minutes ]
```

```
undo blacklist destination-ipv6 destination-ipv6-address [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

不存在目的 IPv6 黑名单表项。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

destination-ipv6-address: 黑名单的 IPv6 地址，用于匹配报文的目的 IPv6 地址。

vpn-instance vpn-instance-name: 黑名单所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该黑名单属于公网。

timeout minutes: 黑名单表项的老化时间。其中，*minutes* 表示老化时间，取值范围为 1~10080，单位为分钟。若未指定本参数，则表示该黑名单表项永不老化，除非用户手动将其删除。

【使用指导】

通过执行 **undo blacklist destination-ipv6** 命令可以删除用户手工添加的目的 IPv6 黑名单表项，动态生成的目的 IPv6 黑名单表项需通过执行 **reset blacklist ipv6** 命令删除。指定

了老化时间的目的黑名单表项不会被保存在配置文件中，且保存配置重启后会被删除。可通过执行 **display blacklist destination-ipv6** 命令查看当前所有生效的目的 IPv6 黑名单表项。

【举例】

将 IPv6 地址 2012::12:25 加入目的 IPv6 黑名单，指定其老化时间为 10 分钟。

```
<Sysname> system-view
```

```
[Sysname] blacklist destination-ipv6 2012::12:25 timeout 10
```

【相关命令】

- **blacklist enable**
- **blacklist global enable**
- **display blacklist destination-ipv6**

1.1.15 blacklist enable

blacklist enable 命令用来开启安全域上的黑名单过滤功能。

undo blacklist enable 命令用来关闭安全域上的黑名单过滤功能。

【命令】

blacklist enable

undo blacklist enable

【缺省情况】

安全域上的黑名单过滤功能处于关闭状态。

【视图】

安全域视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

若全局的黑名单过滤功能处于开启状态，则所有安全域上的黑名单过滤功能均处于开启状态。若全局的黑名单过滤功能处于关闭状态，则安全域上的黑名单过滤功能由本命令决定是否开启。

【举例】

开启安全域 Untrust 上的黑名单过滤功能。

```
<Sysname> system-view
```

```
[Sysname] security-zone name untrust
```

```
[Sysname-security-zone-Untrust] blacklist enable
```

【相关命令】

- **blacklist ip**
- **blacklist ipv6**

1.1.16 blacklist global enable

blacklist global enable 命令用来开启全局黑名单过滤功能。

undo blacklist global enable 命令用来关闭全局黑名单过滤功能。

【命令】

```
blacklist global enable
undo blacklist global enable
```

【缺省情况】

全局黑名单过滤功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

使能全局黑名单过滤功能表示开启所有安全域上的黑名单过滤功能。

【举例】

```
# 开启全局黑名单过滤功能。
<Sysname> system-view
[Sysname] blacklist global enable
```

【相关命令】

- **blacklist enable**
- **blacklist ip**

1.1.17 blacklist ip

blacklist ip 命令用来添加源 IPv4 黑名单表项。

undo blacklist ip 命令用来删除指定的源 IPv4 黑名单表项。

【命令】

```
blacklist ip source-ip-address [ vpn-instance vpn-instance-name ] [ timeout
minutes ]
undo blacklist ip source-ip-address [ vpn-instance vpn-instance-name ]
```

【缺省情况】

不存在源 IPv4 黑名单表项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

source-ip-address: 源黑名单的 IPv4 地址，用于匹配报文的源 IP 地址。

vpn-instance vpn-instance-name: 源黑名单所属的 VPN 实例。其中, *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该源黑名单属于公网。

timeout minutes: 源黑名单表项的老化时间。其中, *minutes* 表示老化时间，取值范围为 1~10080，单位为分钟。若未指定本参数，则表示该源黑名单表项永不老化，除非用户手动将其删除。

【使用指导】

通过执行 **undo blacklist ip** 命令可以删除用户手工添加的源黑名单表项，动态生成的源黑名单表项需通过执行 **reset blacklist ip** 命令删除。指定了老化时间的源黑名单表项不会被保存在配置文件中，且保存配置重启后会被删除。可通过执行 **display blacklist ip** 命令查看当前所有生效的源 IPv4 黑名单表项。

【举例】

将 IP 地址 192.168.1.2 加入源黑名单，指定其老化时间为 20 分钟。

```
<Sysname> system-view  
[Sysname] blacklist ip 192.168.1.2 timeout 20
```

【相关命令】

- **blacklist enable**
- **blacklist global enable**
- **display blacklist ip**

1.1.18 blacklist ipv6

blacklist ipv6 命令用来添加源 IPv6 黑名单表项。

undo blacklist ipv6 命令用来删除指定的源 IPv6 黑名单表项。

【命令】

```
blacklist ipv6 source-ipv6-address [ vpn-instance vpn-instance-name ]  
[ timeout minutes ]  
undo blacklist ipv6 source-ipv6-address [ vpn-instance vpn-instance-name ]
```

【缺省情况】

不存在源 IPv6 黑名单表项。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

source-ipv6-address: 源黑名单的 IPv6 地址，用于匹配报文的源 IP 地址。

vpn-instance vpn-instance-name: 源黑名单所属的 VPN 实例。其中, *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该源黑名单属于公网。

timeout minutes: 源黑名单表项的老化时间。其中, *minutes* 表示老化时间，取值范围为 1~10080，单位为分钟。若未指定本参数，则表示该源黑名单表项永不老化，除非用户手动将其删除。

【使用指导】

通过执行 **undo blacklist ipv6** 命令可以删除用户手工添加的源黑名单表项，动态生成的源黑名单表项需通过执行 **reset blacklist ipv6** 命令删除。指定了老化时间的源黑名单表项不会被保存在配置文件中，且保存配置重启后会被删除。可通过执行 **display blacklist ipv6** 命令查看当前所有生效的源 IPv6 黑名单表项。

【举例】

将 IPv6 地址 2012::12:25 加入源黑名单，指定其老化时间为 10 分钟。

```
<Sysname> system-view
[Sysname] blacklist ipv6 2012::12:25 timeout 10
```

【相关命令】

- **blacklist enable**
- **blacklist global enable**
- **blacklist ip**

1.1.19 blacklist logging enable

blacklist logging enable 命令用来使能黑名单日志功能。

undo blacklist logging enable 命令用来关闭黑名单日志功能。

【命令】

```
blacklist logging enable
undo blacklist logging enable
```

【缺省情况】

黑名单日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

开启黑名单日志功能后，当增加黑名单、删除黑名单、扫描攻击防范动态添加黑名单、黑名单老化被删除时会有相应的日志输出，日志的内容主要包括黑名单的源 IP 地址、VPN 实例名称、添加或删除的原因以及老化时间等。

设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

开启黑名单日志功能，并配置一条黑名单后，输出如下日志信息。

```
<Sysname> system-view
[Sysname] blacklist logging enable
[Sysname] blacklist ip 192.168.100.12
%Mar 13 03:47:49:736 2013 Sysname BLS/5/BLS_ENTRY_ADD:SrcIPAddr(1003)=192.168.100.12;
DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=--; TTL(1051)=;
Reason(1052)=Configuration.
```

删除一条黑名单后，输出如下日志信息。

```
[Sysname] undo blacklist ip 192.168.100.12
%Mar 13 03:49:52:737 2013 Sysname BLS/5/BLS_ENTRY_DEL:SrcIPAddr(1003)=192.168.100.12;
DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=--; Reason(1052)=Configuration.
```

【相关命令】

- **blacklist ip**
- **blacklist ipv6**

1.1.20 blacklist object-group

blacklist object-group 命令通过引用地址对象组配置黑名单。

undo blacklist object-group 命令用来恢复缺省情况。

【命令】

```
blacklist object-group object-group-name
undo blacklist object-group
```

【缺省情况】

未引用地址对象组。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

object-group-name：地址对象组名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

本命令需要和地址对象组功能配合使用，有关地址对象组功能的详细介绍，请参见“安全配置指导”中的“对象组”。

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 通过引用地址对象组 object-group1 配置黑名单。  
<Sysname> system-view  
[Sysname] blacklist object-group object-group1
```

1.1.21 blacklist user

blacklist user 命令用来添加用户黑名单表项。

undo blacklist user 命令用来删除指定用户的黑名单表项。

【命令】

```
blacklist user user-name [ domain domain-name ] [ timeout minutes ]  
undo blacklist user user-name [ domain domain-name ]
```

【缺省情况】

不存在用户黑名单表项。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

user-name: 表示用户的名称，为 1~55 个字符的字符串，区分大小写。

domain domain-name: 表示用户所属的身份识别域。**domain-name** 是身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包括字符“?”。若不指定此参数，则表示用户不属于任何身份识别域。

timeout minutes: 用户黑名单表项的老化时间。其中，**minutes** 表示老化时间，取值范围为 1~1000，单位为分钟。若未指定本参数，则表示该用户黑名单表项永不老化，除非手动将其删除。

【使用指导】

用户黑名单功能需要配合用户身份识别功能使用，有关用户身份识别功能的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

【举例】

```
# 将用户 usera 加入用户黑名单，老化时间为 20 分钟。  
<Sysname> system-view  
[Sysname] blacklist user usera timeout 20  
# 添加一个用户黑名单表项，用户名为 usera，域名为 domaina。
```

```
<Sysname> system-view
[Sysname] blacklist user usera domain domaina timeout 20
```

【相关命令】

- **blacklist global enable**
- **display blacklist user**

1.1.22 client-verify dns enable

client-verify dns enable 命令用来在安全域上开启 DNS 客户端验证功能。

undo client-verify dns enable 命令用来关闭安全域上的 DNS 客户端验证功能。

【命令】

```
client-verify dns enable
undo client-verify dns enable
```

【缺省情况】

安全域上的 DNS 客户端验证功能处于关闭状态。

【视图】

安全域视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

该功能一般应用在设备连接外部网络的安全域上，用来保护内部网络的 DNS 服务器免受外部网络中非法客户端发起的 DNS flood 攻击。当设备监测到某服务器受到了 DNS flood 攻击时，会根据配置的攻击防范处理行为启动相应的防范措施。若防范处理行为配置为对攻击报文进行客户端验证（指定参数为 **client-verify**），则设备会将该服务器 IP 地址添加到受保护 IP 表项中（可通过 **display client-verify dns protected ip** 命令查看），对后续新建 DNS query 请求连接的协商报文进行合法性检查，过滤非法客户端发起的 DNS query 请求报文。

【举例】

```
# 在安全域 DMZ 上开启 DNS 客户端验证功能。
<Sysname> system-view
[Sysname] security-zone name DMZ
[Sysname-security-zone-DMZ] client-verify dns enable
```

【相关命令】

- **client-verify dns protected ip**
- **display client-verify dns protected ip**

1.1.23 client-verify dns-reply enable

client-verify dns-reply enable 命令用来在安全域上开启 DNS reply 验证功能。

undo client-verify dns-reply enable 命令用来关闭安全域上的 DNS reply 验证功能。

【命令】

```
client-verify dns-reply enable
undo client-verify dns-reply enable
```

【缺省情况】

安全域上的 DNS reply 验证功能处于关闭状态。

【视图】

安全域视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

该功能一般应用在设备连接外部网络的安全域上，用来保护内部网络的 DNS 客户端免受外部网络中非法服务器发起的 DNS reply flood 攻击。当设备监测到某客户端受到了 DNS reply flood 攻击时，会根据配置的攻击防范处理行为启动相应的防范措施。若防范处理行为配置为对攻击报文进行 DNS reply 验证（指定参数为 **client-verify**），则设备会将该客户端 IP 地址添加到受保护 IP 表项中（可通过 **display client-verify dns-reply protected ip** 命令查看），对后续 DNS reply 报文进行源探测，过滤非法的 DNS reply 报文。

【举例】

```
# 在安全域 dmz 上开启 DNS reply 验证功能。
<Sysname> system-view
[Sysname] security-zone name dmz
[Sysname-security-zone-DMZ] client-verify dns-reply enable
```

【相关命令】

- **client-verify dns-reply protected ip**
- **display client-verify dns-reply protected ip**

1.1.24 client-verify http enable

client-verify http enable 命令用来在安全域上开启 HTTP 客户端验证功能。
undo client-verify http enable 命令用来关闭安全域上的 HTTP 客户端验证功能。

【命令】

```
client-verify http enable
undo client-verify http enable
```

【缺省情况】

安全域上的 HTTP 客户端验证功能处于关闭状态。

【视图】

安全域视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

该功能一般应用在设备连接外部网络的安全域上，用来保护内部网络的服务器免受外部网络中非法客户端发起的 HTTP flood 攻击。当设备监测到某服务器受到了 HTTP flood 攻击时，会根据配置的攻击防范处理行为启动相应的防范措施。若防范处理行为配置为对攻击报文进行客户端验证（指定参数为 **client-verify**），则设备会将该服务器 IP 地址添加到受保护 IP 表项中（可通过 **display client-verify http protected ip** 命令查看），对后续新建 HTTP get 请求连接的协商报文进行合法性检查，过滤非法客户端发起的 HTTP get 请求报文。

【举例】

```
# 在安全域 DMZ 上开启 HTTP 客户端验证功能。  
<Sysname> system-view  
[Sysname] security-zone name DMZ  
[Sysname- security-zone-DMZ] client-verify http enable
```

【相关命令】

- **client-verify http protected ip**
- **display client-verify http protected ip**

1.1.25 client-verify sip enable

client-verify sip enable 命令用来在安全域上开启 SIP 客户端验证功能。

undo client-verify sip enable 命令用来关闭安全域上的 SIP 客户端验证功能。

【命令】

```
client-verify sip enable  
undo client-verify sip enable
```

【缺省情况】

安全域上的 SIP 客户端验证功能处于关闭状态。

【视图】

安全域视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

该功能一般应用在设备连接外部网络的安全域上，用来保护内部网络的 DNS 服务器免受外部网络中非法客户端发起的 SIP flood 攻击。当设备监测到某 IP 地址受到了 SIP flood 攻击时，会根据配置的攻击防范处理行为启动相应的防范措施。若防范处理行为配置为对攻击报文进行客户端验证（指定参数为 **client-verify**），则设备会将该服务器 IP 地址添加到受保护 IP 表项中（可通过

display client-verify sip protected ip 命令查看), 对后续新建 SIP INVITE 请求报文进行合法性检查, 过滤非法客户端发起的 SIP INVITE 请求报文。

【举例】

```
# 在安全域 DMZ 上开启 SIP 客户端验证功能。
<Sysname> system-view
[Sysname] security-zone name DMZ
[Sysname-security-zone-DMZ] client-verify sip enable
```

【相关命令】

- **client-verify sip protected ip**
- **display client-verify sip protected ip**

1.1.26 client-verify protected ip

client-verify protected ip 命令用来配置 IPv4 类型客户端验证的受保护 IP 地址。

undo client-verify protected ip 命令用来删除指定的受保护 IP 地址。

【命令】

```
client-verify { dns | dns-reply | http | sip | tcp } protected ip  
destination-ip-address [ vpn-instance vpn-instance-name ] [ port  
port-number ]  
undo client-verify { dns | dns-reply | http | sip | tcp } protected ip  
destination-ip-address [ vpn-instance vpn-instance-name ] [ port  
port-number ]
```

【缺省情况】

不存在任何 IPv4 类型客户端验证受保护 IP 地址, 即客户端验证功能未保护任何 IPv4 地址。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

dns: 指定 DNS 客户端验证功能。

dns-reply: 指定 DNS reply 验证功能。

http: 指定 HTTP 客户端验证功能。

sip: 指定 SIP 客户端验证功能。

tcp: 指定 TCP 客户端验证功能。

destination-ip-address: 指定受客户端验证保护的 IPv4 地址, 即会对向该目的地址发送的连接请求进行代理。

vpn-instance vpn-instance-name: 受客户端验证保护的 IP 地址所属的 VPN 实例。其中, **vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。若未指定本参数, 则表示该受保护 IP 地址属于公网。

port port-number: 指定受客户端验证保护的端口号, 取值范围为 1~65535。若未指定本参数, 对于 DNS 客户端验证的受保护 IP, 则表示对端口 53 的 DNS query 连接请求做代理; 对于 DNS reply 验证的受保护 IP, 则表示对端口 53 的 DNS reply 连接请求做代理; 对于 HTTP 客户端验证的受保护 IP, 则表示对端口 80 的 HTTP GET 连接请求做代理; 对于 SIP 客户端验证的受保护 IP, 则表示对端口 5060 的 SIP INVITE 连接请求做代理; 对于 TCP 客户端验证的受保护 IP, 则表示对所有端口的 TCP 连接请求做代理。

【使用指导】

可通过多次执行本命令添加多个 IPv4 类型客户端验证受保护 IP 地址。

【举例】

配置一个 TCP 客户端验证受保护 IPv4 地址为 2.2.2.5、受保护端口号为 25。

```
<Sysname> system-view
```

```
[Sysname] client-verify tcp protected ip 2.2.2.5 port 25
```

配置一个 DNS 客户端验证受保护 IPv4 地址为 2.2.2.5、受保护端口号为 50。

```
<Sysname> system-view
```

```
[Sysname] client-verify dns protected ip 2.2.2.5 port 50
```

【相关命令】

- **display client-verify protected ip**

1.1.27 client-verify protected ipv6

client-verify protected ipv6 命令用来配置 IPv6 类型客户端验证的受保护 IP 地址。

undo client-verify protected ipv6 命令用来删除指定的受保护 IP 地址。

【命令】

```
client-verify { dns | dns-reply | http | sip | tcp } protected ipv6  
destination-ipv6-address [ vpn-instance vpn-instance-name ] [ port  
port-number ]
```

```
undo client-verify { dns | dns-reply | http | sip | tcp } protected ipv6  
destination-ipv6-address [ vpn-instance vpn-instance-name ] [ port  
port-number ]
```

【缺省情况】

不存在任何 IPv6 类型客户端验证受保护 IP 地址, 即客户端验证功能未保护任何 IPv6 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

dns: 指定 DNS 客户端验证功能。

dns-reply: 指定 DNS reply 验证功能。

http: 指定 HTTP 客户端验证功能。

sip: 指定 SIP 客户端验证功能。

tcp: 指定 TCP 客户端验证功能。

destination-ipv6-address: 指定受客户端验证保护的 IPv6 地址，即会对向该目的地址发送的连接请求进行代理。对于受 TCP 客户端验证保护的 IPv6 地址，发送的是 TCP 连接请求；对于受 DNS 客户端验证保护的 IPv6 地址，发送的是 DNS query 请求；对于受 HTTP 客户端验证保护的 IPv6 地址，发送的是 HTTP get 连接请求。

vpn-instance vpn-instance-name: 受客户端验证保护的 IPv6 地址所属的 VPN 实例。其中，**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该受保护 IP 地址属于公网。

port port-number: 指定受客户端验证保护的端口号，取值范围为 1~65535。若未指定本参数，对于 DNS 客户端验证的受保护 IP，则表示对端口 53 的 DNS query 连接请求做代理；对于 DNS reply 验证的受保护 IP，则表示对端口 53 的 DNS reply 连接请求做代理；对于 HTTP 客户端验证的受保护 IP，则表示对端口 80 的 HTTP GET 连接请求做代理；对于 SIP 客户端验证的受保护 IP，则表示对端口 5060 的 SIP INVITE 连接请求做代理；对于 TCP 客户端验证的受保护 IP，则表示对所有端口的 TCP 连接请求做代理。

【使用指导】

可通过多次执行本命令添加多个 IPv6 类型客户端验证受保护 IP 地址。

【举例】

配置一个 TCP 客户端验证受保护 IPv6 地址为 2013::12、受保护端口号为 23。

```
<Sysname> system-view
```

```
[Sysname] client-verify tcp protected ipv6 2013::12 port 23
```

配置一个 HTTP 客户端验证受保护 IPv6 地址为 2013::12。

```
<Sysname> system-view
```

```
[Sysname] client-verify http protected ipv6 2013::12
```

【相关命令】

- **display client-verify protected ipv6**

1.1.28 client-verify tcp enable

client-verify tcp enable 命令用来在安全域上开启 TCP 客户端验证功能。

undo client-verify tcp enable 命令用来关闭安全域上的 TCP 客户端验证功能。

【命令】

client-verify tcp enable [mode { syn-cookie | safe-reset }]

undo client-verify tcp enable

【缺省情况】

安全域上的 TCP 客户端验证功能处于关闭状态。

【视图】

安全域视图

【缺省用户角色】

network-admin

context-admin

【参数】

mode: 指定 TCP 客户端验证的工作模式。不指定该参数时，则表示工作模式为 **syn-cookie**。

syn-cookie: 指定 TCP 客户端验证的工作模式为 **syn-cookie**，即开启 TCP 客户端验证双向代理。

safe-reset: 指定 TCP 客户端验证的工作模式为 **safe-reset**，即开启 TCP 客户端验证单向代理。

【使用指导】

该功能一般应用在设备连接外部网络的安全域上，用来保护内部网络的服务器免受外部网络中非法客户端发起的 SYN flood、SYN-ACK flood、RST flood、FIN flood、ACK flood 攻击。当设备监测到某服务器受到了 SYN flood、SYN-ACK flood、RST flood、FIN flood、ACK flood 攻击时，会根据配置的攻击防范处理行为启动相应的防范措施。若防范处理行为配置为对攻击报文进行客户端验证（指定参数为 **client-verify**），则设备会将该服务器 IP 地址添加到受保护 IP 表项中（可通过 **display client-verify tcp protected ip** 命令查看），并按照指定的单向或双向工作模式，对后续新建 TCP 连接的协商报文进行合法性检查，过滤非法客户端发起的 TCP 连接报文。TCP 客户端验证功能支持两种代理模式：

- 单向代理模式（**safe-reset**）：是指仅对 TCP 连接的正向报文进行处理。
- 双向代理模式（**syn-cookie**）：是指对 TCP 连接的正向和反向报文都进行处理。

用户可以根据实际的组网情况选择不同的代理模式。若从客户端发出的报文经过使能了 TCP 客户端验证功能的设备时，而从服务器端发出的报文不经过该设备，此时只能使用单向代理模式；从客户端发出的报文经和从服务器端发出的报文都经过使能了 TCP 客户端验证功能的设备时，此时可以使用单向代理模式，也可以使用双向代理模式；代理只适合在入安全域上使能，否则无法建立正常连接。

【举例】

在安全域 DMZ 上开启 TCP 客户端验证功能，并指定工作模式为单向代理。

```
<Sysname> system-view
```

```
[Sysname] security-zone name dmz
```

```
[Sysname-security-zone-DMZ] client-verify tcp enable mode safe-reset
```

【相关命令】

- **client-verify tcp protected ip**
- **display client-verify tcp protected ip**

1.1.29 display attack-defense flood statistics ip

display attack-defense flood statistics ip 命令用来显示 IPv4 flood 攻击防范统计信息。

【命令】

```
display attack-defense { ack-flood | dns-flood | dns-reply-flood | fin-flood  
| flood | icmp-flood | rst-flood | sip-flood | syn-flood | syn-ack-flood |  
udp-flood } statistics ip [ ip-address [ vpn vpn-instance-name ] ]  
[ security-zone zone-name ] [ slot slot-number ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ack-flood: 显示 ACK flood 攻击防范统计信息。

dns-flood: 显示 DNS flood 攻击防范统计信息。

dns-reply-flood: 显示 DNS reply flood 攻击防范统计信息。

fin-flood: 显示 FIN flood 攻击防范统计信息。

flood: 显示所有类型的 IPv4 flood 攻击防范统计信息。

http-flood: 显示 HTTP flood 攻击防范统计信息。

icmp-flood: 显示 ICMP flood 攻击防范统计信息。

rst-flood: 显示 RST flood 攻击防范统计信息。

sip-flood: 显示 SIP flood 攻击防范统计信息。

syn-ack-flood: 显示 SYN-ACK flood 攻击防范统计信息。

syn-flood: 显示 SYN flood 攻击防范统计信息。

udp-flood: 显示 UDP flood 攻击防范统计信息。

ip-address: 显示指定目的 IPv4 地址的 flood 攻击防范统计信息。若未指定本参数，则显示所有目的 IPv4 地址的 flood 攻击防范统计信息。

vpn vpn-instance-name: 指定 IPv4 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该 IPv4 地址属于公网。

security-zone zone-name: 显示指定安全域的 flood 攻击防范统计信息，*zone-name* 表示安全域名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

slot slot-number: 显示指定成员设备上的 flood 攻击防范统计信息，*slot-number* 表示设备在 IRF 中的成员编号。若未指定本参数，则表示显示所有成员设备上的 flood 攻击防范统计信息。

count: 仅显示符合指定条件的被进行 flood 攻击检测的 IPv4 地址数目。

【使用指导】

由于 flood 攻击不关心源地址，因此本命令显示的是对指定目的 IPv4 地址的攻击防范统计信息。

【举例】

```
# 显示所有类型的 IPv4 flood 攻击防范统计信息。
<Sysname> display attack-defense flood statistics ip
Slot 1:
IP address      VPN      Detected on  Detect type  State  PPS    Dropped
201.55.7.45     --      Trust1      SYN-ACK-FLOOD Normal  1000   111111111
192.168.11.5    --      Trust2      ACK-FLOOD   Normal  1000   222222222
10.118.21.14    --      Trust4      SIP-FLOOD   Normal  1000   265387945
Slot 2:
IP address      VPN      Detected on  Detect type  State  PPS    Dropped
201.55.1.10     --      Trust1      ACK-FLOOD   Normal  1000   222222222
192.168.100.30  --      Trust3      DNS-FLOOD   Normal  1000   333333333
192.168.100.66  --      Trust4      SYN-ACK-FLOOD Normal  1000   165467998

# 显示所有类型的 flood 攻击检测的 IPv4 地址数目。
<Sysname> display attack-defense flood statistics ip count
Slot 1:
Totally 2 flood entries.
Slot 2:
Totally 0 flood entries.
```

表1-1 display attack-defense flood statistics ip 命令显示信息描述表

字段	描述
IP address	被检测的目的IPv4地址
VPN	目的IPv4地址所属的MPLS L3VPN实例名称，属于公网时显示为“--”
Detect type	检测的flood攻击类型，包括： • ACK flood • DNS flood • DNS reply flood • FIN flood • ICMP flood • ICMPv6 flood • SYN flood • SYN-ACK flood • UDP flood • RST flood • HTTP flood • SIP flood
Detected on	进行攻击检测的位置

字段	描述
State	安全域是否处于攻击状态，可包括以下取值： - Attacked: 受攻击状态 - Normal: 正常状态（当前并未受到攻击）
PPS	指定的目的IPv4地址收到报文的速率（单位为报文每秒）
Dropped	安全域丢弃的flood攻击报文数目
Totally 2 flood entries	被检测的IPv4地址表项数目

1.1.30 display attack-defense flood statistics ipv6

display attack-defense flood statistics ipv6 命令用来显示 IPv6 flood 攻击防范统计信息。

【命令】

```
display attack-defense { ack-flood | dns-flood | dns-reply-flood | fin-flood | flood | http-flood | icmpv6-flood | rst-flood | sip-flood | syn-flood | syn-ack-flood | udp-flood } statistics ipv6 [ ipv6-address [ vpn vpn-instance-name ] ] [ security-zone zone-name ] [ slot slot-number ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ack-flood: 显示指定 ACK flood 类型统计信息。
dns-flood: 显示指定 DNS flood 类型统计信息。
dns-reply-flood: 显示 DNS reply flood 攻击防范统计信息。
fin-flood: 显示指定 FIN flood 类型统计信息。
flood: 显示所有类型的 IPv6 flood 攻击防范统计信息。
http-flood: 显示 HTTP flood 攻击防范统计信息。
icmpv6-flood: 显示指定 ICMPv6 flood 类型统计信息。
rst-flood: 显示指定 RST flood 类型统计信息。
sip-flood: 显示指定 SIP flood 类型统计信息。
syn-flood: 显示指定 SYN flood 类型统计信息。
udp-flood: 显示指定 UDP flood 类型统计信息。

ipv6-address: 显示指定目的 IPv6 地址的 flood 攻击防范统计信息。若未指定本参数，则显示所有目的 IPv6 地址的 flood 攻击防范统计信息。

vpn vpn-instance-name: 指定 IPv6 地址所属的 VPN 实例。其中，**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该 IPv6 地址属于公网。

security-zone zone-name: 显示指定安全域的 flood 攻击防范统计信息，**zone-name** 表示安全域名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

slot slot-number: 显示指定成员设备上的 flood 攻击防范统计信息，**slot-number** 表示设备在 IRF 中的成员编号。若未指定本参数，则表示显示所有成员设备上的 flood 攻击防范统计信息。

count: 仅显示符合指定条件的被进行 flood 攻击检测的 IPv6 地址数目。

【使用指导】

由于 flood 攻击不关心源地址，因此本命令显示的是对指定目的 IPv6 地址的攻击防范统计信息。

【举例】

显示所有类型的 IPv6 flood 攻击防范统计信息。

```
<Sysname> display attack-defense flood statistics ipv6
Slot 1:
IPv6 address      VPN      Detected on  Detect type  State  PPS    Dropped
1::2              --      Trust1      DNS-FLOOD   Normal 1000    111111111
1::3              --      Trust2      SYN-ACK-FLOOD Normal 1000    222222222
17::14            --      Trust4      SIP-FLOOD   Normal 1000    266649789
Slot 2:
IPv6 address      VPN      Detected on  Detect type  State  PPS    Dropped
1::2              --      Trust1      SYN-FLOOD   Normal 1000    468792363
1::5              --      Trust2      ACK-FLOOD   Normal 1000    452213396
1::6              --      Trust4      DNS-FLOOD   Normal 1000    12569985
```

显示所有类型的 flood 攻击检测的 IPv6 地址数目。

```
<Sysname> display attack-defense flood statistics ipv6 count
Slot 1:
Totally 5 flood entries.
Slot 2:
Totally 0 flood entries.
```

表1-2 display attack-defense flood statistics ipv6 命令显示信息描述表

字段	描述
IPv6 address	被检测的目的IPv6地址
VPN	目的IPv6地址所属的MPLS L3VPN实例名称，属于公网时显示为“--”

字段	描述
Detect type	检测的flood攻击类型，包括： • ACK flood • DNS flood • DNS reply flood • FIN flood • ICMP flood • ICMPv6 flood • SYN flood • SYN-ACK flood • UDP flood • RST flood • HTTP flood • SIP flood
Detected on	进行攻击检测的位置
State	安全域是否处于攻击状态，可包括以下取值： • Attacked: 受攻击状态 • Normal: 正常状态（当前并未受到攻击）
PPS	指定的目的IPv6地址收到报文的速率（单位为报文每秒）
Dropped	安全域丢弃的flood攻击报文数目
Totally 5 flood entries	被检测的IPv6地址表项数目

1.1.31 display attack-defense policy

display attack-defense policy 用来显示攻击防范策略的配置信息。

【命令】

display attack-defense policy [*policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，包括英文大/小写字母、数字、下划线和连字符，不区分大小写。若未指定本参数，则表示显示所有攻击防范策略的摘要信息。

【使用指导】

本命令显示的内容主要包括各类型攻击防范的使能情况、对攻击报文的处理方式和相关的阈值参数。

【举例】

显示指定攻击防范策略 abc 的配置信息。

```
<Sysname> display attack-defense policy abc
```

Attack-defense Policy Information

Policy name : abc

Applied list : Trust

Exempt IPv4 ACL: : Not configured

Exempt IPv6 ACL: : vip

Actions: CV-Client verify BS-Block source L-Logging D-Drop N-None

Signature attack defense configuration:

Signature name	Defense	Level	Actions
Fragment	Enabled	Info	L
Impossible	Enabled	Info	L
Teardrop	Disabled	Info	L
Tiny fragment	Disabled	Info	L
IP option abnormal	Disabled	Info	L
Smurf	Disabled	Info	N
Traceroute	Disabled	Medium	L,D
Ping of death	Disabled	Low	L
Large ICMP	Disabled	Medium	L,D
Max length	4000 bytes		
Large ICMPv6	Disabled	Low	L
Max length	4000 bytes		
TCP invalid flags	Disabled	medium	L,D
TCP null flag	Disabled	Low	L
TCP all flags	Enabled	Info	L
TCP SYN-FIN flags	Disabled	Info	L
TCP FIN only flag	Enabled	Info	L
TCP Land	Disabled	Info	L
Winnuke	Disabled	Info	L
UDP Bomb	Disabled	Info	L
UDP Snork	Disabled	Info	L
UDP Fraggle	Enabled	Info	L
IP option record route	Disabled	Info	L
IP option internet timestamp	Enabled	Info	L
IP option security	Disabled	Info	L
IP option loose source routing	Enabled	Info	L
IP option stream ID	Disabled	Info	L
IP option strict source routing	Disabled	Info	L
IP option route alert	Disabled	Info	L

ICMP echo request	Disabled	Info	L
ICMP echo reply	Disabled	Info	L
ICMP source quench	Disabled	Info	L
ICMP destination unreachable	Enabled	Info	L
ICMP redirect	Enabled	Info	L
ICMP time exceeded	Enabled	Info	L
ICMP parameter problem	Disabled	Info	L
ICMP timestamp request	Disabled	Info	L
ICMP timestamp reply	Disabled	Info	L
ICMP information request	Disabled	Info	L
ICMP information reply	Disabled	Medium	L,D
ICMP address mask request	Disabled	Medium	L,D
ICMP address mask reply	Disabled	Medium	L,D
ICMPv6 echo request	Enabled	Medium	L,D
ICMPv6 echo reply	Disabled	Medium	L,D
ICMPv6 group membership query	Disabled	Medium	L,D
ICMPv6 group membership report	Disabled	Medium	L,D
ICMPv6 group membership reduction	Disabled	Medium	L,D
ICMPv6 destination unreachable	Enabled	Medium	L,D
ICMPv6 time exceeded	Enabled	Medium	L,D
ICMPv6 parameter problem	Disabled	Medium	L,D
ICMPv6 packet too big	Disabled	Medium	L,D

Scan attack defense configuration:

Preset defense:

Defense: Disabled

User-defined defense:

Port scan defense: Enabled

Port scan defense threshold: 5000 packets

IP sweep defense: Enabled

IP sweep defense threshold: 8000 packets

Period: 100s

Actions: L

Flood attack defense configuration:

Flood type	Global thres(pps)	Global actions	Service ports	Non-specific
DNS flood	1000	-	53	Disabled
DNS reply flood	1000	-	-	Disabled
HTTP flood	1000	-	80	Disabled
SIP flood	100	L,CV	50	Enabled
SYN flood	1000	-	-	Disabled
ACK flood	1000	-	-	Disabled
SYN-ACK flood	1000	-	-	Disabled
RST flood	1000	-	-	Disabled
FIN flood	1000	-	-	Disabled
UDP flood	1000	-	-	Disabled
ICMP flood	1000	-	-	Disabled
ICMPv6 flood	1000	CV	-	Enabled

Flood attack defense for protected IP addresses:

Address	VPN instance	Flood type	Thres(pps)	Actions	Ports
1::1	--	FIN-FLOOD	10	L, D	-
192.168.1.1	--	SYN-ACK-FLOOD	10	-	-
1::1	--	FIN-FLOOD	-	L	-
2013:2013:2013:2013:	--	DNS-FLOOD	100	L, CV	53
2013:2013:2013:2013					
10::13:	A0123458589	SIP-FLOOD	100	L, CV	5060

表1-3 display attack-defense policy 命令显示信息描述表

字段	描述
Policy name	攻击防范策略名称
Applied list	攻击防范策略应用的对象列表
Exempt IPv4 ACL	IPv4例外列表
Exempt IPv6 ACL	IPv6例外列表
Actions	攻击防范的处理行为，包括以下取值： - CV: 启用客户端验证 - BS: 添加黑名单（老化时间，单位为分钟） - L: 输出告警日志 - D: 丢弃报文 - N: 不采用任何处理行为
Signature attack defense configuration	单包攻击防范配置信息
Signature name	单包的类型
Defense	攻击防范的开启状态，包括以下取值： - Enabled: 开启 - Disabled: 关闭
Level	单包攻击的级别，包括以下取值： - Info: 提示级别 - low: 低级别 - medium: 中级别 - high: 高级别（目前暂无实例）
Actions	单包攻击防范的处理行为，包括以下取值： - L: 输出告警日志 - D: 丢弃报文 - N: 不采用任何处理行为
IP option record route	IP选项record route攻击
IP option security	IP选项security攻击
IP option stream ID	IP选项stream identifier攻击

字段	描述
IP option internet timestamp	IP选项 internet timestamp攻击
IP option loose source routing	IP选项loose source routing攻击
IP option strict source routing	IP选项strict source routing攻击
IP option abnormal	IP选项异常攻击
IP option route alert	IP选项route alert攻击
Fragment	IP分片异常攻击
IP impossible	IP impossible攻击
Tiny fragment	IP tiny fragment攻击
Teardrop	IP teardrop攻击，又称IP overlapping fragments
Large ICMP	Large ICMP攻击
Max length	ICMP报文所允许的最大长度
Smurf	Smurf攻击
Traceroute	Traceroute攻击
Ping of death	Ping of death攻击
ICMP echo request	ICMP echo request攻击
ICMP echo reply	ICMP echo reply攻击
ICMP source quench	ICMP source quench攻击
ICMP redirect	ICMP redirect攻击
ICMP parameter problem	ICMP parameter problem攻击
ICMP timestamp request	ICMP timestamp request攻击
ICMP timestamp reply	ICMP timestamp reply攻击
ICMP information request	ICMP information request攻击
ICMP information reply	ICMP information reply攻击
ICMP address mask request	ICMP address mask request攻击
ICMP address mask reply	ICMP address mask reply攻击
ICMP destination unreachable	ICMP destination unreachable攻击
ICMP time exceeded	ICMP time exceeded攻击
Large ICMPv6	Large ICMPv6攻击
ICMPv6 echo request	ICMPv6 echo request攻击
ICMPv6 echo reply	ICMPv6 echo reply攻击
ICMPv6 group membership query	ICMPv6 group membership query攻击
ICMPv6 group membership report	ICMPv6 group membership report攻击

字段	描述
ICMPv6 group membership reduction	ICMPv6 group membership reduction攻击
ICMPv6 destination unreachable	ICMPv6 destination unreachable攻击
ICMPv6 time exceeded	ICMPv6 time exceeded攻击
ICMPv6 parameter problem	ICMPv6 parameter problem攻击
ICMPv6 packet too big	ICMPv6 packet too big攻击
Winnuke	Winnuke攻击
TCP Land	Land攻击
TCP NULL flag	TCP NULL flag攻击
TCP invalid flags	TCP invalid flags攻击
TCP all flags	TCP所有标志位均被置位攻击，又称圣诞树攻击
TCP SYN-FIN flags	TCP SYN和FIN被同时置位攻击
TCP FIN only flag	TCP 只有FIN被置位的攻击
Fraggle	Fraggle攻击，又称UDP chargen DoS attack
UDP Bomb	UDP Bomb攻击
Snork	Snork攻击
Scan attack defense configuration	扫描攻击防范配置信息
Preset defense	预定义扫描攻击防范配置信息
Defense	扫描攻击防范的开启状态
Level	扫描攻击的级别，包括以下取值： - low: 低级别 - medium: 中级别 - high: 高级别
User-defined defense	用户自定义扫描攻击防范配置信息
Port scan defense	端口扫描攻击防范状态： - Enabled: 开启 - Disabled: 关闭
Port scan defense threshold	端口扫描防范检测阈值
IP sweep defense	IP地址扫描攻击防范状态： - Enabled: 开启 - Disabled: 关闭
IP sweep defense threshold	IP地址扫描防范检测阈值
Period	扫描攻击防范检测周期

字段	描述
Actions	扫描攻击防范的处理行为，包括以下取值： • BS: 添加黑名单（老化时间，单位为分钟） • D: 丢弃报文 • L: 输出告警日志
Flood attack defense configuration	flood攻击防范配置信息
Flood type	flood攻击类型，包括以下取值： • ACK flood • DNS flood • DNS reply flood • FIN flood • ICMP flood • ICMPv6 flood • SYN flood • SYN-ACK flood • UDP flood • RST flood • HTTP flood • SIP flood
Global thres(pps)	flood攻击防范的全局触发阈值，单位为每秒报文数，默认值为1000pps
Global actions	flood攻击防范的全局处理行为，包括以下取值： • D: 丢弃报文 • L: 输出告警日志， • CV: 启用客户端验证 • -: 未配置
Service ports	flood攻击防范的全局检测端口号。该字段只对DNS flood攻击防范和HTTP flood攻击防范生效，对于其它flood攻击防范，显示为“-”
Non-specific	对非受保护IP地址开启SYN flood攻击防范检测的状态
Flood attack defense for protected IP addresses	对受保护IP地址的flood攻击防范配置
Address	指定的IP地址
VPN instance	所属的VPN实例名称，未配置时显示为“--”
Thres(pps)	攻击防范检测的触发阈值，单位为报文每秒，未配置时显示为“1000”

字段	描述
Actions	对指定IP地址采用的攻击防范处理行为，包括 取值： - CV: 启用客户端验证 - BS: 添加黑名单 - L: 输出告警日志 - D: 丢弃报文 - N: 不采用任何处理行为
Ports	flood攻击防范的检测端口号。该字段只对DNS flood攻击防范和HTTP flood攻击防范生效，对于其他攻击防范，显示为“-”

显示所有攻击防范策略的概要配置信息。

```
<Sysname> display attack-defense policy
Attack-defense Policy Brief Information
```

```
-----
Policy Name          Applied list
Atk-policy-1         Trust1
P2                   Trust2
P123                 Trust3
```

表1-4 display attack-defense policy 命令显示信息描述表

字段	描述
Policy Name	攻击防范策略名称
Applied list	攻击防范策略应用的对象列表

【相关命令】

- attack-defense policy

1.1.32 display attack-defense policy ip

display attack-defense policy ip 命令用来显示 flood 攻击防范的 IPv4 类型的受保护 IP 表项。

【命令】

```
display attack-defense policy policy-name { ack-flood | dns-flood |
dns-reply-flood | fin-flood | flood | http-flood | icmp-flood | rst-flood |
sip-flood | syn-ack-flood | syn-flood | udp-flood } ip [ ip-address [ vpn
vpn-instance-name ] ] [ slot slot-number ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

ack-flood: 显示 ACK flood 攻击防范受保护 IP 表项。

dns-flood: 显示 DNS flood 攻击防范受保护 IP 表项。

dns-reply-flood: 显示 DNS reply flood 攻击防范受保护 IP 表项。

fin-flood: 显示 FIN flood 攻击防范受保护 IP 表项。

flood: 显示所有类型的 flood 攻击防范受保护 IP 表项。

http-flood: 显示 HTTP flood 攻击防范受保护 IP 表项。

icmp-flood: 显示 ICMP flood 攻击防范受保护 IP 表项。

rst-flood: 显示 RST flood 攻击防范受保护 IP 表项。

sip-flood: 显示 SIP flood 攻击防范受保护 IP 表项。

syn-ack-flood: 显示 SYN-ACK flood 攻击防范受保护 IP 表项。

syn-flood: 显示 SYN flood 攻击防范受保护 IP 表项。

udp-flood: 显示 UDP flood 攻击防范受保护 IP 表项。

ip ip-address: 显示指定 IPv4 地址的受保护 IP 表项。若未指定 *ip-address* 参数，则表示显示所有 IPv4 类型的受保护 IP 表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的受保护 IP 表项。其中 *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示显示指公网的受保护 IP 表项。

slot slot-number: 显示指定成员设备上的受保护 IP 表项，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的受保护 IP 表项。

count: 显示符合指定条件的 flood 受保护 IP 表项的数目。

【举例】

显示指定攻击防范策略 abc 中所有 flood 攻击防范的 IPv4 类型受保护 IP 表项的信息。

```
<Sysname> display attack-defense policy abc flood ip
```

Slot 1:

IP address	VPN instance	Type	Rate threshold(PPS)	Dropped
123.123.123.123	--	SYN-ACK-FLOOD	100	4294967295
201.55.7.45	--	ICMP-FLOOD	100	10
192.168.11.5	--	DNS-FLOOD	23	100
10.168.200.5	--	SIP-FLOOD	100	102556

Slot 2:

IP address	VPN instance	Type	Rate threshold(PPS)	Dropped
123.123.123.123	--	SYN-ACK-FLOOD	100	2543

```

201.55.7.45      --                ICMP-FLOOD    100                122
192.168.11.5     --                DNS-FLOOD     23                 0

```

显示指定攻击防范策略 abc 中所有 IPv4 类型 flood 受保护 IP 表项的个数。

```
<Sysname> display attack-defense policy abc flood ip count
```

Slot 1:

Totally 3 flood protected IP addresses.

Slot 2:

Totally 0 flood protected IP addresses.

表1-5 display attack-defense flood ip 命令显示信息描述表

字段	描述
Totally 3 flood protected IP addresses	IPv4类型受保护IP表项数目
IP address	受保护的IPv4地址
VPN instance	受保护的IPv4地址所属的MPLS L3VPN实例名称，未指定时显示为“--”
Type	flood攻击类型
Rate threshold(PPS)	配置的flood攻击防范触发阈值（单位为报文每秒），未配置时显示“1000”
Dropped	检测到flood攻击后的丢包数，若只输出日志该项显示为0

1.1.33 display attack-defense policy ipv6

display attack-defense policy ipv6 命令用来显示 flood 攻击防范的 IPv6 类型的受保护 IP 表项。

【命令】

```

display attack-defense policy policy-name { ack-flood | dns-flood |
dns-reply-flood | fin-flood | flood | http-flood | icmpv6-flood | rst-flood
| sip-flood | syn-ack-flood | syn-flood | udp-flood } ipv6 [ ipv6-address
[ vpn vpn-instance-name ] ] [ slot slot-number ] ] [ count ]

```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

ack-flood: 显示 ACK flood 攻击防范受保护 IP 表项。

dns-flood: 显示 DNS flood 攻击防范受保护 IP 表项。

dns-reply-flood: 显示 DNS reply flood 攻击防范受保护 IP 表项。

fin-flood: 显示 FIN flood 攻击防范受保护 IP 表项。

flood: 显示所有类型的 flood 攻击防范受保护 IP 表项。

http-flood: 显示 HTTP flood 攻击防范受保护 IP 表项。

icmpv6-flood: 显示 ICMPv6 flood 攻击防范受保护 IP 表项。

rst-flood: 显示 RST flood 攻击防范受保护 IP 表项。

sip-flood: 显示 SIP flood 攻击防范受保护 IP 表项。

syn-ack-flood: 显示 SYN-ACK flood 攻击防范受保护 IP 表项。

syn-flood: 显示 SYN flood 攻击防范受保护 IP 表项。

udp-flood: 显示 UDP flood 攻击防范受保护 IP 表项。

ipv6 ipv6-address: 显示指定 IPv6 地址的受保护 IP 表项。若未指定 *ipv6-address* 参数，则表示所有 IPv6 类型的受保护 IP 表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的受保护 IP 表项。其中 *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

slot slot-number: 显示指定成员设备上的受保护 IP 表项，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的受保护 IP 表项。

count: 显示符合指定条件的 flood 受保护 IP 表项的数目。

【举例】

显示指定攻击防范策略 abc 中所有 flood 攻击防范的 IPv6 类型受保护 IP 表项。

```
<Sysname> display attack-defense policy abc flood ipv6
```

Slot 1:

IPv6 address	VPN instance	Type	Rate threshold(PPS)	Dropped
2013::127f	--	SYN-ACK-FLOOD	100	4294967295
2::5	--	ACK-FLOOD	100	10
1::5	--	ACK-FLOOD	100	23
10::15	--	SIP-FLOOD	100	1002

Slot 2:

IPv6 address	VPN instance	Type	Rate threshold(PPS)	Dropped
2013::127f	--	SYN-ACK-FLOOD	100	5465
2::5	--	ACK-FLOOD	100	0
1::5	--	ACK-FLOOD	100	122

显示指定攻击防范策略 abc 中所有 flood 攻击防范的 IPv6 类型受保护 IP 表项的个数。

```
<Sysname> display attack-defense policy abc flood ipv6 count
```

Slot 1:

Totally 3 flood protected IP addresses.

Slot 2:

Totally 0 flood protected IP addresses.

表1-6 display flood ipv6 命令显示信息描述表

字段	描述
Totally 3 flood protected IP addresses	IPv6类型受保护IP表项数目
IPv6 address	受保护的IPv6地址
VPN instance	受保护的IPv6地址所属的MPLS L3VPN实例名称，未指定时显示为“--”
Type	flood攻击类型
Rate threshold(PPS)	配置的flood攻击防范触发阈值(单位为报文每秒)，未配置时显示“1000”
Dropped	检测到flood攻击后的丢包数，若只输出日志该项显示为0

1.1.34 display attack-defense scan attacker ip

display attack-defense scan attacker ip 命令用来显示扫描攻击者的 IPv4 地址表项。

【命令】

display attack-defense scan attacker ip [**security-zone** *zone-name* [**slot** *slot-number*]] [**count**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

security-zone zone-name: 显示指定安全域的扫描攻击者的 IPv4 地址表项，*zone-name* 表示安全域名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

slot slot-number: 显示指定成员设备上的扫描攻击者的 IPv4 地址表项，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的扫描攻击者的 IPv4 地址表项。

count: 仅显示符合指定条件的当前扫描攻击者的数目。

【使用指导】

若未指定任何参数，则表示显示所有扫描攻击者的 IPv4 地址表项。

【举例】

显示所有扫描攻击者的 IPv4 地址表项。

```
<Sysname> display attack-defense scan attacker ip
```

Slot 1:

IP	addr(DslitePeer)	VPN instance	Protocol	Detected on	Duration(min)

```

192.168.31.2(--)--TCPDMZ1284
2.2.2.3(--)--UDPDMZ23
Slot 2:
IP addr(DslitePeer) VPN instance Protocol Detected on Duration(min)
192.168.1.100(--)--TCPDMZ1586
202.2.1.172(--)--UDPDMZ258

```

显示所有扫描攻击者的 IPv4 地址表项的个数。

```
<Sysname> display attack-defense scan attacker ip count
```

```

Slot 1:
Totally 3 attackers.
Slot 2:
Totally 0 attackers.

```

表1-7 display attack-defense scan attacker ip 命令显示信息描述表

字段	描述
Total 3 attackers	攻击者的数目
IP addr(DslitePeer)	发起攻击的IP地址
VPN instance	所属的MPLS L3VPN实例名称，属于公网时显示为“--”
Protocol	协议名称
Detected on	进行攻击检测的位置
Duration(min)	检测到攻击的持续时间，单位为分钟

【相关命令】

- scan detect

1.1.35 display attack-defense scan attacker ipv6

display attack-defense scan attacker ipv6 命令用来显示扫描攻击者的 IPv6 地址表项。

【命令】

```
display attack-defense scan attacker ipv6 [ security-zone zone-name [ slot slot-number ] ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

security-zone zone-name: 显示指定安全域的扫描攻击者的 IPv6 地址表项, *zone-name* 表示安全域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包含字符 “-”。

slot slot-number: 显示指定成员设备上的扫描攻击者的 IPv6 地址表项, *slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数, 则表示显示所有成员设备上的扫描攻击者的 IPv6 地址表项。

count: 仅显示符合指定条件的当前扫描攻击者的数目。

【使用指导】

若未指定任何参数, 则表示显示所有扫描攻击者的 IPv6 地址表项。

【举例】

显示扫描攻击者的 IPv6 地址表项。

```
<Sysname> display attack-defense scan attacker ipv6
Slot 1:
IPv6 address      VPN instance      Protocol          Detected on      Duration(min)
2013::2           --                TCP               DMZ              1234
1230::22          --                UDP               DMZ              10
Slot 2:
IPv6 address      VPN instance      Protocol          Detected on      Duration(min)
2004::4           --                TCP               DMZ              1122
1042::2           --                UDP               DMZ              24
```

显示扫描攻击者的 IPv6 地址表项的个数。

```
<Sysname> display attack-defense scan attacker ipv6 count
Slot 1:
Totally 3 attackers.
Slot 2:
Totally 0 attackers.
```

表1-8 display attack-defense scan attacker ipv6 命令显示信息描述表

字段	描述
Totally 3 attackers	攻击者的数目
IPv6 address	发起攻击的IPv6地址
VPN instance	所属的MPLS L3VPN实例名称, 属于公网时显示为 “--”
Protocol	协议名称
Detected on	进行攻击检测的位置
Duration(min)	检测到攻击的持续时间, 单位为分钟

【相关命令】

- **scan detect**

1.1.36 display attack-defense statistics security-zone

display attack-defense statistics security-zone 命令用来显示安全域上的攻击防范统计信息。

【命令】

display attack-defense statistics security-zone *zone-name* [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

zone-name: 指定安全域的名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

slot slot-number: 显示指定成员设备上的攻击防范统计信息，**slot-number** 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的攻击防范统计信息。

【举例】

显示指定 Slot 的 Untrust 上的攻击防范统计信息。

```
<Sysname> display attack-defense statistics security-zone untrust slot 1
```

Slot 1:

Attack policy name: abc

Scanning attack defense statistics:

AttackType	AttackTimes	Dropped
Port scan	2	23
IP sweep	3	33
Distribute port scan	1	10

Flood attack defense statistics:

AttackType	AttackTimes	Dropped
SYN flood	1	0
ACK flood	1	0
SYN-ACK flood	3	5000
RST flood	2	0
FIN flood	2	0
UDP flood	1	0
ICMP flood	1	0
ICMPv6 flood	1	0
DNS flood	1	0
DNS reply flood	1	0
HTTP flood	1	0
SIP flood	1	1000

Signature attack defense statistics:

AttackType	AttackTimes	Dropped
IP option record route	1	100
IP option security	2	0
IP option stream ID	3	0
IP option internet timestamp	4	1
IP option loose source routing	5	0
IP option strict source routing	6	0
IP option route alert	3	0
Fragment	1	0
Impossible	1	1
Teardrop	1	1
Tiny fragment	1	0
IP options abnormal	3	0
Smurf	1	0
Ping of death	1	0
Traceroute	1	0
Large ICMP	1	0
TCP NULL flag	1	0
TCP all flags	1	0
TCP SYN-FIN flags	1	0
TCP FIN only flag	1	0
TCP invalid flag	1	0
TCP Land	1	0
Winnuke	1	0
UDP Bomb	1	0
Snork	1	0
Fraggle	1	0
Large ICMPv6	1	0
ICMP echo request	1	0
ICMP echo reply	1	0
ICMP source quench	1	0
ICMP destination unreachable	1	0
ICMP redirect	2	0
ICMP time exceeded	3	0
ICMP parameter problem	4	0
ICMP timestamp request	5	0
ICMP timestamp reply	6	0
ICMP information request	7	0
ICMP information reply	4	0
ICMP address mask request	2	0
ICMP address mask reply	1	0
ICMPv6 echo request	1	1
ICMPv6 echo reply	1	1
ICMPv6 group membership query	1	0
ICMPv6 group membership report	1	0
ICMPv6 group membership reduction	1	0
ICMPv6 destination unreachable	1	0

ICMPv6 time exceeded	1	0
ICMPv6 parameter problem	1	0
ICMPv6 packet too big	1	0

表1-9 display attack-defense statistics security-zone 命令显示信息描述表

字段	描述
AttackType	攻击类型
AttackTimes	受到攻击的次数
Dropped	丢弃报文的数目
SYN flood	SYN flood攻击，当AttackTimes 为0时，该列不显示
ACK flood	ACK flood攻击，当AttackTimes 为0时，该列不显示
SYN-ACK flood	SYN-ACK flood攻击，当AttackTimes 为0时，该列不显示
RST flood	RST flood攻击，当AttackTimes 为0时，该列不显示
FIN flood	FIN flood攻击，当AttackTimes 为0时，该列不显示
UDP flood	UDP flood 攻击，当AttackTimes 为0时，该列不显示
ICMP flood	ICMP flood攻击，当AttackTimes 为0时，该列不显示
ICMPv6 flood	ICMPv6 flood攻击，当AttackTimes 为0时，该列不显示
DNS flood	DNS flood攻击，当AttackTimes 为0时，该列不显示
DNS reply flood	DNS reply flood攻击，当AttackTimes为0时，该列不显示
HTTP flood	HTTP flood攻击，当AttackTimes 为0时，该列不显示
SIP flood	SIP flood攻击，当AttackTimes 为0时，该列不显示
Port scan	端口扫描攻击，当AttackTimes 为0时，该列不显示
IP Sweep	IP扫描攻击，当AttackTimes 为0时，该列不显示
Distribute port scan	分布式端口扫描攻击，当AttackTimes 为0时，该列不显示
IP option record route	IP选项record route攻击，当AttackTimes 为0时，该列不显示
IP option security	IP选项security攻击，当AttackTimes 为0时，该列不显示
IP option stream ID	IP选项stream identifier攻击，当AttackTimes 为0时，该列不显示
IP option internet timestamp	IP选项 internet timestamp攻击，当AttackTimes 为0时，该列不显示
IP option loose source routing	IP选项loose source routing攻击，当AttackTimes 为0时，该列不显示
IP option strict source routing	IP选项strict source routing攻击，当AttackTimes 为0时，该列不显示
IP option route alert	IP选项strict source routing攻击，当AttackTimes 为0时，该列不显示
Fragment	IP分片异常攻击，当AttackTimes 为0时，该列不显示
Impossible	IP impossible攻击，当AttackTimes 为0时，该列不显示
Teardrop	IP teardrop攻击，又称IP overlapping fragments，当AttackTimes 为0时，该列不显示

字段	描述
Tiny fragment	IP tiny fragment攻击
IP option abnormal	IP选项异常攻击，当AttackTimes 为0时，该列不显示
Smurf	Smurf攻击，当AttackTimes 为0时，该列不显示
Ping of death	Ping of death攻击，当AttackTimes 为0时，该列不显示
Traceroute	Traceroute攻击，当AttackTimes 为0时，该列不显示
Large ICMP	Large ICMP攻击，当AttackTimes 为0时，该列不显示
TCP NULL flag	TCP NULL flag攻击，当AttackTimes 为0时，该列不显示
TCP all flags	TCP所有标志位均被置位攻击，又称圣诞树攻击，当AttackTimes 为0时，该列不显示
TCP SYN-FIN flags	TCP SYN和FIN被同时置位攻击，当AttackTimes 为0时，该列不显示
TCP FIN only flag	TCP 只有FIN被置位的攻击，当AttackTimes 为0时，该列不显示
TCP invalid flag	TCP 非法标志位攻击，当AttackTimes 为0时，该列不显示
TCP Land	TCP Land攻击，当AttackTimes 为0时，该列不显示
Winnuke	Winnuke攻击，当AttackTimes 为0时，该列不显示
UDP Bomb	UDP Bomb攻击，当AttackTimes 为0时，该列不显示
Snork	UDP snork攻击，当AttackTimes 为0时，该列不显示
Fraggle	Fraggle攻击，又称UDP chargen DoS attack，当AttackTimes 为0时，该列不显示
Large ICMPv6	Large ICMPv6攻击，当AttackTimes 为0时，该列不显示
ICMP echo request	ICMP echo request攻击，当AttackTimes 为0时，该列不显示
ICMP echo reply	ICMP echo reply攻击，当AttackTimes 为0时，该列不显示
ICMP source quench	ICMP source quench攻击，当AttackTimes 为0时，该列不显示
ICMP destination unreachable	ICMP destination unreachable攻击，当AttackTimes 为0时，该列不显示
ICMP redirect	ICMP redirect攻击，当AttackTimes 为0时，该列不显示
ICMP time exceeded	ICMP time exceeded攻击，当AttackTimes 为0时，该列不显示
ICMP parameter problem	ICMP parameter problem攻击，当AttackTimes 为0时，该列不显示
ICMP timestamp request	ICMP timestamp request攻击，当AttackTimes 为0时，该列不显示
ICMP timestamp reply	ICMP timestamp reply攻击，当AttackTimes 为0时，该列不显示
ICMP information request	ICMP information request攻击，当AttackTimes 为0时，该列不显示
ICMP information reply	ICMP information reply攻击，当AttackTimes 为0时，该列不显示
ICMP address mask request	ICMP address mask request攻击，当AttackTimes 为0时，该列不显示
ICMP address mask reply	ICMP address mask reply攻击，当AttackTimes 为0时，该列不显示

字段	描述
ICMPv6 echo request	ICMPv6 echo request攻击，当AttackTimes 为0时，该列不显示
ICMPv6 echo reply	ICMPv6 echo reply攻击，当AttackTimes 为0时，该列不显示
ICMPv6 group membership query	ICMPv6 group membership query攻击，当AttackTimes 为0时，该列不显示
ICMPv6 group membership report	ICMPv6 group membership report攻击，当AttackTimes 为0时，该列不显示
ICMPv6 group membership reduction	ICMPv6 group membership reduction攻击，当AttackTimes 为0时，该列不显示
ICMPv6 destination unreachable	ICMPv6 destination unreachable攻击，当AttackTimes 为0时，该列不显示
ICMPv6 time exceeded	ICMPv6 time exceeded攻击，当AttackTimes 为0时，该列不显示
ICMPv6 parameter problem	ICMPv6 parameter problem攻击，当AttackTimes 为0时，该列不显示
ICMPv6 packet too big	ICMPv6 packet too big攻击，当AttackTimes 为0时，该列不显示

1.1.37 display attack-defense top-attack-statistics

display attack-defense top-attack-statistics 命令用来显示 Top10 的攻击排名统计信息。

【命令】

```
display attack-defense top-attack-statistics { last-1-hour | last-24-hours | last-30-days } [ by-attacker | by-type | by-victim ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

last-1-hour: 显示最近 1 小时的统计信息。

last-24-hours: 显示最近 24 小时的统计信息。

last-30-days: 显示最近 30 天的统计信息。

by-attacker: 显示基于攻击者 IP 地址的 Top10 排名统计信息。

by-type: 显示基于攻击类型的统计信息。

by-victim: 显示基于被攻击者 IP 地址的 Top10 排名统计信息。

【使用指导】

若未指定[**by-attacker** | **by-type** | **by-victim**]参数，则同时显示基于攻击者 IP 地址、被攻击者 IP 地址和攻击类型的统计信息。

【举例】

显示最近 1 小时的 Top10 排名统计信息

<Sysname> display attack-defense top-attack-statistics last-1-hour

Top attackers:

No.	VPN instance	Attacker IP	Attacks
1	--	200.200.200.55	21
2	--	200.200.200.21	16
3	--	200.200.200.133	12
4	--	200.200.200.19	10
5	--	200.200.200.4	8
6	--	200.200.200.155	8
7	--	200.200.200.93	5
8	--	200.200.200.67	3
9	--	200.200.200.70	1
10	--	200.200.200.23	1

Top victims:

No.	VPN instance	Victim IP	Attacks
1	--	200.200.200.12	21
2	--	200.200.200.32	16
3	--	200.200.200.14	12
4	--	200.200.200.251	12
5	--	200.200.200.10	7
6	--	200.200.200.77	6
7	--	200.200.200.96	2
8	--	200.200.200.22	2
9	--	200.200.200.154	2
10	--	200.200.200.18	1

Top attack types:

Attack type	Attacks
Scan	155
Syn	155

表1-10 display attack-defense top-attack-statistics 命令显示信息描述表

字段	描述
Top attackers	基于攻击者IP地址的Top10排名统计信息
No.	Top10排名
VPN instance	所属的VPN实例名称，属于公网时显示为空
Attacker IP	攻击者的IP地址
Attacks	丢包数量

字段	描述
Top victims	基于被攻击者IP地址的Top10排名统计信息
Victim IP	被攻击者的IP地址
Top attack types	基于攻击类型的统计信息
Attack type	攻击类型

【相关命令】

- **attack-defense top-attack-statistics enable**

1.1.38 display blacklist destination-ip

display blacklist destination-ip 命令用来显示目的 IPv4 黑名单表项。

【命令】

display blacklist destination-ip [*destination-ip-address* [**vpn-instance** *vpn-instance-name*]] [**slot** *slot-number*] [**count**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

destination-ip-address: 显示指定 IPv4 地址的目的 IPv4 黑名单表项。

vpn-instance *vpn-instance-name*: 显示指定 VPN 实例的目的 IPv4 黑名单表项。其中 *vpn-instance-name* 表示 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

slot *slot-number*: 显示指定成员设备上的目的 IPv4 黑名单表项，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的目的 IPv4 黑名单表项。

count: 显示符合指定条件的目的 IPv4 黑名单个数。

【使用指导】

若未指定任何参数，则表示显示所有的目的 IPv4 黑名单表项。

【举例】

显示所有目的 IPv4 黑名单表项的信息。

```
<Sysname> display blacklist destination-ip
Slot 1:
IP address      VPN instance    Type    Aging (sec)    Dropped
192.168.11.5    --              Dynamic 10             353452
```

```
123.123.123.123 --          Dynamic 123          4294967295
201.55.7.45      --          Manual  Never          14478
```

Slot 2:

```
IP address      VPN instance  Type    Aging (sec)  Dropped
123.55.123.7    --            Dynamic 123      164698
201.55.7.33     --            Manual  Never        845969
```

显示所有目的 IPv4 黑名单表项的个数。

```
<Sysname> display blacklist destination-ip count
```

Slot 1:

Totally 3 blacklist entries.

Slot 2:

Totally 2 blacklist entries.

表1-11 display blacklist destination-ip 命令显示信息描述表

字段	描述
IP address	黑名单表项的IP地址
VPN instance	VPN实例名称，属于公网时显示为“--”
Type	黑名单表项的添加方式，包括： - Dynamic：动态生成 - Manual：手工配置
Aging (sec)	黑名单表项的剩余老化时间，单位为秒。若未指定老化时间，则显示“Never”
Dropped	丢弃的发往该IP地址的报文数目
Totally 3 blacklist entries.	黑名单表项数目

【相关命令】

- blacklist destination-ip**

1.1.39 display blacklist destination-ipv6

display blacklist destination-ipv6 命令用来显示目的 IPv6 黑名单表项。

【命令】

```
display    blacklist    destination-ipv6    [    destination-ipv6-address
[ vpn-instance vpn-instance-name ] ] [ slot slot-number ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
```

context-operator

【参数】

destination-ipv6-address: 显示指定目的 IPv6 地址的黑名单表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的目的 IPv6 黑名单表项。其中 **vpn-instance-name** 表示 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

slot slot-number: 显示指定成员设备上的目的 IPv6 黑名单表项，**slot-number** 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的目的 IPv6 黑名单表项。

count: 仅显示符合指定条件的目的 IPv6 黑名单个数。

【使用指导】

若未指定任何参数，则表示显示所有的目的 IPv6 黑名单表项。

【举例】

显示所有目的 IPv6 黑名单表项的信息。

```
<Sysname> display blacklist ipv6
```

Slot 1:

IPv6 address	VPN instance	Type	Aging (sec)	Dropped
1::4	--	Manual	Never	14478
1::5	--	Dynamic	10	353452
2013:fe07:221a:4011:2013:fe07:221a:4011	--	Dynamic	123	4294967295

Slot 2:

IPv6 address	VPN instance	Type	Aging (sec)	Dropped
1::3	--	Manual	Never	74679
20::33	--	Dynamic	10	1697898

显示所有目的 IPv6 黑名单表项的个数。

```
<Sysname> display blacklist ipv6 count
```

Slot 1:

Totally 3 blacklist entries.

Slot 2:

Totally 2 blacklist entries.

表1-12 display blacklist destination-ipv6 命令显示信息描述表

字段	描述
IPv6 address	黑名单表项的IPv6地址
VPN instance	VPN实例名称，属于公网时显示为“--”
Type	黑名单表项的添加方式，包括： • Dynamic: 动态生成 • Manual: 手工配置
Aging (sec)	黑名单表项的剩余老化时间，单位为秒。若未指定老化时间，则显示“Never”
Dropped	丢弃的发往该IPv6地址的报文数目
Totally 3 blacklist entries.	黑名单表项数目

【相关命令】

- **blacklist destination-ipv6**

1.1.40 display blacklist ip

display blacklist ip 命令用来显示源 IPv4 黑名单表项。

【命令】

display blacklist ip [*source-ip-address* [**vpn-instance** *vpn-instance-name*]
[**ds-lite-peer** *ds-lite-peer-address*]] [**slot** *slot-number*] [**count**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

source-ip-address: 显示指定 IPv4 地址的源黑名单表项。

vpn-instance *vpn-instance-name*: 显示指定 VPN 实例的源 IPv4 黑名单表项。其中 *vpn-instance-name* 表示 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

ds-lite-peer *ds-lite-peer-address*: 显示指定 DS-Lite 隧道对端地址的源 IPv4 黑名单表项。其中，*ds-lite-peer-address* 表示源黑名单的 IPv4 地址所属的 DS-Lite 隧道 B4 端 IPv6 地址。

slot *slot-number*: 显示指定成员设备上的源 IPv4 黑名单表项，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的源 IPv4 黑名单表项。

count: 显示符合指定条件的源 IPv4 黑名单个数。

【使用指导】

若未指定任何参数，则表示显示所有的源 IPv4 黑名单表项。

【举例】

显示所有源 IPv4 黑名单表项的信息。

<Sysname> display blacklist ip

Slot 1:

IP address	VPN instance	DS-Lite tunnel peer	Type	TTL(sec)	Dropped
192.168.11.5	--	--	Dynamic	10	353452
123.123.123.123	--	2013::fe07:221a:4011	Dynamic	123	4294967295
201.55.7.45	--	2013::1	Manual	Never	14478

Slot 2:

IP address	VPN instance	DS-Lite tunnel peer	Type	TTL(sec)	Dropped

```

123.55.123.7      --          --          Dynamic 123      164698
201.55.7.33       --          --          Manual   Never      845969

```

显示所有源 IPv4 黑名单表项的个数。

```
<Sysname> display blacklist ip count
```

Slot 1:

Totally 3 blacklist entries.

Slot 2:

Totally 2 blacklist entries.

表1-13 display blacklist ip 命令显示信息描述表

字段	描述
IP address	源黑名单表项的IP地址
VPN instance	VPN实例名称，属于公网时显示为“--”
DS-Lite tunnel peer	（暂不支持）DS-Lite隧道对端地址。DS-Lite组网下，若本设备为AFTR，此列表示报文来自具体的哪个B4，如果不在DS-Lite组网或本设备不为AFTR，则该字段无意义，显示为“--”
Type	源黑名单表项的添加方式，包括： - Dynamic：动态生成 - Manual：手工配置
TTL(sec)	源黑名单表项的剩余老化时间，单位为秒。若未指定老化时间，则显示“Never”
Dropped	丢弃的来自该IP地址的报文数目
Totally 3 blacklist entries.	源黑名单表项数目

【相关命令】

- blacklist ip**

1.1.41 display blacklist ipv6

display blacklist ipv6 命令用来显示源 IPv6 黑名单表项。

【命令】

```
display blacklist ipv6 [ source-ipv6-address [ vpn-instance
vpn-instance-name ] ] [ slot slot-number ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

source-ipv6-address: 显示指定源 IPv6 地址的黑名单表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的源 IPv6 黑名单表项。其中 **vpn-instance-name** 表示 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

slot slot-number: 显示指定成员设备上的源 IPv6 黑名单表项，**slot-number** 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的源 IPv6 黑名单表项。

count: 仅显示符合指定条件的源 IPv6 黑名单个数。

【使用指导】

若未指定任何参数，则表示显示所有的源 IPv6 黑名单表项。

【举例】

显示所有源 IPv6 黑名单表项的信息。

```
<Sysname> display blacklist ipv6
Slot 1:
IPv6 address      VPN instance      Type    TTL(sec) Dropped
1::4              --                Manual  Never    14478
1::5              --                Dynamic 10      353452
2013:fe07:221a:4011: --          Dynamic 123      4294967295
2013:fe07:221a:4011
Slot 2:
IPv6 address      VPN instance      Type    TTL(sec) Dropped
1::3              --                Manual  Never    74679
20::33            --                Dynamic 10      1697898
```

显示所有源 IPv6 黑名单表项的个数。

```
<Sysname> display blacklist ipv6 count
Slot 1:
Totally 3 blacklist entries.
Slot 2:
Totally 2 blacklist entries.
```

表1-14 display blacklist ipv6 命令显示信息描述表

字段	描述
IPv6 address	源黑名单表项的IPv6地址
VPN instance	VPN实例名称，属于公网时显示为“--”
Type	源黑名单表项的添加方式，包括： • Dynamic: 动态生成 • Manual: 手工配置
TTL(sec)	源黑名单表项的剩余老化时间，单位为秒。若未指定老化时间，则显示“Never”
Dropped	丢弃的来自该IPv6地址的报文数目
Totally 3 blacklist entries.	源黑名单表项数目

【相关命令】

- **blacklist ipv6**

1.1.42 display blacklist user

display blacklist user 命令用来显示用户黑名单表项。

【命令】

display blacklist user [*user-name*] [**domain** *domain-name*] [**count**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

user-name: 表示用户的名称，为 1~55 个字符的字符串，区分大小写。如果不指定该参数，则表示显示所有用户黑名单表项。

domain domain-name: 显示指定身份识别域的用户黑名单表项。*domain-name* 是身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包括字符“?”。若不指定此参数，则显示不属于任何身份识别域的用户黑名单表项。

count: 显示用户黑名单表项的个数。

【举例】

显示所有用户黑名单表项的信息。

```
<Sysname> display blacklist user
```

User name	Domain name	Type	TTL(sec)	Dropped
Alex	domaina	Manual	10	353452
Bob		Manual	123	4294967295
Cary		Manual	Never	14478

显示属于身份识别域 **domaina** 的指定用户黑名单表项。

```
<Sysname> display blacklist user Alex domain domaina
```

User name	Domain name	Type	TTL(sec)	Dropped
Alex	domaina	Manual	10	353452

显示用户黑名单表项的个数。

```
<Sysname> display blacklist user count
```

Totally 3 blacklist entries.

表1-15 display blacklist user 命令显示信息描述表

字段	描述
Username	黑名单表项的用户名称

字段	描述
Domain name	黑名单表项的用户身份识别域
Type	黑名单表项的添加方式，仅支持手工配置“Manual”
TTL(sec)	黑名单表项的剩余老化时间，单位为秒。若未指定老化时间，则显示“Never”
Dropped	丢弃该用户的报文数目
Totally 3 blacklist entries.	用户黑名单表项的数目

【相关命令】

- **blacklist global enable**
- **blacklist user**

1.1.43 display client-verify protected ip

display client-verify protected ip 命令用来显示客户端验证的 IPv4 类型的受保护 IP 表项。

【命令】

```
display client-verify { dns | dns-reply | http | sip | tcp } protected ip  
[ ip-address [ vpn vpn-instance-name ] ] [ port port-number ] [ slot  
slot-number ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

dns: 指定 DNS 客户端验证功能。

dns-reply: 指定 DNS reply 验证功能。

http: 指定 HTTP 客户端验证功能。

sip: 指定 SIP 客户端验证功能。

tcp: 指定 TCP 客户端验证功能。

ip-address: 显示指定 IPv4 地址的受保护 IP 表项。若未指定本参数，则显示所有 IPv4 类型的受保护 IP 表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的受保护 IP 表项。其中 **vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示显示公网中的受保护 IP 地址。

port port-number: 显示指定端口号的受保护 IP 表项, *port-number* 的取值范围为 1~65535。
若未指定本参数, 对于 DNS 客户端验证的受保护 IP, 则表示端口 53; 对于 HTTP 客户端验证的受保护 IP, 则表示端口 80; 对于 TCP 客户端验证的受保护 IP, 则表示所有端口。

slot slot-number: 显示指定成员设备上的受保护 IP 表项, *slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数, 则表示显示所有成员设备上的受保护 IP 表项。

count: 显示符合指定条件的客户端验证受保护 IP 表项。

【举例】

显示所有 IPv4 类型 TCP 客户端验证的受保护 IP 表项。

```
<Sysname> display client-verify tcp protected ip
```

Slot 1:

IP address	VPN instance	Port	Type	Requested	Trusted
192.168.11.5	--	23	Dynamic	353452	555
123.123.123.123	--	65535	Dynamic	4294967295	15151
201.55.7.45	--	10	Manual	15000	222

Slot 2:

IP address	VPN instance	Port	Type	Requested	Trusted
192.168.11.5	--	23	Dynamic	46790	78578
201.55.7.45	--	10	Dynamic	2368	7237
123.123.123.123	--	65535	Manual	24587	1385

显示所有 IPv4 类型 TCP 客户端验证的受保护 IP 表项的个数。

```
<Sysname> display client-verify tcp protected ip count
```

Slot 1:

Totally 3 protected IP addresses.

Slot 2:

Totally 0 protected IP addresses.

表1-16 display client-verify protected ip 命令显示信息描述表

字段	描述
Totally 3 protected IP addresses.	IPv4类型受保护IP表项数目
IP address	受保护IPv4地址
VPN instance	受保护IP地址所属的MPLS L3VPN实例名称，属于公网时显示为“--”
Port	TCP连接的目的端口 any表示对该IP地址的所有端口的TCP连接请求都做代理
Type	受保护IP地址的添加方式，取值包括Dynamic和Manual
Requested	收到的匹配该受保护IP地址的报文数目
Trusted	通过验证的TCP连接请求报文数目

【相关命令】

- client-verify protected ip

1.1.44 display client-verify protected ipv6

display client-verify protected ipv6 命令用来显示客户端验证的 IPv6 类型的受保护 IP 表项。

【命令】

```
display client-verify { dns | dns-reply | http | sip | tcp } protected ipv6  
[ ipv6-address [ vpn vpn-instance-name ] ] [ port port-number ] [ slot  
slot-number ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

dns: 指定 DNS 客户端验证功能。

dns-reply: 指定 DNS reply 验证功能。

http: 指定 HTTP 客户端验证功能。

sip: 指定 SIP 客户端验证功能。

tcp: 指定 TCP 客户端验证功能。

ipv6-address: 显示指定 IPv6 地址的受保护 IP 表项。若未指定本参数，则显示所有 IPv6 类型的受保护 IP 表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的受保护 IP 表项。其中 **vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示显示公网中的受保护 IP 地址。

port port-number: 显示指定端口号的受保护 IP 表项，**port-number** 的取值范围为 1~65535。若未指定本参数，对于 DNS 客户端验证的受保护 IP，则表示端口 53；对于 HTTP 客户端验证的受保护 IP，则表示端口 80；对于 TCP 客户端验证的受保护 IP，则表示所有端口。

slot slot-number: 显示指定成员设备上的受保护 IP 表项，**slot-number** 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的受保护 IP 表项。

count: 显示符合指定条件的客户端验证受保护 IP 表项个数。

【举例】

显示所有 IPv6 类型的 TCP 客户端验证的受保护 IP 表项。

```
<Sysname> display client-verify tcp protected ipv6
```

```
Slot 1:
```

IPv6 address	VPN instance	Port	Type	Requested	Trusted
1:2:3:4:5:6:7:8	--	100	Manual	14478	5501
1023::1123	--	65535	Dynamic	4294967295	15151

```

Slot 2:
IPv6 address      VPN instance      Port  Type      Requested  Trusted
1:2:3:4:5:6:7:8   --                100   Manual    4568       8798
1023::1123        --                65535 Dynamic 15969       4679
# 显示所有 IPv6 类型的 TCP 客户端验证的受保护 IP 表项的个数。
<Sysname> display client-verify tcp protected ip count
Slot 1:
Totally 3 protected IPv6 addresses.
Slot 2:
Totally 0 protected IPv6 addresses.

```

表1-17 display client-verify protected ipv6 命令显示信息描述表

字段	描述
Totally 3 protected IPv6 addresses	IPv6类型受保护IP表项数目
IPv6 address	受保护IPv6地址
VPN instance	受保护IP地址所属的VPN实例名称，属于公网时显示为“--”
Port	TCP连接的目的端口 any表示对该IP地址的所有端口的TCP连接请求都做代理
Type	受保护IP地址的添加方式，取值包括Dynamic和Manual
Requested	收到的匹配该受保护IP地址的报文数目
Trusted	通过验证的TCP连接请求报文数目

【相关命令】

- **client-verify protected ipv6**

1.1.45 display client-verify trusted ip

display client-verify trusted ip 命令用来显示客户端验证的 IPv4 类型的信任 IP 表项。

【命令】

```

display client-verify { dns | dns-reply | http | sip | tcp } trusted ip
[ ip-address [ vpn vpn-instance-name ] ] [ slot slot-number ] [ count ]

```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

dns: 指定 DNS 客户端验证功能。

dns-reply: 指定 DNS reply 验证功能。

http: 指定 HTTP 客户端验证功能。

sip: 指定 SIP 客户端验证功能。

tcp: 指定 TCP 客户端验证功能。

ip-address: 显示指定 IPv4 地址的信任 IP 表项。若未指定本参数，则显示所有 IPv4 类型的信任 IP 表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的信任 IP 表项。其中 *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示信任 IP 表项位于公网。

slot slot-number: 显示指定成员设备上的信任 IP 表项，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的信任 IP 表项。

count: 仅显示符合指定条件的信任 IP 表项的个数。

【举例】

显示所有 IPv4 类型 DNS 客户端验证的信任 IP 表项。

```
<Sysname> display client-verify dns trusted ip
```

Slot 1:

IP address	VPN instance	DS-Lite tunnel peer	TTL(sec)
11.1.1.2	--	--	3600
123.123.123.123	--	--	3550

Slot 2:

IP address	VPN instance	DS-Lite tunnel peer	TTL(sec)
11.1.1.3	--	--	1200

显示所有 IPv4 类型 DNS 客户端验证的信任 IP 表项的个数。

```
<Sysname> display client-verify dns trusted ip count
```

Slot 1:

Totally 3 trusted IP addresses.

Slot 2:

Totally 0 trusted IP addresses.

表1-18 display client-verify trusted ip 命令显示信息描述表

字段	描述
Totally 3 trusted IP addresses	IPv4类型信任IP表项的个数
IP address	信任IPv4地址
VPN instance	信任IP地址所属的MPLS L3VPN实例名称，属于公网时显示为“--”
DS-Lite tunnel peer	（暂不支持）DS-Lite隧道对端地址。DS-Lite组网下，若本设备为AFTR，此列表示报文来自具体的哪个B4，如果不在DS-Lite组网或本设备不为AFTR，则该字段无意义，显示为“--”
TTL(sec)	信任IP地址的剩余老化时间，单位为秒。

1.1.46 display client-verify trusted ipv6

display client-verify trusted ipv6 命令用来显示客户端验证的 IPv6 类型的信任 IP 表项。

【命令】

display client-verify { dns | dns-reply | http | sip | tcp } trusted ipv6
[*ipv6-address* [*vpn vpn-instance-name*]] [*slot slot-number*]] [*count*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

dns: 指定 DNS 客户端验证功能。

dns-reply: 指定 DNS reply 验证功能。

http: 指定 HTTP 客户端验证功能。

sip: 指定 SIP 客户端验证功能。

tcp: 指定 TCP 客户端验证功能。

ipv6-address: 显示指定 IPv6 地址的信任 IP 表项。若未指定本参数，则显示所有 IPv6 类型的信任 IP 表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的信任 IP 表项。其中 *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示信任 IP 表项位于公网。

slot slot-number: 显示指定成员设备上的信任 IP 表项，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的信任 IP 表项。

count: 仅显示符合指定条件的信任 IP 地址的个数。

【举例】

显示所有 IPv6 类型的 DNS 客户端验证的信任 IP 表项。

```
<Sysname> display client-verify dns trusted ipv6
```

Slot 1:

IPv6 address	VPN instance	TTL(sec)
1::3	--	1643
1234::1234	--	1234

Slot 2:

IPv6 address	VPN instance	TTL(sec)
1::3	--	1643

显示所有 IPv6 类型的 DNS 客户端验证的信任 IP 表项的个数。

```
<Sysname> display client-verify dns trusted ipv6 count
```

Slot 1:
Totally 3 trusted IPv6 addresses.
Slot 2:
Totally 0 trusted IPv6 addresses.

表1-19 display client-verify trusted ipv6 命令显示信息描述表

字段	描述
Totally 3 trusted IPv6 addresses	IPv6类型信任IP表项的个数
IPv6 address	信任IPv6地址
VPN instance	VPN实例名称，属于公网时显示为“--”
TTL(sec)	信任IP地址的剩余老化时间，单位为秒。

1.1.47 display whitelist object-group

display whitelist object-group 命令用来显示白名单引用的地址对象组的报文统计信息。

【命令】

display whitelist object-group [*object-group-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

object-group-name: 显示白名单引用的地址对象组的报文统计信息，为 1～31 个字符的字符串，不区分大小写。如果不指定该参数，则表示显示白名单引用的所有地址对象组的报文统计信息。

slot slot-number: 显示指定成员设备上的白名单引用的地址对象组的报文统计信息，*slot-number* 表示设备在 IRF 中的成员编号。如果不指定该参数，则表示显示所有成员设备上的白名单引用的地址对象组的报文统计信息。

【使用指导】

若未指定任何参数，则表示显示白名单引用的所有地址对象组的报文统计信息。

【举例】

显示白名单引用的所有地址对象组的报文统计信息。

```
<Sysname> display whitelist object-group
```

Slot 1:

Object group	Type	Matching Packets
objgrp-1	IPv4	15696

```
objgrp-2                IPv4                855864455
Slot 2:
Object group            Type                Matching Packets
objgrp-1                IPv4                353452
```

表1-20 display whitelist object-group 命令显示信息描述表

字段	描述
Object group	白名单引用的地址对象组
Type	白名单引用的地址对象组类型
Matching packets	当前统计到的报文数量

【相关命令】

- **reset whitelist statistics**
- **whitelist object-group**

1.1.48 dns-flood action

dns-flood action 命令用来配置对 DNS flood 攻击防范的全局处理行为。

undo dns-flood action 命令用来恢复缺省情况。

【命令】

```
dns-flood action { client-verify | drop | logging } *
undo dns-flood action
```

【缺省情况】

不对检测到的 DNS flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

client-verify: 表示自动将受到攻击的 IP 地址添加到 DNS 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 DNS 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

本命令中 **client-verify** 参数的使用需要和 TCP 客户端验证功能配合。开启了 DNS 客户端验证的安全域检测到 DNS flood 攻击时，若本命令中指定了 **client-verify** 参数，则设备会将受攻击的 IP 地址动态添加到相应客户端验证的受保护 IP 列表中，并对与这些 IP 地址建立的连接进行代理。若安全域上未开启相应的代理功能，则不会对任何连接进行代理。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 DNS flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood action drop
```

【相关命令】

- **client-verify dns enable**
- **dns-flood detect**
- **dns-flood detect non-specific**
- **dns-flood threshold**

1.1.49 dns-flood detect

dns-flood detect 命令用来开启对指定 IP 地址的攻击防范检测，并配置 DNS flood 攻击防范检测的触发阈值和对 DNS flood 攻击的处理行为。

undo dns-flood detect 命令用来关闭对指定 IP 地址的 DNS flood 攻击防范检测。

【命令】

```
dns-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance
vpn-instance-name ] [ port port-list ] [ threshold threshold-value ] [ action
{ { client-verify | drop | logging } * | none } ]
undo dns-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 DNS flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip ipv4-address: 指定要保护的 IPv4 地址。该 IPv4 地址不能为 255.255.255.255 或 0.0.0.0。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。该 IPv6 地址不能为组播地址或::。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

port *port-list*: 指定开启 DNS flood 攻击防范检测的端口列表，表示方式为 { *start-port-number* [*to end-port-number*] } &<1-24>。&<1-24>表示前面的参数最多可以输入 24 次。*end-port-number* 必须大于或等于 *start-port-number*。若未指定本参数，则表示使用全局配置的检测端口列表。

threshold *threshold-value*: 指定 DNS flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 DNS 报文数目，取值范围为 1~1000000。

action: 设置对 DNS flood 攻击的处理行为。若未指定本参数，则表示采用 DNS flood 攻击防范的全局处理行为。

client-verify: 表示自动将受到攻击的 IP 地址添加到 DNS 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 DNS 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

使能 DNS flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 DNS 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 DNS flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

每个攻击防范策略下可以同时多个 IP 地址配置 DNS flood 攻击防范检测。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 192.168.1.2 的 DNS flood 攻击防范检测，并指定检测端口为 53、触发阈值为 2000。当设备监测到向该 IP 地址的 53 端口每秒发送的 DNS 报文数持续达到或超过 2000 时，启动 DNS flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood detect ip 192.168.1.2 port 53
threshold 2000
```

【相关命令】

- **dns-flood action**
- **dns-flood detect non-specific**

- **dns-flood port**
- **dns-flood threshold**

1.1.50 dns-flood detect non-specific

dns-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 DNS flood 攻击防范检测。

undo dns-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 DNS flood 攻击防范检测。

【命令】

```
dns-flood detect non-specific
undo dns-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 DNS flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

对所有非受保护 IP 地址开启 DNS flood 攻击防范检测后，设备将采用全局的阈值设置（由 **dns-flood threshold** 命令设置）和处理行为（由 **dns-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

```
# 在攻击防范策略 atk-policy-1 中，对所有非受保护 IP 地址开启 DNS flood 攻击防范检测。
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood detect non-specific
```

【相关命令】

- **dns-flood action**
- **dns-flood detect**
- **dns-flood threshold**

1.1.51 dns-flood port

dns-flood port 命令用来配置 DNS flood 攻击防范的全局检测端口号。

undo dns-flood port 命令用来恢复缺省情况。

【命令】

```
dns-flood port port-list
```

undo dns-flood port

【缺省情况】

DNS flood 攻击防范的全局检测端口号为 53。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

port-list: 指定开启 DNS flood 攻击防范检测的端口列表, 表示方式为{ *start-port-number* [*to end-port-number*] } &<1-32>。&<1-32>表示前面的参数最多可以输入 32 次。*end-port-number* 必须大于或等于 *start-port-number*。

【使用指导】

设备只对指定检测端口上收到的报文进行 DNS flood 攻击检测。

对于所有非受保护 IP 地址,或未指定检测端口的受保护 IP 地址,设备采用全局的检测端口进行 DNS flood 攻击检测。对于所有指定检测端口的受保护 IP 地址,设备针对为每个受保护 IP 地址指定的端口进行 DNS flood 攻击检测。

【举例】

在攻击防范策略 *atk-policy-1* 中配置 DNS flood 攻击防范的全局检测端口为 53 与 61000, 当设备检测到访问 53 端口或 61000 端口的 DNS flood 攻击时, 启动攻击防范措施。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] dns-flood port 53 61000
```

【相关命令】

- **dns-flood action**
- **dns-flood detect**
- **dns-flood detect non-specific**

1.1.52 dns-flood threshold

dns-flood threshold 命令用来配置 DNS flood 攻击防范的全局触发阈值。

undo dns-flood threshold 命令用来恢复缺省情况。

【命令】

dns-flood threshold *threshold-value*

undo dns-flood threshold

【缺省情况】

DNS flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 DNS 报文数目，取值范围为 1~1000000。

【使用指导】

使能 DNS flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 DNS 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 DNS flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

对于未专门配置 DNS flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（DNS 服务器）的 DNS 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 DNS flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 DNS 报文数持续达到或超过 100 时，启动攻击防范措施。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-flood threshold 100
```

【相关命令】

- **dns-flood action**
- **dns-flood detect ip**
- **dns-flood detect non-specific**

1.1.53 dns-reply-flood action

dns-reply-flood action 命令用来配置对 DNS reply flood 攻击防范的全局处理行为。

undo dns-reply-flood action 命令用来恢复缺省情况。

【命令】

```
dns-reply-flood action { client-verify | drop | logging } *
undo dns-reply-flood action
```

【缺省情况】

不对检测到的 DNS reply flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

client-verify: 表示自动将受到攻击的 IP 地址添加到 DNS reply 验证的受保护 IP 列表中。若 DNS reply 验证功能已使能，则对 DNS reply 源端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 DNS reply 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

本命令中 **client-verify** 参数的使用需要和 DNS reply 验证功能配合。开启了 DNS reply 验证的接口或安全域检测到 DNS reply flood 攻击时，若本命令中指定了 **client-verify** 参数，则设备会将受攻击的 IP 地址动态添加到相应 DNS reply 验证的受保护 IP 列表中，并对与这些 IP 地址建立的连接进行代理。若接口或安全域上未开启相应的代理功能，则不会对任何连接进行代理。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 DNS reply flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood action drop
```

【相关命令】

- **client-verify dns-reply enable**
- **dns-reply-flood detect**
- **dns-reply-flood detect non-specific**
- **dns-reply-flood threshold**

1.1.54 dns-reply-flood detect

dns-reply-flood detect 命令用来开启对指定 IP 地址的攻击防范检测，并配置 DNS reply flood 攻击防范检测的触发阈值和对 DNS reply flood 攻击的处理行为。

undo dns-reply-flood detect 命令用来关闭对指定 IP 地址的 DNS reply flood 攻击防范检测。

【命令】

```
dns-reply-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] [ port port-list ] [ threshold threshold-value ] [ action { { client-verify | drop | logging } * | none } ]  
undo dns-reply-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 DNS reply flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为 255.255.255.255 或 0.0.0.0。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

port *port-list*: 指定开启 DNS reply flood 攻击防范检测的端口列表，表示方式为 { *start-port-number* [**to** *end-port-number*] } &<1-24>。&<1-24>表示前面的参数最多可以输入 24 次。*end-port-number* 必须大于或等于 *start-port-number*。若未指定本参数，则表示使用全局配置的检测端口列表。

threshold *threshold-value*: 指定 DNS flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 DNS reply 报文数目，取值范围为 1~1000000，缺省为 1000。

action: 设置对 DNS reply flood 攻击的处理行为。

client-verify: 表示自动将受到攻击的 IP 地址添加到 DNS reply 源端验证的受保护 IP 列表中。若 DNS reply 验证功能已使能，则对 DNS reply 源端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 DNS reply 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

每个攻击防范策略下可以同时为多个 IP 地址配置 DNS reply flood 攻击防范检测。

开启 DNS reply flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 DNS reply 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 DNS reply flood 攻击，则

进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该 IP 地址发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **192.168.1.2** 的 **DNS reply flood** 攻击防范检测，并指定检测端口为 **53**、触发阈值为 **2000**。当设备监测到向该 IP 地址的 **53** 端口每秒发送的 **DNS reply** 报文数持续达到或超过 **2000** 时，启动 **DNS reply flood** 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood detect ip 192.168.1.2 port 53
threshold 2000
```

【相关命令】

- **dns-reply-flood action**
- **dns-reply-flood detect non-specific**
- **dns-reply-flood threshold**
- **dns-reply-flood port**

1.1.55 dns-reply-flood detect non-specific

dns-reply-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 **DNS reply flood** 攻击防范检测。

undo dns-reply-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 **DNS reply flood** 攻击防范检测。

【命令】

```
dns-reply-flood detect non-specific
undo dns-reply-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 **DNS reply-flood** 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```


【使用指导】

对所有非受保护 IP 地址开启 DNS reply flood 攻击防范检测后，设备将采用全局的阈值设置（由 **dns-reply-flood threshold** 命令设置）和处理行为（由 **dns-reply-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 DNS reply-flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood detect non-specific
```

【相关命令】

- **dns-reply-flood action**
- **dns-reply-flood detect**
- **dns-reply-flood threshold**

1.1.56 dns-reply-flood port

dns-reply-flood port 命令用来配置 DNS reply flood 攻击防范的全局检测端口号。

undo dns-reply-flood port 命令用来恢复缺省情况。

【命令】

```
dns-reply-flood port port-list
undo dns-reply-flood port
```

【缺省情况】

DNS reply-flood 攻击防范的全局检测端口号为 53。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

port-list：指定开启 DNS reply flood 攻击防范检测的端口列表，表示方式为 { *start-port-number* [**to** *end-port-number*] } &<1-32>。&<1-32>表示前面的参数最多可以输入 32 次。*end-port-number* 必须大于或等于 *start-port-number*。

【使用指导】

设备只对指定检测端口上收到的报文进行 DNS reply flood 攻击检测。

对于所有非受保护 IP 地址，或未指定检测端口的受保护 IP 地址，设备采用全局的检测端口进行 DNS reply flood 攻击检测。对于所有指定检测端口的受保护 IP 地址，设备针对为每个受保护 IP 地址指定的端口进行 DNS reply flood 攻击检测。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 DNS reply flood 攻击防范的全局检测端口为 53 与 61000，当设备检测到访问 53 端口或 61000 端口的 DNS flood 攻击时，启动攻击防范措施。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood port 53 61000
```

【相关命令】

- **dns-reply-flood action**
- **dns-reply-flood detect**
- **dns-reply-flood detect non-specific**

1.1.57 dns-reply-flood threshold

dns-reply-flood threshold 命令用来配置 DNS reply flood 攻击防范的全局触发阈值。

undo dns-reply-flood threshold 命令用来恢复缺省情况。

【命令】

```
dns-reply-flood threshold threshold-value
undo dns-reply-flood threshold
```

【缺省情况】

DNS reply flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 DNS reply 报文数目，取值范围为 1~1000000。

【使用指导】

开启 DNS reply flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 DNS reply 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 DNS reply flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。

对于未专门配置 DNS reply flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（DNS 客户端）的 DNS reply 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 DNS reply flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 DNS reply 报文数持续达到或超过 100 时，启动攻击防范措施。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] dns-reply-flood threshold 100
```

【相关命令】

- **dns-reply-flood action**
- **dns-reply-flood detect ip**
- **dns-reply-flood detect non-specific**

1.1.58 exempt acl

exempt acl 命令用来配置攻击防范例外列表。

undo exempt acl 命令用来恢复缺省情况。

【命令】

```
exempt acl [ ipv6 ] { acl-number | name acl-name }
undo exempt acl [ ipv6 ]
```

【缺省情况】

未配置攻击防范例外列表。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ipv6: 指定 IPv6 ACL。如果未指定本参数，则表示 IPv4 ACL。

acl-number: 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999: 表示基本 ACL。
- 3000～3999: 表示高级 ACL。

name acl-name: 指定 ACL 的名称。**acl-name** 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

【使用指导】

通过配置例外列表，使用 ACL 过滤不需要进行攻击防范检测的主机报文。当安全域上收到的报文与攻击防范例外列表引用的 ACL 中的 permit 规则匹配时，设备不对其进行攻击防范检测。该配置用于过滤某些被信任的安全主机发送的报文，可以有效的减小误报率，并提高服务器处理效率。

例外列表引用的 ACL 的 permit 规则中仅源地址、目的地址、源端口、目的端口、协议号、L3VPN 和非首片分片标记参数用于匹配报文。

如果配置的攻击防范例外列表中引用的 ACL 不存在，或引用的 ACL 中未定义任何规则，例外列表不会生效。

【举例】

在攻击防范策略 **atk-policy-1** 中配置例外列表 **ACL 2001**，过滤来自主机 **1.1.1.1** 的报文，不对其进行攻击防范检测。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] attack-defense policy atk-policy-1
[attack-defense-policy-atk-policy-1] exempt acl 2001
```

【相关命令】

- **attack-defense policy**

1.1.59 fin-flood action

fin-flood action 命令用来配置对 **FIN flood** 攻击防范的全局处理行为。

undo fin-flood action 命令用来恢复缺省情况。

【命令】

```
fin-flood action { client-verify | drop | logging } *
undo fin-flood action
```

【缺省情况】

不对检测到的 **FIN flood** 攻击采取任何处理行为。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

client-verify: 表示自动将受到攻击的 IP 地址添加到 TCP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 **FIN** 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

本命令中 **client-verify** 参数的使用需要和 TCP 客户端验证功能配合。开启了 TCP 客户端验证的安全域检测到 **ACK flood** 攻击时，若本命令中指定了 **client-verify** 参数，则设备会将受攻击的 IP 地址动态添加到相应客户端验证的受保护 IP 列表中，并对与这些 IP 地址建立的连接进行代理。若安全域上未开启相应的代理功能，则不会对任何连接进行代理。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

#在攻击防范策略 **atk-policy-1** 配置对 **FIN flood** 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] fin-flood action drop
```

【相关命令】

- **client-verify tcp enable**
- **fin-flood detect**
- **fin-flood detect non-specific**
- **fin-flood threshold**

1.1.60 fin-flood detect

fin-flood detect 命令用来开启对指定 IP 地址的 **FIN flood** 攻击防范检测，并配置 **FIN flood** 攻击防范检测的触发阈值和对 **FIN flood** 攻击的处理行为。

undo fin-flood detect 命令用来关闭对指定 IP 地址的 **FIN flood** 攻击防范检测。

【命令】

```
fin-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] [ threshold threshold-value ] [ action { { client-verify | drop | logging } * | none } ]
```

```
undo fin-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 **FIN flood** 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为 255.255.255.255 或 0.0.0.0。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。该 IPv6 地址不能为组播地址或::。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold *threshold-value*: 指定攻击防范的触发阈值。其中, *threshold-value* 为向指定 IP 地址每秒发送的 FIN 报文数目, 取值范围为 1~1000000。

action: 设置对 FIN flood 攻击的处理行为。若未指定本参数, 则表示采用 FIN flood 攻击防范的全局处理行为。

client-verify: 表示自动将受到攻击的 IP 地址添加到 TCP 客户端验证的受保护 IP 列表中。若客户端验证功能使能, 则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文, 即设备检测到攻击发生后, 向被攻击者发送的后续所有 FIN 报文都会被丢弃。

logging: 表示输出告警日志, 即设备检测到攻击发生时, 生成告警信息, 生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

使能 FIN flood 攻击防范后, 设备处于攻击检测状态, 当它监测到向指定 IP 地址发送 FIN 报文的速率持续达到或超过了触发阈值时, 即认为该 IP 地址受到了 FIN flood 攻击, 则进入攻击防范状态, 并根据配置启动相应的防范措施。此后, 当设备检测到向该服务器发送报文的速率低于恢复阈值(触发阈值的 3/4) 时, 即认为攻击结束, 则由攻击防范状态恢复为攻击检测状态, 并停止执行防范措施。

每个攻击防范策略下可以同时多个 IP 地址配置 FIN flood 攻击防范检测。

输出告警日志功能开启后, 设备生成的告警日志信息不会输出到控制台和监视终端, 可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍, 请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 192.168.1.2 的 FIN flood 攻击防范检测, 并指定触发阈值为 2000。当设备监测到向该 IP 地址每秒发送的 FIN 报文数持续达到或超过 2000 时, 启动 FIN flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] fin-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **fin-flood action**
- **fin-flood detect non-specific**
- **fin-flood threshold**

1.1.61 fin-flood detect non-specific

fin-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 FIN flood 攻击防范检测。

undo fin-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 FIN flood 攻击防范检测。

【命令】

```
fin-flood detect non-specific  
undo fin-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 FIN flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

无

【使用指导】

对所有非受保护 IP 地址开启 FIN flood 攻击防范检测后，设备将采用全局的阈值设置（由 **fin-flood threshold** 命令设置）和处理行为（由 **fin-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 FIN flood 攻击防范检测。

```
<Sysname> system-view  
[Sysname] attack-defense policy atk-policy-1  
[Sysname-attack-defense-policy-atk-policy-1] fin-flood detect non-specific
```

【相关命令】

- **fin-flood action**
- **fin-flood detect**
- **fin-flood threshold**

1.1.62 fin-flood threshold

fin-flood threshold 命令用来配置 FIN flood 攻击防范的全局触发阈值。

undo fin-flood threshold 命令用来恢复缺省情况。

【命令】

```
fin-flood threshold threshold-value  
undo fin-flood threshold
```

【缺省情况】

FIN flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 FIN 报文数目，取值范围为 1~1000000。

【使用指导】

使能 FIN flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 FIN 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 FIN flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

对于未专门配置 FIN flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（HTTP 服务器或者 FTP 服务器）的 FIN 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 FIN flood 攻击防范检测的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 FIN 报文数持续达到或超过 100 时，启动 FIN flood 攻击防范。

```
<Sysname> system-view  
[Sysname] attack-defense policy atk-policy-1  
[Sysname-attack-defense-policy-atk-policy-1] fin-flood threshold 100
```

【相关命令】

- **fin-flood action**
- **fin-flood detect**
- **fin-flood detect non-specific**

1.1.63 http-flood action

http-flood action 命令用来配置对 HTTP flood 攻击防范的全局处理行为。

undo http-flood action 命令用来恢复缺省情况。

【命令】

```
http-flood action { client-verify | drop | logging } *  
undo http-flood action
```

【缺省情况】

不对检测到的 HTTP flood 攻击采取任何处理行为。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

client-verify: 表示自动将受到攻击的 IP 地址添加到 HTTP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 HTTP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

本命令中 **client-verify** 参数的使用需要和 HTTP 客户端验证功能配合。开启了 HTTP 客户端验证的安全域检测到 HTTP flood 攻击时，若本命令中指定了 **client-verify** 参数，则设备会将受攻击的 IP 地址动态添加到相应客户端验证的受保护 IP 列表中，并对与这些 IP 地址建立的连接进行代理。若安全域上未开启相应的代理功能，则不会对任何连接进行代理。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 HTTP flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view  
[Sysname] attack-defense policy atk-policy-1  
[Sysname-attack-defense-policy-atk-policy-1] http-flood action drop
```

【相关命令】

- **client-verify http enable**
- **http-flood detect non-specific**
- **http-flood detect**
- **http-flood threshold**

1.1.64 http-flood detect

http-flood detect 命令用来开启对指定 IP 地址的 HTTP flood 攻击防范检测，并配置 HTTP flood 攻击防范的触发阈值和对 HTTP flood 攻击的处理行为。

undo http-flood detect 命令用来关闭对指定 IP 地址的 HTTP flood 攻击防范检测。

【命令】

```
http-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ] [ port port-list ] [ threshold threshold-value ] [ action  
{ { client-verify | drop | logging } * | none } ]
```

```
undo http-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 HTTP flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip ipv4-address: 指定要保护的 IPv4 地址。该 IPv4 地址不能为 255.255.255.255 或 0.0.0.0。

ipv6 ipv6-address: 指定要保护的 IPv6 地址。该 IPv6 地址不能为组播地址或::。

vpn-instance vpn-instance-name: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

port port-list: 指定开启 HTTP flood 攻击防范检测的端口列表，表示方式为 { *start-port-number* [*to end-port-number*] } &<1-24>。&<1-24>表示前面的参数最多可以输入 24 次。*end-port-number* 必须大于或等于 *start-port-number*。若未指定本参数，则表示使用全局配置的检测端口列表。

threshold threshold-value: 指定攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 HTTP 报文数目，取值范围为 1~1000000。

action: 设置对 HTTP flood 攻击的处理行为。若未指定本参数，则表示采用 HTTP flood 攻击防范的全局处理行为。

client-verify: 表示自动将受到攻击的 IP 地址添加到 HTTP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 HTTP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

使能 HTTP flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 HTTP 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 HTTP flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

每个攻击防范策略下可以同时为多个 IP 地址配置 HTTP flood 攻击防范检测。

告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **192.168.1.2** 的 HTTP flood 攻击防范检测，并指定检测端口为 **80** 与 **8080**、触发阈值为 **2000**。当设备监测到向该 IP 地址的 **80** 或 **8080** 端口每秒发送的 HTTP 报文数持续达到或超过 **2000** 时，启动 HTTP flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood detect ip 192.168.1.2 port 80 8080
threshold 2000
```

【相关命令】

- **http-flood action**
- **http-flood detect non-specific**
- **http-flood port**
- **http-flood threshold**

1.1.65 http-flood detect non-specific

http-flood detect non-specific 命令用来对所有非受保护 IPv4 地址开启 HTTP flood 攻击防范检测。

undo http-flood detect non-specific 命令用来关闭对所有非受保护 IPv4 地址的 HTTP flood 攻击防范检测。

【命令】

```
http-flood detect non-specific
undo http-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 HTTP flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

对所有非受保护 IP 地址开启 HTTP flood 攻击防范检测后，设备将采用全局的阈值设置（由 **http-flood threshold** 命令设置）和处理行为（由 **http-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 HTTP flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood detect non-specific
```

【相关命令】

- **http-flood action**
- **http-flood detect**
- **http-flood threshold**

1.1.66 http-flood port

http-flood port 命令用来配置 HTTP flood 攻击防范的全局检测端口号。

undo http-flood port 命令用来恢复缺省情况。

【命令】

```
http-flood port port-list
undo http-flood port
```

【缺省情况】

HTTP flood 攻击防范的全局检测端口号为 80。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

port-list: 指定开启 HTTP flood 攻击防范检测的端口列表, 表示方式为{ *start-port-number* [*to end-port-number*] } &<1-32>。&<1-32>表示前面的参数最多可以输入 32 次。*end-port-number* 必须大于或等于 *start-port-number*。

【使用指导】

设备只对指定检测端口上收到的报文进行 HTTP flood 攻击检测。

对于所有非受保护 IP 地址, 或未指定检测端口的受保护 IP 地址, 设备采用全局的检测端口进行 HTTP flood 攻击检测。对于所有指定检测端口的受保护 IP 地址, 设备针对为每个受保护 IP 地址指定的端口进行 HTTP flood 攻击检测。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 DNS flood 攻击防范的全局检测端口为 80 与 8080, 当设备检测到访问 80 端口或 8080 端口的 HTTP flood 攻击时, 启动攻击防范措施。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] http-flood port 80 8080
```

【相关命令】

- **http-flood action**
- **http-flood detect**
- **http-flood detect non-specific**

1.1.67 http-flood threshold

http-flood threshold 命令用来配置 HTTP flood 攻击防范的全局触发阈值。

undo http-flood threshold 命令用来恢复缺省情况。

【命令】

http-flood threshold *threshold-value*

undo http-flood threshold

【缺省情况】

HTTP flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 HTTP 报文数目，取值范围为 1~1000000。

【使用指导】

使能 HTTP flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 HTTP 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 HTTP flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

对于未专门配置 HTTP flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（HTTP 服务器）的 HTTP 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 HTTP flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 HTTP 报文数持续达到或超过 100 时，启动 HTTP flood 攻击防范。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] http-flood threshold 100
```

【相关命令】

- **http-flood action**
- **http-flood detect**
- **http-flood detect non-specific**

1.1.68 icmp-flood action

icmp-flood action 命令用来配置对 ICMP flood 攻击防范的全局处理行为。

undo icmp-flood action 命令用来恢复缺省情况。

【命令】

```
icmp-flood action { drop | logging } *  
undo icmp-flood action
```

【缺省情况】

不对检测到的 ICMP flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ICMP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 atk-policy-1 中配置对 ICMP flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view  
[Sysname] attack-defense policy atk-policy-1  
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood action drop
```

【相关命令】

- **icmp-flood detect non-specific**
- **icmp-flood detect ip**
- **icmp-flood threshold**

1.1.69 icmp-flood detect ip

icmp-flood detect ip 命令用来开启对指定 IP 地址的 ICMP flood 攻击防范检测，并配置 ICMP flood 攻击防范检测的触发阈值和对 ICMP flood 攻击的处理行为。

undo icmp-flood detect ip 命令用来关闭对指定 IP 地址的 ICMP flood 攻击防范检测。

【命令】

```
icmp-flood detect ip ip-address [ vpn-instance vpn-instance-name ]  
[ threshold threshold-value ] [ action { { drop | logging } * | none } ]  
undo icmp-flood detect ip ip-address [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 ICMP flood 攻击防范触发阈值。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip ip-address: 指定要保护的 IP 地址。该 IP 地址不能为 255.255.255.255 或 0.0.0.0。

vpn-instance vpn-instance-name: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold threshold-value: 指定攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 ICMP 报文数目，取值范围为 1~1000000。

action: 设置对 ICMP flood 攻击的处理行为。若未指定本参数，则表示采用 ICMP flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ICMP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

使能 ICMP flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 ICMP 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 ICMP flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

每个攻击防范策略下可以同时多个 IP 地址配置 ICMP flood 攻击防范检测。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **192.168.1.2** 的 **ICMP flood** 攻击防范检测，并指定触发阈值为 **2000**。当设备监测到向该 IP 地址每秒发送的 **ICMP** 报文数持续达到或超过 **2000** 时，启动 **ICMP flood** 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **icmp-flood action**
- **icmp-flood threshold**
- **icmp-flood detect non-specific**

1.1.70 icmp-flood detect non-specific

icmp-flood detect non-specific 命令用来对所有非受保护 IPv4 地址开启 **ICMP flood** 攻击防范检测。

undo icmp-flood detect non-specific 命令用来关闭对所有非受保护 IPv4 地址的 **ICMP flood** 攻击防范检测。

【命令】

```
icmp-flood detect non-specific
undo icmp-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IPv4 地址开启 **ICMP flood** 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

对任何非受保护 IPv4 地址开启 **ICMP flood** 攻击防范检测后，设备将采用全局的阈值设置（由 **icmp-flood threshold** 命令设置）和处理行为（由 **icmp-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IPv4 地址开启 **ICMP flood** 攻击防范检测。

```
<Sysname> system-view
```



```
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood detect non-specific
```

【相关命令】

- **icmp-flood action**
- **icmp-flood detect ip**
- **icmp-flood threshold**

1.1.71 icmp-flood threshold

icmp-flood threshold 命令用来配置 ICMP flood 攻击防范的全局触发阈值。

undo icmp-flood threshold 命令用来恢复缺省情况。

【命令】

```
icmp-flood threshold threshold-value
undo icmp-flood threshold
```

【缺省情况】

ICMP flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 ICMP 报文数目，取值范围为 1~1000000。

【使用指导】

使能 ICMP flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 ICMP 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 ICMP flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

对于未专门配置 ICMP flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（HTTP 服务器或者 FTP 服务器）的 ICMP 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 atk-policy-1 中配置 ICMP flood 攻击防范检测的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 ICMP 报文数持续达到或超过 100 时，启动 ICMP flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmp-flood threshold 100
```

【相关命令】

- **icmp-flood action**
- **icmp-flood detect**
- **icmp-flood detect non-specific**

1.1.72 icmpv6-flood action

icmpv6-flood action 命令用来配置对 ICMPv6 flood 攻击防范的全局处理行为。

undo icmpv6-flood action 命令用来恢复缺省情况。

【命令】

```
icmpv6-flood action { drop | logging } *  
undo icmpv6-flood action
```

【缺省情况】

不对检测到的 ICMPv6 flood 攻击采取任何防范措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ICMPv6 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 atk-policy-1 中配置对 ICMPv6 flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view  
[Sysname] attack-defense policy atk-policy-1  
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood action drop
```

【相关命令】

- **icmpv6-flood detect ipv6**
- **icmpv6-flood detect non-specific**
- **icmpv6-flood threshold**

1.1.73 icmpv6-flood detect ipv6

icmpv6-flood detect ipv6 命令用来开启对指定 IPv6 地址的 ICMPv6 flood 攻击防范检测，并配置 ICMPv6 flood 攻击防范检测的触发阈值和对 ICMPv6 flood 攻击的处理行为。

undo icmpv6-flood detect ipv6 命令用来关闭对指定 IPv6 地址的 ICMPv6 flood 攻击防范检测。

【命令】

```
icmpv6-flood detect ipv6 ipv6-address [ vpn-instance vpn-instance-name ]  
[ threshold threshold-value ] [ action { { drop | logging } * | none } ]  
undo icmpv6-flood detect ipv6 ipv6-address [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IPv6 地址配置 ICMPv6 flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address: 指定要保护的 IPv6 地址。该 IPv6 地址不能为组播地址或::。

vpn-instance vpn-instance-name: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold threshold-value: 指定攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 ICMPv6 报文数目，取值范围为 1~1000000。

action: 设置对 ICMPv6 flood 攻击的处理行为。若未指定本参数，则表示采用 ICMPv6 flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 ICMPv6 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

使能 ICMPv6 flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 ICMPv6 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 ICMPv6 flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

每个攻击防范策略下可以同时多个 IPv6 地址配置 ICMPv6 flood 攻击防范检测。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **2012::12** 的 ICMPv6 flood 攻击防范检测，并指定触发阈值为 **2000**。当设备监测到向该 IP 地址每秒发送的 ICMP 报文数持续达到或超过 **2000** 时，启动 ICMPv6 flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood detect ipv6 2012::12 threshold 2000
```

【相关命令】

- **icmpv6-flood action**
- **icmpv6-flood detect non-specific**
- **icmpv6-flood threshold**

1.1.74 icmpv6-flood detect non-specific

icmpv6-flood detect non-specific 命令用来对所有非受保护 IPv6 地址开启 ICMPv6 flood 攻击防范检测。

undo icmpv6-flood detect non-specific 命令用来关闭对所有非受保护 IPv6 地址的 ICMPv6 flood 攻击防范检测。

【命令】

```
icmpv6-flood detect non-specific
undo icmpv6-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IPv6 地址开启 ICMPv6 flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

对所有非受保护 IPv6 地址开启 ICMPv6 flood 攻击防范检测后，设备将采用全局的阈值设置（由 **icmpv6-flood threshold** 命令设置）和处理行为（由 **icmpv6-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IPv6 地址开启 ICMPv6 flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood detect non-specific
```

【相关命令】

- **icmpv6-flood action**
- **icmpv6-flood detect ipv6**
- **icmpv6-flood threshold**

1.1.75 icmpv6-flood threshold

icmpv6-flood threshold 命令用来配置 ICMPv6 flood 攻击防范的全局触发阈值。

undo icmpv6-flood threshold 命令用来恢复缺省情况。

【命令】

```
icmpv6-flood threshold threshold-value
undo icmpv6-flood threshold
```

【缺省情况】

ICMPv6 flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 ICMPv6 报文数目，取值范围为 1~1000000。

【使用指导】

使能 ICMPv6 flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 ICMPv6 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 ICMPv6 flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

对于未专门配置 ICMPv6 flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（HTTP 服务器或者 FTP 服务器）的 ICMPv6 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 atk-policy-1 中配置 ICMPv6 flood 攻击防范检测的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 ICMPv6 报文数持续达到或超过 100 时，启动 ICMPv6 flood 攻击防范。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] icmpv6-flood threshold 100
```

【相关命令】

- **icmpv6-flood action**
- **icmpv6-flood detect**
- **icmpv6-flood detect non-specific**

1.1.76 reset attack-defense policy flood

reset attack-defense policy flood 命令用来清除 flood 攻击防范受保护 IP 表项的统计信息。

【命令】

```
reset attack-defense policy policy-name flood protected { ip | ipv6 }  
statistics
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 攻击防范策略名称，为 1~31 个字符的字符串，不区分大小写。合法取值包括大写字母、小写字母、数字、特殊字符“_”和“-”。

ip: 指定 IPv4 类型的 flood 受保护 IP 表项。

ipv6: 指定 IPv6 类型的 flood 受保护 IP 表项。

statistics: 清除指定类型的 flood 受保护 IP 表项的统计信息。

【举例】

```
# 清除攻击防范策略 abc 中所有 IPv4 类型的 flood 保护 IP 表项的统计信息
<Sysname> reset attack-defense policy abc flood protected ip statistics
# 清除攻击防范策略 abc 中所有 IPv6 类型的 flood 保护 IP 表项的统计信息
<Sysname> reset attack-defense policy abc flood protected ipv6 statistics
```

【相关命令】

- **display attack-defense policy ip**
- **display attack-defense policy ipv6**

1.1.77 reset attack-defense statistics security-zone

reset attack-defense statistics security-zone 命令用来清除安全域上的攻击防范的统计信息。

【命令】

reset attack-defense statistics security-zone zone-name

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

zone-name: 指定安全域的名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

【举例】

清除安全域 DMZ 上所有攻击防范的统计信息。

<Sysname> reset attack-defense statistics security-zone dmz

【相关命令】

- **display attack-defense policy**

1.1.78 reset attack-defense top-attack-statistics

reset attack-defense top-attack-statistics 命令用来清除 Top10 的攻击排名统计信息。

【命令】

reset attack-defense top-attack-statistics

【视图】

用户视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

清除 Top10 的攻击排名统计信息。

<Sysname> reset attack-defense top-attack-statistics

【相关命令】

- **attack-defense top-attack-statistics enable**
- **display attack-defense top-attack-statistics**

1.1.79 reset blacklist destination-ip

reset blacklist destination-ip 命令用来清除目的 IPv4 动态黑名单表项。

【命令】

```
reset blacklist destination-ip { destination-ip-address [ vpn-instance  
vpn-instance-name ] | all }
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

destination-ip-address: 清除指定 IPv4 地址的目的 IPv4 动态黑名单表项。其中 **destination-ip-address** 表示黑名单表项的 IPv4 地址。

vpn-instance vpn-instance-name: 清除指定 VPN 实例的目的 IPv4 动态黑名单表项。其中 **vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示清除公网中的目的 IPv4 动态黑名单表项。

all: 表示清除所有目的 IPv4 动态的黑名单表项。

【使用指导】

该命令仅用来清除动态生成的目的 IPv4 的黑名单表项。用户添加的目的 IPv4 黑名单表项需要通过 **undo blacklist destination-ip** 命令来删除。

【举例】

```
# 清除所有目的 IPv4 动态黑名单表项的信息。  
<Sysname> reset blacklist destination-ip all
```

【相关命令】

- **display blacklist destination-ip**

1.1.80 reset blacklist destination-ipv6

reset blacklist destination-ipv6 命令用来清除目的 IPv6 动态黑名单表项。

【命令】

```
reset blacklist destination-ipv6 { destination-ipv6-address [ vpn-instance  
vpn-instance-name ] | all }
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

destination-ipv6-address : 清除指定 IPv6 地址的目的 IPv6 动态黑名单表项。其中 **destination-ipv6-address** 表示黑名单表项的 IPv6 地址。

vpn-instance vpn-instance-name: 清除指定 VPN 实例的目的 IPv6 动态黑名单表项。其中 **vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示清除公网中的指定目的 IPv6 动态黑名单表项。

all: 表示清除所有目的 IPv6 动态黑名单表项。

【使用指导】

该命令仅用来清除动态生成的目的 IPv6 黑名单表项。用户添加的目的 IPv6 黑名单表项需要通过 **undo blacklist destination-ipv6** 命令来删除。

【举例】

```
# 清除所有目的 IPv6 动态黑名单表项的信息。  
<Sysname> reset blacklist destination-ipv6 all
```

【相关命令】

- **display blacklist ipv6**

1.1.81 reset blacklist ip

reset blacklist ip 命令用来清除 IPv4 动态黑名单表项。

【命令】

```
reset blacklist ip { source-ip-address [ vpn-instance vpn-instance-name ] |  
all }
```

【视图】

用户视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

source-ip-address: 清除指定 IPv4 地址的动态黑名单表项。其中 **source-ip-address** 表示黑名单表项的 IPv4 地址。

vpn-instance vpn-instance-name: 清除指定 VPN 实例的动态黑名单表项。其中 **vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示清除公网中的指定动态黑名单表项。

all: 表示清除所有动态 IPv4 的黑名单表项。

【使用指导】

该命令仅用来清除动态生成的 IPv4 的黑名单表项。用户添加的黑名单表项需要通过 **undo blacklist ip** 命令来删除。

【举例】

```
# 清除所有 IPv4 动态黑名单表项的信息。  
<Sysname> reset blacklist ip all
```

【相关命令】

- **display blacklist ip**

1.1.82 reset blacklist ipv6

reset blacklist ipv6 命令用来清除 IPv6 动态黑名单表项。

【命令】

```
reset blacklist ipv6 { source-ipv6-address [ vpn-instance vpn-instance-name ]  
| all }
```

【视图】

用户视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

source-ipv6-address: 清除指定 IPv6 地址的动态黑名单表项。其中 *source-ip-address* 表示黑名单表项的 IPv6 地址。

vpn-instance vpn-instance-name: 清除指定 VPN 实例的动态黑名单表项。其中 *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示清除公网中的指定动态黑名单表项。

all: 表示清除所有动态 IPv6 的黑名单表项。

【使用指导】

该命令仅用来清除动态生成的 IPv6 的黑名单表项。用户添加的黑名单表项需要通过 **undo blacklist ipv6** 命令来删除。

【举例】

```
# 清除所有 IPv6 动态黑名单表项的信息。  
<Sysname> reset blacklist ipv6 all
```

【相关命令】

- **display blacklist ipv6**

1.1.83 reset blacklist statistics

reset blacklist statistics 命令用来清除黑名单表项的统计信息。

【命令】

```
reset blacklist statistics
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

执行本命令后，将清空所有黑名单表项的丢包统计信息。

【举例】

清除所有黑名单表项的丢包统计信息。

```
<Sysname> reset blacklist statistics
```

【相关命令】

- **display blacklist ip**
- **display blacklist ipv6**

1.1.84 reset client-verify protected statistics

reset client-verify protected statistics 命令用来清除客户端验证的受保护 IP 地址的统计信息。

【命令】

```
reset client-verify { dns | dns-reply | http | sip | tcp } protected { ip | ipv6 } statistics
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

dns: 指定 DNS 客户端验证功能。

dns-reply: 指定 DNS reply 验证功能。

http: 指定 HTTP 客户端验证功能。

sip: 指定 SIP 客户端验证功能。

tcp: 指定 TCP 客户端验证功能。

ip: 清除所有 IPv4 类型客户端验证的受保护 IP 地址的统计信息。

ipv6: 清除所有 IPv6 类型客户端验证的受保护 IP 地址的统计信息。

【举例】

清除 TCP 客户端验证的受保护 IP 地址的统计信息。

```
<Sysname> reset client-verify tcp protected ip statistics
```

【相关命令】

- **display client-verify protected ip**
- **display client-verify protected ipv6**

1.1.85 reset client-verify trusted

reset client-verify trusted 命令用来清除客户端验证的信任 IP 表项。

【命令】

reset client-verify { dns | dns-reply | http | sip | tcp } trusted { ip | ipv6 }

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

dns: 指定 DNS 客户端验证功能。

dns-reply: 指定 DNS reply 验证功能。

http: 指定 HTTP 客户端验证功能。

sip: 指定 SIP 客户端验证功能。

tcp: 指定 TCP 客户端验证功能。

ip: 清除所有 IPv4 类型客户端验证的信任 IP 表项。

ipv6: 清除所有 IPv6 类型客户端验证的信任 IP 表项。

【举例】

清除所有 IPv4 类型 DNS 客户端验证的信任 IP 表项。

```
<Sysname> reset client-verify dns trusted ip
```

【相关命令】

- **display client-verify trusted ip**
- **display client-verify trusted ipv6**

1.1.86 reset whitelist statistics

reset whitelist statistics 命令用来清除白名单引用的地址对象组的报文统计信息。

【命令】

reset whitelist statistics

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

执行本命令后，将清空白名单引用的所有地址对象组的报文统计信息。

【举例】

```
# 清除白名单引用的地址对象组的报文统计信息。  
<Sysname> reset whitelist statistics
```

【相关命令】

- **display whitelist object-group**

1.1.87 rst-flood action

rst-flood action 命令用来配置对 RST flood 攻击防范的全局处理行为。

undo rst-flood action 命令用来恢复缺省情况。

【命令】

```
rst-flood action { client-verify | drop | logging } *  
undo rst-flood action
```

【缺省情况】

不对检测到的 RST flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

client-verify: 表示自动将受到攻击的 IP 地址添加到 TCP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 RST 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

本命令中 **client-verify** 参数的使用需要和 TCP 客户端验证功能配合。使能了 TCP 客户端验证的安全域检测到 ACK flood 攻击时，若本命令中指定了 **client-verify** 参数，则设备会将受攻击的 IP 地址动态添加到相应客户端验证的受保护 IP 列表中，并对与这些 IP 地址建立的连接进行代理。若安全域上未使能相应的代理功能，则不会对任何连接进行代理。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 **RST flood** 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] rst-flood action drop
```

【相关命令】

- **client-verify tcp enable**
- **rst-flood detect**
- **rst-flood detect non-specific**
- **rst-flood threshold**

1.1.88 rst-flood detect

rst-flood detect 命令用来开启对指定 IP 地址的 **RST flood** 攻击防范检测，并配置 **RST flood** 攻击防范的触发阈值和对 **RST flood** 攻击的处理行为。

undo rst-flood 命令用来关闭对指定 IP 地址的 **RST flood** 攻击防范检测。

【命令】

```
rst-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] [ threshold threshold-value ] [ action { { client-verify | drop | logging } * | none } ]
```

```
undo rst-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 **RST flood** 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为 255.255.255.255 或 0.0.0.0。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。该 IPv6 地址不能为组播地址或::。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold *threshold-value*: 指定攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 RST 报文数目，取值范围为 1~1000000。

action: 设置对 **RST flood** 攻击的处理行为。若未指定本参数，则表示采用 **RST flood** 攻击防范的全局处理行为。

client-verify: 表示自动将受到攻击的 IP 地址添加到 TCP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 RST 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

使能 RST flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 RST 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 RST flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

每个攻击防范策略下可以同时多个 IP 地址配置 RST flood 攻击防范检测。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 192.168.1.2 的 RST flood 攻击防范检测，并指定触发阈值为 2000。当设备监测到向该 IP 地址每秒发送的 RST 报文数持续达到或超过 2000 时，启动 RST flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **rst-flood action**
- **rst-flood detect non-specific**
- **rst-flood threshold**

1.1.89 rst-flood detect non-specific

rst-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 RST flood 攻击防范检测。

undo rst-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 RST flood 攻击防范检测。

【命令】

```
rst-flood detect non-specific
undo rst-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 RST flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

对所有非受保护 IP 地址开启 RST flood 攻击防范检测后，设备将采用全局的阈值设置（由 **rst-flood threshold** 命令设置）和处理行为（由 **rst-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 RST flood 攻击防范检测。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] rst-flood detect non-specific
```

【相关命令】

- **rst-flood action**
- **rst-flood detect**
- **rst-flood threshold**

1.1.90 rst-flood threshold

rst-flood threshold 命令用来配置 RST flood 攻击防范的全局触发阈值。

undo rst-flood threshold 命令用来恢复缺省情况。

【命令】

rst-flood threshold *threshold-value*

undo rst-flood threshold

【缺省情况】

RST flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

threshold-value：指定向某 IP 地址每秒发送的 RST 报文数目，取值范围为 1~1000000。

【使用指导】

使能 RST flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 RST 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 RST flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

对于未专门配置 RST flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（HTTP 服务器或者 FTP 服务器）的 RST 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 `atk-policy-1` 中配置 RST flood 攻击防范检测的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 RST 报文数持续达到或超过 100 时，启动 RST flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] rst-flood threshold 100
```

【相关命令】

- **rst-flood action**
- **rst-flood detect**
- **rst-flood detect non-specific**

1.1.91 scan detect

scan detect 命令用来配置开启指定级别的扫描攻击防范。

undo scan detect 命令用来关闭指定级别的扫描攻击防范。

【命令】

```
scan detect level { { high | low | medium } | user-defined
{ port-scan-threshold threshold-value | ip-sweep-threshold threshold-value }
* [ period period-value ] } action { { block-source [ timeout minutes ] | drop }
| logging } *
undo scan detect level { high | low | medium }
```

【缺省情况】

扫描攻击防范处于关闭状态。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

level: 指定攻击防范的检测级别。

high: 表示高防范级别，该级别能检测出大部分的扫描攻击，但对活跃主机误报率较高，即将可提供服务的主机的报文错误判断为攻击报文的概率比较高。该级别的扫描攻击检测周期为 10 秒，针对端口扫描的防范阈值为 5000 packets，针对地址扫描的防范阈值为 5000 packets。

low: 表示低防范级别，该级别提供基本的扫描攻击检测，有很低的误报率，但对于一些扫描攻击类型不能检出。该级别的扫描攻击检测周期为 10 秒，针对端口扫描的防范阈值为 100000 packets，针对地址扫描的防范阈值为 100000 packets。**medium:** 表示中防范级别，该级别有适中的攻击检出率与误报率，通常能够检测出 Filtered Scan 等攻击。该级别的扫描攻击检测周期为 10 秒，针对端口扫描的防范阈值为 40000 packets，针对地址扫描的防范阈值为 40000 packets。

user-defined: 表示用户自定义防范规则，用户可根据网络实际情况和需求指定端口扫描、地址扫描的防范阈值和检测周期。

port-scan-threshold threshold-value: 指定端口扫描攻击防范的触发阈值。其中，*threshold-value* 为源 IP 地址每个检测周期内发送的目的端口不同的报文数目，取值范围为 1~1000000000。

ip-sweep-threshold threshold-value: 指定地址扫描攻击防范的触发阈值。其中，*threshold-value* 为源 IP 地址每个检测周期内发往不同目的 IP 地址的报文数目，取值范围为 1~1000000000。

period period-value: 表示检测周期，*period-value* 的取值范围为 1~1000000000，单位为秒，缺省值为 10。

action: 设置对扫描攻击的处理行为。

block-source: 表示阻断并丢弃来自该 IP 地址的后续报文。具体实现是，当设备检测到攻击发生后，会自动将发起攻击的源 IP 地址添加到 IP 黑名单动态表项中，当安全域上的黑名单过滤功能处于开启状态时，来自该 IP 地址的报文将被丢弃。

timeout minutes: 动态添加的黑名单表项的老化时间。其中，*minutes* 表示老化时间，取值范围为 1~10080，单位为分钟，缺省值为 10。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，由该攻击者发送的报文都将被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成记录告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

要使扫描攻击防范添加的 IP 黑名单动态表项生效，必须保证安全域上的黑名单过滤功能处于开启状态。

对于扫描攻击防范动态添加的黑名单，需要配置其老化时间大于扫描攻击的统计周期。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中配置扫描攻击的检测级别为低级别，处理行为是丢弃后续报文。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] scan detect level low action drop
# 在攻击防范策略 atk-policy-1 中配置扫描攻击的检测级别为低级别，处理行为是发日志，阻断并丢弃来自该 IP 地址的后续报文，并设置添加的 IP 黑名单表项的老化时间为 10 分钟。

<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level low action logging
block-source timeout 10
# 在攻击防范策略 atk-policy-1 中配置扫描攻击的检测级别为用户自定义，端口扫描防范阈值是 6000 packets，地址扫描防范阈值是 80000 packets，检测周期是 30 秒，处理行为是发日志，阻断并丢弃来自该 IP 地址的后续报文，并设置添加的 IP 黑名单表项的老化时间为 10 分钟。

<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level user-defined
port-scan-threshold 6000 ip-sweep-threshold 80000 period 30 action logging block-source
timeout 10
```

【相关命令】

- **blacklist enable**
- **blacklist global enable**

1.1.92 signature { large-icmp | large-icmpv6 } max-length

signature { large-icmp | large-icmpv6 } max-length 命令用来配置启动 Large ICMP 攻击防范的 ICMP 报文长度的最大值。

undo signature { large-icmp | large-icmpv6 } max-length 命令用来恢复缺省情况。

【命令】

```
signature { large-icmp | large-icmpv6 } max-length length
undo signature { large-icmp | large-icmpv6 } max-length
```

【缺省情况】

启动 Large ICMP 攻击防范的 ICMP 报文和 ICMPv6 报文长度的最大值均为 4000 字节。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

large-icmp：表示超大 ICMP 报文攻击防范。

large-icmpv6：表示超大 ICMPv6 报文攻击防范。

length：表示 ICMP 报文长度的最大值，ICMP 报文取值范围为 28～65534，ICMPv6 报文取值范围为 48～65534，单位为字节。

【举例】

在攻击防范策略 `atk-policy-1` 中配置启动 Large ICMP 攻击防范的 ICMP 报文长度的最大值为 50000 字节。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] signature large-icmp max-length 50000
```

【相关命令】

- **signature detect**

1.1.93 signature detect

signature detect 命令用来开启指定类型单包攻击报文的特征检测，并设置攻击防范的处理行为。

undo signature detect 命令用来关闭对指定类型的单包攻击报文的特征检测。

【命令】

```
signature detect { fraggle | fragment | impossible | land | large-icmp |  
large-icmpv6 | smurf | snork | tcp-all-flags | tcp-fin-only |  
tcp-invalid-flags | tcp-null-flag | tcp-syn-fin | tiny-fragment | traceroute  
| udp-bomb | winnuke } [ action { { drop | logging } * | none } ]
```

```
undo signature detect { fraggle | fragment | impossible | land | large-icmp |  
large-icmpv6 | smurf | snork | tcp-all-flags | tcp-fin-only |  
tcp-invalid-flags | tcp-null-flag | tcp-syn-fin | tiny-fragment | traceroute  
| udp-bomb | winnuke }
```

```
signature detect { ip-option-abnormal | ping-of-death | teardrop } action  
{ drop | logging } *
```

```
undo signature detect { ip-option-abnormal | ping-of-death | teardrop }
```

```
signature detect icmp-type { icmp-type-value | address-mask-reply |  
address-mask-request | destination-unreachable | echo-reply | echo-request  
| information-reply | information-request | parameter-problem | redirect  
| source-quench | time-exceeded | timestamp-reply | timestamp-request }  
[ action { { drop | logging } * | none } ]
```

```
undo signature detect icmp-type { icmp-type-value | address-mask-reply |  
address-mask-request | destination-unreachable | echo-reply | echo-request  
| information-reply | information-request | parameter-problem | redirect  
| source-quench | time-exceeded | timestamp-reply | timestamp-request }
```

```
signature detect icmpv6-type { icmpv6-type-value | destination-unreachable  
| echo-reply | echo-request | group-query | group-reduction | group-report  
| packet-too-big | parameter-problem | time-exceeded } [ action { { drop |  
logging } * | none } ]
```

```
undo signature detect icmpv6-type { icmpv6-type-value |  
destination-unreachable | echo-reply | echo-request | group-query |
```

```

group-reduction | group-report | packet-too-big | parameter-problem |
time-exceeded }
signature detect ip-option { option-code | internet-timestamp |
loose-source-routing | record-route | route-alert | security | stream-id |
strict-source-routing } [ action { { drop | logging } * | none } ]
undo signature detect ip-option { option-code | internet-timestamp |
loose-source-routing | record-route | route-alert | security | stream-id |
strict-source-routing }
signature detect ipv6-ext-header ext-header-value [ action { { drop | logging }
* | none } ]
undo signature detect ipv6-ext-header next-header-value

```

【缺省情况】

所有类型的单包攻击报文的特征检测均处于关闭状态。

【视图】

攻击防范策略视图

【缺省用户角色】

```

network-admin
context-admin

```

【参数】

fraggle: 表示 Fraggle 类型的报文攻击。

fragment: 表示 IP 分片报文攻击。

icmp-type: 表示 ICMP 类型的报文攻击。可以指定报文的类型值，或者指定报文的类型关键字。

- **icmp-type-value:** 表示 ICMP 报文类型的数值，取值范围为 0~255。
- **address-mask-reply:** 表示 ICMP address mask reply 类型的报文攻击。
- **address-mask-request:** 表示 ICMP address mask request 类型的报文攻击。
- **destination-unreachable:** 表示 ICMP destination unreachable 类型的报文攻击。
- **echo-reply:** 表示 ICMP echo reply 类型的报文攻击。
- **echo-request:** 表示 ICMP echo request 类型的报文攻击。
- **information-reply:** 表示 ICMP information reply 类型的报文攻击。
- **information-request:** 表示 ICMP information request 类型的报文攻击。
- **parameter-problem:** 表示 ICMP para problem 类型的报文攻击。
- **redirect:** 表示 ICMP redirect 类型的报文攻击。
- **source-quench:** 表示 ICMP source quench 类型的报文攻击。
- **time-exceeded:** 表示 ICMP time exceeded 类型的报文攻击。
- **timestamp-reply:** 表示 ICMP timestamp reply 类型的报文攻击。
- **timestamp-request:** 表示 ICMP timestamp request 类型的报文攻击。

icmpv6-type: 表示 ICMPv6 类型的报文攻击。可以指定报文的类型值，或者指定报文的类型关键字。

- **icmpv6-type-value:** 表示 ICMPv6 报文类型的数值，取值范围为 0~255。
- **destination-unreachable:** 表示 ICMPv6 destination unreachable 类型的报文攻击。
- **echo-reply:** 表示 ICMPv6 echo reply 类型的报文攻击。
- **echo-request:** 表示 ICMPv6 echo request 类型的报文攻击。
- **group-query:** 表示 ICMPv6 group query 类型的报文攻击。
- **group-reduction:** 表示 ICMPv6 group reduction 类型的报文攻击。
- **group-report:** 表示 ICMPv6 group report 类型的报文攻击。
- **packet-too-big:** 表示 ICMPv6 packet too big 类型的报文攻击。
- **parameter-problem:** 表示 ICMPv6 para problem 类型的报文攻击。
- **time-exceeded:** 表示 ICMPv6 time exceeded 类型的报文攻击。

impossible: 表示 IP 不可信报文的攻击。

ip-option: 表示 IP 选项类型的报文攻击。可以指定 IP 选项代码值，或者指定 IP 选项关键字。

- **option-code:** 表示 IP 选项代码值，取值范围为 1~255。
- **internet-timestamp:** 表示 IP 选项 timestamp 类型的报文攻击。
- **loose-source-routing:** 表示 IP 选项 loose source route 类型的报文攻击。
- **record-route:** 表示 IP 选项 record packet route 类型的报文攻击。
- **route-alert:** 表示 IP 选项 route alert 类型的报文攻击。
- **security:** 表示 IP 选项 security 类型的报文攻击。
- **stream-id:** 表示 IP 选项 stream identifier 类型的报文攻击。
- **strict-source-routing:** 表示 IP 选项 strict source route 类型的报文攻击。

ip-option-abnormal: 表示 IP 选项异常类型的报文攻击。

ipv6-ext-header ext-header-value: 表示 IPv6 扩展头参数值，取值范围在 0~255。

land: 表示 Land 类型的报文攻击。

large-icmp: 表示超大 ICMP 报文的攻击。

large-icmpv6: 表示超大 ICMPv6 报文的攻击。

ping-of-death: 表示 Ping-of-death 类型的报文攻击。

smurf: 表示 Smurf 类型的报文攻击。

snork: 表示 UDP Snork attack 类型的报文攻击。

tcp-all-flags: 表示 TCP 所有标志位均置位的报文攻击。

tcp-fin-only: 表示 TCP 仅 FIN 标志被置位的报文攻击。

tcp-invalid-flags: 表示 TCP 标志位非法的报文攻击。

tcp-null-flag: 表示 TCP 标志位为零的报文攻击。

tcp-syn-fin: 表示 TCP SYN 和 FIN 标志位被同时置位的报文攻击。

teardrop: 表示 teardrop 类型的报文攻击。

tiny-fragment: 表示 IP 分片报文的攻击。

traceroute: 表示 Trace route 类型的报文攻击。

udp-bomb: 表示 UDP Bomb attack 类型的报文攻击。

winnuke: 表示 WinNuke 类型的报文攻击。

action: 对指定报文攻击所采取的攻击防范处理行为。若未指定本参数，则采用该攻击报文所属的攻击防范级别所对应的默认处理行为。

- **drop:** 设置单包攻击的处理行为为丢弃报文。
- **logging:** 设置单包攻击的处理行为为发送日志。
- **none:** 不采取任何动作。

【使用指导】

可以通过多次执行本命令开启多种类型的单包攻击报文的特征检测。

若通过数值指定了报文类型，则当指定的数值为标准的报文类型值时，在显示信息中将会显示该数值对应的报文类型字符串，否则显示为数值。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 分片攻击报文的特征检测，并指定攻击防范处理行为为丢弃报文。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] signature detect fragment action drop
```

【相关命令】

- **signature level action**

1.1.94 signature level action

signature level action 命令用来配置指定级别单包攻击的处理行为。

undo signature level action 命令用来恢复缺省情况。

【命令】

```
signature level { high | info | low | medium } action { { drop | logging } * | none }
undo signature level { high | info | low | medium } action
```

【缺省情况】

对提示级别和低级别的单包攻击的处理行为是发送日志；对中级别的单包攻击的处理行为是发送日志并丢包；对高级别的单包攻击的处理行为是发送日志并丢包。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

high: 表示高级别的单包攻击，暂无实例。

info: 表示提示级别的单包攻击，例如 Large ICMP。

low: 表示低级别的单包攻击，例如 Traceroute。

medium: 表示中级别的单包攻击，例如 Winnuke。

drop: 设置单包攻击的处理行为为丢弃报文。

logging: 设置单包攻击的处理行为为发送日志。

none: 不采取任何动作。

【使用指导】

系统根据单包攻击结果的严重程度由低到高将其划分为四个攻击级别：提示、低级、中级、高级。开启某一个级别的单包攻击报文的特征检测，相当于批量开启了属于该级别的所有类型的单包攻击报文的特征检测。

若同时通过 **signature detect** 命令开启了具体类型的单包攻击报文的特征检测，则以 **signature detect** 命令配置的参数为准。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对提示级别的单包攻击的处理行为是丢弃后续报文。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy 1
```

```
[Sysname-attack-defense-policy-1] signature level info action drop
```

【相关命令】

- **signature detect**
- **signature level detect**

1.1.95 signature level detect

signature level detect 命令用来开启指定级别单包攻击报文的特征检测。

undo signature level detect 命令用来关闭对指定级别的单包攻击报文的特征检测。

【命令】

```
signature level { high | info | low | medium } detect
```

```
undo signature level { high | info | low | medium } detect
```

【缺省情况】

未开启任何级别的单包攻击报文的特征检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

high: 表示高级别的单包攻击，暂无实例。
info: 表示提示级别的单包攻击，例如 Large ICMP 报文攻击。
low: 表示低级别的单包攻击，例如 Traceroute 报文攻击。
medium: 表示中级别的单包攻击，例如 Winnuke 报文攻击。

【使用指导】

系统根据单包攻击结果的严重程度将其划分为四个级别：提示、低级、中级、高级。开启某一个级别的单包攻击报文的特征检测，相当于批量开启了属于该级别的所有单包攻击报文的特征检测。针对某一级别的单包攻击的处理行为由 **signature level action** 命令指定。若通过 **signature detect** 命令开启了具体的单包攻击报文的特征检测，则对该类攻击报文的处理行为以 **signature detect** 命令配置的参数为准。

可通过 **display attack-defense policy** 命令查看各类型单包攻击所属的级别。

【举例】

在攻击防范策略 **atk-policy-1** 中开启提示级别的单包攻击报文的特征检测。

```
<Sysname> system-view  
[Sysname] attack-defense policy 1  
[Sysname-attack-defense-policy-1] signature level info detect
```

【相关命令】

- **display attack-defense policy**
- **signature detect**
- **signature level action**

1.1.96 sip-flood action

sip-flood action 命令用来配置 SIP flood 攻击防范的全局处理行为。

undo sip-flood action 命令用来恢复缺省情况。

【命令】

```
sip-flood action { client-verify | drop | logging } *  
undo sip-flood action
```

【缺省情况】

不对检测到的 SIP flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

client-verify: 表示自动将受到攻击的 IP 地址添加到 SIP 客户端验证的受保护 IP 列表中。若客户端验证功能已开启，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 SIP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

本命令中 **client-verify** 参数的使用需要和 SIP 客户端验证功能配合。开启了 SIP 客户端验证功能的接口或安全域检测到 SIP flood 攻击时，若本命令中指定了 **client-verify** 参数，则设备会将受攻击的 IP 地址动态添加到相应客户端验证的受保护 IP 列表中，并对与这些 IP 地址建立的连接进行代理。若接口或安全域上未开启 SIP 客户端验证功能，则不会对任何连接进行代理。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 SIP flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] sip-flood action drop
```

【相关命令】

- **client-verify sip enable**
- **sip-flood detect**
- **sip-flood detect non-specific**
- **sip-flood threshold**

1.1.97 sip-flood detect

sip-flood detect 命令用来开启对指定 IP 地址的 SIP flood 攻击防范检测，并配置 SIP flood 攻击防范检测的触发阈值和对 SIP flood 攻击的处理行为。

undo sip-flood detect 命令用来关闭对指定 IP 地址的 SIP flood 攻击防范检测。

【命令】

```
sip-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ] [ port port-list ] [ threshold threshold-value ] [ action  
{ { client-verify | drop | logging } * | none } ]
```

```
undo sip-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址开启 SIP flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为 255.255.255.255 或 0.0.0.0。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。该 IPv6 地址不能为组播地址或::。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

port *port-list*: 指定开启 SIP flood 攻击防范检测的端口列表，表示方式为 { *start-port-number* [*to end-port-number*] } &<1-32>。&<1-32>表示前面的参数最多可以输入 32 次。*end-port-number* 必须大于或等于 *start-port-number*。若未指定本参数，则表示使用全局配置的检测端口列表。

threshold *threshold-value*: 指定 SIP flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 SIP 报文数目，取值范围为 1~1000000，缺省为 1000。

action: 设置对 SIP flood 攻击的处理行为。若未指定本参数，则表示采用 SIP flood 攻击防范的全局处理行为。

client-verify: 表示自动将被攻击的 IP 地址添加到 SIP 客户端验证的受保护 IP 列表中。若客户端验证功能已开启，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 SIP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

开启 SIP flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 SIP 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 SIP flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

每个攻击防范策略下可以同时为多个 IP 地址配置 SIP flood 攻击防范检测。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **192.168.1.2** 的 SIP flood 攻击防范检测，并指定触发阈值为 **2000**。当设备监测到向该 IP 地址每秒发送的 SIP 报文数持续达到或超过 **2000** 时，启动 SIP flood 攻击防范。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] sip-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **client-verify sip enable**
- **sip-flood action**
- **sip-flood detect non-specific**
- **sip-flood port**
- **sip-flood threshold**

1.1.98 sip-flood detect non-specific

sip-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 SIP flood 攻击防范检测。

undo sip-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 SIP flood 攻击防范检测。

【命令】

```
sip-flood detect non-specific
```

```
undo sip-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 SIP flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

对所有非受保护 IP 地址开启 SIP flood 攻击防范检测后，设备将采用全局的阈值设置（由 **sip-flood threshold** 命令设置）和处理行为（由 **sip-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 SIP flood 攻击防范检测。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] sip-flood detect non-specific
```

【相关命令】

- **sip-flood action**
- **sip-flood detect**
- **sip-flood threshold**

1.1.99 sip-flood port

sip-flood port 命令用来配置 SIP flood 攻击防范的全局检测端口号。

undo sip-flood port 命令用来恢复缺省情况。

【命令】

sip-flood port *port-list*
undo sip-flood port

【缺省情况】

SIP flood 攻击防范的全局检测端口号为 5060。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

port-list: 指定开启 SIP flood 攻击防范检测的端口列表，表示方式为{ *start-port-number* [*to end-port-number*] } &<1-32>。&<1-32>表示前面的参数最多可以输入 32 次。*end-port-number* 必须大于或等于 *start-port-number*。

【使用指导】

设备只对指定检测端口上收到的报文进行 SIP flood 攻击检测。

对于所有非受保护 IP 地址，或未指定检测端口的受保护 IP 地址，设备采用全局的检测端口进行 SIP flood 攻击检测。对于所有指定检测端口的受保护 IP 地址，设备针对为每个受保护 IP 地址指定的端口进行 SIP flood 攻击检测。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 SIP flood 攻击防范的全局检测端口为 5060 与 65530，当设备检测到访问 5060 端口或 65530 端口的 SIP flood 攻击时，启动攻击防范措施。

```
<Sysname> system-view  
[Sysname] attack-defense policy atk-policy-1  
[Sysname-attack-defense-policy-atk-policy-1] sip-flood port 5060 65530
```

【相关命令】

- **sip-flood action**
- **sip-flood detect**
- **sip-flood detect non-specific**

1.1.100 sip-flood threshold

sip-flood threshold 命令用来配置 SIP flood 攻击防范的全局触发阈值。

undo sip-flood threshold 命令用来恢复缺省情况。

【命令】

sip-flood threshold *threshold-value*

undo sip-flood threshold

【缺省情况】

SIP flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 SIP 报文数目，取值范围为 1~1000000。开启 SIP flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 SIP 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 SIP flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。

【使用指导】

对于未专门配置 SIP flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象的 SIP 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 SIP flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 SIP 报文数持续达到或超过 100 时，启动攻击防范措施。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] sip-flood threshold 100
```

【相关命令】

- **sip-flood action**
- **sip-flood detect**
- **sip-flood detect non-specific**

1.1.101 syn-ack-flood action

syn-ack-flood action 命令用来配置对 SYN-ACK flood 攻击防范的全局处理行为。

undo syn-ack-flood action 命令用来恢复缺省情况。

【命令】

```
syn-ack-flood action { client-verify | drop | logging }*  
undo syn-ack-flood action
```

【缺省情况】

不对检测到的 SYN-ACK flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

client-verify: 表示自动将受到攻击的 IP 地址添加到 TCP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 SYN-ACK 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成记录告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

本命令中 **client-verify** 参数的使用需要和 TCP 客户端验证功能配合。开启了 TCP 客户端验证的安全域检测到 ACK flood 攻击时，若本命令中指定了 **client-verify** 参数，则设备会将受攻击的 IP 地址动态添加到相应客户端验证的受保护 IP 列表中，并对与这些 IP 地址建立的连接进行代理。若安全域上未开启相应的代理功能，则不会对任何连接进行代理。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 atk-policy-1 中配置对 SYN-ACK flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view  
[Sysname] attack-defense policy atk-policy-1  
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood action drop
```

【相关命令】

- **client-verify tcp enable**
- **syn-ack-flood detect**
- **syn-ack-flood detect non-specific**
- **syn-ack-flood threshold**

1.1.102 syn-ack-flood detect

syn-ack-flood detect 命令用来对指定 IP 地址的 SYN-ACK flood 攻击防范检测，并配置 SYN-ACK flood 攻击防范检测触发阈值和防范行为。

undo syn-ack-flood detect 命令用来关闭对指定 IP 地址的 SYN-ACK flood 攻击防范检测。

【命令】

```
syn-ack-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] [ threshold threshold-value ] [ action { { client-verify | drop | logging } * | none } ]
```

```
undo syn-ack-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 SYN-ACK flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip ipv4-address: 指定要保护的 IPv4 地址。该 IPv4 地址不能为 255.255.255.255 或 0.0.0.0。

ipv6 ipv6-address: 指定要保护的 IPv6 地址。该 IPv6 地址不能为组播地址或::。

vpn-instance vpn-instance-name: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold threshold-value: 指定 SYN-ACK flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 SYN-ACK 报文数目，取值范围为 1~1000000。

action: 设置对 SYN-ACK flood 攻击的处理行为。若未指定本参数，则表示采用 SYN-ACK flood 攻击防范的全局处理行为。

client-verify: 表示自动将受到攻击的 IP 地址添加到 TCP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能，则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 SYN-ACK 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

使能 SYN-ACK flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 SYN-ACK 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 SYN-ACK flood 攻击，则进入

攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

每个攻击防范策略下可以同时为多个 IP 地址配置 SYN-ACK flood 攻击防范检测。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

开启对 IP 地址 192.168.1.2 的 SYN-ACK flood 攻击防范检测，并指定触发阈值为 2000。当设备监测到向该 IP 地址每秒发送的 SYN-ACK 报文数持续达到或超过 2000 时，启动 SYN-ACK 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **syn-ack-flood action**
- **syn-ack-flood detect non-specific**
- **syn-ack-flood threshold**

1.1.103 syn-ack-flood detect non-specific

syn-ack-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 SYN-ACK flood 攻击防范检测。

undo syn-ack-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 SYN-ACK flood 攻击防范检测。

【命令】

```
syn-ack-flood detect non-specific
undo syn-ack-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 SYN-ACK flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

对所有非受保护 IP 地址开启 SYN-ACK flood 攻击防范检测后，设备将采用全局的阈值设置（由 **syn-ack-flood threshold** 命令设置）和处理行为（由 **syn-ack-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 UDP flood 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood detect non-specific
```

【相关命令】

- **syn-ack flood action**
- **syn-ack-flood detect**
- **syn-ack-flood threshold**

1.1.104 syn-ack-flood threshold

syn-ack-flood threshold 命令用来配置 SYN-ACK flood 攻击防范的全局触发阈值。

undo syn-ack-flood threshold 命令用来恢复缺省情况。

【命令】

```
syn-ack-flood threshold threshold-value
undo syn-ack-flood threshold
```

【缺省情况】

SYN-ACK flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 SYN-ACK 报文数目，取值范围为 1~1000000。

【使用指导】

使能 SYN-ACK flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 SYN-ACK 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 SYN-ACK flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

对于未专门配置 SYN-ACK flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（HTTP 服务器或

者 FTP 服务器) 的 SYN-ACK 报文流量较大的应用场景, 建议调大触发阈值, 以免阈值太小对正常的业务流量造成影响; 对于网络状况较差, 且对攻击流量比较敏感的场景, 可以适当调小触发阈值。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 SYN-ACK flood 攻击防范的全局触发阈值为 100, 即当设备监测到向某 IP 地址每秒发送的 SYN-ACK 报文数持续达到或超过 100 时, 启动 SYN-ACK flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-ack-flood threshold 100
```

【相关命令】

- **syn-ack-flood action**
- **syn-ack-flood detect**
- **syn-ack-flood detect non-specific**

1.1.105 syn-flood action

syn-flood action 命令用来配置对 SYN flood 攻击防范的全局处理行为。

undo syn-flood action 命令用来恢复缺省情况。

【命令】

```
syn-flood action { client-verify | drop | logging } *
undo syn-flood action
```

【缺省情况】

不对检测到的 SYN flood 攻击采取任何措施。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

client-verify: 表示自动将受到攻击的 IP 地址添加到 TCP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能, 则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文, 即设备检测到攻击发生后, 向被攻击者发送的后续所有 SYN 报文都会被丢弃。

logging: 表示输出告警日志, 即设备检测到攻击发生时, 生成告警信息, 生成的告警信息将被发送到日志系统。

【使用指导】

本命令中 **client-verify** 参数的使用分别需要和 TCP 客户端验证功能配合。开启了 TCP 客户端验证的安全域检测到 ACK flood 攻击时, 若本命令中指定了 **client-verify** 参数, 则设备会将受

攻击的 IP 地址动态添加到相应客户端验证的受保护 IP 列表中，并对与这些 IP 地址建立的连接进行代理。若安全域上未开启相应的代理功能，则不会对任何连接进行代理。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 SYN flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood action drop
```

【相关命令】

- **syn-flood detect non-specific**
- **syn-flood detect**
- **syn-flood threshold**

1.1.106 syn-flood detect

syn-flood detect 命令用来开启对指定 IP 地址的 SYN flood 攻击防范检测，并配置 SYN flood 攻击防范检测的触发阈值和对 SYN flood 攻击的处理行为。

undo syn-flood detect 命令用来关闭对指定 IP 地址的 SYN flood 攻击防范检测。

【命令】

```
syn-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] [ threshold threshold-value ] [ action { { client-verify | drop | logging } * | none } ]
undo syn-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 SYN flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip *ipv4-address*: 指定要保护的 IPv4 地址。该 IPv4 地址不能为 255.255.255.255 或 0.0.0.0。

ipv6 *ipv6-address*: 指定要保护的 IPv6 地址。该 IPv6 地址不能为组播地址或::。

vpn-instance *vpn-instance-name*: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold threshold-value: 指定 SYN flood 攻击防范的触发阈值。其中, *threshold-value* 为向指定 IP 地址每秒发送的 SYN 报文数目, 取值范围为 1~1000000。

action: 设置对 SYN flood 攻击的处理行为。若未指定本参数, 则表示采用 SYN flood 攻击防范的全局处理行为。

client-verify: 表示自动将受到攻击的 IP 地址添加到 TCP 客户端验证的受保护 IP 列表中。若客户端验证功能已使能, 则对客户端与受保护 IP 地址之间的连接进行代理。

drop: 表示丢弃攻击报文, 即设备检测到攻击发生后, 向被攻击者发送的后续所有 SYN 报文都会被丢弃。

logging: 表示输出告警日志, 即设备检测到攻击发生时, 生成告警信息, 生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

使能 SYN flood 攻击防范后, 设备处于攻击检测状态, 当它监测到向指定 IP 地址发送 SYN 报文的速率持续达到或超过了触发阈值时, 即认为该 IP 地址受到了 SYN flood 攻击, 则进入攻击防范状态, 并根据配置启动相应的防范措施。此后, 当设备检测到向该服务器发送报文的速率低于恢复阈值 (触发阈值的 3/4) 时, 即认为攻击结束, 则由攻击防范状态恢复为攻击检测状态, 并停止执行防范措施。

每个攻击防范策略下可以同时为多个 IP 地址配置 SYN flood 攻击防范检测。

输出告警日志功能开启后, 设备生成的告警日志信息不会输出到控制台和监视终端, 可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍, 请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 192.168.1.2 的 SYN flood 攻击防范检测, 并指定触发阈值为 2000。当设备监测到向该 IP 地址每秒发送的 SYN 报文数持续达到或超过 2000 时, 启动 SYN flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **syn-flood action**
- **syn-flood detect non-specific**
- **syn-flood threshold**

1.1.107 syn-flood detect non-specific

syn-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 SYN flood 攻击防范检测。

undo syn-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 SYN flood 攻击防范检测。

【命令】

```
syn-flood detect non-specific  
undo syn-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 SYN flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

对所有非受保护 IP 地址开启 SYN flood 攻击防范检测后，设备将采用全局的阈值设置（由 **syn-flood threshold** 命令设置）和处理行为（由 **syn-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 SYN flood 攻击防范检测。

```
<Sysname> system-view  
[Sysname] attack-defense policy atk-policy-1  
[Sysname-attack-defense-policy-atk-policy-1] syn-flood detect non-specific
```

【相关命令】

- **syn-flood action**
- **syn-flood detect**
- **syn-flood threshold**

1.1.108 syn-flood threshold

syn-flood threshold 命令用来配置 SYN flood 攻击防范的全局触发阈值。

undo syn-flood threshold 命令用来恢复缺省情况。

【命令】

```
syn-flood threshold threshold-value  
undo syn-flood threshold
```

【缺省情况】

SYN flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
```

context-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 SYN 报文数目，取值范围为 1~1000000。

【使用指导】

使能 SYN flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 SYN 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 SYN flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

对于未专门配置 SYN flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（HTTP 服务器或者 FTP 服务器）的 SYN 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 SYN flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 SYN 报文数持续达到或超过 100 时，启动 SYN flood 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] syn-flood threshold 100
```

【相关命令】

- **syn-flood action**
- **syn-flood detect**
- **syn-flood detect non-specific**

1.1.109 threshold-learn apply

threshold-learn apply 命令用来立即应用最近一次的阈值学习结果。

【命令】

threshold-learn apply

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

在开启阈值学习功能但没有开启阈值学习结果自动应用功能的攻击防范策略中，可以通过执行该命令将最近一次的阈值学习结果作为泛洪攻击防范的阈值。多次执行本命令，最后一次执行的命令生效。在阈值学习结果自动应用功能开启时，此命令不生效。

该功能仅对非受保护 IP 地址也开启攻击防范检测的泛洪攻击类型生效。

【举例】

```
# 在攻击防范策略 atk-policy-1 中立即应用阈值学习功能上次的学习结果。
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn apply
```

【相关命令】

- **threshold-learn enable**

1.1.110 threshold-learn auto-apply enable

threshold-learn auto-apply enable 命令用来开启阈值学习结果自动应用功能。

undo threshold-learn auto-apply enable 命令用来关闭阈值学习结果自动应用功能。

【命令】

```
threshold-learn auto-apply enable
undo threshold-learn auto-apply enable
```

【缺省情况】

阈值学习结果自动应用功能处于关闭状态。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

只有在启用阈值学习功能的攻击防范策略中才可以应用阈值学习结果自动应用功能，且该功能仅对非受保护 IP 地址也开启攻击防范检测的泛洪攻击类型生效。启用该功能后，系统会在每次完成阈值学习后根据阈值学习结果重新设置泛洪攻击阈值，即泛洪攻击阈值为学习值×（1+学习容忍度）。其中，学习值是设备在学习时长内实际网络流量的峰值，学习容忍度则将学习值进行放大，从而避免在正常的峰值流量时造成合法流量的丢包。

通过执行 **threshold-learn enable** 命令可以启用阈值学习功能；通过执行 **threshold-learn tolerance-value** 命令可以配置阈值学习功能的学习容忍度。

【举例】

```
# 在攻击防范策略 atk-policy-1 中开启阈值学习结果自动应用功能。
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn auto-apply enable
```

【相关命令】

- **threshold-learn enable**
- **threshold-learn tolerance-value**

1.1.111 threshold-learn duration

threshold-learn duration 命令用来配置阈值学习时长。

undo threshold-learn duration 命令用来恢复缺省情况。

【命令】

threshold-learn duration *duration*

undo threshold-learn duration

【缺省情况】

流量阈值学习时长为 1440 分钟。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

duration: 阈值学习时长，取值范围为 1~1200000，单位为分钟。

【使用指导】

在应用已启用了阈值学习功能的攻击防范策略时，系统会自动开始进行阈值学习。建议学习时长设置大于 1440 分钟（24 小时），以确保设备学习到一整天的流量。如果在学习过程中修改了该值，则会重新开始学习。

【举例】

在攻击防范策略 **atk-policy-1** 中配置流量阈值学习时长为 2880 分钟（48 小时）。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn duration 2880
```

【相关命令】

- **threshold-learn enable**
- **threshold-learn loop**

1.1.112 threshold-learn enable

threshold-learn enable 命令用来开启泛洪攻击阈值学习功能。

undo threshold-learn enable 命令用来关闭泛洪攻击阈值学习功能。

【命令】

threshold-learn enable

undo threshold-learn enable

【缺省情况】

泛洪攻击阈值学习功能处于关闭状态。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

阈值是触发系统执行防范动作的条件，阈值的设置是否合理将直接影响攻击防范的效果。如果阈值设置过低，则可能造成正常流量被丢弃；而阈值设置过高，则可能在发生攻击时系统不能及时启动防范功能。因此，在配置泛洪攻击防范时，为了合理设置阈值，建议启用阈值学习功能。

【举例】

在攻击防范策略 **atk-policy-1** 中开启流量阈值学习功能。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn enable
```

【相关命令】

- **threshold-learn auto-apply enable**
- **threshold-learn duration**

1.1.113 threshold-learn interval

threshold-learn interval 命令用来配置阈值学习功能的学习间隔。

undo threshold-learn interval 命令用来恢复缺省情况。

【命令】

```
threshold-learn interval interval
```

```
undo threshold-learn interval
```

【缺省情况】

阈值学习功能的学习间隔为 1440 分钟。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval：阈值学习功能的学习间隔，取值范围为 1~1200000，单位为分钟。

【使用指导】

若攻击防范策略中启用了阈值学习功能且学习模式为周期学习，则在应用该策略时，系统会根据学习间隔周期性地对阈值学习。其中，学习间隔是指定从上次学习的结束时间到下次学习开始时间

的间隔时间。通过执行 **threshold-learn enable** 命令可以启用阈值学习功能；通过执行 **threshold-learn mode periodic** 命令可以配置阈值学习为周期学习模式。

【举例】

```
# 在攻击防范策略 atk-policy-1 中配置流量阈值学习周期间隔为 120 分钟。
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn interval 120
```

【相关命令】

- **threshold-learn enable**
- **threshold-learn mode**

1.1.114 threshold-learn mode

threshold-learn mode 命令用来配置阈值学习功能的学习模式。

undo threshold-learn mode 命令用来恢复缺省情况。

【命令】

```
threshold-learn mode { once | periodic }
undo threshold-learn mode
```

【缺省情况】

阈值学习功能的学习模式为单次学习。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

once: 学习模式为单次学习。

periodic: 学习模式为周期学习。

【使用指导】

阈值学习有单次学习和周期学习两种学习模式：

- 单次学习：只进行一次阈值学习。学习时长通过 **threshold-learn duration** 命令进行配置。对于网络流量模型比较稳定的场景可以使用该模式。
- 周期学习：按配置的学习间隔进行周期性的学习。其中，每个周期中的学习时长通过 **threshold-learn duration** 命令进行配置，学习间隔通过 **threshold-learn interval** 命令进行配置。对于网络流量模型易变化的场景可以使用该模式。

【举例】

```
# 在攻击防范策略 atk-policy-1 中配置流量阈值学习模式为周期学习。
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn mode periodic
```

【相关命令】

- **threshold-learn duration**
- **threshold-learn enable**
- **threshold-learn interval**

1.1.115 threshold-learn tolerance-value

threshold-learn tolerance-value 命令用来配置阈值学习功能的学习容忍度。

undo threshold-learn tolerance-value 命令用来恢复缺省情况。

【命令】

```
threshold-learn tolerance-value tolerance-value
undo threshold-learn tolerance-value
```

【缺省情况】

阈值学习功能的学习容忍度为 50%。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

tolerance-value: 学习容忍度，取值范围为 0~4000，单位为百分比。

【使用指导】

由于网络中的流量是时刻变化的，因此将某个学习时长内学习所得的统计值作为防范阈值后，若网络流量突然增大，可能会造成正常流量被丢弃。系统提供一个阈值容忍机制，它允许系统在将学习结果应用之前将阈值扩大指定的范围，然后再应用到网路中。扩大后的阈值为学习值×（1+学习容忍度）。

容忍度机制可以使阈值学习功能更好的应对网络流量的波动。只有当阈值学习结果自动应用功能处于开启状态时，配置学习容忍度才生效。

【举例】

```
# 在攻击防范策略 atk-policy-1 中开启自动应用，设置容忍度为 100。
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn auto-apply enable
[Sysname-attack-defense-policy-atk-policy-1] threshold-learn tolerance-value 100
```

【相关命令】

- **threshold-learn auto-apply enable**

- **threshold-learn enable**

1.1.116 udp-flood action

udp-flood action 命令用来配置对 UDP flood 攻击防范的全局处理行为。

undo udp-flood action 命令用来恢复缺省情况。

【命令】

```
udp-flood action { drop | logging } *
undo udp-flood action
```

【缺省情况】

不对检测到的 UDP flood 攻击进行任何处理。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 UDP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中配置对 UDP flood 攻击防范的全局处理行为是丢弃后续报文。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood action drop
```

【相关命令】

- **udp-flood detect**
- **udp-flood detect non-specific**
- **udp-flood threshold**

1.1.117 udp-flood detect

udp-flood detect 命令用来开启对指定 IP 地址的 UDP flood 攻击防范检测，并配置 UDP flood 攻击防范检测的触发阈值和对 UDP flood 攻击的处理行为。

undo udp-flood detect 命令用来关闭对指定 IP 地址的 UDP flood 攻击防范检测。

【命令】

```
udp-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ] [ threshold threshold-value ] [ action { { drop | logging }  
* | none } ]
```

```
undo udp-flood detect { ip ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

未对任何指定 IP 地址配置 UDP flood 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip ipv4-address: 指定要保护的 IPv4 地址。该 IPv4 地址不能为 255.255.255.255 或 0.0.0.0。

ipv6 ipv6-address: 指定要保护的 IPv6 地址。该 IPv6 地址不能为组播地址或::。

vpn-instance vpn-instance-name: 受保护 IP 地址所属的 VPN 实例。其中，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示该保护 IP 地址属于公网。

threshold threshold-value: 指定 UDP flood 攻击防范的触发阈值。其中，*threshold-value* 为向指定 IP 地址每秒发送的 UDP 报文数目，取值范围为 1~1000000，则表示采用 UDP flood 攻击防范的全局处理行为。

action: 设置对 UDP flood 攻击的处理行为。若未指定本参数，则表示采用 UDP flood 攻击防范的全局处理行为。

drop: 表示丢弃攻击报文，即设备检测到攻击发生后，向被攻击者发送的后续所有 UDP 报文都会被丢弃。

logging: 表示输出告警日志，即设备检测到攻击发生时，生成告警信息，生成的告警信息将被发送到日志系统。

none: 表示不采取任何动作。

【使用指导】

使能 UDP flood 攻击防范后，设备处于攻击检测状态，当它监测到向指定 IP 地址发送 UDP 报文的速率持续达到或超过了触发阈值时，即认为该 IP 地址受到了 UDP flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

每个攻击防范策略下可以同时为多个 IP 地址配置 UDP flood 攻击防范参数。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行 **display logbuffer** 命令进行查看。有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略 **atk-policy-1** 中开启对 IP 地址 **192.168.1.2** 的 **UDP flood** 攻击防范检测，并指定触发阈值为 **2000**。当设备监测到向该 IP 地址每秒发送的 UDP 报文数持续达到或超过 **2000** 时，启动 **UDP flood** 攻击防范。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] udp-flood detect ip 192.168.1.2 threshold 2000
```

【相关命令】

- **udp-flood action**
- **udp-flood detect non-specific**
- **udp-flood threshold**

1.1.118 udp-flood detect non-specific

udp-flood detect non-specific 命令用来对所有非受保护 IP 地址开启 **UDP flood** 攻击防范检测。

undo udp-flood detect non-specific 命令用来关闭对所有非受保护 IP 地址的 **UDP flood** 攻击防范检测。

【命令】

```
udp-flood detect non-specific
undo udp-flood detect non-specific
```

【缺省情况】

未对任何非受保护 IP 地址开启 **UDP flood** 攻击防范检测。

【视图】

攻击防范策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

对所有非受保护 IP 地址开启 **UDP flood** 攻击防范检测后，设备将采用全局的阈值设置（由 **udp-flood threshold** 命令设置）和处理行为（由 **udp-flood action** 命令配置）对这些 IP 地址进行保护。

【举例】

在攻击防范策略 **atk-policy-1** 中，对所有非受保护 IP 地址开启 **UDP flood** 攻击防范检测。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] udp-flood detect non-specific
```

【相关命令】

- **udp-flood action**
- **udp-flood detect**
- **udp-flood threshold**

1.1.119 udp-flood threshold

udp-flood threshold 命令用来配置 UDP flood 攻击防范的全局触发阈值。

undo udp-flood threshold 命令用来恢复缺省情况。

【命令】

udp-flood threshold *threshold-value*

undo udp-flood threshold

【缺省情况】

UDP flood 攻击防范的全局触发阈值为 1000。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

threshold-value: 指定向某 IP 地址每秒发送的 UDP 报文数目，取值范围为 1~1000000。

【使用指导】

使能 UDP flood 攻击防范后，设备处于攻击检测状态，当它监测到向某 IP 地址发送 UDP 报文的速率持续达到或超过了该触发阈值时，即认为该 IP 地址受到了 UDP flood 攻击，则进入攻击防范状态，并根据配置启动相应的防范措施。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

对于未专门配置 UDP flood 攻击防范检测的 IP 地址，设备采用全局的阈值设置来进行保护。阈值的取值需要根据实际网络应用场景进行调整，对于正常情况下到被保护对象（HTTP 服务器或者 FTP 服务器）的 UDP 报文流量较大的应用场景，建议调大触发阈值，以免阈值太小对正常的业务流量造成影响；对于网络状况较差，且对攻击流量比较敏感的场景，可以适当调小触发阈值。

【举例】

在攻击防范策略 **atk-policy-1** 中配置 UDP flood 攻击防范的全局触发阈值为 100，即当设备监测到向某 IP 地址每秒发送的 UDP 报文数持续达到或超过 100 时，启动 UDP flood 攻击防范。

```
<Sysname> system-view
```

```
[Sysname] attack-defense policy atk-policy-1
```

```
[Sysname-attack-defense-policy-atk-policy-1] udp-flood threshold 100
```


【相关命令】

- **udp-flood action**
- **udp-flood detect**
- **udp-flood detect non-specific**

1.1.120 whitelist enable

whitelist enable 命令用来开启安全域上的白名单过滤功能。

undo whitelist enable 命令用来关闭安全域上的白名单过滤功能。

【命令】

```
whitelist enable
undo whitelist enable
```

【缺省情况】

安全域上的白名单过滤功能处于关闭状态。

【视图】

安全域视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

若全局的白名单过滤功能处于开启状态，则所有安全域上的白名单过滤功能均处于开启状态。

若全局的白名单过滤功能处于关闭状态，则安全域上的白名单过滤功能由本命令决定是否开启。

【举例】

```
# 开启安全域 Untrust 上的白名单过滤功能。
<Sysname> system-view
[Sysname] security-zone name untrust
[Sysname-security-zone-Untrust] whitelist enable
```

1.1.121 whitelist global enable

whitelist global enable 命令用来开启全局白名单过滤功能。

undo whitelist global enable 命令用来关闭全局白名单过滤功能。

【命令】

```
whitelist global enable
undo whitelist global enable
```

【缺省情况】

全局白名单过滤功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启全局白名单过滤功能表示开启所有安全域上的白名单过滤功能。

【举例】

开启全局白名单过滤功能。

```
<Sysname> system-view
```

```
[Sysname] whitelist global enable
```

1.1.122 whitelist object-group

whitelist object-group 命令通过引用地址对象组配置白名单。

undo whitelist object-group 命令用来恢复缺省情况。

【命令】

whitelist object-group *object-group-name*

undo whitelist object-group

【缺省情况】

未引用地址对象组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-group-name：地址对象组名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

本命令需要和地址对象组功能配合使用，有关地址对象组功能的详细介绍，请参见“安全配置指导”中的“对象组”。

多次执行本命令，最后一次执行的命令生效。

【举例】

通过引用地址对象组 **object-group1** 配置白名单。

```
<Sysname> system-view
```

```
[Sysname] whitelist object-group object-group1
```

目 录

1 ARP攻击防御.....	1-1
1.1 ARP防止IP报文攻击配置命令.....	1-1
1.1.1 arp source-suppression enable.....	1-1
1.1.2 arp source-suppression limit	1-1
1.1.3 display arp source-suppression.....	1-2
1.2 源MAC地址固定的ARP攻击检测配置命令	1-3
1.2.1 arp source-mac	1-3
1.2.2 arp source-mac aging-time	1-4
1.2.3 arp source-mac exclude-mac	1-4
1.2.4 arp source-mac threshold	1-5
1.2.5 display arp source-mac	1-5
1.3 ARP报文源MAC地址一致性检查配置命令	1-6
1.3.1 arp valid-check enable	1-6
1.4 ARP主动确认配置命令	1-7
1.4.1 arp active-ack enable	1-7
1.5 ARP Detection配置命令	1-8
1.5.1 arp detection enable.....	1-8
1.5.2 arp detection rule.....	1-8
1.5.3 arp detection trust.....	1-9
1.5.4 arp detection validate	1-10
1.5.5 arp restricted-forwarding enable.....	1-11
1.5.6 display arp detection	1-11
1.5.7 display arp detection statistics	1-12
1.5.8 reset arp detection statistics	1-13
1.6 ARP自动扫描、固化配置命令.....	1-14
1.6.1 arp fixup	1-14
1.6.2 arp scan	1-14
1.7 ARP网关保护配置命令	1-15
1.7.1 arp filter source	1-15
1.8 ARP过滤保护配置命令	1-16
1.8.1 arp filter binding.....	1-16

1 ARP攻击防御

1.1 ARP防止IP报文攻击配置命令

1.1.1 arp source-suppression enable

arp source-suppression enable 命令用来开启 ARP 源地址抑制功能。

undo arp source-suppression enable 命令用来关闭 ARP 源地址抑制功能。

【命令】

```
arp source-suppression enable
undo arp source-suppression enable
```

【缺省情况】

ARP 源地址抑制功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

建议在网关设备上开启本功能。

【举例】

```
# 开启 ARP 源地址抑制功能。
<Sysname> system-view
[Sysname] arp source-suppression enable
```

【相关命令】

- **display arp source-suppression**

1.1.2 arp source-suppression limit

arp source-suppression limit 命令用来配置 ARP 源抑制的阈值。

undo arp source-suppression limit 命令用来恢复缺省情况。

【命令】

```
arp source-suppression limit limit-value
undo arp source-suppression limit
```

【缺省情况】

ARP 源抑制的阈值为 10。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

limit-value: ARP 源抑制的阈值，即设备在 5 秒间隔内可以处理的源 IP 相同，但目的 IP 地址不能解析的 IP 报文的最大数目，取值范围为 2~1024。

【使用指导】

如果网络中每 5 秒内从某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。

【举例】

```
# 配置 ARP 源抑制的阈值为 100。
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

【相关命令】

- **display arp source-suppression**

1.1.3 display arp source-suppression

display arp source-suppression 命令用来显示当前 ARP 源抑制的配置信息。

【命令】

display arp source-suppression

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【举例】

```
# 显示当前 ARP 源抑制的配置信息。
<Sysname> display arp source-suppression
ARP source suppression is enabled
Current suppression limit: 100
```

表1-1 display arp source-suppression 显示信息描述表

字段	描述
ARP source suppression is enabled	ARP源抑制功能处于开启状态
Current suppression limit	设备在5秒时间间隔内可以接收到的源IP相同,但目的IP地址不能解析的IP报文的最大数目

1.2 源MAC地址固定的ARP攻击检测配置命令

1.2.1 arp source-mac

arp source-mac 命令用来开启源 MAC 地址固定的 ARP 攻击检测功能,并选择检查模式。

undo arp source-mac 命令用来关闭源 MAC 地址固定的 ARP 攻击检测功能。

【命令】

```
arp source-mac { filter | monitor }
undo arp source-mac [ filter | monitor ]
```

【缺省情况】

源 MAC 地址固定的 ARP 攻击检测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

filter: 配置检查方式为过滤模式。

monitor: 配置检查方式为监控模式。

【使用指导】

建议在网关设备上开启本功能。

本特性根据 ARP 报文的源 MAC 地址对上送 CPU 的 ARP 报文进行统计,在 5 秒内,如果收到同一源 MAC 地址(源 MAC 地址固定)的 ARP 报文超过一定的阈值,则认为存在攻击,系统会将此 MAC 地址添加到攻击检测表项中。当开启了 ARP 日志信息功能(配置 **arp check log enable** 命令),且在该攻击检测表项老化之前,如果设置的检查模式为过滤模式,则会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉;如果设置的检查模式为监控模式,则只打印日志信息,不会将该源 MAC 地址发送的 ARP 报文过滤掉。关于 ARP 日志信息功能的详细描述,请参见“三层技术-IP 业务配置指导”中的“ARP”。

如果 **undo arp source-mac** 命令中未指定检查模式,则关闭任意检查模式的源 MAC 地址固定的 ARP 攻击检测功能。

【举例】

```
# 开启源 MAC 地址固定的 ARP 攻击检测功能，并选择 filter 检查模式。  
<Sysname> system-view  
[Sysname] arp source-mac filter
```

1.2.2 arp source-mac aging-time

arp source-mac aging-time 命令用来配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间。

undo arp source-mac aging-time 命令用来恢复缺省情况。

【命令】

```
arp source-mac aging-time time  
undo arp source-mac aging-time
```

【缺省情况】

源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 300 秒。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

time：源 MAC 地址固定的 ARP 攻击检测表项的老化时间，取值范围为 60～6000，单位为秒。

【举例】

```
# 配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 60 秒。  
<Sysname> system-view  
[Sysname] arp source-mac aging-time 60
```

1.2.3 arp source-mac exclude-mac

arp source-mac exclude-mac 命令用来配置保护 MAC 地址。当配置了保护 MAC 地址之后，即使该 ARP 报文中的 MAC 地址存在攻击也不会被检测过滤。

undo arp source-mac exclude-mac 命令用来取消配置的保护 MAC 地址。

【命令】

```
arp source-mac exclude-mac mac-address&<1-n>  
undo arp source-mac exclude-mac [mac-address&<1-n> ]
```

【缺省情况】

未配置任何保护 MAC 地址。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

mac-address&<1-n>: MAC 地址列表。其中, *mac-address* 表示配置的保护 MAC 地址, 格式为 H-H-H。&<1-n>表示每次最多可以配置的保护 MAC 地址个数。n 的取值为 10。

【使用指导】

如果 **undo** 命令中未指定 MAC 地址, 则取消所有已配置的保护 MAC 地址。

【举例】

```
# 配置源 MAC 地址固定的 ARP 攻击检查的保护 MAC 地址为 001e-1200-0213。  
<Sysname> system-view  
[Sysname] arp source-mac exclude-mac 001e-1200-0213
```

1.2.4 arp source-mac threshold

arp source-mac threshold 命令用来配置源 MAC 地址固定的 ARP 报文攻击检测阈值, 当在固定的时间 (5 秒) 内收到源 MAC 地址固定的 ARP 报文超过该阈值则认为存在 ARP 报文攻击。

undo arp source-mac threshold 命令用来恢复缺省情况。

【命令】

```
arp source-mac threshold threshold-value  
undo arp source-mac threshold
```

【缺省情况】

源 MAC 地址固定的 ARP 报文攻击检测阈值为 30。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

threshold-value: 固定时间内源 MAC 地址固定的 ARP 报文攻击检测的阈值, 单位为报文个数, 取值范围为 1~5000。

【举例】

```
# 配置源 MAC 地址固定的 ARP 报文攻击检测阈值为 30 个。  
<Sysname> system-view  
[Sysname] arp source-mac threshold 30
```

1.2.5 display arp source-mac

display arp source-mac 命令用来显示检测到的源 MAC 地址固定的 ARP 攻击检测表项。

【命令】

display arp source-mac { **interface** *interface-type interface-number* | **slot** *slot-number* }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface *interface-type interface-number*: 显示指定接口检测到的源 MAC 地址固定的 ARP 攻击检测表项, *interface-type interface-number* 表示指定接口的类型和编号。

slot *slot-number*: 显示指定成员设备检测到的源 MAC 地址固定的 ARP 攻击检测表项。
slot-number 表示设备在 IRF 中的成员编号。如果未指定本参数, 则显示主设备上检测到的源 MAC 地址固定的 ARP 攻击检测表项。

【举例】

显示接口 GigabitEthernet1/0/1 检测到的源 MAC 地址固定的 ARP 攻击检测表项。

```
<Sysname> display arp source-mac interface gigabitethernet 1/0/1
Source-MAC          VLAN ID  Interface          Aging-time
23f3-1122-3344      4094    GE1/0/1            10
```

表1-2 display arp source-mac 命令显示信息描述表

字段	描述
Source-MAC	检测到攻击的源MAC地址
VLAN ID	检测到攻击的VLAN ID
Interface	攻击来源的接口
Aging-time	ARP防攻击策略表项老化剩余时间, 单位为秒

1.3 ARP报文源MAC地址一致性检查配置命令

1.3.1 arp valid-check enable

arp valid-check enable 命令用来开启 ARP 报文源 MAC 地址一致性检查功能。

undo arp valid-check enable 命令用来关闭 ARP 报文源 MAC 地址一致性检查功能。

【命令】

arp valid-check enable
undo arp valid-check enable

【缺省情况】

ARP 报文源 MAC 地址一致性检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

ARP 报文源 MAC 地址一致性检查功能主要应用于网关设备。

开启 ARP 报文源 MAC 地址一致性检查功能后，设备会对接收的 ARP 报文进行检查，如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则丢弃该报文。

【举例】

开启 ARP 报文源 MAC 地址一致性检查功能。

```
<Sysname> system-view
```

```
[Sysname] arp valid-check enable
```

1.4 ARP主动确认配置命令

1.4.1 arp active-ack enable

arp active-ack enable 命令用来开启 ARP 主动确认功能。

undo arp active-ack enable 命令用来关闭 ARP 主动确认功能。

【命令】

arp active-ack enable

undo arp active-ack enable

【缺省情况】

ARP 主动确认功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

ARP 的主动确认功能主要应用于网关设备，防止攻击者仿冒用户欺骗网关设备。

【举例】

开启 ARP 主动确认功能。

```
<Sysname> system-view
```

```
[Sysname] arp active-ack enable
```

1.5 ARP Detection配置命令

1.5.1 arp detection enable

arp detection enable 命令用来开启 ARP Detection 功能，即对 ARP 报文进行用户合法性检查。

undo arp detection enable 命令用来关闭 ARP Detection 功能。

【命令】

```
arp detection enable
undo arp detection enable
```

【缺省情况】

ARP Detection 功能处于关闭状态，即不进行用户合法性检查。

【视图】

VLAN 视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 在 VLAN 2 下开启 ARP Detection 功能。
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

【相关命令】

- **arp detection rule**

1.5.2 arp detection rule

arp detection rule 命令用来配置用户合法性检查规则。

undo arp detection rule 命令用来删除用户合法性检查规则。

【命令】

```
arp detection rule rule-id { deny | permit } ip { ip-address [ mask ] | any } mac
{ mac-address [ mask ] | any } [ vlan vlan-id ]
undo arp detection rule [ rule-id ]
```

【缺省情况】

未配置用户合法性检查规则。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

rule-id: 用户合法性规则编号, 取值范围为 0~511, 数值越小表示该用户合法性规则优先级越高。

deny: 丢弃指定范围内的 ARP 报文。

permit: 转发指定范围内的 ARP 报文。

ip { ip-address [mask] | any }: 指定报文的源 IP 地址范围。

- **ip-address**: 表示报文的源 IP 地址, 为点分十进制形式。
- **mask**: 表示源 IP 地址的掩码, 为点分十进制形式。如果未指定该参数, 则 **ip-address** 表示主机地址。
- **any**: 表示任意源 IP 地址。

mac { mac-address [mask] | any }: 指定报文的源 MAC 地址范围。

- **mac-address**: 表示报文的源 MAC 地址, 格式为 H-H-H。
- **mask**: 表示源 MAC 地址的掩码, 格式为 H-H-H。如果未指定该参数, 则 **mac-address** 表示主机 MAC 地址。
- **any**: 表示任意源 MAC 地址。

vlan vlan-id: 指定规则中匹配的 VLAN, **vlan-id** 的取值范围为 1~4094。如果未指定该参数, 则不对报文中的 VLAN 进行匹配检查。

【使用指导】

只有配置了 **arp detection enable** 命令后, 通过命令 **arp detection rule** 配置的规则才生效。

使用 **undo arp detection rule** 命令时, 如果未指定 **rule-id**, 则会删除设备上所有已配置的用户合法性规则。

【举例】

配置用户合法性规则, 规则编号为 0, 规则内容为转发源地址为 10.1.1.1, 掩码为 255.255.0.0, 源 MAC 地址为 0001-0203-0405, 掩码为 ffff-ffff-0000 的 ARP 报文。并在 VLAN2 中开启用户合法性检查功能。

```
<Sysname> system-view
[Sysname] arp detection rule 0 permit ip 10.1.1.1 255.255.0.0 mac 0001-0203-0405
ffff-ffff-0000
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

【相关命令】

- **arp detection enable**

1.5.3 arp detection trust

arp detection trust 命令用来配置接口为 ARP 信任接口。

undo arp detection trust 命令用来恢复缺省情况。

【命令】

```
arp detection trust
undo arp detection trust
```

【缺省情况】

接口为 ARP 非信任接口。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 配置二层以太网接口 GigabitEthernet1/0/1 为 ARP 信任接口。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

1.5.4 arp detection validate

arp detection validate 命令用来开启对 ARP 报文的目的 MAC 地址或源 MAC 地址、IP 地址的有效性检查。

undo arp detection validate 命令用来关闭对 ARP 报文的有效性检查。

【命令】

```
arp detection validate { dst-mac | ip | src-mac } *
undo arp detection validate [ dst-mac | ip | src-mac ] *
```

【缺省情况】

ARP 报文有效性检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

dst-mac: 检查 ARP 应答报文中的目的 MAC 地址，是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，无效的报文需要被丢弃。

ip: 检查 ARP 报文源 IP 和目的 IP 地址，全 1 或者组播 IP 地址都是不合法的，需要丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。

src-mac: 检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致认为有效，否则丢弃。

【使用指导】

开启有效性检查时可以指定某一种检查方式也可以配置成多种检查方式的组合。

关闭时可以指定关闭某一种或多种检查，在不指定检查方式时，表示关闭所有有效性检查。

【举例】

开启对 ARP 报文的 MAC 地址和 IP 地址的有效性检查。

```
<Sysname> system-view
```

```
[Sysname] arp detection validate dst-mac ip src-mac
```

1.5.5 arp restricted-forwarding enable

arp restricted-forwarding enable 命令用来开启 ARP 报文强制转发功能。

undo arp restricted-forwarding enable 命令用来关闭 ARP 报文强制转发功能。

【命令】

arp restricted-forwarding enable

undo arp restricted-forwarding enable

【缺省情况】

ARP 报文强制转发功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

context-admin

【举例】

开启 VLAN 2 的 ARP 报文强制转发功能。

```
<Sysname> system-view
```

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] arp restricted-forwarding enable
```

1.5.6 display arp detection

display arp detection 命令用来显示配置了 ARP Detection 功能的 VLAN。

【命令】

display arp detection

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin

【举例】

显示所有配置了 ARP Detection 功能的 VLAN。
<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1-2, 4-5

表1-3 display arp detection 命令显示信息描述表

字段	描述
ARP detection is enabled in the following VLANs	配置了ARP Detection功能的VLAN信息，如果不存在配置了ARP Detection功能的VLAN，则显示“ARP detection is not enabled in any VLANs.”

【相关命令】

- arp detection enable

1.5.7 display arp detection statistics

display arp detection statistics 命令用来显示 ARP Detection 丢弃报文的统计信息。

【命令】

display arp detection statistics [interface interface-type interface-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface interface-type interface-number：显示指定接口的 ARP Detection 丢弃报文的统计信息。interface-type interface-number 用来指定接口类型和编号。如果未指定本参数，则显示所有接口的 ARP Detection 丢弃报文的统计信息。

【使用指导】

按接口显示用户合法性检查和报文有效性检查的统计情况，只显示 ARP Detection 功能报文的丢弃情况。

【举例】

显示 ARP Detection 丢弃报文的统计信息。

```
<Sysname> display arp detection statistics
State: U-Untrusted T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)      IP      Src-MAC  Dst-MAC  Inspect
GE1/0/1(U)            40      0        0        78
GE1/0/2(U)            0       0        0        0
GE1/0/3(T)            0       0        0        0
GE1/0/4(U)            0       0        30       0
```

表1-4 display arp detection statistics 命令显示信息描述表

字段	描述
State	接口状态： - U: ARP 非信任接口 - T: ARP 信任接口
Interface(State)	ARP报文入接口，State表示该接口的信任状态
IP	ARP报文源和目的IP地址检查不通过丢弃的报文计数
Src-MAC	ARP报文源MAC地址检查不通过丢弃的报文计数
Dst-MAC	ARP报文目的MAC地址检查不通过丢弃的报文计数
Inspect	ARP报文结合用户合法性检查不通过丢弃的报文计数

【相关命令】

- reset arp detection statistics

1.5.8 reset arp detection statistics

reset arp detection statistics 命令用来清除 ARP Detection 的报文丢弃统计信息。

【命令】

```
reset arp detection statistics [ interface interface-type
interface-number ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interface interface-type interface-number: 表示清除指定接口下的 ARP Detection 的报文丢弃统计信息。*interface-type interface-number* 用来指定接口类型和编号。如果未指定本参数，则清除所有接口下的 ARP Detection 报文丢弃统计信息。

【举例】

```
# 清除所有的 ARP Detection 的报文丢弃统计信息。
```



```
<Sysname> reset arp detection statistics
```

【相关命令】

- **display arp detection statistics**

1.6 ARP自动扫描、固化配置命令

1.6.1 arp fixup

arp fixup 命令用来将设备上的动态 ARP 表项转化成静态 ARP 表项。

【命令】

arp fixup

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

本命令将当前的动态 ARP 表项转换为静态 ARP 表项，后续学习到的动态 ARP 表项可以通过再次执行 **arp fixup** 命令进行固化。

固化后的静态 ARP 表项与配置产生的静态 ARP 表项相同。

固化生成的静态 ARP 表项数量同样受到设备可以支持的静态 ARP 表项数目的限制，由于静态 ARP 表项数量的限制可能导致只有部分动态 ARP 表项被固化。

如果用户执行固化前有 D 个动态 ARP 表项，S 个静态 ARP 表项，由于固化过程中存在动态 ARP 表项的老化或者新建动态 ARP 表项的情况，所以固化后的静态 ARP 表项可能为 $(D+S+M-N)$ 个。其中，M 为固化过程中新建的动态 ARP 表项个数，N 为固化过程中老化的动态 ARP 表项个数。

通过固化生成的静态 ARP 表项，可以通过命令行 **undo arp ip-address [vpn-instance-name]** 逐条删除，也可以通过命令行 **reset arp all** 或 **reset arp static** 全部删除。

【举例】

将设备上的动态 ARP 表项转化成静态 ARP 表项。

```
<Sysname> system-view
```

```
[Sysname] arp fixup
```

1.6.2 arp scan

arp scan 命令用来开启 ARP 自动扫描功能。

【命令】

arp scan [start-ip-address to end-ip-address]

【视图】

三层以太网接口视图

三层以太网子接口视图
三层聚合接口视图
三层聚合子接口视图
VLAN 接口视图
以太网冗余接口
以太网冗余子接口

【缺省用户角色】

network-admin
context-admin

【参数】

start-ip-address: ARP 扫描区间的起始 IP 地址。起始 IP 地址必须小于等于终止 IP 地址。
end-ip-address: ARP 扫描区间的终止 IP 地址。

【使用指导】

ARP 自动扫描功能可以对接口下指定地址范围内的邻居进行扫描，对于已存在 ARP 表项的 IP 地址不进行扫描。

如果用户知道局域网内邻居分配的 IP 地址范围，指定了 ARP 扫描区间，则对该范围内的邻居进行扫描，减少扫描等待的时间。如果指定的扫描区间同时在接口下多个 IP 地址的网段内，则发送的 ARP 请求报文的源 IP 地址选择网段范围较小的接口 IP 地址。

如果用户不指定 ARP 扫描区间的起始 IP 地址和终止 IP 地址，则仅对接口下的主 IP 地址网段内的邻居进行扫描。其中，发送的 ARP 请求报文的源 IP 地址就是接口的主 IP 地址。

ARP 扫描区间的起始 IP 地址和终止 IP 地址必须与接口的 IP 地址（主 IP 地址或手工配置的从 IP 地址）在同一网段。

扫描操作可能比较耗时，用户可以通过<Ctrl_C>来终止扫描（在终止扫描时，对于已经收到的邻居应答，会建立该邻居的动态 ARP 表项）。

【举例】

```
# 对接口 GigabitEthernet1/0/1 下的主 IP 地址网段内的邻居进行扫描。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp scan
# 对接口 GigabitEthernet1/0/1 下指定地址范围内的邻居进行扫描。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp scan 1.1.1.1 to 1.1.1.20
```

1.7 ARP网关保护配置命令

1.7.1 arp filter source

arp filter source 命令用来开启 ARP 网关保护功能，配置受保护的网关 IP 地址。

undo arp filter source 命令用来关闭 ARP 网关保护功能，并删除已配置的受保护网关 IP 地址。

【命令】

```
arp filter source ip-address  
undo arp filter source ip-address
```

【缺省情况】

ARP 网关保护功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address：受保护的网关 IP 地址。

【使用指导】

每个接口最多支持配置 8 个受保护的网关 IP 地址。

不能在同一接口下同时配置命令 **arp filter source** 和 **arp filter binding**。

【举例】

在 GigabitEthernet1/0/1 下开启 ARP 网关保护功能，受保护的网关 IP 地址为 1.1.1.1。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] arp filter source 1.1.1.1
```

1.8 ARP过滤保护配置命令

1.8.1 arp filter binding

arp filter binding 命令用来开启 ARP 过滤保护功能并配置 ARP 过滤保护表项。

undo arp filter binding 命令用来删除 ARP 过滤保护表项。

【命令】

```
arp filter binding ip-address mac-address  
undo arp filter binding ip-address
```

【缺省情况】

ARP 过滤保护功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: 允许通过的 ARP 报文的源 IP 地址。

mac-address: 允许通过的 ARP 报文的源 MAC 地址。

【使用指导】

ARP 过滤保护表项可以限制只有特定源 IP 地址和源 MAC 地址的 ARP 报文才允许通过。

每个接口最多支持配置 8 组允许通过的 ARP 报文的源 IP 地址和源 MAC 地址。

不能在同一接口下同时配置命令 **arp filter source** 和 **arp filter binding**。

【举例】

在 GigabitEthernet1/0/1 下开启 ARP 过滤保护功能，允许源 IP 地址为 1.1.1.1、源 MAC 地址为 0e10-0213-1023 的 ARP 报文通过。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 0e10-0213-1023
```

目 录

1 IPv4 uRPF	1-1
1.1 IPv4 uRPF配置命令	1-1
1.1.1 display ip urpf	1-1
1.1.2 display ip urpf statistics security-zone	1-2
1.1.3 ip urpf	1-3
1.1.4 reset ip urpf statistics security-zone	1-4
2 IPv6 uRPF	2-1
2.1 IPv6 uRPF配置命令	2-1
2.1.1 display ipv6 urpf	2-1
2.1.2 display ipv6 urpf statistics security-zone	2-2
2.1.3 ipv6 urpf	2-3
2.1.4 reset ipv6 urpf statistics security-zone	2-4

1 IPv4 uRPF

1.1 IPv4 uRPF配置命令

1.1.1 display ip urpf

display ip urpf 命令用来显示 uRPF 的配置应用情况。

【命令】

display ip urpf [**security-zone** *zone-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

security-zone *zone-name*: 安全域的名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

slot *slot-number*: 显示指定成员设备 uRPF 配置应用情况。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 uRPF 配置应用情况。

【举例】

显示指定安全域上已经应用的 uRPF 的配置情况。

```
<Sysname> display ip urpf security-zone Untrust
uRPF configuration information of security-zone Untrust(failed):
  Check type: strict
  Allow default route
  Link check
  Suppress drop ACL: 3000
```

表1-1 display ip urpf 命令显示信息描述表

字段	描述
uRPF configuration information of security-zone	安全域uRPF配置应用情况
(failed)	当前uRPF配置下发转发芯片失败，原因可能为芯片资源不足。没有该字段时表示下发成功
Check type	uRPF检查类型，包括： • loose: 松散型检查 • strict: 严格型检查

字段	描述
Allow default route	允许缺省路由
Link check	允许对链路信息进行检查
Suppress drop ACL	配置了抑制丢弃，显示配置的ACL编号

1.1.2 display ip urpf statistics security-zone

display ip urpf statistics security-zone 命令用来显示安全域的 uRPF 统计信息。

【命令】

display ip urpf statistics security-zone *zone-name* [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

zone-name: 安全域的名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

slot slot-number: 显示指定成员设备上的 uRPF 统计信息。**slot-number** 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 uRPF 统计信息。

【举例】

显示安全域 Untrust 的 uRPF 统计信息。

```
<Sysname> display ip urpf statistics security-zone Untrust slot 1
uRPF information:
  Drops          : 390712
  Suppressed drops: 0
```

表1-2 display ip urpf statistics security-zone 命令显示信息描述表

字段	描述
uRPF information	uRPF统计信息
Drops	显示丢弃报文的数目
Suppressed drops	配置了抑制丢弃时，显示匹配到ACL未丢弃报文的数目

【相关命令】

- **reset ip urpf statistics security-zone**

1.1.3 ip urpf

ip urpf 命令用来开启 uRPF 功能。

undo ip urpf 命令用来关闭 uRPF 功能。

【命令】

```
ip urpf { loose [ allow-default-route ] [ acl acl-number ] | strict  
[ allow-default-route ] [ acl acl-number ] [ link-check ] }  
undo ip urpf
```

【缺省情况】

uRPF 功能处于关闭状态。

【视图】

安全域视图

【缺省用户角色】

network-admin

context-admin

【参数】

loose: 松散型检查。仅检查报文的源地址是否在转发表中存在，而不再检查报文的入接口与转发表是否匹配。

strict: 严格型检查。不仅检查报文的源地址是否在转发表中存在，而且检查报文的入接口与转发表是否匹配。仅 VLAN 接口视图下可使用该检查方式。

allow-default-route: 允许源地址查转发表时匹配缺省路由表项。

acl acl-number: 访问控制列表，用来抑制报文丢弃。**acl-number** 表示指定的 ACL 编号，取值范围为 2000~3999。其中：

- 基本 ACL 编号的取值范围为 2000~2999。
- 高级 ACL 编号的取值范围为 3000~3999。

link-check: 允许对链路信息进行检查。目前仅支持以太网链路。

【使用指导】

uRPF 功能一般部署在运营商网络接入客户侧设备的边缘位置，也可以部署在运营商网络对接其他运营商设备的边缘位置设备或部署在客户侧边缘位置设备。

选择严格或松散 uRPF 取决于当前组网中是否存在非对称路径，如果运营商设备上行流量的入接口和下行流量的出接口相同则是对称路径，此时建议在运营商网络接入客户侧设备的边缘位置的接口所在的安全域下配置严格 uRPF。一般运营商接入客户侧的组网中都是对称路径。运营商对接其他运营商的边缘位置可能出现非对称路径，此时建议在运营商网络对接其他运营商网络的边缘位置的接口所在的安全域下配置松散 uRPF。

运营商网络边缘位置一般不会有缺省路由指向客户侧设备，所以一般不需要配置 **allow-default-route**。如果在客户侧边缘设备接口所在安全域上面启用 uRPF，这时往往会有缺省路由指向运营商，此时需要配置 **allow-default-route**。

如果一个特定的数据包与 ACL 匹配，即使它没有通过 uRPF 的检查，也会被转发。

配置 **link-check** 后，设备会根据源地址查转发表得到的下一跳后进一步查 ARP 表项来确定源 MAC 地址是否正确。如果运营商是用以太网接口接入客户，此时一个接口同时接多个不同客户，因此建议接口下配置 **link-check** 功能。

【举例】

```
# 在安全域 Untrust 上配置严格型 uRPF 检查。
<Sysname> system-view
[Sysname] security-zone name Untrust
[Sysname-security-zone-Untrust] ip urpf strict
```

【相关命令】

- **display ip urpf**

1.1.4 reset ip urpf statistics security-zone

reset ip urpf statistics security-zone 命令用来清除安全域的 uRPF 统计信息。

【命令】

```
reset ip urpf statistics security-zone zone-name
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

zone-name：安全域的名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

【举例】

```
# 清除安全域 Untrust 的 urpf 统计信息。
<Sysname> reset ip urpf statistics security-zone Untrust
```

【相关命令】

- **display ip urpf statistics security-zone**

2 IPv6 uRPF

2.1 IPv6 uRPF配置命令

2.1.1 display ipv6 urpf

display ipv6 urpf 命令用来显示 IPv6 uRPF 的配置应用情况。

【命令】

display ipv6 urpf [**security-zone** *zone-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

security-zone *zone-name*: 安全域的名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

slot *slot-number*: 显示指定成员设备 IPv6 uRPF 配置应用情况。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 uRPF 配置应用情况。

【举例】

显示指定安全域上的已经应用的 IPv6 uRPF 的配置情况。
<Sysname> display ipv6 urpf security-zone Untrust
IPv6 uRPF configuration information of security-zone Untrust(failed):
 Check type: loose
 Allow default route
 Suppress drop ACL: 2000

表2-1 display ipv6 urpf 命令显示信息描述表

字段	描述
IPv6 uRPF configuration information of security-zone	安全域IPv6 uRPF配置应用情况
(failed)	当前IPv6 uRPF配置下发转发芯片失败，原因可能为芯片资源不足。没有该字段时表示下发成功
Check type	IPv6 uRPF检查类型，包括： • loose: 松散型检查 • strict: 严格型检查
Allow default route	允许缺省路由

字段	描述
Suppress drop ACL	配置了抑制丢弃，显示配置的IPv6 ACL编号

2.1.2 display ipv6 urpf statistics security-zone

display ipv6 urpf statistics security-zone 命令用来显示安全域的 IPv6 uRPF 统计信息。

【命令】

display ipv6 urpf statistics security-zone *zone-name* [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

zone-name: 安全域的名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

slot slot-number: 显示指定成员设备上的 IPv6 uRPF 统计信息。**slot-number** 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 uRPF 统计信息。

【举例】

显示安全域 Untrust 的 IPv6 uRPF 统计信息。

```
<Sysname> display ipv6 urpf statistics security-zone Untrust slot 1
IPv6 uRPF information:
  Drops           : 390712
  Suppressed drops: 0
```

表2-2 display ip urpf statistics security-zone 命令显示信息描述表

字段	描述
IPv6 uRPF information	IPv6 uRPF统计信息
Drops	显示丢弃报文的数目
Suppressed drops	配置了抑制丢弃时，显示匹配到ACL未丢弃报文的数目

【相关命令】

- **reset ipv6 urpf statistics security-zone**

2.1.3 ipv6 urpf

ipv6 urpf 命令用来开启 IPv6 uRPF 功能。

undo ipv6 urpf 命令用来关闭 IPv6 uRPF 功能。

【命令】

```
ipv6 urpf { loose | strict } [ allow-default-route ] [ acl acl-number ]  
undo ipv6 urpf
```

【缺省情况】

IPv6 uRPF 功能处于关闭状态。

【视图】

安全域视图

【缺省用户角色】

network-admin
context-admin

【参数】

loose: 松散型检查。仅检查报文的源地址是否在 IPv6 转发表中存在，而不再检查报文的入接口与 IPv6 转发表是否匹配。

strict: 严格型检查。不仅检查报文的源地址是否在 IPv6 转发表中存在，而且检查报文的入接口与 IPv6 转发表是否匹配。

allow-default-route: 允许源地址查 IPv6 转发时匹配缺省路由表项。

acl acl-number: 访问控制列表，用来抑制报文丢弃。*acl-number* 表示指定的 ACL 编号，取值范围为 2000~3999。其中：

- 基本 ACL 编号的取值范围为 2000~2999。
- 高级 ACL 编号的取值范围为 3000~3999。

【使用指导】

IPv6 uRPF 功能一般部署在运营商网络接入客户侧设备的边缘位置，也可以部署在运营商网络对接其他运营商设备的边缘位置设备或部署在客户侧边缘位置设备。

选择严格或松散 IPv6 uRPF 取决于当前组网中是否存在非对称路径，如果运营商设备上行流量的入接口和下行流量的出接口相同则是对称路径，此时建议在运营商网络接入客户侧设备的边缘位置的接口所在的安全域下配置严格 IPv6 uRPF。一般运营商接入客户侧的组网中都是对称路径。运营商对接其他运营商的边缘位置可能出现非对称路径，此时建议在运营商网络对接其他运营商网络的边缘位置的接口所在的安全域下配置松散 IPv6 uRPF。

如果一个特定的数据包与 ACL 匹配，即使它没有通过 IPv6 uRPF 的检查，也会被转发。

运营商网络边缘位置一般不会有缺省路由指向客户侧设备，所以一般不需要配置 **allow-default-route**。如果在客户侧边缘设备接口所在安全域上面启用 IPv6 uRPF，这时往往会有缺省路由指向运营商，此时需要配置 **allow-default-route**。

【举例】

在安全域 Untrust 上配置松散 IPv6 uRPF 检查。

```
<Sysname> system-view
[Sysname] security-zone name Untrust
[Sysname-security-zone-Untrust] ipv6 urpf loose
```

【相关命令】

- **display ipv6 urpf**

2.1.4 reset ipv6 urpf statistics security-zone

reset ipv6 urpf statistics security-zone 命令用来清除安全域的 IPv6 uRPF 统计信息。

【命令】

```
reset ipv6 urpf statistics security-zone zone-name
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

zone-name: 安全域的名称，为 1~31 个字符的字符串，不区分大小写，不能包含字符“-”。

【举例】

```
# 清除安全域 Untrust 的 IPv6 uRPF 统计信息
<Sysname> reset ipv6 urpf statistics security-zone Untrust
```

【相关命令】

- **display ipv6 urpf statistics security-zone**

目 录

1 加密引擎.....	1-1
1.1 加密引擎配置命令.....	1-1
1.1.1 display crypto-engine.....	1-1
1.1.2 display crypto-engine statistics	1-2
1.1.3 reset crypto-engine statistics	1-4

1 加密引擎

1.1 加密引擎配置命令

1.1.1 display crypto-engine

display crypto-engine 命令用来显示加密引擎的基本信息。

【命令】

display crypto-engine

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

若设备没有硬件加密引擎，则只会显示软件加密引擎信息。

【举例】

显示加密引擎的基本信息。

```
<Sysname> display crypto-engine
Crypto engine name: Software crypto engine
Crypto engine state: Enabled
Crypto engine type: Software
Slot ID: 1
CPU ID: 0
Crypto engine ID: 0
Crypto device name: Software
Crypto device serial number:
Symmetric algorithms: des-cbc des-ecb 3des-cbc aes-cbc aes-ecb aes-ctr camellia_cbc md5
sha1 sha2-256 sha2-384 sha2-512 md5-hmac sha1-hmac sha2-256-hmac sha2-384-hmac sha2-512-hmac
aes-xcbc aes-xcbc-hmac
Asymmetric algorithms:
Random number generation function: Supported

Crypto engine name: Cavium crypto driver
Crypto engine state: Enabled
Crypto engine type: Hardware
Slot ID: 1
CPU ID: 0
Crypto engine ID: 1
```

Crypto device name: Cavium crypto
 Crypto device serial number:
 Symmetric algorithms: des-cbc des-ecb 3des-cbc 3des-ecb aes-cbc aes-ecb aes-ctr md5 sha1 sha2-256 sha2-384 sha2-512 md5-hmac sha1-hmac sha2-256-hmac sha2-384-hmac sha2-512-hmac aes-xcbc-hmac
 Asymmetric algorithms: dh-group1 dh-group2 dh-group5 dh-group14
 Random number generation function: Supported

表1-1 display crypto-engine 命令显示信息描述表

字段	描述
Crypto engine name	加密引擎名称
Crypto engine state	加密引擎的状态 对于硬件加密引擎，包括以下两种： - Enabled: 已开启 - Disable: 关闭 对于软件加密引擎，只包含以下一种： - Enabled: 已开启
Crypto engine type	加密引擎的类型，包括以下两种： - Hardware: 硬件 - Software: 软件
CPU ID	CPU编号
Crypto engine ID	加密引擎ID号
Crypto device name	加密设备的名称 软件加密引擎，显示为Software；硬件加密引擎，显示信息以设备实际情况为准
Crypto device serial number	加密设备的序列号 软件加密引擎，显示为空；硬件加密引擎，显示信息以设备实际情况为准
Symmetric algorithms	支持的对称加密算法
Asymmetric algorithms	支持的非对称加密算法
Random number generation function	是否支持获取随机数的功能 - Supported: 支持 - Not supported: 不支持

1.1.2 display crypto-engine statistics

display crypto-engine statistics 命令用来显示加密引擎的统计信息。

【命令】

display crypto-engine statistics [engine-id engine-id slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

engine-id *engine-id*: 显示指定加密引擎的统计信息，*engine-id* 为加密引擎 ID 编号，取值范围为 0~4294967295。

slot *slot-number*: 显示指定成员设备上的加密引擎统计信息，*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

如果未开启硬件加密引擎或者设备上没有硬件加密引擎，则只会显示软件加密引擎的统计信息。
若不指定任何参数，则显示所有成员设备上的加密引擎统计信息。

【举例】

显示所有加密引擎统计信息。

```
<Sysname> display crypto-engine statistics
Slot ID: 1
CPU ID: 0
Crypto engine ID: 0
Submitted sessions: 0
Failed sessions: 0
Symmetric operations: 0
Symmetric errors: 0
Asymmetric operations: 0
Asymmetric errors: 0
Get-random operations: 0
Get-random errors: 0
```

显示指定 slot 上的加密引擎号为 1 的加密引擎统计信息。

```
<Sysname> display crypto-engine statistics engine-id 1 slot 1
Submitted sessions: 0
Failed sessions: 0
Symmetric operations: 0
Symmetric errors: 0
Asymmetric operations: 0
Asymmetric errors: 0
Get-random operations: 0
Get-random errors: 0
```

表1-2 display crypto-engine statistics 命令显示信息描述表

字段	描述
Crypto engine ID	加密引擎ID
Submitted sessions	已创建的会话数目
Failed sessions	创建失败的会话数目
Symmetric operations	加密引擎使用对称算法的操作次数
Symmetric errors	加密引擎使用对称算法操作失败的次数
Asymmetric operations	加密引擎使用非对称算法操作的次数
Asymmetric errors	加密引擎使用非对称算法操作失败的次数
Get-random operations	加密引擎获取随机数操作的次数
Get-random errors	加密引擎获取随机数操作失败的次数

【相关命令】

- **reset crypto-engine statistics**

1.1.3 reset crypto-engine statistics

reset crypto-engine statistics 命令用来清除加密引擎的统计信息。

【命令】

reset crypto-engine statistics [*engine-id engine-id slot slot-number*]

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

engine-id engine-id: 清除指定加密引擎的统计信息，*engine-id* 为加密引擎 ID 编号，取值范围为 0~4294967295。

slot slot-number: 清除指定成员设备上的加密引擎统计信息，*slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

若不指定任何参数，清除所有成员设备上的加密引擎统计信息。

【举例】

清除加密引擎的统计信息。

```
<Sysname> reset crypto-engine statistics
```

清除指定 slot 上的加密引擎号为 1 的加密引擎统计信息。

```
<Sysname> reset crypto-engine statistics engine-id 1 slot 1
```

【相关命令】

- **display crypto-engine statistics**

目 录

1 安全域	1-1
1.1 安全域配置命令	1-1
1.1.1 display security-zone	1-1
1.1.2 display zone-pair security	1-2
1.1.3 import interface	1-3
1.1.4 import interface vlan	1-3
1.1.5 import ip	1-4
1.1.6 import ipv6	1-5
1.1.7 security-zone	1-6
1.1.8 security-zone intra-zone default permit	1-7
1.1.9 zone-pair security	1-8
1.1.10 zone-pair vsip-filter enable	1-9

1 安全域

1.1 安全域配置命令

1.1.1 display security-zone

display security-zone 命令用来显示安全域信息，包括缺省安全域和自定义的安全域信息。

【命令】

display security-zone [name zone-name]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

name zone-name：安全域的名称，为 1~31 个字符的字符串，不区分大小写。若不指定本参数，则显示所有安全域的信息。

【使用指导】

安全域的显示顺序是先显示缺省安全域信息，再按照安全域名称的字母排序显示自定义的安全域信息。

【举例】

```
# 显示安全域 myZone 的信息。
<Sysname> display security-zone name myZone
Name: myZone
Members:
  Service path 2 reversed
  GigabitEthernet1/0/1
  GigabitEthernet1/0/2 in VLAN 3
  VLAN 150-200
  192.168.1.0 255.255.255.0
  192.168.0.0 255.255.0.0 vpn-instance abc
  1001:1002::0 32
```

表1-1 display security-zone 命令输出信息描述

字段	描述
Name	安全域名称

字段	描述
Members	安全域成员，包括以下几种取值： • 三层接口名称 • 二层以太网接口名称和所属的 VLAN 编号 • VLAN 编号 • 公网中的 IP 子网 • 公网中的 IPv6 子网 • VPN 中的 IP 子网 • VPN 中的 IPv6 子网 • None，该安全域中没有成员

1.1.2 display zone-pair security

display zone-pair security 命令用来显示已创建的所有域间实例的信息。

【命令】

display zone-pair security

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示所有安全域间实例的信息。

```
<Sysname> display zone-pair security
Source zone   Destination zone
DMZ           Local
Trust         Local
```

表1-2 display zone-pair security 命令输出信息描述

字段	描述
Source zone	源安全域名称
Destination zone	目的安全域名称

1.1.3 import interface

import interface 命令用来向安全域中添加三层接口成员，包括三层以太网接口、三层以太网子接口和其它三层逻辑接口。

undo import interface 命令用来从安全域中移除三层接口成员。

【命令】

```
import interface layer3-interface-type layer3-interface-number  
undo import interface layer3-interface-type layer3-interface-number
```

【缺省情况】

安全域中不存在三层接口成员。

【视图】

安全域视图

【缺省用户角色】

network-admin
context-admin

【参数】

layer3-interface-type layer3-interface-number: 指定添加到安全域的三层接口的接口类型和接口编号。

【使用指导】

缺省的安全域 **Local** 中不允许添加任何接口，其它缺省的安全域中允许添加接口。

可以通过多次执行本命令向同一个安全域添加多个三层接口成员。

一个三层接口只允许加入一个安全域。若要修改接口所属安全域时，需要执行以下操作：

- (1) 首先在相应安全域中使用 **undo import interface** 命令将相应接口从原安全域中删除。
- (2) 再使用 **import interface** 命令将其加入其它安全域。

【举例】

```
# 向安全域 Trust 中添加三层以太网接口 GigabitEthernet1/0/1。  
<Sysname> system-view  
[Sysname] security-zone name trust  
[Sysname-security-zone-Trust] import interface gigabitethernet 1/0/1
```

1.1.4 import interface vlan

import interface vlan 命令用来向安全域中添加二层接口和 VLAN 成员。

undo import interface vlan 命令用来从安全域中移除二层接口和 VLAN 成员。

【命令】

```
import interface layer2-interface-type layer2-interface-number vlan  
vlan-list  
undo import interface layer2-interface-type layer2-interface-number vlan  
vlan-list
```

【缺省情况】

安全域中不存在二层接口和 VLAN 成员。

【视图】

安全域视图

【缺省用户角色】

network-admin

context-admin

【参数】

layer2-interface-type layer2-interface-number: 指定添加到安全域的二层接口的接口类型和接口编号。

vlan *vlan-list*: 指定接口所属的 VLAN 列表。VLAN 列表表示多个 VLAN，表示方式为 *vlan-list* = { *vlan-id1* [**to** *vlan-id2*] } &<1-10>。其中，*vlan-id1*、*vlan-id2* 为已创建的 VLAN 编号。&<1-10>表示前面的参数最多可以输入 10 次。*vlan-id2* 必须大于 *vlan-id1*。VLAN ID 的取值范围为 1~4094。

【使用指导】

缺省的安全域 Local 中不允许添加任何接口或者 VLAN，其它缺省的安全域中允许添加接口和 VLAN。可以通过多次执行本命令，向安全域中添加多个二层接口和 VLAN 成员。

一个二层接口和所属的 VLAN 只允许加入一个安全域。若要修改接口或者 VLAN 所属安全域时，需要执行以下操作：

- (1) 首先在相应安全域中使用 **undo import interface vlan** 命令将相应接口或者 VLAN 从原安全域中删除。
- (2) 再使用 **import interface vlan** 命令将其加入其它安全域。

【举例】

```
# 向安全域 Untrust 中添加二层以太网接口 GigabitEthernet1/0/1 和对应的 VLAN 10。  
<Sysname> system-view  
[Sysname] security-zone name untrust  
[Sysname-security-zone-Untrust] import interface gigabitethernet 1/0/1 vlan 10
```

1.1.5 import ip

import ip 命令用来向安全域中添加 IPv4 子网成员。

undo import ip 命令用来从安全域中删除 IPv4 子网成员。

【命令】

```
import ip ip-address { mask-length | mask } [ vpn-instance vpn-instance-name ]  
undo import ip ip-address { mask-length | mask } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

安全域中不存在 IPv4 子网成员。

【视图】

安全域视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: 指定子网 IPv4 地址或主机地址。

mask-length: 表示子网的掩码长度，即掩码中连续“1”的个数，取值范围为 0~32。

mask: 表示 IPv4 子网相应的子网掩码，为点分十进制格式。

vpn-instance vpn-instance-name: 指定子网所属的 VPN 实例。**vpn-instance-name** 表示设备中存在的 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。不指定该参数时，表示子网位于公网中。

【使用指导】

缺省的安全域 Local 中不允许添加任何 IPv4 子网成员，其它缺省的安全域中允许添加 IPv4 子网成员。

可以通过多次执行本命令，向安全域中添加多个 IPv4 子网成员。

完全相同的子网不能添加到不同的安全域中，例如 1.1.1.1/24 与 1.1.1.2/24 相同，均对应 IPv4 子网 1.1.1.0/24，不能分别添加到不同安全域。

如果两个子网的网段有包含关系，例如 1.1.1.1/24 与 1.1.2.2/16，后者包含前者，但系统认为是两个不同子网，可以分别配置到同一安全域或者不同安全域。当配置到不同安全域时，报文最终将匹配掩码最长的子网所在的安全域。如 IP 地址为 1.1.1.3 的报文会匹配到 1.1.1.1/24 所在的安全域。

需要注意的是，在使用此种方式添加安全域成员时，为使动态路由协议建立成功，则必须将其使用的组播或广播地址加入安全域。

【举例】

添加地址为 192.168.1.0、掩码长度为 24 的 IPv4 子网到安全域 a。

```
<Sysname> system-view
```

```
[Sysname] security-zone name a
```

```
[Sysname-security-zone-a] import ip 192.168.1.0 24
```

添加地址为 192.168.2.1、掩码为 255.255.255.0 的 IPv4 子网到安全域 a。

```
<Sysname> system-view
```

```
[Sysname] security-zone name a
```

```
[Sysname-security-zone-a] import ip 192.168.2.1 255.255.255.0
```

添加地址为 192.168.2.1、掩码为 255.255.255.0、VPN 实例名为 abc 的 IPv4 子网到安全域 a。

```
<Sysname> system-view
```

```
[Sysname] security-zone name a
```

```
[Sysname-security-zone-a] import ip 192.168.2.1 255.255.255.0 vpn-instance abc
```

1.1.6 import ipv6

import ipv6 命令用来向安全域中添加 IPv6 子网成员。

undo import ipv6 命令用来从安全域中删除 IPv6 子网成员。

【命令】

```
import ipv6 ipv6-address prefix-length [ vpn-instance vpn-instance-name ]
undo import ipv6 ipv6-address prefix-length [ vpn-instance
vpn-instance-name ]
```

【缺省情况】

安全域中不存在 IPv6 子网成员。

【视图】

安全域视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address: 指定子网 IPv6 地址。

prefix-length: 指定 IPv6 地址的前缀长度，取值范围为 1~128。

vpn-instance vpn-instance-name: 指定子网所属的 VPN 实例。**vpn-instance-name** 表示设备中存在的 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。不指定该参数时，表示子网位于公网中。

【使用指导】

缺省的安全域 Local 中不允许添加任何 IPv6 子网成员，其它缺省的安全域中允许添加 IPv6 子网成员。

可以通过多次执行本命令，向安全域中添加多个 IPv6 子网成员。

完全相同的 IPv6 子网不能添加到不同的安全域中，例如 1:1:1::1/32 与 1:1:1::2/32 相同，均对应 IPv6 子网 1:1:1::0/32，不能分别添加到不同安全域。

如果两个子网的网段有包含关系，例如 1:1:1::0/48 与 1:1:1::0/32，后者包含前者，但系统会认为是两个不同子网，可以分别配置到同一安全域或者不同安全域。当配置到不同安全域时，报文最终将匹配前缀最长的子网所在的安全域。如 IP 地址为 1:1:1::2 的报文会匹配到 1:1:1::0/48 所在的安全域。

【举例】

将 IPv6 子网 1001:1002::0/32 添加到安全域 a。

```
<Sysname> system-view
```

```
[Sysname] security-zone name a
```

```
[Sysname-security-zone-a] import ipv6 1001:1002::1 32
```

将 VPN 实例 abc 中的 IPv6 子网 1001:1002::0/32 添加到安全域 a。

```
<Sysname> system-view
```

```
[Sysname] security-zone name a
```

```
[Sysname-security-zone-a] import ipv6 1001:1002::1 32 vpn-instance abc
```

1.1.7 security-zone

security-zone 命令用来创建安全域，并进入安全域视图。如果指定的安全域已经存在，则直接进入安全域视图。

undo security-zone 命令用来删除安全域。

【命令】

```
security-zone name zone-name  
undo security-zone name zone-name
```

【缺省情况】

存在安全域 Local、Trust、DMZ、Management 和 Untrust。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

name zone-name: 安全域的名称, 为 1~31 个字符的字符串, 不区分大小写, 不能是字符串“any”, 使用字符 “\” 和 “” 时需要使用转义字符\。

【使用指导】

当首次执行创建安全域或者创建域间策略有关的命令时, 系统会自动创建以下缺省安全域: Local、Trust、DMZ、Management 和 Untrust。

可通过多次执行本命令, 创建多个安全域。

删除一个安全域时, 以此安全域为源域或目的域的域间实例也会被删除, 而且在该域间实例上已经应用的域间策略会被自动解除应用。缺省安全域不能被删除。

【举例】

```
# 创建安全域 zonetest, 并进入该安全域视图。  
<Sysname> system-view  
[Sysname] security-zone name zonetest  
[Sysname-security-zone-zonetest]
```

【相关命令】

- **display security-zone**

1.1.8 security-zone intra-zone default permit

security-zone intra-zone default permit 命令用来配置同一安全域内接口间报文处理的缺省动作为允许。

undo security-zone intra-zone default permit 命令用来恢复缺省情况。

【命令】

```
security-zone intra-zone default permit  
undo security-zone intra-zone default permit
```

【缺省情况】

同一安全域内报文过滤的缺省动作为拒绝。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

对于同一安全域内接口间的报文，若设备上不存在当前域到当前域的域间策略，设备缺省会将其拒绝，可以通过配置安全域内接口间报文处理的缺省动作为允许来放行报文。

【举例】

配置同一安全域内接口间报文处理的缺省动作为允许。

```
<Sysname> system-view
```

```
[Sysname] security-zone intra-zone default permit
```

1.1.9 zone-pair security

zone-pair security 命令用来创建安全域间实例，并进入安全域间实例视图。如果指定的安全域实例已经存在，则直接进入安全域实例视图。

undo zone-pair security 命令用来删除指定的安全域间实例。

【命令】

```
zone-pair security source { source-zone-name | any } destination  
{ destination-zone-name | any }
```

```
undo zone-pair security source { source-zone-name | any } destination  
{ destination-zone-name | any }
```

【缺省情况】

不存在安全域间实例。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

source *source-zone-name*: 源安全域的名称，为 1~31 个字符的字符串，不区分大小写。指定的安全域必须已存在。

destination *destination-zone-name*: 目的安全域的名称，为 1~31 个字符的字符串，不区分大小写。指定的安全域必须已存在。

any: 表示任意安全域。

【使用指导】

安全域间实例用于指定域间策略（如 ASPF 策略、安全策略等）需要检测的业务流的源安全域和目的安全域，它们分别描述了经过网络设备的业务流的首包要进入的安全域和要离开的安全域。在安全域间实例上应用域间策略可实现对指定业务流进行域间策略检查。

有具体安全域的安全域间实例的匹配优先级高于 **any** 到 **any** 的安全域间实例。

Management 和 Local 安全域间之间的报文只能匹配 Management 与 Local 之间的安全域间实例。

删除安全域间实例后，在域间实例上已经应用的域间策略将不生效，对应的引用关系同时被取消。

【举例】

创建源安全域 Trust 到目的安全域 Untrust 的安全域间实例。

```
<Sysname> system-view
[Sysname] zone-pair security source trust destination untrust
[Sysname-zone-pair-security-Trust-Untrust]
```

【相关命令】

- **display zone-pair security**

1.1.10 zone-pair vsip-filter enable

zone-pair vsip-filter enable 命令用来在安全域间实例上开启 SLB 虚服务 IP 过滤功能。

undo zone-pair vsip-filter enable 命令在安全域间实例上关闭 SLB 虚服务 IP 过滤功能。

【命令】

```
zone-pair vsip-filter enable
undo zone-pair vsip-filter enable
```

【缺省情况】

安全域间 LB 虚服务 IP 过滤功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

该功能一般应用在 SLB 业务的安全域间实例处理流程中。对于通过虚服务 IP 从外部网络访问内部网络的流量，当该功能处于关闭状态时，设备使用实服务器 IP 匹配包过滤规则中的目的 IP；当该功能处于开启状态时，设备使用虚服务 IP 匹配包过滤规则中的目的 IP。

【举例】

应用 IPv4 高级 ACL 3000 对源安全域 Untrust 到目的安全域 DMZ 的报文进行过滤，允许目的 IP 为 SLB 虚服务地址 10.10.10.10 的报文通过，并开启域间 SLB 虚服务地址过滤功能。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source any destination 10.10.10.10 0
```

```
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] zone-pair security source untrust destination dmz
[Sysname-zone-pair-security-Untrust-DMZ] packet-filter 3000
[Sysname-zone-pair-security-Untrust-DMZ] quit
[Sysname] zone-pair vsip-filter enable
```

目 录

1 安全策略.....	1-1
1.1 安全策略配置命令.....	1-1
1.1.1 accelerate enhanced enable	1-1
1.1.2 action.....	1-2
1.1.3 app-group	1-2
1.1.4 application	1-3
1.1.5 counting enable.....	1-4
1.1.6 description (security-policy rule view)	1-5
1.1.7 description (security-policy view).....	1-5
1.1.8 destination-ip	1-6
1.1.9 destination-zone	1-7
1.1.10 disable.....	1-8
1.1.11 display security-policy	1-8
1.1.12 display security-policy statistics	1-10
1.1.13 group move	1-11
1.1.14 group name	1-12
1.1.15 group rename.....	1-13
1.1.16 logging enable.....	1-14
1.1.17 move rule	1-15
1.1.18 parent-group	1-15
1.1.19 profile	1-16
1.1.20 reset security-policy statistics.....	1-17
1.1.21 rule	1-17
1.1.22 security-policy	1-18
1.1.23 security-policy config-logging send-time	1-19
1.1.24 security-policy disable	1-20
1.1.25 service.....	1-20
1.1.26 session aging-time	1-21
1.1.27 session persistent aging-time.....	1-22
1.1.28 source-ip	1-23
1.1.29 source-mac.....	1-24
1.1.30 source-zone.....	1-25
1.1.31 time-range	1-26

1.1.32 track.....	1-26
1.1.33 user	1-27
1.1.34 user-group.....	1-28
1.1.35 vrf.....	1-29

1 安全策略

1.1 安全策略配置命令

1.1.1 accelerate enhanced enable

accelerate enhanced enable 命令用来激活安全策略规则的加速功能。

【命令】

accelerate enhanced enable

【视图】

IPv4 安全策略视图

IPv6 安全策略视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

安全策略加速功能生效后，使用激活规则的加速功能可以使后续新增或修改规则的加速功能生效。激活规则的加速功能包括如下方式：

- 手动激活：是指新增或修改规则后，手动执行 **accelerate enhanced enable** 命令使这些规则立即加速。
- 自动激活：是指设备按照固定时间间隔进行周期性判断是否需要安全策略加速，在一个时间间隔内若安全策略的过滤条件发生变化，则间隔时间到达后会进行安全策略加速，否则，不会进行加速。当每种类型安全策略规则小于等于 100 条时，此时间间隔为 2 秒；当每种类型安全策略规则大于 100 条时，此时间间隔为 20 秒。这种方式能够避免因忘记手工激活规则而导致新增或修改规则不生效的问题。

安全策略的加速功能默认开启，且不能手动关闭。但是激活安全策略规则加速功能时，内存资源不足会导致安全策略加速失效。

安全策略加速失效后，设备无法对报文进行快速匹配，但是仍然可以进行原始的慢速匹配。

为使新增或修改的规则可以对报文进行匹配，必须激活这些规则的加速功能。

若安全策略规则中指定的 IP 地址对象组中包含用户或用户组，则此条安全策略规则失效，将无法匹配任何报文。

安全策略规则中引用对象组的内容发生变化后，也需要重新激活该规则的加速功能。

【举例】

激活安全策略规则的加速功能。

```
<Sysname> system-view
```

```
[Sysname] security-policy ip
```

```
[Sysname-security-policy-ip] accelerate enhanced enable
```

1.1.2 action

action 命令用来配置安全策略规则的动作。

【命令】

action { drop | pass }

【缺省情况】

安全策略规则动作是丢弃。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

drop: 表示丢弃符合条件的报文。

pass: 表示允许符合条件的报文通过。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

为安全策略规则 **rule1** 配置动作为丢弃。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] action drop
```

【相关命令】

- **display security-policy**

1.1.3 app-group

app-group 命令用来配置作为安全策略规则过滤条件的应用组。

undo app-group 命令用来删除作为安全策略规则过滤条件的应用组。

【命令】

app-group app-group-name

undo app-group [app-group-name]

【缺省情况】

不存在应用组过滤条件。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin
context-admin

【参数】

app-group-name: 表示应用组的名称，为 1~63 个字符的字符串，不区分大小写，且不能为字符串 invalid 和 other。使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有应用组类型的过滤条件。有关应用组的详细介绍，请参见“安全配置指导”中的“APR”。

【使用指导】

多次执行本命令，可配置多个应用组作为安全策略规则的过滤条件。

【举例】

```
# 配置作为安全策略规则 rule1 过滤条件的应用组为 app1 和 app2。  
<Sysname> system-view  
[Sysname] security-policy ip  
[Sysname-security-policy-ip] rule 0 name rule1  
[Sysname-security-policy-ip-0-rule1] app-group app1  
[Sysname-security-policy-ip-0-rule1] app-group app2
```

【相关命令】

- **app-group**（安全命令参考/APR）
- **display security-policy**

1.1.4 application

application 命令用来配置作为安全策略规则过滤条件的应用。

undo application 命令用来删除作为安全策略规则过滤条件的应用。

【命令】

```
application application-name  
undo application [application-name ]
```

【缺省情况】

不存在应用过滤条件。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin
context-admin

【参数】

application-name: 表示应用的名称，为 1~63 个字符的字符串，不区分大小写，且不能为字符串 invalid 和 other。使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有应用类型的过滤条件。有关应用的详细介绍，请参见“安全配置指导”中的“APR”。

【使用指导】

多次执行本命令，可配置多个应用作为安全策略规则的过滤条件。

为使安全策略中配置的应用可以被识别，必须先放行应用所依赖的基础协议报文。

在端口仿冒网络环境中，必须先放行仿冒的基础协议报文，才能识别出仿冒报文中的应用。

【举例】

配置作为安全策略规则 rule1 过滤条件的应用为 139Mail 和 51job。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] application 139Mail
[Sysname-security-policy-ip-0-rule1] application 51job
```

【相关命令】

- **display security-policy**
- **nbar application**（安全命令参考/APR）
- **port-mapping**（安全命令参考/APR）

1.1.5 counting enable

counting enable 命令用来开启安全策略规则匹配统计功能。

undo counting enable 命令用来关闭安全策略规则匹配统计功能。

【命令】

```
counting enable
undo counting enable
```

【缺省情况】

安全策略规则匹配统计功能处于关闭状态。

【视图】

安全策略规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

此功能用来对匹配安全策略规则的报文进行统计，可通过执行 **display security-policy statistics** 命令来查看相关报文的统计信息。

【举例】

为安全策略规则 rule1 开启规则匹配统计功能。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] counting enable
```

【相关命令】

- **display security-policy**
- **display security-policy statistics**

1.1.6 description (security-policy rule view)

description 命令用来配置安全策略规则的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description text

undo description

【缺省情况】

不存在安全策略规则的描述信息。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: 表示安全策略规则的描述信息，为 1~127 个字符的字符串，区分大小写。

【举例】

为 IPv4 安全策略规则 0 配置描述信息为 This rule is used for source-ip ip1。

```
<Sysname> system-view
```

```
[Sysname] security-policy ip
```

```
[Sysname-security-policy-ip] rule 0 name rule1
```

```
[Sysname-security-policy-ip-0-rule1] description This rule is used for source-ip ip1
```

【相关命令】

- **display security-policy ip**
- **display security-policy ipv6**

1.1.7 description (security-policy view)

description 命令用来配置安全策略的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description text

undo description

【缺省情况】

不存在安全策略的描述信息。

【视图】

IPv4 安全策略视图

IPv6 安全策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: 表示安全策略的描述信息，为 1~127 个字符的字符串，区分大小写。

【举例】

配置安全策略的描述信息为 “zone-pair security office to library”。

```
<Sysname> system-view
```

```
[Sysname] security-policy ip
```

```
[Sysname-security-policy-ip] description zone-pair security office to library
```

【相关命令】

- **display security-policy**

1.1.1.8 destination-ip

destination-ip 命令用来配置作为安全策略规则过滤条件的目的 IP 地址。

undo destination-ip 命令用来删除作为安全策略规则过滤条件的目的 IP 地址。

【命令】

destination-ip *object-group-name*

undo destination-ip [*object-group-name*]

【缺省情况】

不存在目的 IP 地址过滤条件。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-group-name: 表示目的地址对象组的名称，为 1~31 个字符的字符串，不区分大小写，且不能为字符串 **any**。使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有目的 IP 地址类型的过滤条件。有关地址对象组的详细介绍，请参见“安全配置指导”中的“对象组”。

【使用指导】

多次执行本命令，可配置多个目的 IP 地址作为安全策略规则的过滤条件。

配置目的 IP 地址作为安全策略规则的过滤条件时，若指定的地址对象组不存在，该配置仍会配置成功，同时也会在系统中创建一个名称为指定名称的空配置地址对象组，但此条过滤条件不会匹配任何报文。

【举例】

配置作为安全策略规则 rule1 过滤条件的目的地址对象组为 client1 和 client2。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] destination-ip client1
[Sysname-security-policy-ip-0-rule1] destination-ip client2
```

【相关命令】

- **display security-policy**
- **object-group**（安全命令参考/对象组）

1.1.9 destination-zone

destination-zone 命令用来配置作为安全策略规则过滤条件的目的安全域。

undo destination-zone 命令用来删除作为安全策略规则过滤条件的目的安全域。

【命令】

```
destination-zone destination-zone-name
undo destination-zone [destination-zone-name ]
```

【缺省情况】

不存在目的安全域过滤条件。

【视图】

安全策略规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

destination-zone-name: 表示目的安全域的名称，为 1~31 个字符的字符串，不区分大小写。使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有目的安全域类型的过滤条件。有关安全域的详细介绍，请参见“安全配置指导”中的“安全域”。

【使用指导】

多次执行本命令，可配置多个目的安全域作为安全策略规则的过滤条件。

【举例】

配置作为安全策略规则 rule1 过滤条件的目的安全域为 Trust 和 server。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
```

```
[Sysname-security-policy-ip-0-rule1] destination-zone trust
[Sysname-security-policy-ip-0-rule1] destination-zone server
```

【相关命令】

- **display security-policy**
- **security-zone**（安全命令参考/安全域）

1.1.10 disable

disable 命令用来禁用安全策略规则。

undo disable 命令用来启用安全策略规则。

【命令】

```
disable
undo disable
```

【缺省情况】

安全策略规则处于启用状态。

【视图】

安全策略规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 禁用安全策略规则 rule1。
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] disable
```

【相关命令】

- **display security-policy**

1.1.11 display security-policy

display security-policy 命令用来显示安全策略的配置信息。

【命令】

```
display security-policy { ip | ipv6 }
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```


context-admin
context-operator

【参数】

ip: 表示显示 IPv4 安全策略的配置信息。
ipv6: 表示显示 IPv6 安全策略的配置信息。

【举例】

显示 IPv4 安全策略的配置信息。
<Sysname> display security-policy ip
Security-policy ip

```
rule 0 name der (Inactive)
  action pass
  profile er
  vrf re
  logging enable
  counting enable
  time-range dere
  track positive 23
  session aging-time 5000
  session persistent aging-time 2400
  source-zone trust
  destination-zone trust
  source-ip erer
  destination-ip client1
  service ftp
  app-group ere
  application 110Wang
  user der
  user-group ere
```

表1-1 display security-policy 命令显示信息描述表

字段	描述
rule <i>id</i> name <i>rule-name</i>	表示规则的ID和名称
action pass	表示规则动作，其取值如下： - pass: 表示允许报文通过 - drop: 表示丢弃报文
profile <i>app-profile-name</i>	表示引用的DPI应用profile
vrf <i>vrf-name</i>	表示MPLS L3VPN的VPN实例名称
logging enable	表示开启了对符合规则过滤条件的报文记录日志信息的功能
counting enable	表示开启了安全策略规则匹配统计的功能
time-range <i>time-range-name</i>	表示此规则生效的时间段

字段	描述
track negative 1 (Active)	表示安全策略规则生效状态与Track项的Negative状态关联，且此规则的状态为Active，规则的生效状态取值包括： - Active：表示生效状态 - Inative：表示禁用状态
track positive 1 (Inactive)	表示安全策略规则生效状态与Track项的Positive或NotReady状态关联，且此规则的状态为Active，规则的生效状态取值包括： - Active：表示生效状态 - Inative：表示禁用状态
session aging-time <i>time-value</i>	表示此规则中设置的会话老化时间，单位为秒
session persistent aging-time <i>time-value</i>	表示此规则中设置的长连接会话的老化时间，单位为小时
source-zone <i>zone-name</i>	表示规则配置了源安全域作为过滤条件
destination-zone <i>zone-name</i>	表示规则配置了目的安全域作为过滤条件
source-ip <i>object-group-name</i>	表示规则配置了源IP地址作为过滤条件
destination-ip <i>object-group-name</i>	表示规则配置了目的IP地址作为过滤条件
service <i>object-group-name</i>	表示规则配置了服务作为过滤条件
app-group <i>app-group-name</i>	表示规则配置了应用组作为过滤条件
application <i>application-name</i>	表示规则配置了应用作为过滤条件
user <i>user-name</i>	表示规则配置了用户作为过滤条件
user-group <i>user-group-name</i>	表示规则配置了用户组作为过滤条件

【相关命令】

- security-policy ip
- security-policy ipv6

1.1.12 display security-policy statistics

display security-policy statistics 命令用来显示安全策略的统计信息。

【命令】

display security-policy statistics { ip | ipv6 } [rule *rule-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ip: 表示显示 IPv4 安全策略的统计信息。

ipv6: 表示显示 IPv6 安全策略的统计信息。

rule rule-name: 表示显示指定安全策略规则的统计信息。*rule-name* 是安全策略规则的名称，为 1~127 个字符的字符串，不区分大小写。若不指定此参数，则显示指定 IP 类型的所有安全策略统计信息。

【举例】

显示 IPv4 安全策略下名称为 **abc** 的规则统计信息。

```
<Sysname> display security-policy statistics ip rule abc
IPv4 security policy rule: abc
Action: pass (5 packets, 1000 bytes)
```

表1-2 display security-policy statistics 命令显示信息描述表

字段	描述
IPv4 security policy rule <i>name</i>	IPv4安全策略规则，名称为 <i>name</i>
Action	表示安全策略规则动作，其取值包括如下： - pass: 表示允许报文通过 - drop: 表示丢弃报文
x packets, y bytes	该安全策略规则匹配x个报文，共y字节（本字段仅在配置安全策略规则配置了 counting enable 或 logging enable 命令时显示，当未匹配任何报文时不显示本字段）

【相关命令】

- reset security-policy statistics

1.1.13 group move

group move group-name1 { after | before } { group group-name2 | rule rule-name }
命令用来移动安全策略组。

【命令】

group move group-name1 { after | before } { group group-name2 | rule rule-name }

【视图】

安全策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

group-name1: 表示需要被移动的安全策略组的名称，为 1~63 个字符的字符串，不区分大小写。

after: 表示将安全策略组 *group-name1* 移动到安全策略组 *group-name2* 或安全策略规则 *rule-name* 之后。

before: 表示将安全策略组 *group-name1* 移动到安全策略组 *group-name2* 或安全策略规则 *rule-name* 之前。

group group-name2: 表示目标安全策略组的名称，为 1~63 个字符的字符串，不区分大小写。

rule rule-name: 表示目标安全策略规则的名称，为 1~127 个字符的字符串，不区分大小写。

【使用指导】

通过移动安全策略组可以批量改变安全策略规则的优先级。

如果目标安全策略规则已经属于其他安全策略组，按照其在安全策略组中的位置，受如下原则的约束。

- 如果规则位于策略组中间位置，则不能移动。
- 如果规则位于策略组开始位置，只可以移动到目标规则之前。
- 如果规则位于策略组结束位置，只可以移动到目标规则之后。

【举例】

将安全策略组 *group1* 移动到安全策略组 *group2* 之前。

```
<Sysname> system-view
```

```
[Sysname] security-policy ip
```

```
[Sysname-security-policy-ip] group move group1 before group group2
```

1.1.14 group name

group name 命令用来创建安全策略组，并将指定的安全策略规则加入此安全策略组。如果指定的安全策略组已经存在，则将指定的安全策略规则加入此安全策略组。

undo group name 命令用来删除安全策略组。

【命令】

```
group name group-name [ from rule-name1 to rule-name2 ] [ description  
description-text ] [ disable | enable ]
```

```
undo group name group-name [ description | include-member ]
```

【缺省情况】

不存在安全策略组。

【视图】

安全策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name: 表示安全策略组的名称，为 1~63 个字符的字符串，不区分大小写。

from rule-name1: 表示加入安全策略组规则的起始规则，*rule-name1* 是安全策略规则的名称，为 1~127 个字符的字符串，不区分大小写。若不指定本参数，则表示创建空的安全策略组。

to rule-name2: 表示加入安全策略组规则的结束规则，*rule-name2* 是安全策略规则的名称，为 1~127 个字符的字符串，不区分大小写。

description description-text: 表示安全策略组的描述信息，为 1~127 个字符的字符串，区分大小写。缺省情况下，安全策略组不存在描述信息。

disable: 表示禁用安全策略组。

enable: 表示启用安全策略组，安全策略组缺省处于启用状态。

include-member: 执行 **undo** 命令行时，若指定本参数，则表示删除安全策略组及其策略组中的所有安全策略规则。

【使用指导】

安全策略组可以实现对安全策略规则的批量操作，例如批量启用、禁用、删除和移动安全策略规则。将安全策略规则加入安全策略组时，会将指定范围内若干连续的安全策略规则加入同一个安全策略组。

只有当安全策略规则及其所属的安全策略组均处于启用状态时，安全策略规则才能生效。

将安全策略规则加入安全策略组时，起始规则要在结束规则前面，并且起始规则和结束规则之间的规则不能属于其他安全策略组。

执行 **undo** 命令行时的具体功能如下：

- **undo group name group-name** 命令用来仅删除安全策略组，但不删除策略组中的规则。
- **undo group name group-name description** 命令用来仅删除安全策略组的描述信息。
- **undo group name group-name include-member** 命令用来删除安全策略组及其策略组中的所有规则。

【举例】

创建一个名称为 **group1** 的安全策略组，并将安全策略规则 **rule-name1** 到 **rule-name10** 之间的所有安全策略规则加入此安全策略组，其描述信息为 **marketing**。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] group name group1 from rule-name1 to rule-name10 enable
description marketing
```

1.1.15 group rename

group rename 命令用来重命名安全策略组。

【命令】

group rename old-name new-name

【视图】

安全策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

old-name: 表示安全策略组的原有名称，为 1~63 个字符的字符串，不区分大小写。

new-name: 表示安全策略组的新名称，为 1~63 个字符的字符串，不区分大小写。

【举例】

把安全策略组 group1 重命名为 group2。

```
<Sysname> system-view
```

```
[Sysname] security-policy ip
```

```
[Sysname-security-policy-ip] group rename group1 group2
```

1.1.16 logging enable

logging enable 命令用来开启安全策略规则记录日志的功能。

undo logging enable 命令用来关闭安全策略规则记录日志的功能。

【命令】

logging enable

undo logging enable

【缺省情况】

安全策略规则记录日志的功能处于关闭状态。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启此功能后，设备对匹配规则的报文生成安全策略日志信息，此日志信息将会被交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。

安全策略日志不会输出到控制台和监视终端。当信息中心配置的规则将安全策略日志输出到控制台和监视终端时，若仍需要查看安全策略日志，可通过执行 **display logbuffer** 命令或在 Web 页面中查看。有关信息中心和 **display logbuffer** 命令的详细描述，请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

在安全策略规则 rule1 中开启安全策略规则记录日志的功能。

```
<Sysname> system-view
```

```
[Sysname] security-policy ip
```

```
[Sysname-security-policy-ip] rule 0 name rule1
```

```
[Sysname-security-policy-ip-0-rule1] logging enable
```

【相关命令】

- **display security-policy**

1.1.17 move rule

move rule 命令用来移动安全策略规则。

【命令】

move rule *rule-id* **before** *insert-rule-id*

【视图】

IPv4 安全策略视图

IPv6 安全策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-id: 指定待移动安全策略规则的编号，取值范围为 0～65534。

insert-rule-id: 表示移动到指定编号的规则之前，取值范围为 0～65535，其中指定编号为 65535 时表示移动到所有规则之后。

【使用指导】

如果 *insert-rule-id* 与 *rule-id* 相同或其指定的规则不存在，则不执行任何移动操作。

【举例】

在 IPv4 安全策略上，将安全策略规则 5 移动到规则 2 之前。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] move rule 5 before 2
```

【相关命令】

- **rule**
- **security-policy ip**
- **security-policy ipv6**

1.1.18 parent-group

parent-group *group-name* 命令用来配置安全策略规则所属的安全策略组。

undo parent-group 命令用来恢复缺省情况。

【命令】

parent-group *group-name*

undo parent-group

【缺省情况】

安全策略规则不属于安全策略组。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin
context-admin

【参数】

group-name: 表示安全策略规则需要加入的安全策略组的名称，为 1～63 个字符的字符串，不区分大小写。

【举例】

```
# 配置安全策略规则 rule1 属于安全策略组 group1。  
<Sysname> system-view  
[Sysname] security-policy ip  
[Sysname-security-policy-ip] rule 1 name rule1  
[Sysname-security-policy-ip-1-rule1] parent-group group1
```

1.1.19 profile

profile 命令用来在安全策略规则中引用 DPI 应用 profile。

undo profile 命令用来删除在安全策略规则中引用的 DPI 应用 profile。

【命令】

```
profile app-profile-name  
undo profile
```

【缺省情况】

安全策略规则中未引用 DPI 应用 profile。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin
context-admin

【参数】

app-profile-name: 表示 DPI 应用 profile 的名称，为 1～63 个字符的字符串，不区分大小写。
有关 DPI 应用 profile 的详细介绍，请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

【使用指导】

通过在安全策略规则中引用 DPI 应用 profile 可实现对符合安全策略过滤条件的报文进行相关 DPI 业务的处理。有关 DPI 各业务的详细介绍，请参见“DPI 深度安全配置指导”中的相关模块。

此命令仅在安全策略规则动作为允许的情况下才生效。

【举例】

```
# 在 IPv4 安全策略规则 rule1 中引用名称为 p1 的 DPI 应用 profile。  
<Sysname> system-view  
[Sysname] security-policy ip  
[Sysname-security-policy-ip] rule 0 name rule1
```



```
[Sysname-security-policy-ip-0-rule1] action pass
[Sysname-security-policy-ip-0-rule1] profile p1
```

【相关命令】

- **action pass**
- **app-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **display security-policy ip**

1.1.20 reset security-policy statistics

reset security-policy statistics 命令用来清除安全策略的统计信息。

【命令】

```
reset security-policy statistics [ ip | ipv6 ] [ rule rule-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip: 表示清除 IPv4 安全策略的统计信息。

ipv6: 表示清除 IPv6 安全策略的统计信息。

rule rule-name: 表示清除安全策略规则的统计信息。*rule-name* 是安全策略规则的名称，为 1~127 个字符的字符串，不区分大小写。

【使用指导】

若未指定任何参数，则清除所有安全策略的统计信息。

【举例】

清除 IPv4 安全策略下名称为 **abc** 的规则统计信息。

```
<Sysname> reset security-policy statistics ip rule abc
```

【相关命令】

- **display security-policy statistics**

1.1.21 rule

rule 命令用来创建安全策略规则，并进入安全策略规则视图。如果指定的安全策略规则已经存在，则直接进入安全策略规则视图。

undo rule 命令用来删除指定的安全策略规则。

【命令】

```
rule { rule-id | [ rule-id ] name rule-name }
undo rule { rule-id | name rule-name } *
```

【缺省情况】

不存在安全策略规则。

【视图】

IPv4 安全策略视图

IPv6 安全策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-id: 指定安全策略规则的编号，取值范围为 0~65534。若未指定本参数，系统将从 0 开始，自动分配一个大于现有最大编号的最小编号，步长为 1。若新编号超出了编号上限（65534），则选择当前未使用的最小编号作为新的编号。

rule-name: 表示安全策略规则的名称，为 1~127 个字符的字符串，不区分大小写，且全局唯一，不能为 default，创建规则时必须配置名称。

【举例】

为 IPv4 安全策略创建规则 0，并为该规则配置规则名称为 rule1。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1]
```

【相关命令】

- **display security-policy ip**
- **display security-policy ipv6**

1.1.22 security-policy

security-policy 命令用来进入安全策略视图。

undo security-policy 命令用来删除安全策略视图下面的所有配置。

【命令】

```
security-policy { ip | ipv6 }
undo security-policy { ip | ipv6 }
```

【缺省情况】

安全策略视图下不存在配置。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip: 表示 IPv4 安全策略视图。

ipv6: 表示 IPv6 安全策略视图。

【举例】

进入 IPv4 安全策略视图。

```
<Sysname> system-view
```

```
[Sysname] security-policy ip
```

```
[Sysname-security-policy-ip]
```

【相关命令】

- **display security-policy**

1.1.23 security-policy config-logging send-time

security-policy config-logging send-time 命令用来配置每天发送安全策略内容日志的时间。

undo security-policy config-logging send-time 命令用来恢复缺省情况。

【命令】

```
security-policy config-logging send-time time
```

```
undo security-policy config-logging send-time
```

【缺省情况】

发送安全策略内容日志的时间为每天的零点。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

time: 配置每天发送安全策略内容日志的时间, *time* 的格式为 hh:mm, 取值范围为 00:00~23:59。

【使用指导】

在快速日志输出模块中开启生成安全策略国家电网日志功能后（即执行 **customlog format security-policy sgcc** 命令），设备会在每天指定的时间以国家电网日志的格式发送此时所有处于生效状态安全策略规则的配置信息。有关快速日志输出的详细介绍，请参见“网络管理和监控配置指导”中的“快速日志输出”。

【举例】

配置每天发送安全策略内容日志的时间为 13 点 15 分。

```
<Sysname>system-view
```

```
[Sysname] security-policy config-logging send-time 13:15
```

【相关命令】

- **customlog format security-policy sgcc**（网络管理和监控命令参考/快速日志输出）
- **customlog host export security-policy**（网络管理和监控命令参考/快速日志输出）

1.1.24 security-policy disable

security-policy disable 命令用来关闭安全策略功能。

undo security-policy disable 命令用来开启安全策略功能。

【命令】

```
security-policy disable
undo security-policy disable
```

【缺省情况】

安全策略功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

只有开启安全策略功能后，配置的安全策略才能生效。

【举例】

```
# 关闭安全策略功能
<Sysname> system-view
[Sysname] security-policy disable
```

1.1.25 service

service 命令用来配置作为安全策略规则过滤条件的服务。

undo service 命令用来删除作为安全策略规则过滤条件的服务。

【命令】

```
service { object-group-name | any }
undo service [ object-group-name | any ]
```

【缺省情况】

不存在服务过滤条件。

【视图】

安全策略规则视图

【缺省用户角色】

```
network-admin
```

context-admin

【参数】

object-group-name: 表示服务对象组的名称，为 1~31 个字符的字符串，不区分大小写。

any: 表示将设备中的所有服务作为安全策略规则的过滤条件。

【使用指导】

多次执行本命令，可配置多个服务对象组作为安全策略规则的过滤条件。

配置服务作为安全策略规则的过滤条件时，若指定的服务对象组不存在，该配置仍会配置成功，同时也会在系统中创建一个名称为指定名称的空配置服务对象组，但此条过滤条件不会匹配任何报文。

使用 **undo** 命令时若不指定任何参数，则表示删除此规则中所有服务类型的过滤条件。

【举例】

配置作为安全策略规则 rule1 过滤条件的服务对象组为 http 和 ftp。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] service http
[Sysname-security-policy-ip-0-rule1] service ftp
```

【相关命令】

- **display security-policy**
- **object-group**（安全命令参考/对象组）

1.1.26 session aging-time

session aging-time 命令用来为安全策略规则配置会话的老化时间。

undo session aging-time 命令用来恢复缺省情况。

【命令】

```
session aging-time time-value
undo session aging-time
```

【缺省情况】

未配置安全策略规则的会话老化时间。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin
context-admin

【参数】

time-value: 指定会话的老化时间，取值范围为 1~2000000，单位为秒。

【使用指导】

此命令用来为匹配某条安全策略规则而生成的稳态会话设置老化时间。且此命令的配置仅影响后续生成的会话，对于已经生效的会话不产生作用。

若某安全策略规则中配置了会话的老化时间，则匹配上该规则且进入稳定状态的会话需要遵循规则中配置的老化时间进行老化；非稳态会话按照缺省的会话老化时间（1 小时）进行老化。

若进入稳态的会话报文匹配上的安全策略规则中未配置会话老化时间，则该会话基于会话管理模块配置的老化时间（**session aging-time application** 和 **session aging-time state** 命令的配置）进行老化。有关会话管理相关配置的详细介绍，请参见“安全配置指导”中的“会话管理”。

【举例】

为 IPv4 安全策略的规则 rule1 配置会话老化时间为 5000 秒。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] action pass
[Sysname-security-policy-ip-0-rule1] session aging-time 5000
```

【相关命令】

- **display security-policy**
- **session aging-time application**（安全命令参考/会话管理）
- **session aging-time state**（安全命令参考/会话管理）
- **session persistent acl**（安全命令参考/会话管理）

1.1.27 session persistent aging-time

session persistent aging-time 命令用来为安全策略规则配置长连接会话的老化时间。

undo session persistent aging-time 命令用来恢复缺省情况。

【命令】

```
session persistent aging-time time-value
undo session persistent aging-time
```

【缺省情况】

未配置安全策略规则的长连接会话老化时间。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

time-value：指定长连接会话的老化时间，取值范围为 0～24000，单位为小时，0 表示永不老化。

【使用指导】

此命令用来为匹配某条安全策略规则而生成的长连接会话设置老化时间。且此命令的配置仅影响后续生成的会话，对于已经生效的会话不产生作用。

此命令配置的长连接会话老化时间优先级高于 **session aging-time** 命令配置的会话老化时间和会话管理模块 **session persistent acl** 命令配置的长连接老化时间。有关 **session persistent acl** 命令的详细介绍，请参见“安全命令参考”中的“会话管理”。

长连接老化时间仅在 TCP 会话进入稳态（TCP-EST 状态）时生效。

【举例】

为 IPv4 安全策略中规则 rule1 配置长连接会话老化时间为 1 小时。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] action pass
[Sysname-security-policy-ip-0-rule1] session persistent aging-time 1
```

【相关命令】

- **display security-policy ip**
- **session persistent acl**（安全命令参考/会话管理）

1.1.28 source-ip

source-ip 命令用来配置作为安全策略规则过滤条件的源 IP 地址。

undo source-ip 命令用来删除作为安全策略规则过滤条件的源 IP 地址。

【命令】

```
source-ip object-group-name
undo source-ip [object-group-name ]
```

【缺省情况】

不存在源 IP 地址过滤条件。

【视图】

安全策略规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

object-group-name: 表示源地址对象组的名称，为 1~31 个字符的字符串，不区分大小写，且不能为字符串 any。使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有源 IP 地址类型的过滤条件。有关地址对象组的详细介绍，请参见“安全配置指导”中的“对象组”。

【使用指导】

多次执行本命令，可配置多个源 IP 地址作为安全策略规则的过滤条件。

配置源 IP 地址作为安全策略规则的过滤条件时,若指定的地址对象组不存在,该配置仍会配置成功,同时也会在系统中创建一个名称为指定名称的空配置地址对象组,但此条过滤条件不会匹配任何报文。

【举例】

配置作为安全策略规则 rule1 过滤条件的源地址对象组为 server1 和 server2。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] source-ip server1
[Sysname-security-policy-ip-0-rule1] source-ip server2
```

【相关命令】

- **display security-policy**
- **object-group** (安全命令参考/对象组)

1.1.29 source-mac

source-mac 命令用来配置作为安全策略规则过滤条件的源 MAC 地址。

undo source-mac 命令用来删除作为安全策略规则过滤条件的源 MAC 地址。

【命令】

```
source-mac object-group-name
undo source-mac [object-group-name ]
```

【缺省情况】

安全策略规则中不存在过滤条件。

【视图】

IPv4 安全策略规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

object-group-name: 表示源 MAC 地址对象组的名称,为 1~31 个字符的字符串,不区分大小写,且不能为字符串 any。使用 **undo** 命令时若不指定此参数,则表示删除此规则中所有源 MAC 地址类型的过滤条件。有关 MAC 地址对象组的详细介绍,请参见“安全配置指导”中的“对象组”。

【使用指导】

多次执行本命令,可配置多个源 MAC 地址作为安全策略规则的过滤条件。

配置源 MAC 地址作为安全策略规则的过滤条件时,若指定的地址对象组不存在,该配置仍会配置成功,同时也会在系统中创建一个名称为指定名称的空配置地址对象组,但此条过滤条件不会匹配任何报文。

【举例】

配置作为安全策略规则 rule1 过滤条件的源 MAC 地址对象组为 mac1 和 mac2。


```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] source-mac mac1
[Sysname-security-policy-ip-0-rule1] source-mac mac2
```

【相关命令】

- **display security-policy**
- **object-group**（安全命令参考/对象组）

1.1.30 source-zone

source-zone 命令用来配置作为安全策略规则过滤条件的源安全域。

undo source-zone 命令用来删除作为安全策略规则过滤条件的源安全域。

【命令】

```
source-zone source-zone-name
undo source-zone [source-zone-name ]
```

【缺省情况】

不存在源安全域过滤条件。

【视图】

安全策略规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

source-zone-name: 表示源安全域的名称，为 1~31 个字符的字符串，不区分大小写。使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有源安全域类型的过滤条件。有关安全域的详细介绍，请参见“安全配置指导”中的“安全域”。

【使用指导】

多次执行本命令，可配置多个源安全域作为安全策略规则的过滤条件。

【举例】

配置作为安全策略规则 rule1 过滤条件的源安全域为 Trust 和 DMZ。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] source-zone trust
[Sysname-security-policy-ip-0-rule1] source-zone dmz
```

【相关命令】

- **display security-policy**
- **security-zone**（安全命令参考/安全域）

1.1.31 time-range

time-range 命令用来配置安全策略规则生效的时间段。

undo time-range 命令用来恢复缺省情况。

【命令】

```
time-range time-range-name  
undo time-range
```

【缺省情况】

不限制安全策略规则生效的时间。

【视图】

安全策略规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

time-range-name: 表示时间段的名称，为 1~32 个字符的字符串，不区分大小写。有关时间段的详细介绍，请参见“ACL 配置指导”中的“时间段”。

【配置指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 为安全策略规则 rule1 配置生效时间段为 work。  
<Sysname> system-view  
[Sysname] security-policy ip  
[Sysname-security-policy-ip] rule 0 name rule1  
[Sysname-security-policy-ip-0-rule1] time-range work
```

【相关命令】

- **display security-policy**
- **time-range** (ACL 命令参考/时间段)

1.1.32 track

track 命令用来配置安全策略规则与 Track 项联动。

undo track 命令用来取消安全策略规则与 Track 项联动。

【命令】

```
track { negative | positive } track-entry-number  
undo track
```

【缺省情况】

安全策略规则未与 Track 项联动。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

negative: 指定安全策略规则与 Track 项的 Negative 状态联动。

positive: 指定安全策略规则与 Track 项的 Positive 状态联动。

track-entry-number: 表示关联的 Track 项序号，取值范围为 1~1024。有关 Track 的详细介绍，请参见“可靠性配置指导”中的“Track”。

【使用指导】

配置安全策略规则与 Track 项的 Negative 状态联动后，当安全策略规则收到 Negative 状态的 Track 通知时，将此规则置为有效状态（Active），当安全策略规则收到 Positive 状态的 Track 通知时，将此规则置为失效状态（Inactive）。

配置安全策略规则与 Track 项的 Positive 状态联动后，当安全策略规则收到 Positive 状态的 Track 通知时，将此规则置为有效状态（Active），当安全策略规则收到 Negative 状态的 Track 通知时，将此规则置为失效状态（Inactive）。

多次执行本命令，最后一次执行的命令生效。

【举例】

为安全策略规则 rule1 配置规则与 Track 项的 Positive 状态联动。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] track positive 10
```

【相关命令】

- **display security-policy**
- **track bfd**（可靠性命令参考/Track）
- **track interface**（可靠性命令参考/Track）
- **track ip route reachability**（可靠性命令参考/Track）
- **track nqa**（可靠性命令参考/Track）

1.1.33 user

user 命令用来配置作为安全策略规则过滤条件的用户。

undo user 命令用来删除作为安全策略规则过滤条件的用户。

【命令】

```
user username [ domain domain-name ]
```

```
undo user [ username [ domain domain-name ] ]
```

【缺省情况】

不存在用户过滤条件。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

username: 表示用户的名称，为 1~55 个字符的字符串，区分大小写，不能是 a、al 和 all，且不能包含特殊字符 “\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”、和 “@”。使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有用户类型的过滤条件。有关用户的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

domain domain-name: 表示在指定的身份识别域中匹配此用户。**domain-name** 是身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“:”、“*”、“?”、“<”、“>” 和 “@” 字符。若不指定此参数，则表示在不属于任何身份识别域的用户中匹配此用户。

【使用指导】

多次执行本命令，可配置多个用户作为安全策略规则的过滤条件。

使用 **undo** 命令时若不指定用户，则表示删除此规则中所有用户类型的过滤条件；若不指定身份识别域，则表示删除此规则中不属于任何身份识别域的用户。

有关身份识别用户和身份识别域的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

【举例】

配置作为安全策略规则 rule1 过滤条件的用户为 usera 和 userb，身份识别域均为 test。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] user usera domain test
[Sysname-security-policy-ip-0-rule1] user userb domain test
```

【相关命令】

- **display security-policy**
- **user-identity enable**（安全命令参考/用户身份识别与管理）
- **user-identity static-user**（安全命令参考/用户身份识别与管理）

1.1.34 user-group

user-group 命令用来配置作为安全策略规则过滤条件的用户组。

undo user-group 命令用来删除作为安全策略规则过滤条件的用户组。

【命令】

user-group user-group-name [domain domain-name]

undo user-group [user-group-name [domain domain-name]]

【缺省情况】

不存在用户组过滤条件。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-group-name: 表示用户组的名称，为 1~200 个字符的字符串，不区分大小写。使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有用户组类型的过滤条件。有关用户组的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

domain domain-name: 表示在指定的身份识别域中匹配此用户组，**domain-name** 是身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包括“/”、“\”、“|”、“:”、“*”、“?”、“<”、“>”以及“@”字符。若不指定此参数，则表示在不属于任何身份识别域的用户组中匹配此用户组。

【使用指导】

多次执行本命令，可配置多个用户组作为安全策略规则的过滤条件。

使用 **undo** 命令时若不指定用户组，则表示删除此规则中所有用户组类型的过滤条件；若不指定身份识别域，则表示删除此规则中不属于任何身份识别域的用户组。

有关身份识别用户组和身份识别域的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

【举例】

配置作为安全策略规则 rule1 过滤条件的用户组为 groupa 和 groupb，身份识别域均为 test。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] user-group groupa domain test
[Sysname-security-policy-ip-0-rule1] user-group groupb domain test
```

【相关命令】

- **display security-policy**
- **user-group**（安全命令参考/AAA）

1.1.35 vrf

vrf 命令用来配置安全策略规则对入接口指定 VPN 多实例中的报文有效。

undo vrf 命令用来恢复缺省情况。

【命令】

vrf vrf-name

undo vrf

【缺省情况】

安全策略规则对公网的报文有效。

【视图】

安全策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

vrf-name: 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

【配置指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

配置安全策略规则 rule1 对入接口的 VPN 多实例 vpn1 中的报文生效。

```
<Sysname> system-view
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 0 name rule1
[Sysname-security-policy-ip-0-rule1] vrf vpn1
```

【相关命令】

- **display security-policy**

目 录

1 用户身份识别和管理	1-1
1.1 用户身份识别和管理命令	1-1
1.1.1 account-update-interval	1-1
1.1.2 connection-detect	1-1
1.1.3 connection-detect enable	1-2
1.1.4 display user-identity	1-3
1.1.5 display user-identity active-user-group	1-6
1.1.6 display user-identity all	1-7
1.1.7 display user-identity online-user	1-8
1.1.8 display user-identity restful-server	1-10
1.1.9 display user-identity security-manage-server	1-11
1.1.10 display user-identity user-import-policy	1-12
1.1.11 encryption	1-14
1.1.12 import-type	1-15
1.1.13 ip	1-15
1.1.14 ldap-scheme	1-16
1.1.15 listen-port	1-17
1.1.16 login-name	1-18
1.1.17 reset user-identity dynamic-online-user	1-19
1.1.18 reset user-identity user-account	1-20
1.1.19 reset user-identity user-group	1-20
1.1.20 restful-server	1-21
1.1.21 uri	1-22
1.1.22 user-identity enable	1-24
1.1.23 user-identity online-user import policy	1-24
1.1.24 user-identity online-user-name-match	1-25
1.1.25 user-identity restful-server	1-26
1.1.26 user-identity security-manage-server	1-27
1.1.27 user-identity static-user	1-27
1.1.28 user-identity user-account auto-import policy	1-29
1.1.29 user-identity user-account export url	1-29
1.1.30 user-identity user-account import policy	1-31
1.1.31 user-identity user-account import url	1-32

1.1.32 user-identity user-import-policy	1-33
1.1.33 vpn-instance	1-33

1 用户身份识别和管理

1.1 用户身份识别和管理命令

1.1.1 account-update-interval

account-update-interval 命令用来配置自动导入身份识别用户账户的周期。

undo account-update-interval 命令用来恢复缺省情况。

【命令】

account-update-interval *interval*

undo account-update-interval

【缺省情况】

自动导入身份识别用户账户的周期为 24 小时。

【视图】

身份识别用户导入策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval: 表示导入身份识别用户账户的周期，取值范围为 1~65536，单位为小时。

【使用指导】

身份识别用户导入策略处于开启状态时，设备将以本命令指定的周期从服务器上导入所有身份识别用户账户，使得设备与服务器上的账户信息定期保持一致。

【举例】

在身份识别用户导入策略 **policy1** 中，配置自动导入身份识别用户账户的周期为 12 小时。

```
<Sysname> system-view
```

```
[Sysname] user-identity user-import-policy policy1
```

```
[Sysname-identity-user-impolicy-policy1] account-update-interval 12
```

【相关命令】

- **user-identity user-account auto-import policy**

1.1.2 connection-detect

connection-detect 命令用来配置对 RESTful 服务器的探测参数。

undo connection-detect 命令用来恢复缺省情况。

【命令】

connection-detect { *interval interval* | *maximum max-times* }

undo connection-detect { interval | maximum }

【缺省情况】

对 RESTful 服务器的探测周期为 5 分钟，每周期内的最大探测次数为 3。

【视图】

RESTful 服务器视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval interval: 探测周期，取值范围为 1~10，单位为分钟。

maximum max-times: 每个探测周期内的最大探测次数，取值范围为 1~5。

【使用指导】

如果对设备与 RESTful 服务器的连接状态要求比较高，建议设置较小的探测周期，以及较大的探测次数。

配置的探测周期不建议太小，因为探测周期过小会增加设备与 RESTful 服务器交互的频率，增加 RESTful 服务器负担，具体配置请结合 RESTful 服务器的性能参数综合考虑。

【举例】

配置对 RESTful 服务器 rest1 的探测周期为 2 分钟，每周期内的最大探测次数为 3。

```
<Sysname> system-view
```

```
[Sysname] user-identity restful-server rest1
```

```
[Sysname-restfulserver-rest1] connection-detect interval 2
```

```
[Sysname-restfulserver-rest1] connection-detect maximum 3
```

【相关命令】

- **connection-detect enable**
- **display user-identity restful-server**
- **login-name**
- **uri**
- **user-identity restful-server**

1.1.3 connection-detect enable

connection-detect enable 命令用来开启对 RESTful 服务器的探测功能。

undo connection-detect enable 命令用来关闭对 RESTful 服务器的探测功能。

【命令】

connection-detect enable

undo connection-detect enable

【缺省情况】

对 RESTful 服务器的探测功能处于关闭状态。

【视图】

RESTful 服务器视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启本探测功能后，设备将立即与该 RESTful 服务器进行交互，探测与 RESTful 服务器的连接状态（可达或者不可达）。此连接状态可被安全业务模块作为用户接入控制策略的参考信息。

开启本探测功能前，必须要配置 RESTful 视图下的 **login-name** 以及 **uri** 命令。

设备在一个探测周期内（时长由 **connection-detect interval interval** 命令设置），会尝试发起多次探测（次数由 **connection-detect maximum max-times** 命令设置）来决定服务器是否可达，具体如下：

- 只要设备收到服务器回应，即认为服务器可达，并停止探测。
- 若设备在最大尝试次数达到之后，仍然未收到服务器回应，则认为服务器不可达。

上一轮探测周期结束后，设备自动进入下一轮探测，过程同上。

关闭本探测功能后，设备将停止与 RESTful 服务器进行探测交互。

【举例】

开启对 RESTful 服务器 rest1 的探测功能。

```
<Sysname> system-view
```

```
[Sysname] user-identity restful-server rest1
```

```
[Sysname-restfulserver-rest1] connection-detect enable
```

【相关命令】

- **connection-detect**
- **display user-identity restful-server**
- **login-name**
- **uri**
- **user-identity restful-server**

1.1.4 display user-identity

display user-identity 命令用来显示指定的身份识别用户或身份识别用户组。

【命令】

```
display user-identity { domain domain-name | null-domain } { user [ user-name  
[ group ] ] | user-group [ group-name [ member { group | user } ] ] }
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

domain *domain-name*: 表示身份识别域的名称，为 1~255 个字符的字符串，不区分大小写。

null-domain: 表示未加入任何身份识别域的身份识别用户或身份识别用户组。

user: 显示身份识别用户信息。

user-name: 身份识别用户名，为 1~55 个字符的字符串，区分大小写。若不指定该参数，则表示显示所有身份识别用户的信息。

group: 显示用户所属用户组。若不指定该参数，则不显示用户组信息。

user-group: 显示身份识别用户组信息。

group-name: 用户组名，为 1~200 个字符的字符串，不区分大小写。若不指定该参数，则表示显示所有身份识别用户组的配置信息。

member: 显示身份识别的成员信息。若不指定该参数，则不显示成员信息。

group: 用户组成员。

user: 用户成员。

【使用指导】

本命令显示的身份识别用户或身份识别用户组信息，包括从本地用户数据库学习的和从 CSV 文件、服务器导入的身份识别用户账户以及身份识别用户组的信息。

【举例】

显示 system 域下所有身份识别用户组的信息。

```
<Sysname> display user-identity domain system user-group
```

Identity domain: system

Group ID	Group name
0x888	abc
0x123	gp1

Total 2 records matched.

显示 system 域下身份识别用户组 abc 的信息。

```
<Sysname> display user-identity domain system user-group abc
```

Identity domain: system

Group ID	Group name
0x888	abc

Total 1 records matched.

显示 system 域下身份识别用户组 abc 中的用户成员信息。

```
<Sysname> display user-identity domain system user-group abc member user
```

Identity domain: system

User ID	Username
0x234	user1
0xffffffff	user2

Total 2 records matched.

显示 system 域下身份识别用户组 abc 中的用户组成员信息。

```
<Sysname> display user-identity domain system user-group abc member group
```

Identity domain: system

Group ID	Group name
0x567	group1
0x111	group2

Total 2 records matched.

显示 system 域下所有身份识别用户的信息。

```
<Sysname> display user-identity domain system user
```

Identity domain: system

User ID	Username
0x234	user1
0xffffffff	user2

Total 2 records matched.

显示 system 域下身份识别用户 user1 的信息。

```
<Sysname> display user-identity domain system user user1
```

Identity domain: system

User ID	Username
0x234	user1

Total 1 records matched.

显示 system 域下身份识别用户 user1 的用户组信息。

```
<Sysname> display user-identity domain system user user1 group
```

Identity domain: system

Group ID	Group name
0x888	abc
0x123	gp1

Total 2 records matched.

显示未加入任何身份识别域的身份识别用户信息。

```
<Sysname> display user-identity null-domain user
```

User ID	Username
0x1	test
0x3	jj
0x2	abc

Total 3 records matched.

表1-1 display user-identity 命令显示信息描述表

字段	描述
Identity domain	身份识别用户或身份识别用户组所属身份识别域的名称 若用户或用户组不属于任何身份识别域，则不显示该字段
Username	用户名

字段	描述
User ID	用户ID
Group name	用户组名
Group ID	用户组ID
Total <i>n</i> records matched	匹配的用户或用户组数目

【相关命令】

- **reset user-identity user-account**
- **reset user-identity user-group**

1.1.5 display user-identity active-user-group

display user-identity active-user-group 命令用来显示激活的身份识别用户组。

【命令】

```
display user-identity active-user-group { all | domain domain-name | null-domain }
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

all: 显示所有身份识别域下的激活用户组。

domain *domain-name*: 显示指定身份识别域下的激活用户组。*domain-name* 表示身份识别域的名称，为 1~255 个字符的字符串，不区分大小写。

null-domain: 显示未加入任何身份识别域的激活用户组。

【使用指导】

当身份识别用户组被安全策略等安全特性引用之后，若该引用配置生效，则该用户组将处于激活状态。只有身份识别用户组处于激活状态时，该用户组才能在基于用户身份的访问控制过程中生效。

【举例】

显示身份识别域 **system** 下的激活的身份识别用户组信息。

```
<Sysname> display user-identity active-user-group domain system
Identity domain: system
  Group ID      Group name
  0x888         abc
  0x123         gp1
```

Total 2 records matched.

表1-2 display user-identity active-user-group 命令显示信息描述表

字段	描述
Identity domain	身份识别用户组所属的身份识别域名 若用户不属于任何身份识别域，则不显示该字段
Group ID	身份识别用户组的ID
Group name	身份识别用户组名
Total <i>n</i> records matched	匹配的用户组数目

【相关命令】

- **reset user-identity user-group**

1.1.1.6 display user-identity all

display user-identity all 命令用来显示所有身份识别用户或身份识别用户组。

【命令】

display user-identity all { user | user-group }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

user: 显示身份识别用户信息。

user-group: 显示身份识别用户组信息。

【使用指导】

本命令显示的身份识别用户或身份识别用户组信息，包括从本地用户数据库学习的和从 CSV 文件以及第三方服务器导入的身份识别用户账户及身份识别用户组的信息。

【举例】

显示所有身份识别用户信息。

```
<Sysname> display user-identity all user
Identity domain: system
  User ID      Username
  ----      -
  0x121        test1
  0x123        test2
```

```
Identity domain: 11
  User ID      Username
  0x888        test3
  0x899        test4
```

Total 4 records matched.

表1-3 display user-identity all user 命令显示信息描述表

字段	描述
Identity domain	身份识别用户所属身份识别域的名称 若用户不属于任何身份识别域，则不显示该字段
User ID	用户ID
Username	用户名
Total <i>n</i> records matched	匹配的用户数目

显示所有身份识别用户组。

```
<Sysname> display user-identity all user-group
```

```
Identity domain: system
  Group ID      Group name
  0x888         abc
  0x123         gp1
Identity domain: 11
  Group ID      Group name
  0x255         001
  0x256         002
```

Total 4 records matched.

表1-4 display user-identity all user-group 命令显示信息描述表

字段	描述
Identity domain	身份识别用户组所属身份识别域的名称 若用户组不属于任何身份识别域，则不显示该字段
Group ID	用户组ID
Group name	用户组
Total <i>n</i> records matched	匹配的用户组数目

【相关命令】

- **reset user-identity user-account**
- **reset user-identity user-group**

1.1.7 display user-identity online-user

display user-identity online-user 命令用来显示在线身份识别用户。

【命令】

display user-identity online-user { domain *domain-name* | null-domain } name *user-name*

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

domain *domain-name*: 指定在线身份识别用户所属的身份识别域。*domain-name* 表示身份识别域名，为 1~255 个字符的字符串，不区分大小写。

null-domain: 表示未加入任何身份识别域的在线身份识别用户。

name *user-name*: 指定在线身份识别用户的用户名。*user-name* 表示用户名，为 1~55 个字符的字符串，区分大小写，不能携带域名。

【使用指导】

在线身份识别用户包括两类：由静态配置生成的静态在线身份识别用户，以及由设备动态生成的动态在线身份识别用户。

【举例】

显示 system 域下名称为 user1 的在线身份识别用户信息。

```
<Sysname> display user-identity online-user domain system name user1
User name: user1
  Identity domain: system
  IP   : 199.199.0.15
  MAC  : 0001-0002-0003
  Type: Static

Total 1 records matched.
```

表1-5 display user-identity online-user 命令显示信息描述表

字段	描述
User name	身份识别用户的名称
Identity domain	身份识别用户所属的身份识别域 若用户不属于任何身份识别域，则不显示该字段
IP	身份识别用户的IP地址
MAC	身份识别用户的MAC地址 若没有获取到MAC地址信息，则不显示该字段

字段	描述
Type	身份识别用户的类型，包括以下取值： - Static: 静态在线身份识别用户 - Dynamic: 动态在线身份识别用户
Total <i>n</i> records matched	匹配的用户数目

【相关命令】

- **reset user-identity dynamic-online-user**
- **user-identity static-user**

1.1.8 display user-identity restful-server

display user-identity restful-server 命令用来显示 RESTful 服务器配置。

【命令】

display user-identity restful-server [*server-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

server-name: 表示 RESTful 服务器的名称，为 1~31 个字符的字符串，不区分大小写。如果不指定本参数，则表示显示所有 RESTful 服务器的配置信息。

【举例】

显示 RESTful 服务器 rest1 的配置。

```
<Sysname> display user-identity restful-server rest1
RESTful server name: rest1
  Login name: u1
  Vpn Instance: v1
  Get User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUser
  Get User Group URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUserGroup
  Get Online User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/onlineUser
  Put Online User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOnlineUser
  Put Offline User URI: http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOfflineUser
  Connectivity detection: Enabled
    Detection interval: 1 minutes
    Maximum times: 1
  Connectivity status: Reachable
```

表1-6 display user-identity restful-server 命令显示信息描述表

字段	描述
Login name	连接到RESTful服务器所需的用户名
Vpn Instance	RESTful服务器所属VPN实例名称 若属于公网，则不显示本字段
Get User URI	请求用户账户信息的URI
Get User Group URI	请求用户组信息的URI
Get Online User URI	请求在线用户信息的URI
Put Online User URI	上传在线用户信息的URI
Put Offline User URI	上传下线用户信息的URI
Connectivity detection	RESTful服务器探测功能的开启状态 - Enabled: 开启 - Disabled: 关闭
Detection interval	设备对RESTful服务器的探测周期，单位为分钟
Maximum times	设备对RESTful服务器的最大探测次数
Connectivity status	设备对RESTful服务器的探测结果 - Reachable: 可达 - Unreachable: 不可达 若未开启RESTful服务器探测功能，则不显示本字段

【相关命令】

- connection-detect
- connection-detect enable
- login-name
- uri
- user-identity restful-server
- vpn-instance

1.1.1.9 display user-identity security-manage-server

display user-identity security-manage-server 命令用来显示 Security Manage 服务器集的配置信息。

【命令】

display user-identity security-manage-server [*server-set-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

server-set-name: 表示 Security Manage 服务器集的名称，为 1~31 个字符的字符串，不区分大小写。如果不指定本参数，则表示显示所有 Security Manage 服务器集的配置信息。目前，系统中仅能存在一个 Security Manage 服务器集。

【举例】

```
# 显示 Security Manage 服务器集 sec1 的配置信息。
<Sysname> display user-identity security-manage-server sec1
Security management server set: sec1
  IP addresses: 192.168.0.1,10.113.0.1
  Listening port: 8200
  Encryption algorithm: 3DES
```

Total 1 records matched

表1-7 display user-identity security-manage-server 命令显示信息描述表

字段	描述
Security management server set	Security Manage服务器集的名称
IP address	Security Manage服务器的IP地址
Listening port	设备监听Security Manage服务器的端口号
Encryption algorithm	与Security Manage服务器交互报文时使用的加密算法
Total <i>n</i> records matched	匹配的Security Manage服务器集数目

【相关命令】

- **encryption**
- **ip**
- **listen-port**
- **user-identity security-manage-server**

1.1.10 display user-identity user-import-policy

display user-identity user-import-policy 命令用来显示身份识别用户导入策略。

【命令】

display user-identity user-import-policy [*policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

policy-name: 表示身份识别用户导入策略名，为 1~31 个字符的字符串，不区分大小写。若不指定该参数，则显示所有的身份识别用户导入策略。

【举例】

```
# 显示身份识别用户导入策略 policy1 的配置信息。
<Sysname> display user-identity user-import-policy policy1
Policy name: policy1
Interval time: 24 hours
RESTful server name:
    ser1
LDAP import type: All
LDAP scheme name:
    ldap-scheme
```

Total 1 records matched.

表1-8 display user-identity user-import-policy 命令显示信息描述表

字段	描述
Policy name	身份识别用户导入策略名称
Interval time	自动导入身份识别用户账户的周期，单位为小时
RESTful server name	RESTful服务器名称
LDAP import type	从LDAP服务器上导入的用户信息类型，包括以下取值： - All: 表示导入用户和用户组信息 - User: 表示导入用户信息 - Group: 表示导入用户组信息
LDAP scheme name	LDAP方案名称
Total <i>n</i> records matched	匹配的策略数目

【相关命令】

- import-type
- user-identity user-import-policy

1.1.11 encryption

encryption 命令用来配置与 Security Manage 服务器交互使用的加密算法与共享密钥。

undo encryption 命令用来恢复缺省情况。

【命令】

```
encryption algorithm { 3des | aes128 } key { simple | cipher } string
undo encryption algorithm
```

【缺省情况】

未配置与 Security Manage 服务器交互时使用的加密算法与共享密钥。

【视图】

Security Manage 服务器集视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

algorithm: 表示加密算法。

3des: 表示 3DES 算法。

aes128: 表示密钥长度为 128 比特的 AES 算法。

key: 表示共享密钥。

cipher: 以密文形式设置密钥。

simple: 以明文形式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。加密方式为 **3des** 时，明文密钥为 1~24 个字符的字符串，密文密钥为 1~65 个字符的字符串；加密方式为 **aes128** 时，明文密钥为 1~16 个字符的字符串，密文密钥为 1~53 个字符的字符串。

【使用指导】

设备与 Security Manage 服务器连接时，使用配置的加密算法和共享密钥对交互的报文进行加密和解密。配置加密算法和共享密钥必须与要连接的 Security Manage 服务器使用的加密算法和共享密钥保持一致，否则设备无法正确处理与该服务器交互的报文。

【举例】

在 Security Manage 服务器集 sec1 中，配置和 Security Manage 服务器交互使用的加密算法为 3des、共享密钥为明文 123。

```
<Sysname> system-view
[Sysname] user-identity security-manage-server sec1
[Sysname-identity-sec-manage-server-sec1] encryption algorithm 3des key simple 123
```

【相关命令】

- **display user-identity security-manage-server**

1.1.12 import-type

import-type 命令用来配置从 LDAP 服务器上导入的用户信息类型。

undo import-type 命令用来恢复缺省情况。

【命令】

```
import-type { all | group | user }  
undo import-type
```

【缺省情况】

未配置从 LDAP 服务器上导入的用户信息类型，允许导入用户和用户组信息。

【视图】

身份识别用户导入策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

all: 表示导入用户和用户组信息。

group: 表示导入用户组信息。

user: 表示导入用户信息。

【使用指导】

根据实际导入需求选择一个对应的类型进行配置，导入时会根据配置的导入类型从 LDAP 服务器将该类型信息导入到设备上。

多次配置本命令，仅最后一次执行的命令生效。

【举例】

```
# 配置从 LDAP 服务器上导入的用户类型为所有类型，即包括用户和用户组信息。  
<Sysname> system-view  
[Sysname] user-identity user-import-policy policy  
[Sysname-identity-user-impolicy-policy] import-type all
```

【相关命令】

- **display user-identity user-import-policy**

1.1.13 ip

ip 命令用来配置 Security Manage 服务器的 IP 地址。

undo ip 命令用来删除配置的 Security Manage 服务器的 IP 地址。

【命令】

```
ip ip-address<1-10>  
undo ip { ip-address<1-10> | all }
```

【缺省情况】

未配置 Security Manage 服务器的 IP 地址。

【视图】

Security Manage 服务器集视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address&<1-10>: 指定服务器的 IP 地址，不能为全 0 地址。&<1-10>表示前面的参数最多可以输入 10 次。

all: 表示所有 IP 地址。

【使用指导】

一个 Security Manage 服务器集视图中，最多可以配置 20 个 Security Manage 服务器的 IP 地址。

【举例】

在 Security Manage 服务器集 sec1 中，配置服务器 IP 地址包括 192.168.0.1 和 10.113.0.1。

```
<Sysname> system-view
```

```
[Sysname] user-identity security-manage-server sec1
```

```
[Sysname-identity-sec-manage-server-sec1] ip 192.168.0.1 10.113.0.1
```

【相关命令】

- **display user-identity security-manage-server**

1.1.14 ldap-scheme

ldap-scheme 命令用来指定 LDAP 方案。

undo ldap-scheme 命令用来删除 LDAP 方案。

【命令】

```
ldap-scheme ldap-scheme-name
```

```
undo ldap-scheme ldap-scheme-name
```

【缺省情况】

未指定 LDAP 方案。

【视图】

身份识别用户导入策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ldap-scheme-name: LDAP 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

指定的 LDAP 方案中定义了 LDAP 服务器的相关参数，用户可以通过执行 **user-identity user-account import policy** 命令从该方案定义的 LDAP 服务器上导入身份识别用户账户信息。但是，系统不支持从 LDAP 服务器上导入在线身份识别用户信息。

最多可以指定 16 个 LDAP 方案，使得可以同时从多个 LDAP 服务器上导入身份识别用户账户信息。

【举例】

在身份识别用户导入策略 policy1 中，指定名称为 ser2 的 LDAP 方案。

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy1
[Sysname-identity-user-impolicy-policy1] ldap-scheme ser2
```

【相关命令】

- **display user-identity user-import-policy**
- **ldap scheme**（安全命令参考/AAA）

1.1.15 listen-port

listen-port 命令用来配置设备监听 Security Manage 服务器的端口号。

undo listen-port 命令用来恢复缺省情况。

【命令】

```
listen-port port-num
undo listen-port
```

【缺省情况】

设备监听 Security Manage 服务器的端口号为 8001。

【视图】

Security Manage 服务器集视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

port-num：表示 UDP 端口号，取值范围为 1~65535。

【使用指导】

配置的设备监听 Security Manage 服务器的端口号必须与 Security Manage 服务器发送在线用户消息使用的端口号保持一致，否则设备无法与该服务器成功建立连接。

【举例】

在 Security Manage 服务器集 sec1 中，配置设备监听 Security Manage 服务器的端口号为 8084。

```
<Sysname> system-view
[Sysname] user-identity security-manage-server sec1
[Sysname-identity-sec-manage-server-sec1] listen-port 8084
```

【相关命令】

- **display user-identity security-manage-server**

1.1.16 login-name

login-name 命令用来配置登录到 RESTful 服务器所需的用户名和密码。

undo login-name 命令用来恢复缺省情况。

【命令】

```
login-name user-name password { cipher | simple } string
undo login-name
```

【缺省情况】

未配置登录到 RESTful 服务器所需的用户名和密码。

【视图】

RESTful 服务器视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

user-name: 表示用户名，为 1~55 字符的字符串，区分大小写。

password: 表示密码。

cipher: 表示以密文方式设置密码。

simple: 表示以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串。

【使用指导】

设备与 RESTful 服务器建立连接时，服务器首先需要验证连接请求发起方的合法性。本命令配置的用户名和密码，即为设备向 RESTful 服务器提供的身份信息。RESTful 服务器验证该用户名和密码成功后，才允许连接请求发起方与之建立连接，以及获取相应的服务器资源。

本命令指定的用户名和密码，必须在 RESTful 服务器上已经存在。

【举例】

配置与 RESTful 服务器 rest1 建立连接时使用的登录用户名为 abc，密码为明文 123。

```
<Sysname> system-view
[Sysname] user-identity restful-server rest1
[Sysname-restfulserver-rest1] login-name abc password simple 123
```

【相关命令】

- **display user-identity restful-server**
- **user-identity restful-server**

1.1.17 reset user-identity dynamic-online-user

reset user-identity dynamic-online-user 命令用来删除动态的在线身份识别用户。

【命令】

```
reset user-identity dynamic-online-user { all | { domain domain-name |  
null-domain } [ name user-name ] | { ip ipv4-address | ipv6 ipv6-address } [ mac  
mac-address ] }
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

all: 所有动态的在线身份识别用户信息。

domain domain-name: 身份识别用户所属的身份识别域。*domain-name* 表示域名，为 1~255 个字符的字符串，不区分大小写。

null-domain: 未加入任何身份识别域的身份识别用户信息。

name user-name: 表示用户名，为 1~55 个字符的字符串，区分大小写。如果不指定该参数，则表示指定身份识别域或者未加入任何身份识别域的所有在线身份识别用户。

ip ipv4-address: 身份识别用户的 IPv4 地址。

ipv6 ipv6-address: 身份识别用户的 IPv6 地址。

mac mac-address: 身份识别用户的 MAC 地址，格式为 H-H-H。若不指定该参数，则表示同一用户名，不同 MAC 地址的所有在线身份识别用户。

【使用指导】

动态的在线身份识别用户信息是指，设备从远程服务器上动态学习到的在线身份识别用户信息。静态的在线身份识别用户信息是由静态配置产生的，不能通过本命令删除，可以通过执行 **undo user-identity static-user** 命令删除。

【举例】

删除全部动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user all
```

删除身份识别域 **abc** 下的所有动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user domain abc
```

删除身份识别域 **dom1** 下名称为 **user1** 的动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user domain dom1 name user1
```

删除用户名为 **user2** 且未加入任何身份识别域的动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user null-domain name user2
```

删除 IP 地址为 **1.2.3.4** 的动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user ip 1.2.3.4
```

删除 IP 地址为 **1.2.3.4**、MAC 地址为 **2222-3333-4444** 的动态在线身份识别用户信息。

```
<Sysname> reset user-identity dynamic-online-user ip 1.2.3.4 mac 2222-3333-4444
```

【相关命令】

- **display user-identity online-user**

1.1.18 reset user-identity user-account

reset user-identity user-account 命令用来删除身份识别用户账户。

【命令】

```
reset user-identity user-account { all | { domain domain-name | null-domain }  
[ name user-name ] }
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

all: 所有身份识别用户账户信息。

domain *domain-name*: 表示身份识别域的名称，为 1~255 个字符的字符串，不区分大小写。

null-domain: 未加入任何身份识别域的身份识别用户账户信息。

name *user-name*: 表示身份识别用户的账户名，为 1~55 个字符的字符串，区分大小写。若不指定该参数，则表示删除所有指定身份识别域的或未加入任何身份识别域的身份识别用户帐户。

【使用指导】

此命令用来删除从服务器导入或者从 CSV 文件导入的身份识别用户账户信息。

从本地用户数据库中学习到的身份识别用户账户不能通过该命令删除。

【举例】

删除所有身份识别用户账户信息。

```
<Sysname> reset user-identity user-account all
```

删除身份识别域 **dom1** 下名称为 **test** 的身份识别用户账户信息。

```
<Sysname> reset user-identity user-account domain dom1 name test
```

【相关命令】

- **display user-identity all user**

1.1.19 reset user-identity user-group

reset user-identity user-group 命令用来删除身份识别用户组。

【命令】

```
reset user-identity user-group { all | { domain domain-name | null-domain }  
[ name group-name ] }
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

all: 所有身份识别用户组信息。

domain *domain-name*: 表示身份识别域的名称，为 1~255 个字符的字符串，不区分大小写。

null-domain: 未加入任何身份识别域的身份识别用户组。

name *group-name*: 身份识别用户组名，为 1~200 个字符的字符串，不区分大小写。若不指定该参数，则表示删除所有指定身份识别域的或未加入任何身份识别域的身份识别用户组。

【使用指导】

本命令用来删除从远程服务器和 CVS 文件导入的身份识别用户组，而从本地用户数据库学习到的身份识别用户组不能通过该命令删除。

【举例】

删除全部身份识别用户组信息。

```
<Sysname> reset user-identity user-group all
```

删除身份识别域 dom1 下名称为 g1 的身份识别用户组信息。

```
<Sysname> reset user-identity user-group domain dom1 name g1
```

【相关命令】

- **display user-identity all user-group**

1.1.20 restful-server

restful-server 命令用来指定 RESTful 服务器。

undo restful-server 命令用来恢复缺省情况。

【命令】

```
restful-server server-name
```

```
undo restful-server server-name
```

【缺省情况】

未指定 RESTful 服务器。

【视图】

身份识别用户导入策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

server-name: RESTful 服务器名称, 为 1~31 个字符的字符串, 不区分大小写。

【使用指导】

指定的 RESTful 服务器中定义了 RESTful 服务器的相关参数, 用户可以通过执行 **user-identity user-account import policy** 命令从该服务器上导入身份识别用户账户, 通过执行 **user-identity online-user import policy** 命令从该服务器上导入在线身份识别用户。最多只能指定一个 RESTful 服务器。如需指定其它的 RESTful 服务器, 请先通过 **undo restful-server** 命令删除已经指定的 RESTful 服务器。

【举例】

在身份识别用户导入策略 policy1 中, 指定名称为 ser1 的 RESTful 服务器。

```
<Sysname> system-view
[Sysname] user-identity user-import-policy policy1
[Sysname-identity-user-impolicy-policy1] restful-server ser1
```

【相关命令】

- **display user-identity restful-server**
- **display user-identity user-import-policy**
- **user-identity restful-server**

1.1.21 uri

uri 命令用来指定 RESTful 服务器的 URI。

undo uri 命令用来删除指定的 RESTful 服务器 URI。

【命令】

```
uri { get-online-user | get-user-database | get-user-group-database |
put-offline-user | put-online-user } uri-string
undo uri { get-online-user | get-user-database | get-user-group-database |
put-offline-user | put-online-user }
```

【缺省情况】

未指定 RESTful 服务器的 URI。

【视图】

RESTful 服务器视图

【缺省用户角色】

network-admin
context-admin

【参数】

get-online-user: 表示请求网络接入类在线用户信息的 URI。

get-user-database: 表示请求网络接入类用户账户信息的 URI。

get-user-group-database: 表示请求用户组信息的 URI。

put-offline-user: 表示上传下线用户信息的 URI。

put-online-user: 表示上传在线用户信息的 URI。

uri-string: URI 名称，为 1~255 字符的字符串，不区分大小写。

【使用指导】

本命令指定的 URI 必须与 RESTful 服务器上提供各类用户资源服务的 URI 保持一致，否则将会导致用户信息交互失败。

新增或删除一个在线身份识别用户时，若该用户来源不是指定的 RESTful 服务器，则设备会将这些上线/下线用户信息上传给 RESTful 服务器。

可通过多次执行本命令，指定的不同服务类型的 RESTful 服务器 URI。

【举例】

指定向 RESTful 服务器 rest1 请求网络接入类在线用户信息的 URI 为 http://1.1.1.1:8080/imcrs/ssm/imcuser/onlineUser。

```
<Sysname> system-view
```

```
[Sysname] user-identity restful-server rest1
```

```
[Sysname-restfulserver-rest1] uri get-online-user
```

```
http://1.1.1.1:8080/imcrs/ssm/imcuser/onlineUser
```

指定向 RESTful 服务器 rest1 请求网络接入类用户账户信息的 URI 为 http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUser。

```
<Sysname> system-view
```

```
[Sysname] user-identity restful-server rest1
```

```
[Sysname-restfulserver-rest1] uri get-user-database
```

```
http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUser
```

指定向 RESTful 服务器 rest1 请求用户组信息的 URI 为 http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUserGroup。

```
<Sysname> system-view
```

```
[Sysname] user-identity restful-server rest1
```

```
[Sysname-restfulserver-rest1] uri get-user-group-database
```

```
http://1.1.1.1:8080/imcrs/ssm/imcuser/accessUserGroup
```

指定向 RESTful 服务器 rest1 上传下线用户信息的 URI 为 http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOfflineUser。

```
<Sysname> system-view
```

```
[Sysname] user-identity restful-server rest1
```

```
[Sysname-restfulserver-rest1] uri put-offline-user
```

```
http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOfflineUser
```

指定向 RESTful 服务器 rest1 上传在线用户信息的 URI 为 http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOnlineUser。

```
<Sysname> system-view
```

```
[Sysname] user-identity restful-server rest1
```

```
[Sysname-restfulserver-rest1] uri put-online-user
```

```
http://1.1.1.1:8080/imcrs/ssm/imcuser/uploadOnlineUser
```

【相关命令】

- **display user-identity restful-server**
- **user-identity restful-server**

1.1.22 user-identity enable

user-identity enable 命令用来开启用户身份识别功能。

undo user-identity enable 命令用来关闭用户身份识别功能。

【命令】

```
user-identity enable
undo user-identity enable
```

【缺省情况】

用户身份识别功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启用户身份识别功能后，用户身份识别模块才会与接入模块以及应用模块一起联动实现基于用户身份的访问控制。

【举例】

```
# 开启用户身份识别功能。
<Sysname> system-view
[Sysname] user-identity enable
```

1.1.23 user-identity online-user import policy

user-identity online-user import policy 命令用来导入服务器上的在线身份识别用户。

【命令】

```
user-identity online-user import policy policy-name
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

policy-name: 身份识别用户导入策略名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

执行该命令后，系统将向身份识别用户导入策略中指定的服务器发起一次连接请求，之后导入服务器上的网络接入类在线用户信息（用户名、身份识别域名、用户组名、IP 地址、MAC 地址）。

只有用户身份识别功处于开启状态，才能成功执行本命令。

【举例】

```
# 从名称为 policy1 的身份识别用户导入策略指定的服务器上导入在线身份识别用户。  
<Sysname> system-view  
[Sysname] user-identity online-user import policy policy1  
Loading...Done.
```

【相关命令】

- **user-identity user-account auto-import policy**
- **user-identity user-import-policy**

1.1.24 user-identity online-user-name-match

user-identity online-user-name-match 命令用来配置在线用户身份识别的用户名匹配模式。

undo user-identity online-user-name-match 命令用来恢复缺省情况。

【命令】

```
user-identity online-user-name-match { keep-original | with-domain |  
without-domain }  
undo user-identity online-user-name-match
```

【缺省情况】

在线用户身份识别的用户名匹配模式为 **keep-original**。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

keep-original: 使用用户输入的用户名进行身份识别用户账户匹配。例如，用户的认证域为 **abc**，用户输入的用户名为 **test@123**，则使用用户名 **test@123** 进行身份识别用户账户匹配。

with-domain: 使用用户的认证域进行身份识别用户账户匹配，即将采用“用户的纯用户名@认证域名”格式进行用户账户匹配。例如，用户的认证域为 **abc**，用户输入的用户名为 **test@123**，则使用用户名 **test@abc** 进行身份识别用户账户匹配。

without-domain: 不对用户账户的域名进行匹配，即使用户输入的纯用户名与设备上未加入任何身份识别域的身份识别用户账户进行匹配。例如，用户的认证域为 **abc**，用户输入的用户名为 **test@123**，则使用用户名 **test** 与未加入身份识别域的用户账户进行匹配。

【使用指导】

设备创建一条在线身份识别用户表项之前，首先检查该用户是否能够匹配上本地的身份识别用户账户，如果能够匹配上，才会生成对应的在线身份识别用户表项。本命令用来配置设备采用哪种用户名格式去匹配身份识别用户账户。

【举例】

```
# 配置在线用户身份识别的用户名匹配模式 with-domain。  
<Sysname> system-view  
[Sysname] user-identity online-user-name-match with-domain
```

1.1.25 user-identity restful-server

user-identity restful-server 命令用来创建 RESTful 服务器，并进入 RESTful 服务器视图。如果指定的 RESTful 服务器已经存在，则直接进入 RESTful 服务器视图。

undo user-identity restful-server 命令用来删除指定的 RESTful 服务器。

【命令】

```
user-identity restful-server server-name  
undo user-identity restful-server server-name
```

【缺省情况】

不存在 RESTful 服务器。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

server-name: RESTful 服务器的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

RESTful 服务器视图用于配置 RESTful 服务器的相关参数，包括服务器 URI 和登录用户。系统中仅能存在一个 RESTful 服务器。

【举例】

```
# 创建名称为 rest1 的 RESTful 服务器，并进入该服务器视图。  
<Sysname> system-view  
[Sysname] user-identity restful-server rest1  
[Sysname-restfulserver-rest1]
```

【相关命令】

- **display user-identity restful-server**
- **login-name**
- **uri**
- **user-identity user-import-policy**

1.1.26 user-identity security-manage-server

user-identity security-manage-server 命令用来创建 Security Manage 服务器集，并进入 Security Manage 服务器集视图。如果指定的 Security Manage 服务器集已经存在，则直接进入 Security Manage 服务器集视图。

undo user-identity security-manage-server 命令用来删除指定的 Security Manage 服务器集。

【命令】

```
user-identity security-manage-server server-set-name  
undo user-identity security-manage-server server-set-name
```

【缺省情况】

不存在 Security Manage 服务器集。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

server-set-name: Security Manage 服务器集的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

Security Manage 服务器集视图用于配置 Security Manage 服务器的相关参数，包括 IP 地址、端口号、共享密钥。

系统中仅能存在一个 Security Manage 服务器集。

【举例】

```
# 创建名称为 sec1 的 Security Manage 服务器集，并进入该服务器集视图。  
<Sysname> system-view  
[Sysname] user-identity security-manage-server sec  
[Sysname-identity-sec-manage-server-sec1]
```

【相关命令】

- **display user-identity security-manage-server**
- **encryption**
- **ip**
- **listen-port**

1.1.27 user-identity static-user

user-identity static-user 命令用来配置静态类型的身份识别用户。

undo user-identity static-user 命令用来删除指定的静态类型的身份识别用户。

【命令】

```
user-identity static-user user-name [ domain domain-name ] bind { ipv4  
ipv4-address | ipv6 ipv6-address } [ mac mac-address ]  
undo user-identity static-user user-name [ domain domain-name ] [ bind { ipv4  
ipv4-address | ipv6 ipv6-address } [ mac mac-address ] ]
```

【缺省情况】

不存在静态类型的身份识别用户。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

user-name: 静态类型的身份识别用户名，为 1~55 个字符的字符串，区分大小写。

domain domain-name: 指定用户所属的身份识别域。**domain-name** 表示身份识别域的名称，为 1~255 个字符的字符串，不区分大小写。若不指定该参数，则表示用户不属于任何身份识别域。

bind: 指定与该用户名绑定的 IP 地址属性。

ipv4 ipv4-address: 指定用户的 IPv4 地址。**ipv4-address** 不能为全 0 地址、全 1 地址以及组播 IP 地址。

ipv6 ipv6-address: 指定用户的 IPv6 地址。**ipv6-address** 不能为全 0 地址、组播地址、环回地址以及链路本地地址。

mac mac-address: 指定用户的 MAC 地址，格式为 H-H-H。若不指定该参数，则表示不限制该 IP 地址用户的 MAC 地址。

【使用指导】

当管理员允许某些用户不需要通过认证，也能够和相关安全特性的管理下访问网络时，就可以通过本命令将这类用户手工添加为身份识别用户。

若 **undo** 命令中不指定 **bind** 参数，则表示删除使用指定用户名的所有静态类型的身份识别用户。

可以通过多次执行本命令添加多个静态类型的身份识别用户。

一个用户名可以绑定多个 IP 地址或者多个 IP 地址和 MAC 地址的组合，但同一个 IP 地址或者 IP 地址和 MAC 地址的组合不能被多个用户名绑定。

配置的静态类型的身份识别用户，只有在用户身份识别功能处于开启状态，且能够匹配上本地身份识别用户账户的情况下，才能生成对应的静态在线身份识别用户。

【举例】

配置一个静态类型的身份识别用户：用户名为 test，身份识别域为 dom1，绑定的 IP 地址为 109.15.0.15。

```
<Sysname> system-view  
[Sysname] user-identity static-user test domain dom1 bind ipv4 109.15.0.15
```

【相关配置】

- **display user-identity online-user**
- **user-identity enable**

1.1.28 user-identity user-account auto-import policy

user-identity user-account auto-import policy 命令用来开启身份识别用户账户自动导入功能。

undo user-identity user-account auto-import policy 命令用来关闭身份识别用户账户自动导入功能。

【命令】

user-identity user-account auto-import policy *policy-name*
undo user-identity user-account auto-import policy *policy-name*

【缺省情况】

身份识别用户自动账户导入功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 身份识别用户导入策略名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

开启指定策略的身份识别用户账户自动导入功能后，身份识别模块首先会从该策略指定的服务器上导入所有身份识别用户账户信息和所有在线身份识别用户信息，然后定期从该服务器上自动导入身份识别用户账户信息（导入周期由 **account-update-interval** 命令配置）。

需要注意的是，成功导入在线身份识别用户信息的前提是，用户身份识别功能处于开启状态（通过 **user-identity enable** 命令配置）。

【举例】

```
# 开启策略 policy1 的身份识别用户账户自动导入功能。  
<Sysname> system-view  
[Sysname] user-identity user-account auto-import policy policy1
```

【相关命令】

- **account-update-interval**
- **user-identity user-import-policy**

1.1.29 user-identity user-account export url

user-identity user-account export url 命令用来将身份识别用户账户导出到 CSV 文件。

【命令】

```
user-identity user-account export url url-string [ { domain domain-name |  
null-domain } [ user user-name ] | template ] [ vpn-instance  
vpn-instance-name ]
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

url-string: URL，为 1~255 字符的字符串，不区分大小写。

domain domain-name: 身份识别域的名称，为 1~255 个字符的字符串，不区分大小写。

null-domain: 表示导出未加入身份识别域的所有身份识别用户账户信息。

user user-name: 身份识别用户账户名，为 1~55 个字符的字符串，区分大小写。若不指定该参数，则表示指定条件下的所有身份识别用户账户。

template: 表示导出一个标准的 CSV 文件模板。用户可根据此模板编辑符合设备要求的 CSV 文件用于导入身份识别用户。

vpn-instance vpn-instance-name: 表示 CSV 文件保存路径所属 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定该参数，则表示 CSV 文件保存路径位于公网。

【使用指导】

身份识别用户账户信息导出时必须以 CSV 格式保存，即保存的文件扩展名为 csv。

若不指定任何参数，则表示将设备上的所有身份识别用户账户信息导出到一个 CSV 文件。

本命令支持 TFTP 和 FTP 两种文件上传方式，具体的 URL 格式要求如下：

- TFTP 协议 URL 格式：tftp://server/path/filename，server 为 TFTP 服务器 IP 地址或主机名，例如 tftp://1.1.1.1/user/user.csv。
- FTP 协议 URL 格式：
 - 携带用户名和密码的格式为 ftp://username:password@server/path/filename。其中，username 为 FTP 用户名，password 为 FTP 认证密码，server 为 FTP 服务器 IP 地址或主机名，例如 ftp://1:1@1.1.1.1/user/user.csv。如果 FTP 用户名中携带域名，则该域名会被设备忽略，例如 ftp://1@abc:1@1.1.1.1/user/user.csv 将被当作 ftp://1:1@1.1.11/user/user.csv 处理。
 - 不需要携带用户名和密码的格式为 ftp://server/path/filename，例如 ftp://1.1.1.1/user/user.csv。
 - FTP 协议 URL 字符串中的用户名或密码携带 [表 1-9](#) 中的特殊字符时，需要按照对应的输入格式输入才能正常执行操作。

表1-9 特殊字符输入对照表

特殊字符	输入格式
\	\\
"	\"
/	%2F
:	%3A
@	%40

成功执行该命令后，将会在目标服务器上生成一个指定名称的 CSV 文件。若相同配置条件下重复导出，新的文件将会覆盖已有文件。

【举例】

将身份识别域 **dom1** 中的所有身份识别用户账户信息导出到 CSV 文件中，文件保存路径为 **tftp://1.1.1.1/user.csv**。

```
<Sysname> system-view
```

```
[Sysname] user-identity user-account export url tftp://1.1.1.1/user.csv domain dom1
```

【相关命令】

- **user-identity user-account import url**

1.1.30 user-identity user-account import policy

user-identity user-account import policy 命令用来导入服务器上的身份识别用户账户。

【命令】

```
user-identity user-account import policy policy-name
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: 身份识别用户导入策略名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

执行该命令后，系统将立即向身份识别用户导入策略中指定的服务器发起请求，并导入服务器上的所有身份识别用户账户信息。

【举例】

从名称为 **policy1** 的身份识别用户导入策略指定的服务器上导入身份识别用户账户。

```
<Sysname> system-view
```

```
[Sysname] user-identity user-account import policy policy1
```

【相关命令】

- **user-identity user-import-policy**

1.1.31 user-identity user-account import url

user-identity user-account import url 命令用来从 CSV 文件中导入身份识别用户账户。

【命令】

```
user-identity user-account import url url-string [ vpn-instance  
vpn-instance-name ] [ auto-create-group | override | start-line line-number ]  
*
```

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

url-string: 要导入的 CSV 文件的 URL，为 1~255 个字符的字符串，不区分大小写。

vpn-instance vpn-instance-name: 表示待导入 CSV 文件所属 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定该参数，则表示 CSV 文件保存路径位于公网。

auto-create-group: 表示当设备上不存在身份识别用户账户所属的身份识别用户组时，系统会自动创建该身份识别用户组。若不指定该参数，则表示当设备上不存在该身份识别用户组时，系统不会创建该身份识别用户组。

override: 表示当导入的身份识别用户账户已经存在于设备上时，系统使用导入的身份识别用户账户覆盖掉已有的同名身份识别用户账户。若不指定该参数，则表示不导入文件中的同名身份识别用户账户信息，即保留设备上原有的同名身份识别用户账户信息。

start-line line-number: 表示从 CSV 文件的指定行开始导入身份识别用户账户。
line-number 为文件内容的行编号，取值范围为 1~1048576。若不指定该参数，则表示从文件中第一行开始导入。

【使用指导】

导入文件必须是 CSV 格式，即文件扩展名为 csv。

可以通过 **user-identity user-account export url** 命令导出符合导入要求的 CSV 文件模板。

【举例】

从 ftp://1.1.1.1/newpath 路径的 user.csv 文件中导入身份识别用户账户信息，且从该文件的第二行开始导入。

```
<Sysname> system-view
```

```
[Sysname] user-identity user-account import url ftp://1.1.1.1/newpath/user.csv start-line  
2
```


【相关命令】

- **user-identity user-account export url**

1.1.32 user-identity user-import-policy

user-identity user-import-policy 命令用来创建身份识别用户导入策略，并进入身份识别用户导入策略视图。如果指定的身份识别用户导入策略已经存在，则直接进入身份识别用户导入策略视图。

undo user-identity user-import-policy 命令用来删除指定的身份识别用户导入策略。

【命令】

user-identity user-import-policy *policy-name*

undo user-identity user-import-policy *policy-name*

【缺省情况】

不存在身份识别用户导入策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: 策略名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

身份识别用户导入策略用于配置用户身份识别模块从服务器上导入身份识别用户信息的策略，可导入的用户信息包括身份识别用户账户信息和在线身份识别用户信息。目前，系统支持的服务器为 UNIS iMC 服务器和 LDAP 服务器。

系统中仅能存在一个身份识别用户导入策略。如需配置其它身份识别用户导入策略，请先通过 **undo user-identity user-import-policy** 命令删除已有的身份识别用户导入策略。

【举例】

创建名称为 policy1 的身份识别用户导入策略，并进入该策略视图。

```
<Sysname> system-view
```

```
[Sysname] user-identity user-import-policy policy1
```

```
[Sysname-identity-user-impolicy-policy1]
```

【相关命令】

- **display user-identity user-import-policy**

1.1.33 vpn-instance

vpn-instance 命令用来配置 RESTful 服务器所属的 VPN。

undo vpn-instance 命令用来恢复缺省情况。

【命令】

```
vpn-instance vpn-instance-name  
undo vpn-instance
```

【缺省情况】

未配置 RESTful 服务器的 VPN，表示 RESTful 服务器位于公网。

【视图】

RESTful 服务器视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

vpn-instance-name: MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

本命令指定的 VPN 为设备与 RESTful 服务器通信的接口所属的 VPN。

【举例】

```
# 配置 RESTful 服务器的所属的 VPN 为 v1。  
<Sysname> system-view  
[Sysname] user-identity restful-server r1  
[Sysname-restfulserver-r1] vpn-instance v1
```

【相关命令】

- **display user-identity restful-server**
- **user-identity restful-server**

目 录

1 ND攻击防御	1-1
1.1 ND协议报文源MAC地址一致性检查命令	1-1
1.1.1 ipv6 nd check log enable	1-1
1.1.2 ipv6 nd mac-check enable	1-1

1 ND攻击防御

1.1 ND协议报文源MAC地址一致性检查命令

1.1.1 ipv6 nd check log enable

ipv6 nd check log enable 命令用来开启 ND 日志信息功能。

undo ipv6 nd check log enable 命令用来关闭 ND 日志信息功能。

【命令】

```
ipv6 nd check log enable
undo ipv6 nd check log enable
```

【缺省情况】

ND 日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

设备生成的 ND 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

为了防止设备输出过多的 ND 日志信息，一般情况下建议不要开启此功能。

【举例】

```
# 开启 ND 日志信息功能。
<Sysname> system-view
[Sysname] ipv6 nd check log enable
```

1.1.2 ipv6 nd mac-check enable

ipv6 nd mac-check enable 命令用来开启 ND 协议报文源 MAC 地址一致性检查功能。

undo ipv6 nd mac-check enable 命令用来关闭 ND 协议报文源 MAC 地址一致性检查功能。

【命令】

```
ipv6 nd mac-check enable
undo ipv6 nd mac-check enable
```

【缺省情况】

ND 协议报文源 MAC 地址一致性检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

网关设备开启该功能后，会对接收到的 ND 协议报文进行检查，如果 ND 报文中的源 MAC 地址和以太网数据帧首部的源 MAC 地址不一致，则丢弃该报文。

【举例】

开启 ND 协议报文源 MAC 地址一致性检查功能。

```
<Sysname> system-view
```

```
[Sysname] ipv6 nd mac-check enable
```

目 录

1 keychain	1-1
1.1 keychain配置命令	1-1
1.1.1 accept-lifetime	1-1
1.1.2 accept-tolerance	1-3
1.1.3 authentication-algorithm	1-4
1.1.4 default-send-key	1-4
1.1.5 display keychain	1-5
1.1.6 key	1-7
1.1.7 keychain	1-8
1.1.8 key-string	1-9
1.1.9 send-lifetime	1-10
1.1.10 tcp-algorithm-id	1-12
1.1.11 tcp-kind	1-13

1 keychain

1.1 keychain配置命令

1.1.1 accept-lifetime

accept-lifetime 命令用来配置用来校验接收报文时 **key** 的生命周期。

undo accept-lifetime 命令用来恢复缺省情况。

【命令】

```
accept-lifetime daily start-day-time to end-day-time
accept-lifetime date { month-day<1-31> | start-month-day to
end-month-day }
accept-lifetime day { week-day | start-week-day to end-week-day }
accept-lifetime month { month | start-month to end-month }
accept-lifetime utc start-time start-date { duration { duration-value |
infinite } | to end-time end-date }
undo accept-lifetime
```

【缺省情况】

未配置用来校验接收报文时 **key** 的生命周期。

【视图】

key 视图

【缺省用户角色】

network-admin
context-admin

【参数】

daily: 用来校验接收报文时 **key** 在每天指定的时间内生效。

- **start-day-time to end-day-time**: 指定每天内连续的时间范围, **start-day-time** 表示起始时间, **end-day-time** 表示结束时间, 格式均为 HH:MM:SS (小时:分钟:秒), HH 取值范围为 0~23, MM 和 SS 取值范围为 0~59。如果要配置成整分, 则可以不输入秒; 如果要配置成整点, 则可以不输入分和秒。

date: 用来校验接收报文时 **key** 在每月指定的日期内生效。

- **month-day &<1-31>**: 取值范围为 1~31, &<1-31>表示前面的参数最多可以输入 31 次。
- **start-month-day to end-month-day**: 指定每月内的连续日期范围, **start-month-day** 表示起始日期; **end-month-day** 表示结束日期, 结束日期必须大于起始日期。

day: 用来校验接收报文时 **key** 在每周指定的日期内生效。

- **week-day**: 取值为: mon、tue、wed、thu、fri、sat、sun。本参数可输入多次,但不可重复。
- **start-week-day to end-week-day**: 指定每周内的连续日期范围, **start-week-day** 表示起始日期; **end-week-day** 表示结束日期,结束日期必须大于起始日期。

month: 用来校验接收报文时 **key** 在每年指定的月份内生效。

- **month**: 取值为: jan、feb、mar、apr、may、jun、jul、aug、sep、oct、nov、dec。本参数可输入多次,但不可重复。
- **start-month to end-month**: 指定每年内的连续月份范围, **start-month** 表示起始月份; **end-month** 表示结束月份,结束月份必须大于起始月份。

utc: 绝对时间模式的生命周期,表示用来校验接收报文时 **key** 在指定时间范围内(如 2015 年 9 月 1 日 8 点至 2015 年 9 月 3 日 18 点)生效。

- **start-time**: 开始时间,格式为 HH:MM:SS(小时:分钟:秒),取值范围为 0:0:0~23:59:59。如果要配置成整分,则可以不输入秒;如果要配置成整点,则可以不输入分和秒。
- **start-date**: 开始日期,格式为 MM/DD/YYYY(月/日/年)或 YYYY/MM/DD(年/月/日),MM 的取值范围为 1~12,DD 的取值范围与月份有关,YYYY 的取值范围为 2000~2035。
- **duration duration-value**: 指定 **key** 的生命周期从设置的 **start-time** 和 **start-date** 开始所持续时间,取值范围为 1~2147483646,单位为秒。
- **duration infinite**: 表示从设置的 **start-time** 和 **start-date** 开始, **key** 永远可以用来验证接收的报文。
- **to**: 指定结束时间和日期。
- **end-time**: 结束时间,格式为 HH:MM:SS(小时:分钟:秒),取值范围为 0:0:0~23:59:59。
- **end-date**: 结束日期,格式为 MM/DD/YYYY(月/日/年)或 YYYY/MM/DD(年/月/日),MM 的取值范围为 1~12,DD 的取值范围与月份有关,YYYY 的取值范围为 2000~2035。

【使用指导】

只有同时满足如下条件的 **key**,才是有效 **key**,才可被应用程序用于对接收的报文进行校验:

- 配置了认证密钥。
- 配置了认证算法。
- 对于绝对时间模式,系统当前的绝对时间处于 **accept-lifetime** 指定的时间范围内;对于各种周期性时间模式,系统当前的本地时间处于 **accept-lifetime { daily | date | day | month }**指定的时间范围内。

如果应用程序接收到的报文中携带 **key-id** 信息,且该 **key-id** 对应的 **key** 是有效的,则使用该 **key** 对接收到的报文进行校验;如果该 **key-id** 对应的 **key** 是无效的,则报文校验失败。

如果应用程序接收到的报文中没有携带 **key-id** 信息,将使用当前 **keychain** 中所有的有效 **key** 对接收到的报文进行校验,如果接收到的报文无法通过任何一个有效 **key** 的校验,则报文校验失败。应用程序可以使用多个有效 **key** 对接收到的报文进行校验。

【举例】

在工作于绝对时间模式的 **keychain abc** 中,配置用来校验接收报文时 **key 1** 的生命周期为 2015 年 1 月 21 日 12 时 30 分到 2015 年 1 月 21 日 18 点 30 分。

```
<Sysname> system-view
```

```
[Sysname] keychain abc mode absolute
```



```
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] accept-lifetime utc 12:30 2015/1/21 to 18:30 2015/1/21
# 在工作于 weekly 时间模式的 keychain 123 中，配置用来校验接收报文的 key 1 在每周五生效。
<Sysname> system-view
[Sysname] keychain 123 mode periodic weekly
[Sysname-keychain-123] key 1
[Sysname-keychain-123-key-1] accept-lifetime day fri
```

【相关命令】

- **display keychain**

1.1.2 accept-tolerance

accept-tolerance 命令用来为 keychain 中的 key 延长其在报文接收时的生命周期。

undo accept-tolerance 命令用来恢复缺省情况。

【命令】

```
accept-tolerance { value | infinite }
undo accept-tolerance
```

【缺省情况】

没有为 keychain 中的 key 延长其在报文接收时的生命周期。

【视图】

keychain 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

value: 表示 key 的生命周期的延长时间，取值范围为 1~8640000，单位为秒。

infinite: 为指定 keychain 中的 key 无限延长其在报文接收时的生命周期，即 key 在报文接收的过程中永久有效。

【使用指导】

当用户需要修改认证双方的校验信息时，可能会出现由于校验信息的不匹配导致的业务中断。配置本命令后，由 **accept-lifetime utc** 指定的 key 的生命周期的开始和结束时间都将做相应的延长，从而避免上述情况的发生。

【举例】

在工作于绝对时间模式的 keychain abc 中，为 key 延长其在报文接收时的生命周期，延长值为 100 秒。

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] accept-tolerance 100
```

在工作于绝对时间模式的 keychain abc 中，为 key 延长其在报文接收时的生命周期，延长值为无限大。

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] accept-tolerance infinite
```

【相关命令】

- **display keychain**

1.1.3 authentication-algorithm

authentication-algorithm 命令用来配置 key 的认证算法。

undo authentication-algorithm 命令用来恢复缺省情况。

【命令】

```
authentication-algorithm { hmac-md5 | hmac-sha-1 | hmac-sha-256 | md5 }
undo authentication-algorithm
```

【缺省情况】

未配置 key 的认证算法。

【视图】

key 视图

【缺省用户角色】

network-admin
context-admin

【参数】

hmac-md5: HMAC-MD5 认证算法。

hmac-sha-1: HMAC-SHA-1 认证算法。

hmac-sha-256: HMAC-SHA-256 认证算法。

md5: MD5 认证算法。

【使用指导】

如果应用程序不支持 **authentication-algorithm** 配置的认证算法，则无法使用该 key 进行报文校验。

【举例】

在工作于绝对时间模式的 keychain abc 中，配置 key 1 的认证算法为 MD5。

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] authentication-algorithm md5
```

【相关命令】

- **display keychain**

1.1.4 default-send-key

default-send-key 命令用来为 keychain 指定一个缺省发送 key。

undo default-send-key 命令用来恢复缺省情况。

【命令】

```
default-send-key
undo default-send-key
```

【缺省情况】

keychain 中不存在缺省发送 key。

【视图】

key 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

当 keychain 中的发送 key 处于非活跃状态时，可以通过使用缺省的发送 key 对报文进行认证。同一个 keychain 中，只能将一个 key 指定为缺省的发送 key，且需要为该缺省的发送 key 配置认证算法和认证密钥。

【举例】

```
# 在工作于绝对时间模式的 keychain abc 中，指定 key 1 为缺省发送 key。
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] default-send-key
```

【相关命令】

- **display keychain**

1.1.5 display keychain

display keychain 命令用来显示 keychain 的信息。

【命令】

```
display keychain [ name keychain-name [ key key-id ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

name keychain-name: keychain 名称，为 1~63 个字符的字符串，区分大小写。如果不指定本参数，则显示所有 keychain 的信息。

key key-id: key 的标识符，取值范围为 0~281474976710655。如果不指定本参数，则显示属于某 keychain 的全部 key 的信息。

【举例】

显示 keychain 的信息。

<Sysname> display keychain

```
Keychain name      : abc
Mode               : absolute
Accept tolerance   : 0
TCP kind value     : 254
TCP algorithm value
  HMAC-MD5         : 5
  HMAC-SHA-256     : 7
  MD5              : 3
Default send key ID : None
Active send key ID  : 1
Active accept key IDs: 1 2

Key ID             : 1
Key string          : $c$3$vuJpEX3Lah7xcSR2uqmrTK2IZQJZguJh3g==
Algorithm           : md5
Send lifetime       : 01:00:00 2015/01/22 to 01:00:00 2015/01/25
Send status         : Active
Accept lifetime     : 01:00:00 2015/01/22 to 01:00:00 2015/01/27
Accept status       : Active

Key ID             : 2
Key string          : $c$3$vuJpEX3Lah7xcSR2uqmrTK2IZQJZguJh3g==
Algorithm           : md5
Send lifetime       : 01:00:01 2015/01/25 to 01:00:00 2015/01/27
Send status         : Inactive
Accept lifetime     : 01:00:00 2015/01/22 to 01:00:00 2015/01/27
Accept status       : Active
```

表1-1 display keychain 命令显示信息描述表

字段	描述
Keychain name	keychain名称

字段	描述
Mode	keychain的时间模式： - absolute: 绝对时间模式 - periodic daily: 按天的周期性时间模式 - periodic weekly: 按周的周期性时间模式 - periodic monthly: 按月的周期性时间模式 - periodic yearly: 按年的周期性时间模式
Accept tolerance	key在报文接收时的容忍度，单位为秒
TCP kind value	TCP增强认证选项中的类型值。缺省情况下为254
TCP algorithm value	TCP认证算法所对应的算法ID。缺省情况下，HMAC-MD5对应的算法ID为5，HMAC-SHA-256认证算法的算法ID是7，MD5对应的算法ID为3
Default send key ID	缺省发送key的ID、以及缺省发送key的状态
Active send key ID	用于对发送报文进行校验的有效key
Active accept key IDs	用于对接收报文进行校验的有效key
Key ID	key的标识符
Key string	key的认证密钥（密文形式）
Algorithm	key的认证算法： - hmac-md5: HMAC-MD5 认证算法 - hmac-sha-1: HMAC-SHA-1 认证算法 - hmac-sha-256: HMAC-SHA-256 认证算法 - md5: MD5 认证算法
Send lifetime	用来校验发送报文时key的生命周期
Send status	用来校验发送报文时，key是否有效： - Active: key 有效 - Inactive: key 无效
Accept lifetime	用来校验接收报文时key的生命周期
Accept status	用来校验接收报文时，key是否有效： - Active: key 有效 - Inactive: key 无效

1.1.6 key

key 命令用来创建一个 key，并进入 key 视图。如果指定的 key 已经存在，则直接进入 key 视图。
undo key 命令用来删除指定的 key 及 key 视图下的所有配置。

【命令】

key *key-id*

undo key *key-id*

【缺省情况】

不存在 key。

【视图】

keychain 视图

【缺省用户角色】

network-admin

context-admin

【参数】

key-id: key 的标识符，取值范围为 0~281474976710655。

【使用指导】

一个 keychain 下可以配置多个 key，各个 key 必须指定不同的 *key-id*。

【举例】

在工作于绝对时间模式的 keychain abc 中，创建标识符为 1 的 key，并进入 key 视图。

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1]
```

【相关命令】

- **display keychain**

1.1.7 keychain

keychain 命令用来创建一个 keychain，并进入 keychain 视图。如果指定的 keychain 已经存在，则直接进入 keychain 视图。

undo keychain 命令用来删除指定的 keychain 及 keychain 视图下的所有配置。

【命令】

```
keychain keychain-name [ mode { absolute | periodic { daily | monthly | weekly | yearly } } ]
```

```
undo keychain keychain-name
```

【缺省情况】

不存在 keychain。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

keychain-name: keychain 名，为 1~63 个字符的字符串，区分大小写。

mode: keychain 工作的时间模式。

absolute: 绝对时间模式。该模式的 keychain 中，key 的生命周期是从指定的起始日期、时间到指定的结束日期、时间，各个日期和时间都是 UTC（UTC，Coordinated Universal Time，国际协调时间）绝对时间，不受系统的时区和夏令时的影响。

periodic: 周期性时间模式。所有周期性时间模式的 keychain 中，key 的生命周期都是根据系统的本地时间计算的，会受到系统的时区和夏令时的影响。

daily: 按天的周期性时间模式。

monthly: 按月的周期性时间模式。

weekly: 按周的周期性时间模式。

yearly: 按年的周期性时间模式。

【使用指导】

创建 keychain 时必须指定其工作的时间模式。对于已存在的 keychain，不可修改其工作的时间模式。进入已存在的 keychain 视图时可以不指定其工作的时间模式。

【举例】

创建名为 abc 的 keychain，指定其工作在绝对时间模式下，并进入 keychain 视图。

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc]
```

【相关命令】

- **display keychain**

1.1.8 key-string

key-string 命令用来配置 key 的认证密钥。

undo key-string 命令用来恢复缺省情况。

【命令】

```
key-string { cipher | plain } string
undo key-string
```

【缺省情况】

未配置 key 的认证密钥。

【视图】

key 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

cipher: 以密文方式设置密钥。

plain: 以明文方式设置密钥，该密码将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~255 个字符的字符串，密文密钥为 33~373 个字符的字符串。

【使用指导】

key 的认证密钥的明文长度有可能会超出应用程序支持的范围，这种情况下应用程序需要截取自己支持的长度范围的明文密钥来对报文进行校验。

【举例】

在工作于绝对时间模式的 keychain abc 中，以明文形式设置 key 1 的密钥为 123456。

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] key-string plain 123456
```

【相关命令】

- **display keychain**

1.1.9 send-lifetime

send-lifetime 命令用来配置用来校验发送报文时 **key** 的生命周期。

undo send-lifetime 命令用来恢复缺省情况。

【命令】

```
send-lifetime daily start-day-time to end-day-time
send-lifetime date { month-day<1-31> | start-month-day to end-month-day }
send-lifetime day { week-day | start-week-day to end-week-day }
send-lifetime month { month | start-month to end-month }
send-lifetime utc start-time start-date { duration { duration-value |
infinite } | to end-time end-date }
undo send-lifetime
```

【缺省情况】

未配置用来校验发送报文时 **key** 的生命周期。

【视图】

key 视图

【缺省用户角色】

network-admin
context-admin

【参数】

daily: 用来校验发送报文时 **key** 在每天指定的时间内生效。

- **start-day-time to end-day-time:** 指定每天内连续的时间范围, *start-day-time* 表示起始时间, *end-day-time* 表示结束时间, 格式均为 HH:MM:SS (小时:分钟:秒), HH 取值范围为 0~23, MM 和 SS 取值范围为 0~59。如果要配置成整分, 则可以不输入秒; 如果要配置成整点, 则可以不输入分和秒。

date: 用来校验发送报文时 key 在每月指定的日期内生效。

- **month-day &<1-31>:** 取值范围为 1~31, &<1-31>表示前面的参数最多可以输入 31 次。
- **start-month-day to end-month-day:** 指定每月内的连续日期范围, *start-month-day* 表示起始日期; *end-month-day* 表示结束日期, 结束日期必须大于起始日期。

day: 用来校验发送报文时 key 在每周指定的日期内生效。

- **week-day:** 取值为: mon、tue、wed、thu、fri、sat、sun。本参数可输入多次, 但不可重复。
- **start-week-day to end-week-day:** 指定每周内的连续日期范围, *start-week-day* 表示起始日期; *end-week-day* 表示结束日期, 结束日期必须大于起始日期。

month: 用来校验发送报文时 key 在每年指定的月份内生效。

- **month:** 取值为: jan、feb、mar、apr、may、jun、jul、aug、sep、oct、nov、dec。本参数可输入多次, 但不可重复。
- **start-month to end-month:** 指定每年内的连续月份范围, *start-month* 表示起始月份; *end-month* 表示结束月份, 结束月份必须大于起始月份。

utc: 绝对时间模式的生命周期, 表示用来校验发送报文时 key 在指定时间范围内 (如 2015 年 9 月 1 日 8 点至 2015 年 9 月 3 日 18 点) 生效。

- **start-time:** 开始时间, 格式为 HH:MM:SS (小时:分钟:秒), 取值范围为 0:0:0~23:59:59。如果要配置成整分, 则可以不输入秒; 如果要配置成整点, 则可以不输入分和秒。
- **start-date:** 开始日期, 格式为 MM/DD/YYYY (月/日/年) 或 YYYY/MM/DD (年/月/日), MM 的取值范围为 1~12, DD 的取值范围与月份有关, YYYY 的取值范围为 2000~2035。
- **duration duration-value:** 指定 key 的生命周期从设置的 *start-time* 和 *start-date* 开始所持续时间, 取值范围为 1~2147483646, 单位为秒。
- **duration infinite:** 表示从设置的 *start-time* 和 *start-date* 开始, key 永远可以用来验证发送的报文。
- **to:** 指定结束时间和日期。
- **end-time:** 结束时间, 格式为 HH:MM:SS (小时:分钟:秒), 取值范围为 0:0:0~23:59:59。
- **end-date:** 结束日期, 格式为 MM/DD/YYYY (月/日/年) 或 YYYY/MM/DD (年/月/日), MM 的取值范围为 1~12, DD 的取值范围与月份有关, YYYY 的取值范围为 2000~2035。

【使用指导】

只有同时满足如下条件的 key, 才是有效 key, 才可被应用程序用于对发送的报文进行校验:

- 配置了认证密钥。
- 配置了认证算法。
- 对于绝对时间模式, 系统当前的绝对时间处于 **send-lifetime utc** 指定的时间范围内; 对于各种周期性时间模式, 系统当前的本地时间处于 **send-lifetime { daily | date | day | month }** 指定的时间范围内。

同一个 keychain 内的各个 key 使用 **send-lifetime** 指定的生命周期不可重叠，以确保在同一时刻，应用程序只使用一个 key 对发送的报文进行校验。

【举例】

在工作于绝对时间模式的 keychain abc 下，配置用来校验发送报文时 key 1 的生命周期为 2015 年 1 月 21 日 12 时 30 分到 2015 年 1 月 21 日 18 点 30 分。

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] key 1
[Sysname-keychain-abc-key-1] send-lifetime utc 12:30 2015/1/21 to 18:30 2015/1/21
```

在工作于 weekly 时间模式的 keychain 123 下，配置用来校验接收报文的 key 1 在每周五生效。

```
<Sysname> system-view
[Sysname] keychain 123 mode periodic weekly
[Sysname-keychain-123] key 1
[Sysname-keychain-123-key-1] send-lifetime day fri
```

【相关命令】

- **display keychain**

1.1.10 tcp-algorithm-id

tcp-algorithm-id 命令用来配置 keychain 支持的 TCP 认证算法的算法 ID。

undo tcp-algorithm-id 命令用来恢复缺省情况。

【命令】

```
tcp-algorithm-id { hmac-md5 | hmac-sha-256 | md5 } algorithm-id
undo tcp-algorithm-id { hmac-md5 | hmac-sha-256 | md5 }
```

【缺省情况】

MD5 认证算法的算法 ID 是 3，HMAC-MD5 认证算法的算法 ID 是 5，HMAC-SHA-256 认证算法的算法 ID 是 7。

【视图】

keychain 视图

【缺省用户角色】

network-admin
context-admin

【参数】

hmac-md5: 采用 HMAC-MD5 认证算法，密钥长度为 16 字节。

hmac-sha-256: 采用 HMAC-SHA-256 认证算法，密钥长度为 16 字节。

md5: 采用 MD5 认证算法，密钥长度为 16 字节。

algorithm-id: 认证算法的算法 ID，取值范围为 1~63。

【使用指导】

建立 TCP 连接时使用 **keychain** 认证的应用程序,其发送和接收的 TCP 报文中会携带增强认证选项,增强认证选项中的 **algorithm-id** 字段用来表示认证算法的算法 ID。由于 **algorithm-id** 不是 IANA (Internet Assigned Numbers Authority, 因特网地址分配组织) 统一定义的,不同的厂商使用 **algorithm-id** 所代表的算法类型不尽相同。在与友商设备互通时,本端对 **algorithm-id** 的配置必须与对端的保持一致,例如,当友商设备中 HMAC-MD5 认证算法的算法 ID 是 3 时,需要在本端设备上配置 **tcp-algorithm-id hmac-md5 3** 命令才能互通。

【举例】

在工作于绝对时间模式的 **keychain abc** 中,配置 HMAC-MD5 认证算法的算法 ID 为 1。

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] tcp-algorithm-id hmac-md5 1
```

【相关命令】

- **display keychain**

1.1.11 tcp-kind

tcp-kind 命令用来配置 TCP 增强认证选项中的类型值。

undo tcp-kind 命令用来恢复缺省情况。

【命令】

```
tcp-kind kind-value
undo tcp-kind
```

【缺省情况】

TCP 增强认证选项中的类型值为 254。

【视图】

keychain 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

kind-value: TCP 增强认证选项中的类型值,取值范围为 28~255。

【使用指导】

建立 TCP 连接时使用 **keychain** 认证的应用程序,其发送和接收的 TCP 报文中会携带增强认证选项,通信双方所指定的增强认证选项中的类型值必须保持一致,否则会导致报文校验失败。

【举例】

在工作于绝对时间模式的 **keychain abc** 下,配置 TCP 增强认证选项中的类型值为 252。

```
<Sysname> system-view
[Sysname] keychain abc mode absolute
[Sysname-keychain-abc] tcp-kind 252
```

【相关命令】

- `display keychain`

目 录

1 IP-MAC绑定	1-1
1.1 IP-MAC绑定配置命令	1-1
1.1.1 display ip-mac binding ipv4	1-1
1.1.2 display ip-mac binding ipv6	1-2
1.1.3 display ip-mac binding statistics	1-3
1.1.4 display ip-mac binding status	1-4
1.1.5 ip-mac binding enable	1-5
1.1.6 ip-mac binding interface	1-6
1.1.7 ip-mac binding ipv4	1-6
1.1.8 ip-mac binding ipv6	1-7
1.1.9 ip-mac binding no-match action deny	1-9
1.1.10 reset ip-mac binding statistics	1-9

1 IP-MAC绑定

1.1 IP-MAC绑定配置命令

1.1.1 display ip-mac binding ipv4

display ip-mac binding ipv4 命令用来显示 IPv4-MAC 绑定表项。

【命令】

display ip-mac binding ipv4 [*ipv4-address*] [**mac-address** *mac-address*]
[**vlan** *vlan-id* | **vpn-instance** *vpn-instance-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ipv4-address: 显示指定 IPv4 地址的 IPv4-MAC 绑定表项，该地址不能为全 0 地址、组播地址、环回地址。如果未指定该参数，则显示所有 IPv4 地址的 IPv4-MAC 绑定表项。

mac-address mac-address: 显示指定 MAC 地址的 IPv4-MAC 绑定表项，*mac-address* 为绑定的 MAC 地址，格式为 H-H-H。该地址不能为全 0 地址、全 F 地址以及组播 MAC 地址。如果未指定该参数，则显示所有 MAC 地址的 IPv4-MAC 绑定表项。

vlan vlan-id: 显示属于指定 VLAN 的 IPv4-MAC 绑定表项，*vlan-id* 为指定 VLAN 的编号，取值范围为 1~4094。若未指定本参数，则表示显示属于所有 VLAN 的 IPv4-MAC 绑定表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的 IPv4-MAC 绑定表项。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，则表示显示公网中的 IPv4-MAC 绑定表项。

【举例】

显示 IPv4-MAC 绑定表项。

<Sysname> display ip-mac binding ipv4

Total entries: 1

IP address	MAC address	VPN instance	VLAN ID
1.1.1.1	0000-0000-0001	--	N/A

表1-1 display ip-mac binding ipv4 命令显示信息描述表

字段	描述
Total entries	IPv4-MAC绑定表项总数

字段	描述
IP address	IPv4-MAC绑定表项的IPv4地址
MAC address	IPv4-MAC绑定表项的MAC地址
VPN instance	IPv4-MAC绑定表项所属的VPN实例名称，属于公网时显示为“--”
VLAN ID	IPv4-MAC绑定表项所属的VLAN

【相关命令】

- ip-mac binding ipv4**

1.1.2 display ip-mac binding ipv6

display ip-mac binding ipv6 命令用来显示 IPv6-MAC 绑定表项。

【命令】

```
display ip-mac binding ipv6 [ ipv6-address ] [ mac-address mac-address ]
[ vlan vlan-id | vpn-instance vpn-instance-name ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

ipv6-address: 显示指定 IPv6 地址的 IPv6-MAC 绑定表项，该地址不能为全 0 地址、组播地址、环回地址。如果未指定该参数，则显示所有 IPv6 地址的 IPv6-MAC 绑定表项。

mac-address mac-address: 显示指定 MAC 地址的 IPv6-MAC 绑定表项，*mac-address* 为绑定的 MAC 地址，格式为 H-H-H。该地址不能为全 0 地址、全 F 地址以及组播 MAC 地址。如果未指定该参数，则显示所有 MAC 地址的 IPv6-MAC 绑定表项。

vlan vlan-id: 显示属于指定 VLAN 的 IPv4-MAC 绑定表项，*vlan-id* 为指定 VLAN 的编号，取值范围为 1~4094。若未指定本参数，则表示显示属于所有 VLAN 的 IPv4-MAC 绑定表项。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的 IPv6-MAC 绑定表项。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。该 VPN 实例必须已经存在。若未指定本参数，则表示显示公网中的 IPv4-MAC 绑定表项。

【举例】

显示 IPv6-MAC 绑定表项。

```
<Sysname> display ip-mac binding ipv6
```

```
Total entries: 1
```

IP address	MAC address	VPN instance	VLAN ID
10::10	0000-0000-0001	--	N/A

表1-2 display ip-mac binding ipv6 命令显示信息描述表

字段	描述
Total entries	IPv6-MAC绑定表项总数
IP address	IPv6-MAC绑定表项的IPv6地址
MAC address	IPv6-MAC绑定表项的MAC地址
VPN instance	IPv6-MAC绑定表项所属的VPN实例名称，属于公网时显示为“--”
VLAN ID	IPv6-MAC绑定表项所属的VLAN

【相关命令】

- **ip-mac binding ipv6**

1.1.3 display ip-mac binding statistics

display ip-mac binding statistics 命令用来显示 IP-MAC 绑定功能过滤报文的统计信息。

【命令】

display ip-mac binding statistics [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备上 IP-MAC 绑定功能过滤报文的统计信息, *slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数, 则显示所有成员设备上 IP-MAC 绑定功能过滤报文的统计信息。

【使用指导】

本命令会对 IP-MAC 绑定功能过滤的所有报文进行统计。

当配置未匹配 IP-MAC 绑定表项报文的缺省动作为阻断时, 与 IP-MAC 绑定表项不一致而被过滤的报文不会分别进行统计, 而是会统计在未匹配 IP-MAC 绑定表项丢弃的 IPv4 报文数目中。

【举例】

```
# 显示指定 Slot 上 IP-MAC 绑定功能过滤报文的统计信息。
<Sysname> display ip-mac binding statistics slot 1
Slot 1:
Statistics about dropped packets:
IPv4 drop statistics:
    IPv4 ip-mac binding dropped packets because partial match ip: 3
```



```

IPv4 ip-mac binding dropped packets because partial match mac: 0
IPv4 ip-mac binding dropped packets because no match entry: 12
IPv6 drop statistics:
IPv6 ip-mac binding dropped packets because partial match ip: 0
IPv6 ip-mac binding dropped packets because partial match mac: 0
IPv6 ip-mac binding dropped packets because no match entry: 0

```

表1-3 display ip-mac binding statistics 命令显示信息描述表

字段	描述
IPv4 drop statistics	被丢弃的IPv4报文的统计信息
IPv4 ip-mac binding dropped packets because partial match ip	由于源MAC地址未匹配IP-MAC绑定表项丢弃的IPv4报文数目
IPv4 ip-mac binding dropped packets because partial match mac	由于源IP地址未匹配IP-MAC绑定表项丢弃的IPv4报文数目
IPv4 ip-mac binding dropped packets because no match entry	由于源IP地址和源MAC地址均未匹配IP-MAC绑定表项丢弃的IPv4报文数目
IPv6 drop statistics	被丢弃的IPv6报文的统计信息
IPv6 ip-mac binding dropped packets because partial match ip	由于源MAC地址未匹配IP-MAC绑定表项丢弃的IPv6报文数目
IPv6 ip-mac binding dropped packets because partial match mac	由于源IP地址未匹配IP-MAC绑定表项丢弃的IPv6报文数目
IPv6 ip-mac binding dropped packets because no match entry	由于源IP地址和源MAC地址均未匹配IP-MAC绑定表项丢弃的IPv6报文数目

【相关命令】

- **reset ip-mac binding statistics**

1.1.4 display ip-mac binding status

display ip-mac binding status 命令用来显示 IP-MAC 绑定功能状态。

【命令】

display ip-mac binding status

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【使用指导】

通过该命令可以查看 IP-MAC 绑定功能的开启状态以及对于未匹配地址绑定表的报文的默认处理动作。

【举例】

```
# 显示 IP-MAC 绑定功能状态。  
<Sysname> display ip-mac binding status  
ip-mac binding: Disabled  
ip-mac binding no-match action: Deny
```

表1-4 display ip-mac binding status 命令显示信息描述表

字段	描述
ip-mac binding	表示IP-MAC绑定功能的状态，包括： - Enabled: 开启 - Disabled: 关闭
ip-mac binding no-match action	表示未匹配地址绑定表的报文的默认动作，包括： - Permit: 放行 - Deny: 丢弃

1.1.5 ip-mac binding enable

ip-mac binding enable 命令用来开启 IP-MAC 绑定功能。
undo ip-mac binding enable 命令用来关闭 IP-MAC 绑定功能。

【命令】

```
ip-mac binding enable  
undo ip-mac binding enable
```

【缺省情况】

IP-MAC 绑定功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

IP-MAC 绑定功能是指在设备上建立 IP 地址与 MAC 地址的绑定表项，并依据该表项对接收的报文进行过滤。具体的过滤机制为：如果源 IP 地址和源 MAC 地址均与 IP-MAC 绑定表项一致，则转发该报文；如果源 IP 地址或源 MAC 地址未匹配 IP-MAC 绑定表项，则认为该报文是非法报文，并将其丢弃；如果源 IP 地址和源 MAC 地址均未匹配 IP-MAC 绑定表项，则报文的处理方式由用户配置的缺省动作决定。

本功能生成的绑定关系属于静态绑定，所以只适用于用户的 IP 地址是固定的情况。如果用户采用 DHCP 方式进行 IP 地址的动态分配，则不建议使用本功能，如果使用，可能会造成正常用户无法通信。

【举例】

```
# 开启 IP-MAC 绑定功能
<Sysname> system-view
[Sysname] ip-mac binding enable
```

1.1.6 ip-mac binding interface

ip-mac binding interface 命令用来批量生成 IP-MAC 绑定表项。

【命令】

ip-mac binding interface *interface-type interface-number*

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interface-type interface-number：表示指定接口的接口类型和接口编号。接口类型只能为三层以太网接口及其子接口、三层聚合接口及其子接口、冗余接口及其子接口以及 VLAN 接口。

【使用指导】

可通过执行本命令将指定接口下的 ARP 表项和 ND 表项批量加入地址绑定表中。对于根据 ARP 表项和 ND 表项生成的但与地址绑定表中已有内容冲突的表项，设备保留原有表项，只将无冲突的新生成表项添加到地址绑定表中。

执行本命令后，只会将指定接口下现有的 ARP 表项和 ND 表项批量加入地址绑定表中。若需要将后续新增的 ARP 表项和 ND 表项加入地址绑定表中，则需要再次执行本命令。

对于批量生成的 IP-MAC 绑定表项，需要通过 **undo ip-mac binding ipv4** 或 **undo ip-mac binding ipv6** 命令删除。

IP-MAC 绑定表项为静态表项，因此在执行绑定操作后，不会随原接口下 ARP 表项或 ND 表项的变化而变化。

【举例】

```
# 批量生成 IP-MAC 绑定表项。
<Sysname> system-view
[Sysname] ip-mac binding interface gigabitethernet 0/0/1
```

1.1.7 ip-mac binding ipv4

ip-mac binding ipv4 命令用来配置 IPv4-MAC 绑定表项。

undo ip-mac binding ipv4 命令用来删除 IPv4-MAC 绑定表项。

【命令】

ip-mac binding ipv4 *ipv4-address mac-address mac-address* [**vlan** *vlan-id* | **vpn-instance** *vpn-instance-name*]

```
undo ip-mac binding ipv4 { all | ipv4-address mac-address mac-address [ vlan  
vlan-id | vpn-instance vpn-instance-name ] }
```

【缺省情况】

未配置 IPv4-MAC 绑定表项。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-address: 指定 IPv4-MAC 绑定表项的 IPv4 地址，该地址不能为全 0 地址、组播地址、环回地址。

mac-address mac-address: 指定 IPv4-MAC 绑定表项的 MAC 地址，*mac-address* 为绑定 MAC 地址，格式为 H-H-H。该地址不能为全 0 地址、全 F 地址以及组播 MAC 地址。

vlan vlan-id: 指定 IPv4-MAC 绑定表项所属的 VLAN，*vlan-id* 为指定 VLAN 的编号，取值范围为 1~4094。

vpn-instance vpn-instance-name: 指定 IPv4-MAC 绑定表项所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。该 VPN 实例必须已经存在。如果未指定本参数，则表示 IPv4-MAC 绑定表项属于公网。

all: 删除所有 IPv4-MAC 绑定表项。

【使用指导】

如果 IPv4 地址与 MAC 地址的绑定关系可以预先确定，则可以通过静态配置的方式进行绑定。在配置时，对于一个 IPv4 地址，只能绑定一个 MAC 地址；对于一个 MAC 地址，可以绑定多个 IPv4 地址。当需要修改某个表项中 IPv4 地址绑定的 MAC 地址时，需要先将原来的表项删除再重新添加新的表项。

本命令配置的 IP-MAC 绑定表项全局生效。设备中最多允许保留 1024 个 IPv4-MAC 绑定表项。

【举例】

配置 IPv4-MAC 绑定表项，允许源 IP 地址为 192.168.0.1 且源 MAC 地址为 0001-0001-0001 的报文通过。

```
<Sysname> system-view
```

```
[Sysname] ip-mac binding ipv4 192.168.0.1 mac-address 0001-0001-0001
```

【相关命令】

- **display ip-mac binding ipv4**

1.1.8 ip-mac binding ipv6

ip-mac binding ipv6 命令用来配置 IPv6-MAC 绑定表项。

undo ip-mac binding ipv6 命令用来删除 IPv6-MAC 绑定表项。

【命令】

```
ip-mac binding ipv6 ipv6-address mac-address mac-address [ vlan vlan-id |  
vpn-instance vpn-instance-name ]  
undo ip-mac binding ipv6 { all | ipv6-address mac-address mac-address [ vlan  
vlan-id | vpn-instance vpn-instance-name ] }
```

【缺省情况】

未配置 IPv6-MAC 绑定表项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address: 指定 IPv6-MAC 绑定表项的 IPv6 地址，该地址不能为全 0 地址、组播地址、环回地址。

mac-address mac-address: 指定 IPv6-MAC 绑定表项的 MAC 地址，*mac-address* 为绑定 MAC 地址，格式为 H-H-H。该地址不能为全 0 地址、全 F 地址以及组播 MAC 地址。

vlan vlan-id: 指定 IPv6-MAC 绑定表项所属的 VLAN，*vlan-id* 为指定 VLAN 的编号，取值范围为 1~4094。

vpn-instance vpn-instance-name: 指定 IPv6-MAC 绑定表项所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。该 VPN 实例必须已经存在。如果未指定本参数，则表示 IPv6-MAC 绑定表项属于公网。

all: 删除所有 IPv6-MAC 绑定表项。

【使用指导】

如果 IPv6 地址与 MAC 地址的绑定关系可以预先确定，则可以通过静态配置的方式进行绑定。在配置时，对于一个 IPv6 地址，只能绑定一个 MAC 地址；对于一个 MAC 地址，可以绑定多个 IPv6 地址。当需要修改某个表项中 IPv6 地址绑定的 MAC 地址时，需要先将原来的表项删除再重新添加新的表项。

本命令配置的 IP-MAC 绑定表项全局生效。设备中最多允许保留 1024 个 IPv6-MAC 绑定表项。

【举例】

配置 IPv6-MAC 绑定表项，允许源 IPv6 地址为 2012::12:25 且源 MAC 地址为 0001-0001-0001 的报文通过。

```
<Sysname> system-view
```

```
[Sysname] ip-mac binding ipv6 2012::12:25 mac-address 0001-0001-0001
```

【相关命令】

- **display ip-mac binding ipv6**

1.1.9 ip-mac binding no-match action deny

ip-mac binding no-match action deny 命令用来配置未匹配 IP-MAC 绑定表项报文的缺省动作为丢弃。

undo ip-mac binding no-match action deny 命令用来恢复默认的缺省动作。

【命令】

```
ip-mac binding no-match action deny
undo ip-mac binding no-match action deny
```

【缺省情况】

未匹配 IP-MAC 绑定表项报文的缺省动作为放行。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

当要求只允许源 IP 和源 MAC 与地址表项完全匹配的报文通过时，可以将未匹配报文的动作配置为 deny。

【举例】

```
# 配置未匹配 IP-MAC 绑定表项的报文的缺省动作为丢弃。
<Sysname> system-view
[Sysname] ip-mac binding no-match action deny
```

1.1.10 reset ip-mac binding statistics

reset ip-mac binding statistics 命令用来清除 IP-MAC 绑定功能过滤报文的统计信息。

【命令】

```
reset ip-mac binding statistics [ slot slot-number ]
```

【视图】

系统视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 清除指定成员设备上 IP-MAC 绑定功能过滤报文的统计信息, *slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数, 则清除所有成员设备上 IP-MAC 绑定功能过滤报文的统计信息。

【举例】

清除 IP-MAC 绑定功能过滤报文的统计信息。

```
<Sysname> reset ip-mac binding statistics
```

【相关命令】

- **display ip-mac binding statistics**

目 录

1 IPoE	1-1
1.1 IPv4 IPoE配置命令	1-1
1.1.1 display ip subscriber interface-leased	1-1
1.1.2 display ip subscriber interface-leased statistics	1-4
1.1.3 display ip subscriber offline statistics	1-5
1.1.4 display ip subscriber session	1-7
1.1.5 display ip subscriber session statistics	1-11
1.1.6 display ip subscriber subnet-leased	1-12
1.1.7 display ip subscriber subnet-leased statistics	1-15
1.1.8 ip subscriber 8021p	1-17
1.1.9 ip subscriber access-user log enable	1-17
1.1.10 ip subscriber dhcp domain	1-19
1.1.11 ip subscriber dhcp max-session	1-20
1.1.12 ip subscriber dhcp password option60	1-20
1.1.13 ip subscriber dhcp username	1-22
1.1.14 ip subscriber dscp	1-23
1.1.15 ip subscriber enable	1-24
1.1.16 ip subscriber initiator dhcp enable	1-25
1.1.17 ip subscriber initiator unclassified-ip enable	1-26
1.1.18 ip subscriber interface-leased	1-27
1.1.19 ip subscriber nas-port-id format	1-28
1.1.20 ip subscriber nas-port-id nasinfo-insert	1-30
1.1.21 ip subscriber nas-port-type	1-31
1.1.22 ip subscriber password	1-32
1.1.23 ip subscriber service-identify	1-33
1.1.24 ip subscriber session static	1-34
1.1.25 ip subscriber subnet-leased	1-35
1.1.26 ip subscriber timer quiet	1-37
1.1.27 ip subscriber trust	1-37
1.1.28 ip subscriber unclassified-ip domain	1-39
1.1.29 ip subscriber unclassified-ip max-session	1-40
1.1.30 ip subscriber unclassified-ip username	1-40
1.1.31 ip subscriber user-detect	1-42

1.1.32 ip subscriber vlan	1-43
1.1.33 ip subscriber whitelist enable	1-44
1.1.34 reset ip subscriber offline statistics	1-45
1.1.35 reset ip subscriber session	1-45
1.2 IPv6 IPoE配置命令	1-46
1.2.1 display ipv6 subscriber interface-leased	1-46
1.2.2 display ipv6 subscriber interface-leased statistics	1-50
1.2.3 display ipv6 subscriber offline statistics	1-51
1.2.4 display ipv6 subscriber session	1-52
1.2.5 display ipv6 subscriber session statistics	1-57
1.2.6 display ipv6 subscriber subnet-leased	1-58
1.2.7 display ipv6 subscriber subnet-leased statistics	1-61
1.2.8 ipv6 subscriber 8021p	1-63
1.2.9 ipv6 subscriber access-user log enable	1-64
1.2.10 ipv6 subscriber dhcp domain	1-65
1.2.11 ipv6 subscriber dhcp max-session	1-66
1.2.12 ipv6 subscriber dhcp password option16	1-66
1.2.13 ipv6 subscriber dhcp username	1-68
1.2.14 ipv6 subscriber dscp	1-69
1.2.15 ipv6 subscriber enable	1-70
1.2.16 ipv6 subscriber initiator dhcp enable	1-71
1.2.17 ipv6 subscriber initiator ndrs enable	1-72
1.2.18 ipv6 subscriber initiator unclassified-ip enable	1-73
1.2.19 ipv6 subscriber interface-leased	1-74
1.2.20 ipv6 subscriber nas-port-id format	1-75
1.2.21 ipv6 subscriber nas-port-id nasinfo-insert	1-77
1.2.22 ipv6 subscriber nas-port-type	1-78
1.2.23 ipv6 subscriber ndrs domain	1-79
1.2.24 ipv6 subscriber ndrs max-session	1-80
1.2.25 ipv6 subscriber ndrs username	1-81
1.2.26 ipv6 subscriber password	1-82
1.2.27 ipv6 subscriber service-identify	1-83
1.2.28 ipv6 subscriber session static	1-84
1.2.29 ipv6 subscriber subnet-leased	1-86
1.2.30 ipv6 subscriber timer quiet	1-87
1.2.31 ipv6 subscriber trust	1-88

1.2.32 ipv6 subscriber unclassified-ip domain	1-89
1.2.33 ipv6 subscriber unclassified-ip max-session	1-90
1.2.34 ipv6 subscriber unclassified-ip username	1-91
1.2.35 ipv6 subscriber user-detect	1-92
1.2.36 ipv6 subscriber vlan	1-94
1.2.37 ipv6 subscriber whitelist enable	1-94
1.2.38 reset ipv6 subscriber offline statistics	1-95
1.2.39 reset ipv6 subscriber session	1-96

1 IPoE

1.1 IPv4 IPoE配置命令

1.1.1 display ip subscriber interface-leased

display ip subscriber interface-leased 命令用来显示 IPv4 IPoE 接口专线用户信息。

【命令】

```
display ip subscriber interface-leased [ interface interface-type
interface-number ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

interface interface-type interface-number: 显示指定接口上的 IPv4 IPoE 接口专线用户信息, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 将显示所有接口上的 IPv4 IPoE 接口专线用户信息。

slot slot-number: 显示指定成员设备上的 IPv4 IPoE 接口专线用户信息, *slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数, 将显示所有成员设备上的 IPv4 IPoE 接口专线用户信息。

【举例】

显示接口 GigabitEthernet1/0/1 上的 IPv4 IPoE 接口专线用户信息。

```
<Sysname> display ip subscriber interface-leased interface gigabitethernet 1/0/1
```

Basic:

```
Access interface      : GE1/0/1
VPN instance          : N/A
Username              : a
User ID               : 0x30000000
State                 : Online
Service node          : Slot 1 CPU 0
Domain                : radius
Login time            : May 14 20:04:42 2014
Online time (hh:mm:ss) : 00:16:37
```

AAA:

```
IP pool              : ipoe
```

Session idle time : N/A
 Session duration : N/A, remaining: N/A
 Remaining traffic : N/A
 Max multicast addresses : 4
 Multicast address list : N/A

QoS:

User profile : unis (active)
 Session group profile : N/A
 Inbound CAR : CIR 1000bps PIR 2000bps CBS 500bit (active)
 Outbound CAR : CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:

Uplink packets/bytes : 0/0
 Downlink packets/bytes : 0/0

ITA:

Level-1 Uplink packets/bytes: 0/0
 Downlink packets/bytes: 0/0
 Level-2 Uplink packets/bytes: 0/0
 Downlink packets/bytes: 0/0

表1-1 display ip subscriber interface-leased 命令显示信息描述表

字段	描述
Basic	IPoE会话的基本信息
Access interface	用户所在的接口名称
VPN instance	用户所属的MPLS L3VPN实例，N/A表示用户属于公网
Username	用户认证时使用的用户名
User ID	用户ID，只有用户在线后才会由系统分配，0xffffffff表示暂未分配
State	用户状态： - Init: 初始化 - Offline: 正在下线 - Auth: 认证中 - AuthFail: 认证失败 - AuthPass: 认证通过 - AssignedIP: 用户已具备 IP 地址 - Online: 用户在线 - Backup: 备份状态，表示该用户是由对端备份到本端的
Service node	为用户提供认证服务的节点信息
Domain	认证使用的认证域名
Login time	用户登录时间，即用户授权成功的时间，格式为设备时间，如：MM-DD hh:mm:ss YYYY
Online time (hh:mm:ss)	用户本次上线的在线时长

字段	描述
AAA	IPoE会话的AAA授权信息
IP pool	AAA授权的DHCP地址池名称，N/A表示AAA未授权该属性
Session idle time	用户闲置切断时间，单位为秒，N/A表示不进行闲置切断
Session duration	AAA授权的IPoE会话超时时间，单位为秒 - N/A: 表示未下发会话时长 - Unlimited: 表示会话时长无限制
remaining	AAA授权的IPoE会话剩余时长 - 当 AAA 未授权 IPoE 会话超时时间时，该字段始终显示为 N/A - 当 AAA 授权 IPoE 会话超时时间时 - 如果用户通过三层以太网接口/三层以太网子接口上线，该字段始终显示具体的剩余时长或 Unlimited（表示会话时长无限制） - 如果用户通过三层聚合接口/三层聚合子接口上线，则只有在本命令中指定 Service node 所在的 slot 或接口时，才会显示具体的剩余时长或 Unlimited（表示会话时长无限制），否则显示为 N/A
Remaining traffic	授权的剩余流量，单位为字节，N/A表示未对用户指定授权流量
Max multicast addresses	AAA授权用户可加入的组播组的最大数目
Multicast address list	AAA授权用户可加入的组播组地址列表，N/A表示AAA未授权该属性
QoS	IPoE会话的QoS信息
User profile	AAA授权的User Profile名称。若未授权User Profile，则显示为N/A。授权状态包括如下： - active: AAA 授权 User Profile 成功 - inactive: AAA 授权 User Profile 失败或者设备上不存在该 User Profile - 授权结果未知
Session group profile	AAA授权的Session Group Profile名称。若未授权Session Group Profile，则显示为N/A。授权状态包括如下： - active: AAA 授权 Session Group Profile 成功 - inactive: AAA 授权 Session Group Profile 失败或者设备上不存在该 Session Group Profile - 授权结果未知
Inbound CAR	入方向CAR值（CIR：入方向平均速率，单位为bps；PIR：入方向峰值速率，单位为bps；CBS：入方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： - active: 表示入方向 CAR 限速下发成功 - inactive: 表示入方向 CAR 限速下发失败
Outbound CAR	出方向CAR值（CIR：出方向平均速率，单位为bps；PIR：出方向峰值速率，单位为bps；CBS：出方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： - active: 表示出方向 CAR 限速下发成功 - inactive: 表示出方向 CAR 限速下发失败

字段	描述
Flow statistic	IPoE会话的流量统计信息
Uplink packets/bytes	上行流量报文数/字节数
Downlink packets/bytes	下行流量报文数/字节数
ITA	IPoE会话的ITA（Intelligent Target Accounting，智能靶向计费）业务流量统计信息
Level- <i>n</i> Uplink packets/bytes	计费等级为 <i>n</i> 的上行流量报文数/字节数， <i>n</i> 的取值范围为1~8
Downlink packets/bytes	计费等级为 <i>n</i> 的下行流量报文数/字节数， <i>n</i> 的取值范围为1~8

【相关命令】

- **ip subscriber enable**

1.1.2 display ip subscriber interface-leased statistics

display ip subscriber interface-leased statistics 命令用来显示 IPv4 IPoE 接口专线用户统计信息。

【命令】

display ip subscriber interface-leased statistics [**interface** *interface-type interface-number*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上的 IPv4 IPoE 接口专线用户统计信息，*interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数，将显示所有接口上 IPv4 IPoE 接口专线用户已经上线和正在上线的统计信息。

slot *slot-number*: 显示指定成员设备上的 IPv4 IPoE 接口专线用户统计信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示所有成员设备上的 IPv4 IPoE 接口专线用户统计信息。

【举例】

显示设备上 IPv4 IPoE 接口专线用户统计信息。

```
<Sysname> display ip subscriber interface-leased statistics
Total          : 100
Init           : 0
```

```

Authenticating      : 20
Authenticate fail   : 0
Authenticate pass    : 20
Assigned IP         : 10
Online              : 50
Backup              : 0

```

表1-2 display ip subscriber interface-leased statistics 命令显示信息描述表

字段	描述
Total	接入的总用户数
Init	处于初始状态的用户数
Authenticating	处于正在认证状态的用户数
Authenticate fail	处于认证失败状态的用户数
Authenticate pass	处于认证成功状态的用户数
Assigned IP	处于拥有IP地址状态的用户数
Online	处于在线状态的用户数
Backup	处于备份状态的用户数

1.1.3 display ip subscriber offline statistics

display ip subscriber offline statistics 命令用来显示 IPv4 IPoE 用户下线原因的统计信息。

【命令】

```
display ip subscriber offline statistics [ interface interface-type interface-number ]
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

interface interface-type interface-number: 显示指定接口上 IPoE 用户下线原因的统计信息, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 将显示所有接口上 IPoE 用户下线原因的统计信息。

【举例】

显示接口 GigabitEthernet1/0/1 上 IPv4 IPoE 用户下线原因的统计信息。

```

<Sysname> display ip subscriber offline statistics interface gigabitethernet 1/0/1
Total                : 100
User request         : 0
DHCP lease expire    : 0
AAA lease expire     : 0
Command cut          : 80
AAA terminate        : 0
Authenticate fail    : 0
Authorization fail    : 0
Idle timeout         : 10
Detect fail          : 10
Not enough resource   : 0
Interface down        : 0
Interface shutdown    : 0
VSRP event           : 0
DHCP notify          : 0
Other                : 0

```

表1-3 display ip subscriber offline statistics 命令显示信息描述表

字段	描述
Total	下线的总用户数
User request	用户主动要求下线的用户数
DHCP lease expire	DHCP租约到期正常下线的用户数
AAA lease expire	AAA租约到期正常下线的用户数
Command cut	通过命令行下线的用户数
AAA terminate	AAA强制下线的用户数
Authenticate fail	认证失败的用户数
Authorization fail	授权失败的用户数
Idle timeout	用户空闲超时下线的用户数
Detect fail	在线探测失败下线的用户数
Not enough resource	硬件资源不足下线的用户数
Interface down	因接口状态为down下线的用户数
Interface shutdown	主动shutdown接口导致下线的用户数
VSRP event	收到VSRP（Virtual Service Redundancy Protocol，虚拟业务冗余协议）事件通知而下线的用户数
DHCP notify	DHCP通知下线的用户数
Other	其它状况触发下线的用户数

【相关命令】

- **reset ip subscriber offline statistics**

1.1.4 display ip subscriber session

display ip subscriber session 命令用来显示 IPv4 IPoE 个人会话信息。

【命令】

```
display ip subscriber session [ interface interface-type interface-number ]  
[ domain domain-name | ip ip-address [ vpn-instance vpn-instance-name ] | mac  
mac-address | static | username name ] [ slot slot-number ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上的 IPv4 IPoE 个人会话，*interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数，将显示所有接口上的 IPv4 IPoE 个人会话。

domain *domain-name*: 显示使用指定 ISP 域认证的 IPv4 IPoE 个人会话，*domain-name* 为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。

ip *ip-address*: 显示指定源 IP 地址的 IPv4 IPoE 个人会话，*ip-address* 为指定的 IP 地址。

vpn-instance *vpn-instance-name*: 指定用户所属的 VPN 实例，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 IPv4 个人 IPoE 会话位于公网中。

mac *mac-address*: 显示指定源 MAC 地址的 IPv4 IPoE 个人会话，形式为 H-H-H。

static: 显示静态配置的 IPv4 IPoE 个人会话，不指定该参数时将显示静态配置的 IPv4 IPoE 个人会话和动态触发创建的 IPv4 IPoE 个人会话。

username *name*: 显示指定用户名的 IPv4 IPoE 个人会话，其中，*name* 为 1~255 个字符的字符串，区分大小写。

slot *slot-number*: 显示指定成员设备上的 IPv4 IPoE 个人会话，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示所有成员设备上的 IPv4 IPoE 个人会话。

verbose: 显示 IPv4 IPoE 个人会话的详细信息。如果不指定该参数，则只显示 IPoE 会话的简要信息。

【举例】

显示用户 IP 为 1.1.1.1，所属 VPN 实例为 vpn1 的 IPv4 IPoE 会话简要信息。

```
<Sysname> display ip subscriber session ip 1.1.1.1 vpn-instance vpn1
```

```
    Type: D-DHCP    S-Static    U-Unclassified-IP
```

Interface	IP address	MAC address	Type	State

GE1/0/1 1.1.1.1 000d-88f8-0eab D Online

显示所有 IPv4 IPoE 个人会话的详细信息。

<Sysname> display ip subscriber session verbose

Basic:

Description : -
Username : abc
Domain : radius
VPN instance : N/A
IP address : 1.1.1.1
MAC address : 000d-88f8-0eab
Service-VLAN/Customer-VLAN : -/-
Access interface : GE1/0/1
User ID : 0x380800b5
VPI/VCI(for ATM) : -/-
DHCP lease : N/A
DHCP remain lease : N/A
Login time : May 9 08:56:29 2014
Online time (hh:mm:ss) : 00:16:37
Service node : Slot 1 CPU 0
Type : Static
State : Online

AAA:

IP pool : N/A
Session idle time : N/A
Session duration : N/A, remaining: N/A
Remaining traffic : N/A
Max multicast addresses : 4
Multicast address list : N/A

QoS:

User profile : abc (active)
Session group profile : N/A
Inbound CAR : CIR 1000bps PIR 2000bps CBS 500bit (active)
Outbound CAR : CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:

Uplink packets/bytes : 594341/76075648
Downlink packets/bytes : 0/0

ITA:

Level-1 Uplink packets/bytes: 66038/8452864
 Downlink packets/bytes: 0/0
Level-2 Uplink packets/bytes: 66038/8452864
 Downlink packets/bytes: 0/0

表1-4 display ip subscriber session 命令显示信息描述表

字段	描述
Basic	IPoE会话的基本信息
Description	IPoE会话的描述信息（“-”表示没有描述信息）
Username	用户认证时使用的用户名
Domain	用户认证时使用的认证域名
VPN instance	用户所属的MPLS L3VPN实例，N/A表示用户属于公网
IP address	用户的IP地址
MAC address	用户的MAC地址
Service-VLAN/Customer-VLAN	用户所在的公网VLAN/私网VLAN（“-”表示没有VLAN信息）
Access interface	用户接入的接口名称
User ID	用户ID，只有用户在线后才会由系统分配，0xffffffff表示暂未分配
VPI/VCI(for ATM)	ATM的PVC信息
DHCP lease	DHCP服务器分配给用户的IP地址租约时间，单位为秒 - N/A：表示无DHCP租约 - Unlimited：表示租约无限长
DHCP remain lease	DHCP服务器分配给用户的IP地址租约剩余时长 只在Service node上可以查看到有效的剩余时长，非Service node上该字段显示为N/A
Login time	用户登录时间，即用户授权成功的时间，格式为设备时间，如：MM-DD hh:mm:ss YYYY
Online time (hh:mm:ss)	用户本次上线的在线时长
Service node	为用户提供认证服务的节点信息
Type	IPoE会话的创建类型： - DHCP：DHCP报文触发创建 - Unclassified-IP：未知源IP报文触发创建 - Static：静态配置
State	用户状态： - Init：初始化 - Offline：正在下线中 - Auth：认证中 - AuthFail：认证失败 - AuthPass：认证通过 - AssignedIP：会话已具备IP地址 - Online：用户在线 - Backup：备份状态，表示该用户是由对端备份到本端的

字段	描述
AAA	IPoE会话的AAA授权信息
IP pool	AAA授权的DHCP地址池名称，N/A表示AAA未授权该属性
Session idle time	用户闲置切断时间，单位为秒，N/A表示不进行闲置切断
Session duration	AAA授权的IPoE会话超时时间，单位为秒 - N/A: 表示未授权会话时长 - Unlimited: 表示会话时长无限制
remaining	AAA授权的IPoE会话剩余时长 - 当 AAA 未授权 IPoE 会话超时时间时，该字段始终显示为 N/A - 当 AAA 授权 IPoE 会话超时时间时 - 如果用户通过三层以太网接口/三层以太网子接口上线，该字段始终显示具体的剩余时长或 Unlimited（表示会话时长无限制） - 如果用户通过三层聚合接口/三层聚合子接口上线，则只有在本命令中指定 Service node 所在的 slot 或接口时，才会显示具体的剩余时长或 Unlimited（表示会话时长无限制），否则显示为 N/A
Remaining traffic	授权的剩余流量，单位为字节，N/A表示未对用户指定授权流量
Max multicast addresses	AAA授权用户可加入的组播组的最大数目
Multicast address list	AAA授权用户可加入的组播组地址列表，N/A表示AAA未授权该属性
QoS	IPoE会话的QoS信息
User profile	AAA授权的User Profile名称。若未授权User Profile，则显示为N/A。授权状态包括如下： - active: AAA 授权 User Profile 成功 - inactive: AAA 授权 User Profile 失败或者设备上不存在该 User Profile - 授权结果未知
Session group profile	AAA授权的Session Group Profile名称。若未授权Session Group Profile，则显示为N/A。授权状态包括如下： - active: AAA 授权 Session Group Profile 成功 - inactive: AAA 授权 Session Group Profile 失败或者设备上不存在该 Session Group Profile - 授权结果未知
Inbound CAR	入方向CAR值（CIR: 入方向平均速率，单位为bps；PIR: 入方向峰值速率，单位为bps；CBS: 入方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： - active: 表示入方向 CAR 限速下发成功 - inactive: 表示入方向 CAR 限速下发失败
Outbound CAR	出方向CAR值（CIR: 出方向平均速率，单位为bps；PIR: 出方向峰值速率，单位为bps；CBS: 出方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： - active: 表示出方向 CAR 限速下发成功 - inactive: 表示出方向 CAR 限速下发失败

字段	描述
Flow statistic	IPoE会话的流量统计信息
Uplink packets/bytes	上行流量报文数/字节数
Downlink packets/bytes	下行流量报文数/字节数
ITA	IPoE会话的ITA（Intelligent Target Accounting，智能靶向计费）业务流量统计信息
Level- <i>n</i> Uplink packets/bytes	计费等级为 <i>n</i> 的上行流量报文数/字节数， <i>n</i> 的取值范围为1~8
Downlink packets/bytes	计费等级为 <i>n</i> 的下行流量报文数/字节数， <i>n</i> 的取值范围为1~8

1.1.5 display ip subscriber session statistics

display ip subscriber session statistics 命令用来显示 IPv4 IPoE 个人用户统计信息。

【命令】

```
display ip subscriber session statistics [ session-type { dhcp | static | unclassified-ip } ] [ interface interface-type interface-number ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

session-type: 用户上线类型。不指定该参数，则表示显示所有类型的 IPv4 IPoE 个人用户统计信息。

dhcp: 表示 DHCP 用户。

static: 表示静态个人用户。

unclassified-ip: 表示未知源 IP 用户。

interface *interface-type interface-number*: 显示指定接口上的 IPv4 IPoE 个人用户统计信息，*interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数，将显示所有接口上已经上线和正在上线的 IPv4 IPoE 个人用户统计信息。

slot *slot-number*: 显示指定成员设备上的 IPv4 IPoE 个人用户统计信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示所有成员设备上的 IPv4 IPoE 个人用户统计信息。

【举例】

显示接口 GigabitEthernet1/0/1 上的 IPv4 IPoE 个人用户统计信息。

```
<Sysname> display ip subscriber session statistics session-type dhcp interface
gigabitethernet 1/0/1
Total                : 100
Init                 : 0
Authenticating       : 20
Authenticate fail     : 0
Authenticate pass    : 20
Assigned IP          : 10
Online                : 50
Backup               : 0
```

表1-5 display ip subscriber session statistics 命令显示信息描述表

字段	描述
Total	接入的总用户数
Init	处于初始状态的用户数
Authenticating	处于正在认证状态的用户数
Authenticate fail	处于认证失败状态的用户数
Authenticate pass	处于认证成功状态的用户数
Assigned IP	处于成功分配到IP地址状态的用户数
Online	处于在线状态的用户数
Backup	处于备份状态的用户数

【相关命令】

- **reset ip subscriber session**

1.1.6 display ip subscriber subnet-leased

display ip subscriber subnet-leased 命令用来显示 IPv4 IPoE 子网专线用户信息。

【命令】

```
display ip subscriber subnet-leased [ interface interface-type
interface-number ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface interface-type interface-number: 显示指定接口上的 IPv4 IPoE 子网专线用户信息, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 将显示所有接口上的 IPv4 IPoE 子网专线用户信息。

slot slot-number: 显示指定成员设备上的 IPv4 IPoE 子网专线用户信息, *slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数, 将显示所有成员设备上的 IPv4 IPoE 子网专线用户信息。

【举例】

显示接口 GigabitEthernet1/0/1 上的 IPv4 IPoE 子网专线用户信息。

```
<Sysname> display ip subscriber subnet-leased interface gigabitethernet 1/0/1
```

Basic:

Access interface	: GE1/0/1
VPN instance	: N/A
Username	: a
Network	: 11.11.11.0/24
User ID	: 0x30000001
State	: Online
Service node	: Slot 1 CPU 0
Domain	: radius
Login time	: May 14 20:08:35 2014
Online time (hh:mm:ss)	: 00:16:37

AAA:

IP pool	: N/A
Session idle time	: N/A
Session duration	: N/A, remaining: N/A
Remaining traffic	: N/A
Max multicast addresses	: 4
Multicast address list	: N/A

QoS:

User profile	: cc (active)
Session group profile	: N/A
Inbound CAR	: CIR 1000bps PIR 2000bps CBS 500bit (active)
Outbound CAR	: CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:

Uplink	packets/bytes	: 0/0
Downlink	packets/bytes	: 0/0

ITA:

Level-1 Uplink	packets/bytes: 0/0
Downlink	packets/bytes: 0/0
Level-2 Uplink	packets/bytes: 0/0
Downlink	packets/bytes: 0/0

表1-6 display ip subscriber subnet-leased 命令显示信息描述表

字段	描述
Basic	IPoE会话的基本信息
Access interface	用户所在的接口名称
VPN instance	用户所属的MPLS L3VPN实例，N/A表示用户属于公网
User name	用户认证时使用的用户名
Network	用户所在的子网地址
User ID	用户ID，只有用户在线后才会由系统分配，0xffffffff表示暂未分配
State	用户的认证状态 • Init: 初始化 • Offline: 正在下线中 • Auth: 认证中 • AuthFail: 认证失败 • AuthPass: 认证通过 • AssignedIP: 会话已具备 IP 地址 • Online: 用户在线 • Backup: 备份状态，表示该用户是由对端备份到本端的
Service node	为用户提供认证服务的节点信息
Domain	用户认证时使用的认证域名
Login time	用户登录时间，即用户授权成功的时间，格式为设备时间，如：MM-DD hh:mm:ss YYYY
Online time (hh:mm:ss)	用户本次上线的在线时长
AAA	IPoE会话的AAA授权信息
IP pool	AAA授权的DHCP地址池名称，N/A表示AAA未授权该属性
Session idle time	用户闲置切断时间，单位为秒，N/A表示不进行闲置切断
Session duration	AAA授权的IPoE会话超时时间，单位为秒 • N/A: 表示未授权会话时长 • Unlimited: 表示会话时长无限制
remaining	AAA授权的IPoE会话剩余时长 • 当 AAA 未授权 IPoE 会话超时时间时，该字段始终显示为 N/A • 当 AAA 授权 IPoE 会话超时时间时 ◦ 如果用户通过三层以太网接口/三层以太网子接口上线，该字段始终显示具体的剩余时长或 Unlimited（表示会话时长无限制） ◦ 如果用户通过三层聚合接口/三层聚合子接口上线，则只有在本命令中指定 Service node 所在的 slot 或接口时，才会显示具体的剩余时长或 Unlimited（表示会话时长无限制），否则显示为 N/A
Remaining traffic	授权的剩余流量，单位为字节，N/A表示未对用户指定授权流量
Max multicast addresses	AAA授权用户可加入的组播组的最大数目

字段	描述
Multicast address list	AAA授权用户可加入的组播组地址列表，N/A表示AAA未授权该属性
QoS	IPoE会话的QoS信息
User profile	AAA授权的User Profile名称。若未授权User Profile，则显示为N/A。授权状态包括如下： - active: AAA 授权 User Profile 成功 - inactive: AAA 授权 User Profile 失败或者设备上不存在该 User Profile - 授权结果未知
Session group profile	AAA授权的Session Group Profile名称。若未授权Session Group Profile，则显示为N/A。授权状态包括如下： - active: AAA 授权 Session Group Profile 成功 - inactive: AAA 授权 Session Group Profile 失败或者设备上不存在该 Session Group Profile - 授权结果未知
Inbound CAR	入方向CAR值（CIR：入方向平均速率，单位为bps；PIR：入方向峰值速率，单位为bps；CBS：入方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： - active: 表示入方向 CAR 限速下发成功 - inactive: 表示入方向 CAR 限速下发失败
Outbound CAR	出方向CAR值（CIR：出方向平均速率，单位为bps；PIR：出方向峰值速率，单位为bps；CBS：出方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： - active: 表示出方向 CAR 限速下发成功 - inactive: 表示出方向 CAR 限速下发失败
Flow statistic	IPoE会话的流量统计信息
Uplink packets/bytes	上行流量报文数/字节数
Downlink packets/bytes	下行流量报文数/字节数
ITA	IPoE会话的ITA（Intelligent Target Accounting，智能靶向计费）业务流量统计信息
Level- <i>n</i> Uplink packets/bytes	计费等级为 <i>n</i> 的上行流量报文数/字节数， <i>n</i> 的取值范围为1~8
Downlink packets/bytes	计费等级为 <i>n</i> 的下行流量报文数/字节数， <i>n</i> 的取值范围为1~8

【相关命令】

- ip subscriber enable**

1.1.7 display ip subscriber subnet-leased statistics

display ip subscriber subnet-leased statistics 命令用来显示 IPv4 IPoE 子网专线用户统计信息。

【命令】

display ip subscriber subnet-leased statistics [**interface** *interface-type* *interface-number*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface *interface-type* *interface-number*: 显示指定接口上的 IPv4 IPoE 子网专线用户统计信息，*interface-type* *interface-number* 表示接口类型和接口编号。如果未指定本参数，将显示所有接口上 IPv4 IPoE 用户已经上线和正在上线的子网专线统计信息。

slot *slot-number*: 显示指定成员设备上的 IPv4 IPoE 子网专线用户统计信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示所有成员设备上的 IPv4 IPoE 子网专线用户统计信息。

【举例】

显示接口 GigabitEthernet1/0/1 上的 IPv4 IPoE 子网专线用户统计信息。

```
<Sysname> display ip subscriber subnet-leased statistics interface gigabitethernet 1/0/1
Total                : 100
Init                 : 0
Authenticating       : 20
Authenticate fail    : 0
Authenticate pass    : 20
Assigned IP          : 10
Online               : 50
Backup               : 0
```

表1-7 display ip subscriber subnet-leased statistics 命令显示信息描述表

字段	描述
Total	接入的总用户数
Init	处于初始状态的用户数
Authenticating	处于正在认证状态的用户数
Authenticate fail	处于认证失败状态的用户数
Authenticate pass	处于认证成功状态的用户数
Assigned IP	处于成功分配到IP地址状态的用户数
Online	处于在线状态的用户数
Backup	处于备份状态的用户数

1.1.8 ip subscriber 8021p

ip subscriber 8021p 命令用来配置 IPv4 接入用户的 IP 报文的内/外层 VLAN tag 中的 802.1p 值与认证域的映射关系。

undo ip subscriber 8021p 命令用来删除指定 802.1p 值与认证域的映射关系。

【命令】

```
ip subscriber 8021p 8021p-list domain domain-name  
undo ip subscriber 8021p 8021p-list
```

【缺省情况】

未配置 IPv4 接入用户的 IP 报文的内/外层 VLAN tag 中的 802.1p 值与认证域的映射关系。

【视图】

三层以太网子接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

8021p-list: 802.1p 值列表，表示一个或多个 802.1p 值，表示方式为 **8021p-list = { 8021p-value [to 8021p-value] }&<1-8>**，其中，**8021p-value** 为指定 **8021p** 的编号，取值范围为 0~7。**&<1-8>** 表示前面的参数最多可以输入 8 次。

domain domain-name: 表示与指定的 8021p 范围相关联的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“”、“.”、“*”、“?”、“<”、“>” 以及 “@” 字符。

【使用指导】

本命令用来配置指定 802.1p 值范围内的 IPv4 接入用户（包括未知源 IP 接入用户、静态 IPoE 接入用户和 IPoE 子网/接口专线用户）认证时使用的认证域，通过指定的认证域对进行认证、授权、计费。

【举例】

在子接口 GigabitEthernet1/0/1.100 上配置内层 VLAN TAG 中 802.1p 值范围为 2 到 5 的 IPv4 接入用户认证使用的认证域为 1pdm。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1.100  
[Sysname-GigabitEthernet1/0/1.100] ip subscriber service-identify 8021p second-vlan  
[Sysname-GigabitEthernet1/0/1.100] ip subscriber 8021p 2 to 5 domain 1pdm
```

【相关命令】

- **ip subscriber service-identify**

1.1.9 ip subscriber access-user log enable

ip subscriber access-user log enable 命令用来开启 IPv4 IPoE 接入用户日志信息功能。

undo ip subscriber access-user log enable 命令用来关闭 IPv4 IPoE 接入用户日志信息功能。

【命令】

```
ip subscriber access-user log enable [ successful-login | failed-login |  
logout [ normal ] [ abnormal ] ] *  
undo ip subscriber access-user log enable [ successful-login | failed-login  
| logout [ normal ] [ abnormal ] ] *
```

【缺省情况】

IPv4 IPoE 接入用户日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

successful-login: 表示 IPv4 IPoE 接入用户上线成功日志功能。

failed-login: 表示 IPv4 IPoE 接入用户上线失败日志功能。

logout: 表示 IPv4 IPoE 接用户下线日志功能。

normal: 表示 IPv4 IPoE 接用户正常下线日志功能。

abnormal: 表示 IPv4 IPoE 接用户异常下线日志功能。

【使用指导】



注意

为了防止设备输出过多的 IPv4 IPoE 日志信息，一般情况下建议不要开启此功能。

IPv4 IPoE 接入用户日志是为了满足网络管理员维护的需要，对用户的上线成功、上线失败、正常下线和异常下线的信息进行记录，包括用户名、IP 地址、接口名称、两层 VLAN、MAC 地址、上线失败原因、下线原因等。设备生成的 IPv4 IPoE 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

配置本命令时，如果未指定任何参数，将同时开启用户的上线成功、上线失败、正常下线和异常下线日志功能。

通过 **undo** 命令关闭日志功能时，如果未指定任何参数，将同时关闭用户的上线成功、上线失败、正常下线和异常下线日志功能。

【举例】

开启 IPv4 IPoE 接入用户日志信息功能。

```
<Sysname> system-view  
[Sysname] ip subscriber access-user log enable
```

1.1.10 ip subscriber dhcp domain

ip subscriber dhcp domain 命令用来配置 IPv4 DHCP 个人接入用户使用的认证域。

undo ip subscriber dhcp domain 命令用来恢复缺省情况。

【命令】

ip subscriber dhcp domain *domain-name*

undo ip subscriber dhcp domain

【缺省情况】

IPv4 DHCP 个人接入用户的认证域为缺省认证域。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain-name: 指定认证使用的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括“/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>”以及“@”字符。

【使用指导】

本命令用来配置 DHCP 报文触发接入的 IPv4 DHCP 个人接入用户在认证时使用的域名，该域名必须在接入设备上存在且配置完整。

- 配置 **ip subscriber dhcp domain** 命令后，如果 DHCP 报文中携带 Option 60，Option 60 内容符合域名的格式要求，并且接口配置了 **ip subscriber trust option60** 命令，则 IPoE 用户使用 Option 60 中的信息作为指定的认证域进行认证；否则，使用本命令指定的认证域。
- 如果不配置 **ip subscriber dhcp domain** 命令，且 DHCP 报文中未携带 Option 60，则使用缺省认证域认证。

当用户需要将 Option 60 字段中的信息按字符串形式解析时，请确保 Option 60 字段内容中不出现字符串结束字符和不可见字符，否则在生成域名时将产生异常。

【举例】

配置接口 GigabitEthernet1/0/1 上的 IPv4 DHCP 个人接入用户使用的认证域为 ipoe。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber dhcp domain ipoe
```

【相关命令】

- ip subscriber initiator dhcp enable**
- ip subscriber trust**

1.1.11 ip subscriber dhcp max-session

ip subscriber dhcp max-session 命令用来配置接口上允许 DHCPv4 报文触发创建的 IPv4 IPoE 会话的最大数目。

undo ip subscriber dhcp max-session 命令用来恢复缺省情况。

【命令】

ip subscriber dhcp max-session *max-number*
undo ip subscriber dhcp max-session

【缺省情况】

未配置接口上允许 DHCPv4 报文触发创建的 IPv4 IPoE 会话的最大数目。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

max-number: 允许 DHCPv4 报文触发创建的 IPv4 IPoE 会话的最大数目, 取值范围为 1~64000。

【使用指导】

DHCPv4 报文触发创建的 IPv4 IPoE 会话数目达到最大值后, 后续 DHCPv4 报文不能触发创建 IPv4 IPoE 会话。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 上允许 DHCPv4 报文触发创建的 IPv4 IPoE 会话的最大数目为 100。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ip subscriber dhcp max-session 100
```

【相关命令】

- **display ip subscriber session**
- **ip subscriber initiator dhcp enable**
- **reset ip subscriber session**

1.1.12 ip subscriber dhcp password option60

ip subscriber dhcp password option60 命令用来配置 IPv4 DHCP 个人接入用户使用 DHCPv4 报文中的 Option 60 作为认证密码。

undo ip subscriber dhcp password option60 命令用来恢复缺省情况。

【命令】

ip subscriber dhcp password option60 [*offset offset*] [*length length*]
undo ip subscriber dhcp password option60

【缺省情况】

IPv4 DHCP 个人接入用户未使用 DHCPv4 报文中的 Option 60 作为认证密码。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

offset *offset*: 表示从 Option 60 首部偏移指定字节后的内容作为认证密码, *offset* 表示字节偏移量, 取值范围为 1~63, 单位为字节。如果未指定本参数, 将从 Option 60 首部后的内容作为认证密码。

length *length*: 表示从 Option 60 首部偏移 *offset* 所处的位置开始, 取指定长度的字节作为认证密码, *length* 表示获取字节的长度, 取值范围为 1~63, 单位为字节。如果未指定本参数, 将从 Option 60 首部偏移 *offset* 所处的位置开始取剩余的所有内容作为认证密码。

【使用指导】

IPv4 DHCP 个人接入用户支持通过多种方式获取认证密码, 并按如下优先顺序选择第一个可用的认证密码进行认证:

- 同时满足如下条件时, 则使用本命令配置方式获取的密码作为认证密码:
 - 接口上配置了 **ip subscriber dhcp password option60** 命令;
 - 接口上配置了 **ip subscriber trust option60** 命令并且 DHCPv4 报文中携带的 Option 60 中内容符合可见字符的格式要求。
- 使用 **ip subscriber password** 命令配置的密码作为认证密码。
- 使用缺省字符串 **vlan** 作为认证密码。

ip subscriber dhcp password option60 命令用来配置 IPv4 DHCP 用户在认证时使用的密码, 该密码必须与认证服务器上配置的密码保持一致。

当用户需要将 Option 60 字段中的信息作为认证密码时, 请确保 Option 60 字段内容中不出现字符串结束字符和不可见字符, 否则在生成用户密码时将产生异常。

【举例】

配置接口 GigabitEthernet1/0/1 上的 IPv4 DHCP 个人接入用户使用从 Option 60 首部偏移 10 个字节后的 20 个字节内容作为认证密码。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber dhcp password option60 offset 10 length 20
```

【相关命令】

- **ip subscriber initiator dhcp enable**
- **ip subscriber password**
- **ip subscriber trust**
- **ip subscriber dhcp username**

1.1.13 ip subscriber dhcp username

ip subscriber dhcp username 命令用来配置 IPv4 DHCP 个人接入用户的认证用户名的命名规则。

undo ip subscriber dhcp username 命令用来恢复缺省情况。

【命令】

```
ip subscriber dhcp username include { circuit-id [ separator separator ] |
client-id [ separator separator ] | nas-port-id [ separator separator ] | port
[ separator separator ] | remote-id [ separator separator ] | second-vlan
[separator separator ] | slot [ separator separator ] | source-mac
[ address-separator address-separator ] [ separator separator ] | subslot
[separator separator ] | sysname [separator separator ] | vendor-class
[ separator separator ] | vendor-specific [ separator separator ] | vlan
[separator separator ] } *
undo ip subscriber dhcp username
```

【缺省情况】

IPv4 DHCP 个人接入用户使用报文源 MAC 地址作为认证用户名。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

circuit-id: 表示以 DHCP 报文中的 Option82 sub-option1 字段中的信息为用户名。

client-id: 表示以 DHCP 报文中的 Option61 字段中的信息作为用户名。

nas-port-id: 表示以认证报文中的 NAS-PORT-ID 属性作为用户名。

port: 表示以用户接入的端口号作为用户名。

remote-id: 表示以 DHCP 报文中的 Option82 sub-option2 字段中的信息作为用户名。

second-vlan: 表示以认证报文中的内层 VLAN 作为用户名。

slot: 表示以用户接入的槽位号作为用户名。

source-mac: 表示以用户报文的源 MAC 地址作为用户名。

address-separator address-separator: MAC 地址分隔符，可以为任意可配置的可见字符。若指定了分隔符，例如“-”，则用户名形如 xxxx-xxxx-xxxx；若不指定该参数，则用户名为 xxxxxxxxxxxx 形式。建议不要使用@作为分隔符，避免携带@字符的用户名在 AAA 服务器端不能被正确解析。

subslot: 表示以用户接入的子卡号作为用户名。

sysname: 表示以用户接入设备的设备名作为用户名。

vendor-class: 表示以 DHCP 报文中的 Option60 字段中的信息作为用户名。

vendor-specific: 表示以 DHCP 报文中的 Option82 sub-option9 字段中的信息作为用户名。

vlan: 表示以认证报文中的外层 VLAN 作为用户名。

separator separator: 当前字段分隔符，用在当前字段后面以连接后面的一个字段，可以为任意可配置的可见字符。建议不要使用@作为分隔符，避免携带@字符的用户名在 AAA 服务器端不能被正确解析。

【使用指导】

该命令用来配置 IPv4 DHCP 用户在认证时使用的用户名的命名规则，根据该命名规则获取的用户名必须与认证服务器上配置的用户名保持一致。

在允许的用户名类型范围内，该命令支持任意形式、任意顺序的用户名组合。例如：若配置 **ip subscriber dhcp username include vendor-class vendor-specific**，则用户名为 Option60 字段内容和 Option82 sub9 字段内容的拼接，且两个字段之间无分隔符。

为保证设备对 Option 字段中的信息进行正确解析，请确保 Option 字段内容中不出现字符串结束符和不可见字符，否则可能生成错误的用户名。

【举例】

配置接口 GigabitEthernet1/0/1 上 IPv4 DHCP 个人接入用户使用 Client Identifier Option 字段中的信息作为用户名。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber dhcp username include client-id
```

配置接口 GigabitEthernet1/0/1 上 IPv4 DHCP 个人接入用户使用接入设备的设备名、接入的槽位号、接入的子卡号、接入的端口号和认证报文中的外层 VLAN 信息作为用户名，所选用的字段之间均使用#作为分隔符。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber dhcp username include sysname separator # slot  
separator # subslot separator # port separator # vlan
```

【相关命令】

- **ip subscriber initiator dhcp enable**
- **ip subscriber password**

1.1.14 ip subscriber dscp

ip subscriber dscp 命令用来配置 IPv4 接入用户的 IP 报文的 DSCP 值与认证域的映射关系。

undo ip subscriber dscp 命令用来删除指定 DSCP 值与认证域的映射关系。

【命令】

```
ip subscriber dscp dscp-value-list domain domain-name
```

```
undo ip subscriber dscp dscp-value-list
```

【缺省情况】

未配置 IPv4 接入用户的 IP 报文的 DSCP 值与认证域的映射关系。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

dscp-value-list: DSCP 值列表, 表示一个或多个 DSCP 的值, 表示方式为 **dscp-value-list = dscp-value [to dscp-value] }&<1-8>**。其中, **dscp-value** 为指定的 DSCP 的值, 取值范围为 0~63。&<1-8>表示前面的参数最多可以输入 8 次。

domain domain-name: 表示与指定的 DSCP 范围相关联的 ISP 域名, 为 1~255 个字符的字符串, 不区分大小写, 不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。

【使用指导】

本命令用来配置指定 DSCP 范围内的 IPv4 接入用户（包括未知源 IP 接入用户、静态 IPoE 接入用户和 IPoE 子网/接口专线用户）认证时使用的认证域, 通过指定的认证域进行认证、授权、计费。

【举例】

在接口 GigabitEthernet1/0/1 上配置 DSCP 值范围为 1 到 4 的 IPv4 接入用户认证使用的认证域为 dscpdm。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber service-identify dscp
[Sysname-GigabitEthernet1/0/1] ip subscriber dscp 1 to 4 domain dscpdm
```

【相关命令】

- **ip subscriber service-identify**

1.1.15 ip subscriber enable

ip subscriber enable 命令用来在接口上开启 IPv4 IPoE 功能并指定用户的接入模式。

undo ip subscriber enable 命令用来关闭接口上的 IPv4 IPoE 功能。

【命令】

```
ip subscriber { l2-connected | routed } enable
undo ip subscriber { l2-connected | routed } enable
```

【缺省情况】

接口上的 IPv4 IPoE 功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

l2-connected: 指定二层接入模式。

routed: 指定三层接入模式。

【使用指导】

只有在接口上开启了 IPv4 IPoE 功能后，其它的 IPv4 IPoE 相关配置才能生效。

不能通过重复执行本命令修改 IPoE 的接入模式。如需修改 IPoE 的接入模式，请先通过 **undo ip subscriber enable** 命令关闭 IPoE 功能，再执行 **ip subscriber enable** 命令。

在聚合接口视图下开启 IPv4 IPoE 功能时，必须同时通过 **service** 命令指定聚合接口下流量的业务处理板；否则会产生无法统计用户流量的现象。有关 **service** 命令的详细介绍请参见“二层技术-以太网交换命令参考”中的“以太网链路聚合”。

【举例】

在接口 GigabitEthernet1/0/1 上开启二层接入模式的 IPv4 IPoE 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber l2-connected enable
```

【相关命令】

- **service**（二层技术-以太网交换命令参考/以太网链路聚合）

1.1.16 ip subscriber initiator dhcp enable

ip subscriber initiator dhcp enable 命令用来在接口上开启 DHCPv4 报文触发生成 IPv4 IPoE 会话的功能。

undo ip subscriber initiator dhcp enable 命令用来关闭接口上 DHCPv4 报文触发生成 IPv4 IPoE 会话的功能。

【命令】

```
ip subscriber initiator dhcp enable
undo ip subscriber initiator dhcp enable
```

【缺省情况】

接口上 DHCPv4 报文触发生成 IPv4 IPoE 会话的功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

接口上开启该功能后，收到的首个 DHCP Discover 报文或直接申请地址的 DHCP Request 报文会触发生成 IPv4 IPoE 会话；关闭该功能后，该接口上收到的 DHCPv4 报文不能触发生成 IPv4 IPoE 会话，已有的由 DHCPv4 报文触发生成的 IPv4 IPoE 会话不会被删除。

接口上可同时配置 DHCPv4 报文和未知源 IPv4 报文触发生成 IPv4 IPoE 会话的功能。

【举例】

在接口 GigabitEthernet1/0/1 上开启 DHCPv4 报文触发生成 IPv4 IPoE 会话的功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber initiator dhcp enable
```

【相关命令】

- **display ip subscriber session**
- **ip subscriber enable**
- **ip subscriber initiator unclassified-ip enable**
- **reset ip subscriber session**

1.1.17 ip subscriber initiator unclassified-ip enable

ip subscriber initiator unclassified-ip enable 命令用来在接口上开启未知源 IPv4 报文触发生成 IPv4 IPoE 会话的功能。

undo ip subscriber initiator unclassified-ip enable 命令用来关闭接口上的未知源 IPv4 报文触发生成 IPv4 IPoE 会话的功能。

【命令】

```
ip subscriber initiator unclassified-ip enable
undo ip subscriber initiator unclassified-ip enable
```

【缺省情况】

接口上的未知源 IPv4 报文触发生成 IPv4 IPoE 会话的功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

接口开启该功能后，收到的未知源 IPv4 报文会触发生成 IPv4 IPoE 会话；关闭该功能后，该接口上收到的未知源 IPv4 报文不能触发生成 IPv4 IPoE 会话，已有的由未知源 IPv4 报文触发生成的 IPv4 IPoE 会话不会被删除。

接口上可同时配置 DHCPv4 报文和未知源 IPv4 报文触发生成 IPv4 IPoE 会话的功能。

【举例】

在接口 GigabitEthernet1/0/1 上开启未知源 IPv4 报文触发生成 IPv4 IPoE 会话的功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber initiator unclassified-ip enable
```

【相关命令】

- **display ip subscriber session**

- **ip subscriber enable**
- **ip subscriber initiator dhcp enable**
- **reset ip subscriber session**

1.1.18 ip subscriber interface-leased

ip subscriber interface-leased 命令用来配置 IPv4 IPoE 接口专线用户。

undo ip subscriber interface-leased 命令用来恢复缺省情况。

【命令】

```
ip subscriber interface-leased username name password { ciphertext |
plaintext } string [ domain domain-name ]
undo ip subscriber interface-leased
```

【缺省情况】

未配置 IPv4 IPoE 接口专线用户。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

username name: 指定用户认证时使用的用户名，其中 *name* 为 1~255 个字符的字符串，区分大小写。

password: 指定用户认证时使用的密码。

ciphertext: 以密文方式设置密码。

plaintext: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串。

domain domain-name: 指定认证使用的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。如果未指定该参数，将使用缺省认证域来认证用户。关于缺省认证域的相关配置请参见“安全配置指导”中的“AAA”。

【使用指导】

一个 IPv4 IPoE 接口专线用户代表了该接口接入的所有 IPv4 用户，接口上接入的所有 IPv4 用户统一认证、授权和计费。该 IPoE 专线用户认证成功后，接口上接入的所有 IPv4 用户流量均允许通过，且共享一个 IPv4 IPoE 会话，并基于接口进行授权和计费。

每个接口只能配置一个 IPv4 IPoE 接口专线用户，并且不能通过重复执行本命令修改已配置的 IPv4 IPoE 接口专线用户的 **username**、**password** 或 **domain** 参数。如需修改这些参数，请先通过 **undo ip subscriber interface-leased** 命令删除已配置的 IPv4 IPoE 接口专线用户，再执行 **ip subscriber interface-leased** 命令。

同一接口下，IPoE 个人接入用户、IPoE 接口专线用户和 IPoE 子网专线用户的配置互斥，只能选择其中的一种配置。

【举例】

在接口 GigabitEthernet1/0/1 上配置一个 IPv4 IPoE 接口专线用户：认证使用的用户名为 intuser，认证使用的密码为明文 pw123。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber interface-leased username intuser password  
plaintext pw123
```

【相关命令】

- **display ip subscriber interface-leased**

1.1.19 ip subscriber nas-port-id format

ip subscriber nas-port-id format 命令用来配置 IPv4 IPoE 接入用户进行认证时，接入设备向 RADIUS 服务器发送的 NAS-PORT-ID 属性的封装格式。

undo ip subscriber nas-port-id format 命令用来恢复缺省情况。

【命令】

ip subscriber nas-port-id format cn-telecom { version1.0 | version2.0 }

undo ip subscriber nas-port-id format

【缺省情况】

按 version 1.0 的格式填充 RADIUS 的 NAS-PORT-ID 属性。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

version1.0：封装格式为 version 1.0，表示发送给 RADIUS 服务器的 NAS-PORT-ID 属性以电信 163 大后台要求的格式填充。不同接口类型的封装内容形式有所不同，具体请参见表 1-8。其中，封装内容中的各参数含义为：

- *slot_num*：表示 BRAS 接入接口的槽位号。
- *subslot_num*：表示 BRAS 接入接口的子槽位号。
- *port_num*：表示 BRAS 接入接口的端口号。
- *vlan_id*：表示接入用户的 VLAN ID。
- *inner-vlan*：表示接入用户的内层 VLAN ID。
- *outer-vlan*：表示接入用户的外层 VLAN ID。
- *vpi*：表示 BRAS 接入接口的 VPI。
- *vci*：表示 BRAS 接入接口的 VCI。

表1-8 version 1.0 封装格式

接口类型	封装内容形式
三层以太网接口和三层聚合接口	slot=s lot_num;subslot=subs lot_num;port=port_num;vlanid=0
三层以太网子接口和三层聚合子接口（携带单层VLAN Tag接入）	slot=s lot_num;subslot=subs lot_num;port=port_num;vlanid=vlan_id
三层以太网子接口和三层聚合子接口（携带双层VLAN Tag接入）	slot=s lot_num;subslot=subs lot_num;port=port_num;vlanid=inner-vlan;vlanid2=outer-vlan
基于ATM链路的三层虚拟以太网接口（IPoEoA接入）	slot=s lot_num;subslot=subs lot_num;port=port_num;vpi=vpi;vci=vci

version2.0: 封装格式为version 2.0，表示发送给RADIUS服务器的NAS-PORT-ID属性以YDT 2275-2011 宽带接入用户线路（端口）标识要求的格式填充。version 2.0 封装格式的内容形式为：
{eth|trunk|atm} NAS_slot/NAS_subslot/NAS_port:svlan.cvlan
AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port。其中，各字段的含义请参见 表 1-9：

表1-9 version 2.0 封装格式

字段	描述
{eth trunk atm}	表示BRAS接入接口的类型，包括以太网接口、trunk类型的以太网接口或ATM接口
NAS_slot	表示BRAS接入接口的槽位号
NAS_subslot	表示BRAS接入接口的子槽位号
NAS_port	表示BRAS接入接口的端口号
svlan	表示接入用户的SVLAN ID
cvlan	表示接入用户的CVLAN ID
AccessNodeIdentifier	表示接入节点的标识
ANI_rack	表示接入节点机架号
ANI_frame	表示接入节点机框号
ANI_slot	表示接入节点槽位号
ANI_subslot	表示接入节点子槽位号
ANI_port	表示接入节点端口号

【举例】

在接口 GigabitEthernet1/0/1 上配置设备使用 version 2.0 格式封装 RADIUS 的 NAS-PORT-ID 属性。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber nas-port-id format cn-telecom version2.0
```

【相关命令】

- **ip subscriber initiator dhcp enable**
- **ip subscriber trust**
- **ip subscriber nas-port-id nasinfo-insert**

1.1.20 ip subscriber nas-port-id nasinfo-insert

ip subscriber nas-port-id nasinfo-insert 命令用来配置设备提取出 DHCPv4 报文的 Option 82 Circuit-ID 子选项内容并和 NAS 信息一起作为 NAS-PORT-ID 属性字符串。

undo ip subscriber nas-port-id nasinfo-insert 命令用来恢复缺省情况。

【命令】

```
ip subscriber nas-port-id nasinfo-insert  
undo ip subscriber nas-port-id nasinfo-insert
```

【缺省情况】

如果收到的 DHCPv4 报文带有 Option 82 Circuit-ID 子选项，则直接使用该子选项内容作为 NAS-PORT-ID 属性字符串。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

在 DHCP 中继组网环境下，接入设备能捕获用户的 DHCPv4 报文，并从报文中提取出 DHCP Option82 Circuit-ID 子选项信息。在配置了 NAS-PORT-ID 属性的封装格式为 version 2.0 格式，且信任 DHCP Option 82 的情况下，若配置了本命令，则接入设备处理如下：

- 如果收到的 DHCP 报文带有 Option82 Circuit-ID 子选项，则从收到的 DHCP 报文中解析 Option82 Circuit-ID 子选项，并按 version 2.0 格式要求将提取出的 DHCPv4 报文的 Option 82 Circuit-ID 子选项内容和 NAS 信息一起作为 RADIUS 的 NAS-PORT-ID 属性内容。
- 如果收到的 DHCP 报文不带 Option82 Circuit-ID 子选项，则按 version 2.0 格式要求封装，填充 NAS-PORT-ID 属性中的 NAS 信息字段(NAS_slot/NAS_subslot/NAS_port:svlan.cvlan)，并将 AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port 部分修改为 0/0/0/0/0/0。

本功能对原 DHCP 报文中 Option82 子选项不产生任何影响。

【举例】

在接口 GigabitEthernet1/0/1 上配置设备使用 DHCPv4 客户端上报的 Option82 信息，并在其中插入 NAS 信息，然后将其封装为 RADIUS 的 NAS-PORT-ID 属性。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1
```



```
[Sysname-GigabitEthernet1/0/1] ip subscriber nas-port-id nasinfo-insert
```

【相关命令】

- **ip subscriber initiator dhcp enable**
- **ip subscriber trust**
- **ip subscriber nas-port-id format**

1.1.21 ip subscriber nas-port-type

ip subscriber nas-port-type 命令用来配置接口的 IPv4 IPoE 接入端口类型。

undo ip subscriber nas-port-type 命令用来恢复缺省情况。

【命令】

```
ip subscriber nas-port-type { 802.11 | adsl-cap | adsl-dmt | async | cable |  
ethernet | g.3-fax | hdlc | idsl | isdn-async-v110 | isdn-async-v120 |  
isdn-sync | piafs | sdsl | sync | virtual | wireless-other | x.25 | x.75 | xdsl }  
undo ip subscriber nas-port-type
```

【缺省情况】

IPv4 IPoE 接入端口类型为 Ethernet 类型。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

802.11: 符合 Wireless-IEEE 802.11 标准的接口类型，对应的编码值为 19。

adsl-cap: ADSL-CAP (Asymmetric DSL, Carrierless Amplitude Phase Modulation) 接口类型，对应的编码值为 12。

adsl-dmt: ADSL-DMT (Asymmetric DSL, Discrete Multi-Tone) 接口类型，对应的编码值为 13。

async: Async 接口类型，对应的编码值为 0。

cable: Cable 接口类型，对应的编码值为 17。

ethernet: Ethernet 接口类型，对应的编码值为 15。

g.3-fax: G.3 Fax 接口类型，对应的编码值为 10。

hdlc: HDLC 接口类型，对应的编码值为 7。

idsl: IDSL (ISDN Digital Subscriber Line) 接口类型，对应的编码值为 14。

isdn-async-v110: ISDN Async V.110 接口类型，对应的编码值为 4。

isdn-async-v120: ISDN Async V.120 接口类型，对应的编码值为 3。

isdn-sync: ISDN Sync 接口类型，对应的编码值为 2。

piafs: 符合 PIAFS (PHS (Personal Handyphone System) Internet Access Forum Standard) 标准的接口类型，对应的编码值为 6。

sdsl: SDSL（Symmetric DSL）接口类型，对应的编码值为 11。

sync: Sync 接口类型，对应的编码值为 1。

virtual: Virtual 接口类型，对应的编码值为 5。

wireless-other: Wireless-other 接口类型，对应的编码值为 18。

x.25: X.25 接口类型，对应的编码值为 8。

x.75: X.75 接口类型，对应的编码值为 9。

xdsl: XDSL（Digital Subscriber Line of unknown type）接口类型，对应的编码值为 16。

【使用指导】

此处配置的端口接入类型值将作为向 RADIUS 服务器发送的 RADIUS 请求报文的 NAS-Port-Type 属性值，用于向 RADIUS 服务器正确传递用户的接入端口信息。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 的 IPv4 IPoE 接入端口类型为 SDSL。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ip subscriber nas-port-type dsdl
```

1.1.22 ip subscriber password

ip subscriber password 命令用来配置 IPv4 IPoE 个人接入用户的认证密码。

undo ip subscriber password 命令用来恢复缺省情况。

【命令】

```
ip subscriber password { ciphertext | plaintext } string  
undo ip subscriber password
```

【缺省情况】

IPv4 IPoE 个人接入用户的认证密码为字符串 **vlan**。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ciphertext: 以密文方式设置密码。

plaintext: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串。

【使用指导】

ip subscriber password 命令用来配置 IPv4 IPoE 个人接入用户（包括动态和静态 IPoE 个人接入用户）的认证密码，该密码必须与认证服务器上配置的密码保持一致。

其中，对于动态 IPv4 DHCP 个人接入用户支持通过多种方式获取认证密码，具体请参见 **ip subscriber dhcp password option60** 命令。

【举例】

配置接口 GigabitEthernet1/0/1 上 IPoE 个人接入用户认证时使用的密码为明文 123。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber password plaintext 123
```

【相关命令】

- **ip subscriber dhcp username**
- **ip subscriber unclassified-ip username**
- **ip subscriber dhcp password option60**

1.1.23 ip subscriber service-identify

ip subscriber service-identify 命令用来配置 IPv4 接入用户的业务识别方式。

undo ip subscriber service-identify 命令用来恢复缺省情况。

【命令】

三层以太网接口视图/三层聚合口视图

ip subscriber service-identify dscp

undo ip subscriber service-identify

三层以太网子接口视图/三层聚合子接口视图

ip subscriber service-identify { 8021p { second-vlan | vlan } | dscp | second-vlan | vlan }

undo ip subscriber service-identify

【缺省情况】

未配置 IPv4 接入用户的业务识别方式。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

8021p second-vlan: 表示 QinQ 模式下基于内层 VLAN Tag 中的 802.1p 值识别业务。

8021p vlan: 表示基于 VLAN Tag 中的 802.1p 值识别业务，QinQ 模式下基于外层 VLAN Tag 中的 802.1p 值识别业务。

dscp: 表示基于 DSCP 值识别业务。

second-vlan: QinQ 模式下基于内层 VLAN ID 识别业务。

vlan: 表示基于 VLAN ID 识别业务，QinQ 模式下基于外层 VLAN ID 识别业务。

【使用指导】

IPv4 接入用户（包括未知源 IP 接入用户、静态 IPoE 接入用户和 IPoE 子网/接口专线用户）认证时使用的认证域由报文中携带的业务信息来决定。不同的业务特征可以对应不同的认证域，每一个接口可以指定仅识别某种类型业务的报文。例如，接口上若指定了基于 DSCP 值识别业务，且通过 **ip subscriber dscp 1 domain aabcc** 命令指定了 DSCP 值 1 与认证域 aabcc 的映射关系，则 IP 报文 DSCP 值为 1 的用户认证时将会使用认证域 aabcc。

一个接口上只能指定一个业务识别方式。

【举例】

配置接口 GigabitEthernet1/0/1 上的 IPv4 接入用户认证使用基于 DSCP 的业务识别方式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber service-identify dscp
```

【相关命令】

- **ip subscriber 8021p**
- **ip subscriber dscp**
- **ip subscriber vlan**

1.1.24 ip subscriber session static

ip subscriber session static 命令用来配置静态 IPv4 IPoE 会话。

undo ip subscriber session static 命令用来删除指定的静态 IPv4 IPoE 会话。

【命令】

```
ip subscriber session static ip ip-address [ vlan vlan-id [ second-vlan vlan-id ] ] [ mac mac-address ] [ domain domain-name ] [ description string ]
undo ip subscriber session static ip ip-address [ vlan vlan-id [ second-vlan vlan-id ] ]
```

【缺省情况】

未配置静态 IPv4 IPoE 会话。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip ip-address: 表示用户的 IPv4 地址。

vlan vlan-id: 表示用户报文的外层 VLAN。其中 *vlan-id* 表示 VLAN ID，取值范围为 1~4094。本参数仅子接口支持，非子接口不支持。

second-vlan vlan-id: 表示用户报文的内层 VLAN。其中 *vlan-id* 表示 VLAN ID，取值范围为 1~4094。本参数仅子接口支持，非子接口不支持。

mac mac-address: 表示用户的 MAC 地址，形式为 H-H-H。

domain domain-name: 指定认证使用的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。如果未指定该参数，将使用缺省认证域来认证用户。关于缺省认证域的相关配置请参见“安全配置指导”中的“AAA”。

description string: 指定静态会话的描述信息，为 1~31 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。如果未指定该参数，则静态会话无描述信息。

【使用指导】

静态 IPoE 会话的匹配优先级高于动态 IPoE 会话。若已经存在静态 IPoE 会话，则与之匹配的 IP 报文不会触发新的动态 IPoE 会话；若存在一个未知源 IP 报文、DHCP 报文触发建立的动态 IPoE 会话，则再配置一个能与该未知源 IP 报文、DHCP 接入用户 IP 报文匹配的静态 IPoE 会话，会覆盖已经存在的动态 IPoE 会话。

当静态会话中指定的 IP 地址与 DHCP 地址池中可分配的 IP 地址存在交集时，则对于 DHCPv4 地址池需要通过命令 **dhcp server forbidden-ip** 或 **forbidden-ip** 配置交集 IP 地址为不参与自动分配的 IP 地址。有关配置不参与自动分配 IP 地址命令的详细介绍，请参见“三层技术-IP 业务命令参考”中的“DHCP”。

系统支持配置多个静态 IPoE 会话，并根据命令中指定参数的不同分为如下三种情况：

- IP（无外层 VLAN 和内层 VLAN）相同的静态 IPoE 会话；
- IP、外层 VLAN（无内层 VLAN）两个参数相同的静态 IPoE 会话；
- IP、外层 VLAN、内层 VLAN 三个参数相同的静态 IPoE 会话。

上述三种情况的静态 IPoE 会话每种情况最多只能存在一条，并且不能通过重复执行本命令修改上述三种中的 **mac** 和 **domain** 参数。如需修改 **mac** 和 **domain** 参数，请先通过 **undo ip subscriber session static** 命令删除指定静态 IPoE 会话对应的当前配置后再执行 **ip subscriber session static** 命令。

同一接口下，静态 IPoE 会话、接口专线用户和子网专线用户的配置互斥，只能选择其中的一种配置。

【举例】

在接口 GigabitEthernet1/0/1 上配置一条静态 IPv4 IPoE 会话：用户 IP 地址为 1.1.1.1，认证使用的认证域为 dm1。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber session static ip 1.1.1.1 domain dm1
```

【相关命令】

- **display ip subscriber session**

1.1.25 ip subscriber subnet-leased

ip subscriber subnet-leased 命令用来配置 IPv4 IPoE 子网专线用户。

undo ip subscriber subnet-leased 命令用来删除指定的 IPv4 IPoE 子网专线用户。

【命令】

```
ip subscriber subnet-leased ip ip-address { mask | mask-length } username  
name password { ciphertext | plaintext } string [ domain domain-name ]  
undo ip subscriber subnet-leased ip ip-address { mask | mask-length }
```

【缺省情况】

未配置 IPv4 IPoE 子网专线用户。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip *ip-address*: 表示用户的 IPv4 地址。

mask: IP 地址的网络掩码，为点分十进制形式。

mask-length: IP 地址的网络掩码长度，取值范围为 1~31。

username name: 指定用户认证时使用的用户名，其中 *name* 为 1~255 个字符的字符串，区分大小写。

password: 指定用户认证时使用的密码。

ciphertext: 以密文方式设置密码。

plaintext: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串。

domain domain-name: 指定认证使用的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。如果未指定该参数，将使用缺省认证域来认证用户。关于缺省认证域的相关配置请参见“安全配置指导”中的“AAA”。

【使用指导】

一个 IPv4 IPoE 子网专线用户代表了该接口接入的所有该子网内 IPv4 用户，该子网内的所有 IPv4 用户统一认证、授权和计费。该 IPoE 专线用户认证成功后，接口上接入的所有该子网内 IPv4 用户流量均允许通过，且共享一个 IPv4 IPoE 会话，并基于子网进行授权和计费。

每个子网只能配置一个 IPv4 IPoE 子网专线用户。

同一接口下，IPoE 个人接入用户、IPoE 接口专线用户和 IPoE 子网专线用户的配置互斥，只能选择其中的一种配置。

【举例】

在接口 GigabitEthernet1/0/1 上配置一个 IPv4 IPoE 子网专线用户：子网网段为 1.1.1.1/24，认证使用的用户名为 netuser，认证使用的明文密码为 pw123。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber subnet-leased ip 1.1.1.1 24 username netuser  
password plaintext pw123
```

【相关命令】

- **display ip subscriber subnet-leased**

1.1.26 ip subscriber timer quiet

ip subscriber timer quiet 命令用来配置 IPv4 IPoE 用户的静默时间。

undo ip subscriber timer quiet 命令用来恢复缺省情况。

【命令】

```
ip subscriber timer quiet time
```

```
undo ip subscriber timer quiet
```

【缺省情况】

IPv4 IPoE 用户的静默时间功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

time: IPoE 用户的静默时间，取值范围为 10~3600，单位为秒。

【使用指导】

本命令用来设置用户认证失败以后，设备需要等待的时间间隔。在静默期间，设备不对来自认证失败用户的报文进行认证处理，直接丢弃，可以防止该类用户报文持续发送给服务器认证而对设备性能造成影响。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。

【举例】

在接口 GigabitEthernet1/0/1 上配置 IPv4 IPoE 用户的静默时间为 100 秒。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber timer quiet 100
```

1.1.27 ip subscriber trust

ip subscriber trust 命令用来配置信任 DHCPv4 报文中的指定 Option。

undo ip subscriber trust 命令用来取消信任 DHCPv4 报文中指定的 Option。

【命令】

```
ip subscriber trust { option60 | option82 }
```

```
undo ip subscriber trust { option60 | option82 }
```

【缺省情况】

不信任 DHCPv4 报文中的任何 Option。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

option60：表示信任 DHCPv4 报文中的 Option 60。

option82：表示信任 DHCPv4 报文中的 Option 82。

【使用指导】

DHCP 组网环境中，接入设备可以提取用户的 DHCP-DISCOVER 报文中的 Option 60 信息。如果接入设备信任 DHCPv4 报文中的 Option 60 信息，则：

- 在 Option 60 内容有效（无非法字符“/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>”等），且没有域名分隔符@字符的情况下，IPoE 用户使用整个 Option 60 的内容作为指定的认证域进行认证。
- 在 Option 60 内容有效（无非法字符“/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>”等），且其中包含了域名分隔符@字符的情况下，IPoE 用户使用@字符之后的字符串作为指定的认证域进行认证。如果在 Option 60 内容中包括多个@字符，则使用最后一个@字符之后的字符串作为 IPoE 用户的认证域名。

如果接入设备不信任 DHCPv4 报文中的 Option 60 信息，但是接口上配置了 **ip subscriber dhcp domain** 命令，则 IPoE 用户使用该命令指定的认证域进行认证；否则，使用缺省认证域进行认证。

DHCP 中继组网环境中，接入设备可以提取用户的 DHCP-DISCOVER 报文中的 Option 82 信息。如果接入设备信任 DHCPv4 报文中的 Option 82，则：

- 接入设备在采用 version 2.0 格式封装 RADIUS NAS-PORT-ID 属性时，会根据 Option 82 信息中的 Circuit-ID 子选项内容封装发往 RADIUS 服务器的 NAS-PORT-ID 属性；
- 接入设备会根据 Option 82 中的 Circuit-ID 子选项内容封装发往 RADIUS 服务器的 DSL_AGENT_CIRCUIT_ID 属性；
- 接入设备会根据 Option 82 中的 Remote-ID 子选项内容封装发往 RADIUS 服务器的 DSL_AGENT_REMOTE_ID 属性。

如果不信任 DHCPv4 报文中的 Option 82，则接入设备在封装以上 RADIUS 属性时，不采用 Option 82 中的任何信息。

【举例】

在接口 GigabitEthernet1/0/1 上配置设备信任 DHCPv4 报文中的 Option 82。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber trust option82
```


【相关命令】

- **ip subscriber dhcp domain**
- **ip subscriber initiator dhcp enable**
- **ip subscriber nas-port-id format**
- **ip subscriber nas-port-id nasinfo-insert**

1.1.28 ip subscriber unclassified-ip domain

ip subscriber unclassified-ip domain 命令用来配置 IPv4 接入用户使用的认证域。

undo ip subscriber unclassified-ip domain 命令用来恢复缺省情况。

【命令】

ip subscriber unclassified-ip domain *domain-name*
undo ip subscriber unclassified-ip domain

【缺省情况】

IPv4 接入用户的认证域为缺省认证域。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

domain-name: 认证使用的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括“/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>”以及“@”字符。

【使用指导】

该命令用来配置 IPv4 报文触发接入的 IPv4 接入用户（包括未知源 IP 接入用户、静态 IPoE 接入用户和 IPoE 子网/接口专线用户）在认证时使用的认证域，该域名必须在接入设备上存在且配置完整。

如果指定接口上配置了 **ip subscriber service-identify**，则优先使用 **ip subscriber service-identify** 指定的业务识别方式获取对应的认证域。只有在未匹配到 **ip subscriber service-identify** 命令指定的认证域时，才使用 **ip subscriber unclassified-ip domain** 命令指定的认证域。如果 **ip subscriber unclassified-ip domain** 命令也未配置，则使用缺省认证域。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 上的 IPv4 接入用户使用的认证域为 ipoe。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ip subscriber unclassified-ip domain ipoe
```

【相关命令】

- **ip subscriber initiator unclassified-ip enable**

- **ip subscriber service-identify**

1.1.29 ip subscriber unclassified-ip max-session

ip subscriber unclassified-ip max-session 命令用来配置接口上允许未知源 IPv4 报文触发创建的动态 IPv4 IPoE 会话的最大数目。

undo ip subscriber unclassified-ip max-session 命令用来恢复缺省情况。

【命令】

ip subscriber unclassified-ip max-session *max-number*
undo ip subscriber unclassified-ip max-session

【缺省情况】

未配置接口上允许未知源 IPv4 报文创建的动态 IPv4 IPoE 会话的最大数目。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

max-number: 允许未知源 IPv4 报文触发创建的 IPv4 IPoE 会话的最大数目,取值范围为 1~64000。

【使用指导】

未知源 IPv4 报文触发创建的 IPv4 IPoE 会话数目达到最大值后, 后续未知源 IPv4 报文不能触发创建 IPv4 IPoE 会话。

【举例】

配置接口 GigabitEthernet1/0/1 上允许未知源 IPv4 报文触发创建的 IPv4 IPoE 会话的最大数目为 100。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber unclassified-ip max-session 100
```

【相关命令】

- **display ip subscriber session**
- **ip subscriber initiator unclassified-ip enable**
- **reset ip subscriber session**

1.1.30 ip subscriber unclassified-ip username

ip subscriber unclassified-ip username 命令用来配置 IPv4 未知源 IP 接入用户和静态个人用户的认证用户名的命名规则。

undo ip subscriber unclassified-ip username 命令用来恢复缺省情况。

【命令】

```
ip subscriber unclassified-ip username include { nas-port-id [ separator  
separator ] | port [ separator separator ] | second-vlan [separator separator ]  
| slot [ separator separator ] | source-ip [ address-separator  
address-separator ] [ separator separator ] | source-mac [ address-separator  
address-separator ] [ separator separator ] | subslot [ separator separator ]  
| sysname [ separator separator ] | vlan [ separator separator ] } *  
undo ip subscriber unclassified-ip username
```

【缺省情况】

IPv4 未知源 IP 接入用户和静态个人用户采用用户报文的源 IPv4 地址作为认证用户名。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

nas-port-id: 表示使用用户的 NAS-PORT-ID 属性作为用户名。

port: 表示以用户接入的端口号作为用户名。

second-vlan: 表示以认证报文中的内层 VLAN 作为用户名。

slot: 表示以用户接入的槽位号作为用户名

source-ip: 表示使用用户报文的源 IPv4 地址作为用户名。

address-separator address-separator: IPv4 地址分隔符, 可以为任意可配置的可见字符。
若指定了分隔符, 例如 “-”, 则用户名形如 192-168-1-1; 若不指定该参数, 则用户名为 x.x.x.x 形式。建议不要使用 @ 作为分隔符, 避免携带 @ 字符的用户名在 AAA 服务器端不能被正确解析。

source-mac: 表示使用用户报文的源 MAC 地址作为用户名。

address-separator address-separator: MAC 地址分隔符, 可以为任意可配置的可见字符。若指定了分隔符, 例如 “-”, 则用户名形如 xxxx-xxxx-xxxx; 若不指定该参数, 则用户名为 xxxxxxxxxxxx 形式。建议不要使用 @ 作为分隔符, 避免携带 @ 字符的用户名在 AAA 服务器端不能被正确解析。

subslot: 表示以用户接入的子卡号作为用户名。

sysname: 表示以用户接入设备的设备名作为用户名。

vlan: 表示以认证报文中的外层 VLAN 作为用户名。

separator separator: 当前字段分隔符, 用在当前字段后面以连接后面的一个字段, 可以为任意可配置的可见字符。建议不要使用 @ 作为分隔符, 避免携带 @ 字符的用户名在 AAA 服务器端不能被正确解析。

【使用指导】

本命令用来配置未知源 IP 接入用户和静态个人用户在认证时使用的用户名的命名规则, 根据该命名规则获取的用户名必须与认证服务器上配置的用户名保持一致。

在允许的用户名类型范围内，该命令支持任意形式、任意顺序的用户名组合。例如：若配置 **ip subscriber unclassified-ip username include source-ip source-mac**，则用户名为源 IPv4 地址字段和源 MAC 地址字段内容的拼接，且两个字段之间无分隔符。

【举例】

配置接口 GigabitEthernet1/0/1 上的未知源 IP 接入用户和静态个人用户使用用户报文的源 IPv4 地址作为用户名。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber unclassified-ip username include source-ip
```

配置接口 GigabitEthernet1/0/1 上的未知源 IP 接入用户和静态个人用户使用接入设备的设备名、接入的槽位号、接入的子卡号、接入的端口号和认证报文中的外层 VLAN 信息作为用户名，所选用的字段之间均使用#作为分隔符。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip subscriber unclassified-ip username include sysname  
separator # slot separator # subslot separator # port separator # vlan
```

【相关命令】

- **ip subscriber initiator unclassified-ip enable**
- **ip subscriber password**

1.1.31 ip subscriber user-detect

ip subscriber user-detect 命令用来开启静态/动态 IPv4 IPoE 个人接入用户在线探测功能，并配置其探测方式。

undo ip subscriber user-detect 命令用来关闭静态/动态 IPv4 IPoE 个人接入用户在线探测功能。

【命令】

```
ip subscriber user-detect { arp | icmp } retry retries interval interval  
undo ip subscriber user-detect
```

【缺省情况】

静态/动态 IPv4 IPoE 个人接入用户在线探测功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

arp：表示使用 ARP 请求报文作为探测报文。

icmp：表示使用 ICMP 请求报文作为探测报文。

retry retries: 探测失败后允许重复尝试的最大次数，取值范围为 2~5。例如，retries 值为 2 表示连续三次失败就认为用户不在线。

interval interval: 探测的时间间隔，取值范围为 30~1200，单位为秒。

【使用指导】

接口上的静态/动态 IPoE 个人接入用户上线后，设备会定时统计用户流量。若一个探测间隔（*interval*）内用户流量无变化，则该探测间隔结束后，设备将发送一次探测报文。如果设备在探测间隔内未收到用户的报文，则认为一次探测失败。

若设备首次探测失败，将继续做指定次数（*retries*）的重复探测，若全部探测尝试都失败（即一直未收到该用户报文），则认为此用户不在线，停止发送探测报文并删除用户；若设备在探测中收到用户的报文，则认为用户在线，重置探测定时器并开始下一次探测。

对于与接口在同一网段内的静态/动态 IPv4 IPoE 个人接入用户，可使用 ARP 请求或 ICMP 请求报文对用户进行探测；对于与接口不在同一网段内的静态/动态 IPv4 IPoE 个人接入用户，应使用 ICMP 请求报文对用户进行探测。

接口上不可同时启用两种方式对静态/动态 IPv4 IPoE 个人接入用户进行探测。

【举例】

开启接口 GigabitEthernet1/0/1 上使用 ARP 请求报文对静态/动态 IPv4 IPoE 个人接入用户进行在线探测，探测失败后允许重复尝试 5 次，探测的时间间隔为 100 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber user-detect arp retry 5 interval 100
```

【相关命令】

- **ip subscriber enable**

1.1.32 ip subscriber vlan

ip subscriber vlan 命令用来配置 IPv4 接入用户的 IP 报文的内/外层 VLAN 值与认证域的映射关系。

undo ip subscriber vlan 命令用来删除指定内/外层 VLAN 值与认证域的映射关系。

【命令】

```
ip subscriber vlan vlan-list domain domain-name
undo ip subscriber vlan vlan-list
```

【缺省情况】

未配置 IPv4 接入用户的 IP 报文的内/外层 VLAN 与认证域的映射关系。

【视图】

三层以太网子接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

vlan-list: VLAN 列表, 表示一个或多个 VLAN, 表示方式为 **vlan-list = { vlan-id [to vlan-id] }**<1-10>, 其中, **vlan-id** 为指定 VLAN 的编号, 取值范围为 1~4094。<1-10> 表示前面的参数最多可以输入 10 次。

domain domain-name: 表示与指定的 VLAN 范围相关联的 ISP 域名, 为 1~255 个字符的字符串, 不区分大小写, 不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。

【使用指导】

本命令用来配置指定 VLAN 范围内 IPv4 接入用户（包括未知源 IP 接入用户、静态 IPoE 接入用户和 IPoE 子网/接口专线用户）进行认证时使用的认证域, 通过指定的认证域进行认证、授权、计费。

【举例】

在子接口 GigabitEthernet1/0/1.100 上配置内层 VLAN ID 范围为 2 到 100 的 IPv4 接入用户认证使用的认证域为 vlandm。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.100
[Sysname-GigabitEthernet1/0/1.100] ip subscriber service-identify second-vlan
[Sysname-GigabitEthernet1/0/1.100] ip subscriber vlan 2 to 100 domain vlandm
```

【相关命令】

- **ip subscriber service-identify**

1.1.33 ip subscriber whitelist enable

ip subscriber whitelist enable 命令用来开启 IPv4 IPoE 白名单功能。

undo ip subscriber whitelist enable 命令用来关闭 IPv4 IPoE 白名单功能。

【命令】

```
ip subscriber whitelist enable
undo ip subscriber whitelist enable
```

【缺省情况】

IPv4 IPoE 白名单功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启 IPv4 IPoE 白名单功能后, 仅匹配到静态 IPv4 IPoE 会话的 IPv4 流量才会触发 IPoE 认证, 其余流量 IPoE 不做任何处理, 均直接放行。

在一些组网环境中, 接口上可能需要同时开启 IPoE 和 Portal 功能, 例如: 监控摄像头等哑终端使用 IPoE 进行免认证上线, 同时宽带拨号用户使用 Portal 进行 Web 认证上线; 这种组网环境可配置 IPoE 白名单功能。当接口同时开启 IPv4 IPoE 白名单功能和 Portal 功能时:

- 如果用户 IPv4 流量可以匹配到静态 IPv4 IPoE 会话，则按静态 IPv4 IPoE 认证流程处理。当需要对 IPoE 用户进行免认证时，domain 认证域下的 IPoE 认证及授权方式必须配置为 **none**。
- 如果用户 IPv4 流量未匹配任何静态 IPv4 IPoE 会话，则进入 Portal 认证流程处理。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上开启 IPv4 IPoE 白名单功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip subscriber whitelist enable
```

1.1.34 reset ip subscriber offline statistics

reset ip subscriber offline statistics 命令用来清除 IPv4 IPoE 用户下线统计信息。

【命令】

```
reset ip subscriber offline statistics [ interface interface-type interface-number ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interface interface-type interface-number：表示清除指定接口上的 IPv4 IPoE 用户下线统计信息，**interface-type interface-number** 表示接口类型和接口编号。如果未指定本参数，将清除所有接口上的 IPv4 IPoE 用户下线统计信息。

【举例】

```
# 清除接口 GigabitEthernet1/0/1 上的 IPv4 IPoE 用户下线统计信息。
<Sysname> reset ip subscriber offline statistics interface gigabitethernet 1/0/1
```

【相关命令】

- **display ip subscriber offline statistics**

1.1.35 reset ip subscriber session

reset ip subscriber session 命令用来清除动态个人 IPv4 IPoE 会话和重置静态 IPv4 IPoE 会话，强制用户下线。

【命令】

```
reset ip subscriber session [ interface interface-type interface-number ]  
[ domain domain-name | ip ip-address [ vpn-instance vpn-instance-name ] | mac  
mac-address | username name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface *interface-type interface-number*: 表示清除指定接口动态个人 IPv4 IPoE 会话和重置静态 IPv4 IPoE 会话, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 将清除所有接口动态个人 IPv4 IPoE 会话和重置静态 IPv4 IPoE 会话。

domain *domain-name*: 表示清除和重置使用指定 ISP 域认证的 IPv4 IPoE 会话, *domain-name* 为 1~255 个字符的字符串, 不区分大小写, 不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。

ip *ip-address*: 表示清除指定 IP 地址的 IPv4 IPoE 会话, *ip-address* 为指定的 IP 地址。

vpn-instance *vpn-instance-name*: 表示清除和重置指定 VPN 实例的 IPv4 IPoE 会话, *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示 IPv4 IPoE 会话位于公网中。

mac *mac-address*: 表示清除和重置指定源 MAC 地址的 IPv4 IPoE 会话, 形式为 H-H-H。

username *name*: 表示清除和重置指定用户名的 IPv4 IPoE 会话, *name* 为 1~255 个字符的字符串, 区分大小写。

【使用指导】

本命令用来清除动态个人 IPv4 IPoE 会话和重置静态 IPv4 IPoE 会话信息, 并强制用户下线, 如果不指定条件, 则表示删除所有动态 IPv4 IPoE 会话和重置所有静态 IPv4 IPoE 会话。

专线用户和静态个人用户的会话不能通过 **reset ip subscriber session** 命令清除, 只能通过相应的 **undo** 命令删除配置的方式清除。

【举例】

清除接口 GigabitEthernet1/0/1 上动态个人 IPv4 IPoE 会话和重置静态 IPv4 IPoE 会话, 强制用户下线。

```
<Sysname> reset ip subscriber session interface gigabitethernet 1/0/1
```

【相关命令】

- **display ip subscriber session**

1.2 IPv6 IPoE配置命令

1.2.1 display ipv6 subscriber interface-leased

display ipv6 subscriber interface-leased 命令用来显示 IPv6 IPoE 接口专线用户信息。

【命令】

display ipv6 subscriber interface-leased [**interface** *interface-type interface-number*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface interface-type interface-number: 显示指定接口上的 IPv6 IPoE 接口专线用户信息, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 将显示所有接口上的 IPv6 IPoE 接口专线用户信息。

slot slot-number: 显示指定成员设备上的 IPv6 IPoE 接口专线用户信息, *slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数, 将显示所有成员设备上的 IPv6 IPoE 接口专线用户信息。

【举例】

显示接口 GigabitEthernet1/0/1 上的 IPv6 IPoE 接口专线用户信息。

```
<Sysname> display ipv6 subscriber interface-leased interface gigabitethernet 1/0/1
```

Basic:

Access interface	: GE1/0/1
VPN instance	: N/A
Username	: a
User ID	: 0x40000000
State	: Online
Service node	: Slot 1 CPU 0
Domain	: radius6
Login time	: May 14 20:20:11 2014
Online time (hh:mm:ss)	: 00:16:37

AAA:

IP pool	: ipoe
Session idle time	: N/A
Session duration	: N/A, remaining: N/A
Remaining traffic	: N/A
Max multicast addresses	: 4
Multicast address list	: N/A

QoS:

User profile	: unis6 (active)
Session group profile	: N/A
Inbound CAR	: CIR 1000bps PIR 2000bps CBS 500bit (active)
Outbound CAR	: CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:

Uplink	packets/bytes	: 0/0
Downlink	packets/bytes	: 0/0

ITA:

```

Level-1 Uplink   packets/bytes: 0/0
              Downlink packets/bytes: 0/0
Level-2 Uplink   packets/bytes: 0/0
              Downlink packets/bytes: 0/0

```

表1-10 display ipv6 subscriber interface-leased 命令显示信息描述表

字段	描述
Basic	IPoE会话的基本信息
Access interface	用户所在的接口名称
VPN instance	用户所属的MPLS L3VPN实例，N/A表示用户属于公网
Username	用户认证时使用的用户名
User ID	用户ID，只有用户在线后才会由系统分配，0xffffffff表示暂未分配
State	用户的认证状态 • Init: 初始化 • Offline: 正在下线 • Auth: 认证中 • AuthFail: 认证失败 • AuthPass: 认证通过 • AssignedIP: 用户已具备 IP 地址 • Online: 用户在线 • Backup: 备份状态，表示该用户是由对端备份到本端的
Service node	为用户提供认证服务的节点信息
Domain	认证使用的认证域名
Login time	用户登录时间，即用户授权成功的时间，格式为设备时间，如：MM-DD hh:mm:ss YYYY
Online time (hh:mm:ss)	用户本次上线的在线时长
AAA	IPoE会话的AAA授权信息
IP pool	AAA授权的DHCP地址池名称，N/A表示AAA未授权该属性
Session idle time	用户闲置切断时间，单位为秒，N/A表示不进行闲置切断
Session duration	AAA授权的IPoE会话超时时间，单位为秒 • N/A: 表示未授权会话时长 • Unlimited: 表示会话时长无限制

字段	描述
remaining	AAA授权的IPoE会话剩余时长 - 当 AAA 未授权 IPoE 会话超时时间时，该字段始终显示为 N/A - 当 AAA 授权 IPoE 会话超时时间时 - 如果用户通过三层以太网接口/三层以太网子接口上线，该字段始终显示具体的剩余时长或 Unlimited（表示会话时长无限制） - 如果用户通过三层聚合接口/三层聚合子接口上线，则只有在本命令中指定 Service node 所在的 slot 或接口时，才会显示具体的剩余时长或 Unlimited（表示会话时长无限制），否则显示为 N/A
Remaining traffic	授权的剩余流量，单位为字节，N/A表示未对用户指定授权流量
Max multicast addresses	AAA授权用户可加入的组播组的最大数目
Multicast address list	AAA授权用户可加入的组播组地址列表，N/A表示AAA未授权该属性
QoS	IPoE会话的QoS信息
User profile	AAA授权的User Profile名称。若未授权User profile，则显示为N/A。授权状态包括如下： active: AAA 授权 User Profile 成功 inactive: AAA 授权 User Profile 失败或者设备上不存在该 User Profile - 授权结果未知
Session group profile	AAA授权的Session Group Profile名称。若未授权Session Group Profile，则显示为N/A。授权状态包括如下： active: AAA 授权 Session Group Profile 成功 inactive: AAA 授权 Session Group Profile 失败或者设备上不存在该 Session Group Profile - 授权结果未知
Inbound CAR	入方向CAR值（CIR：入方向平均速率，单位为bps；PIR：入方向峰值速率，单位为bps；CBS：入方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： active: 表示入方向 CAR 限速下发成功 inactive: 表示入方向 CAR 限速下发失败
Outbound CAR	出方向CAR值（CIR：出方向平均速率，单位为bps；PIR：出方向峰值速率，单位为bps；CBS：出方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： active: 表示出方向 CAR 限速下发成功 inactive: 表示出方向 CAR 限速下发失败
Flow statistic	IPoE会话的流量统计信息
Uplink packets/bytes	上行流量报文数/字节数
Downlink packets/bytes	下行流量报文数/字节数
ITA	IPoE会话的ITA（Intelligent Target Accounting，智能靶向计费）业务流量统计信息
Level- <i>n</i> Uplink packets/bytes	计费等级为 <i>n</i> 的上行流量报文数/字节数， <i>n</i> 的取值范围为1~8

字段	描述
Downlink packets/bytes	计费等级为n的下行流量报文数/字节数， <i>n</i> 的取值范围为1~8

【相关命令】

- **ipv6 subscriber enable**

1.2.2 display ipv6 subscriber interface-leased statistics

display ipv6 subscriber interface-leased statistics 命令用来显示 IPv6 IPoE 接口专线用户统计信息。

【命令】

display ipv6 subscriber interface-leased statistics [**interface** *interface-type interface-number*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上的 IPv6 IPoE 接口专线用户统计信息，*interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数，将显示所有接口上 IPv4 IPoE 接口专线用户已经上线和正在上线的统计信息。

slot *slot-number*: 显示指定成员设备上的 IPv6 IPoE 接口专线用户统计信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示所有成员设备上的 IPv6 IPoE 接口专线用户统计信息。

【举例】

显示设备上 IPv6 IPoE 接口专线用户统计信息。

```
<Sysname> display ipv6 subscriber interface-leased statistics
Total                : 100
Init                 : 0
Authenticating       : 20
Authenticate fail     : 0
Authenticate pass    : 20
Assigned IP          : 10
Online                : 50
Backup               : 0
```

表1-11 display ipv6 subscriber interface-leased statistics 命令显示信息描述表

字段	描述
Total	接入的总用户数
Init	处于初始状态的用户数
Authenticating	处于正在认证状态的用户数
Authenticate fail	处于认证失败状态的用户数
Authenticate pass	处于认证成功状态的用户数
Assigned IP	处于成功分配到IP地址状态的用户数
Online	处于在线状态的用户数
Backup	处于备份状态的用户数

1.2.3 display ipv6 subscriber offline statistics

display ipv6 subscriber offline statistics 命令用来显示 IPv6 IPoE 用户下线原因的统计信息。

【命令】

display ipv6 subscriber offline statistics [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface interface-type interface-number: 显示指定接口上 IPoE 用户下线原因的统计信息, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 将显示所有接口上 IPoE 用户下线原因的统计信息。

【举例】

```
# 显示接口 GigabitEthernet1/0/1 上 IPv6 IPoE 用户下线原因的统计信息
<Sysname> display ipv6 subscriber offline statistics interface gigabitethernet1/0/1
Total                : 100
User request         : 0
DHCP lease expire   : 0
AAA lease expire     : 0
Command cut         : 80
AAA terminate        : 0
```

```

Authenticate fail    : 0
Authorization fail   : 0
Idle timeout         : 10
Detect fail          : 10
Not enough resource  : 0
Interface down       : 0
Interface shutdown   : 0
VSRP event           : 0
DHCP notify          : 0
Other                : 0

```

表1-12 display ipv6 subscriber offline statistics 命令显示信息描述表

Total	下线的总用户数
User request	用户主动要求下线的用户数
DHCP lease expired	DHCP租约到期正常下线的用户数
AAA lease expired	AAA租约到期正常下线的用户数
Command cut	通过命令行下线的用户数
AAA terminate	AAA强制下线的用户数
Authenticate fail	认证失败的用户数
Authorization fail	授权失败的用户数
Idle timeout	用户空闲超时下线的用户数
Detect fail	在线探测失败下线的用户数
Not enough resource	硬件资源不足下线的用户数
Interface down	因接口状态为down下线的用户数
Interface shutdown	主动shutdown接口导致下线的用户数
VSRP event	收到VSRP（Virtual Service Redundancy Protocol，虚拟业务冗余协议）事件通知而下线的用户数
DHCP notify	DHCP通知下线的用户数
Other	其它状况触发下线的用户数

【相关命令】

- **reset ipv6 subscriber offline statistics**

1.2.4 display ipv6 subscriber session

display ipv6 subscriber session 命令用来显示 IPv6 IPoE 个人会话信息。

【命令】

```

display ipv6 subscriber session [ interface interface-type
interface-number ] [ domain domain-name | ipv6 ipv6-address [ vpn-instance

```

vpn-instance-name] | **mac** *mac-address* | **static** | **username** *name*] [**slot** *slot-number*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上的 IPv6 IPoE 个人会话，*interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数，将显示所有接口上的 IPv6 IPoE 个人会话。

domain *domain-name*: 显示使用指定 ISP 域认证的 IPv6 IPoE 个人会话，*domain-name* 为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>”以及 “@” 字符。

ipv6 *ipv6-address*: 显示指定源 IP 地址的 IPv6 IPoE 个人会话，*ipv6-address* 为指定的 IPv6 地址。

vpn-instance *vpn-instance-name*: 指定用户所属的 VPN 实例，*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 IPv6 IPoE 个人会话位于公网中。

mac *mac-address*: 显示指定源 MAC 地址的 IPv6 IPoE 个人会话，形式为 H-H-H。

static: 显示静态配置的 IPv6 IPoE 个人会话，不指定该参数时将显示静态配置的 IPv6 IPoE 个人会话和动态触发创建的 IPv6 IPoE 个人会话。

username *name*: 显示指定用户名的 IPv6 IPoE 个人会话，其中，*name* 为 1~255 个字符的字符串，区分大小写。

slot *slot-number*: 显示指定成员设备上 IPv6 IPoE 个人会话，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示所有成员设备上 IPv6 IPoE 会话。

verbose: 显示 IPv6 IPoE 个人会话的详细信息。如果不指定该参数，则只显示 IPoE 会话的简要信息。

【举例】

显示用户 IP 为 2000::1，所属 VPN 实例为 vpn1 的 IPv6 IPoE 会话简要信息。

```
<Sysname> display ipv6 subscriber session ipv6 2000::1 vpn-instance vpn1
```

```
Type: D-DHCP      S-Static      U-Unclassified-IP      N-NDRS
```

Interface	IP address	MAC address	Type	State

RAGG1024	2000::1	000d-88f8-0eab	D	Online

显示所有 IPv6 IPoE 个人会话的详细信息。

```
<Sysname> display ipv6 subscriber session verbose
```

```
Basic:
```

```

Description          : -
Username             : abc
Domain               : radius6
VPN instance         : N/A
IP address           : 2000::1
MAC address          : 000d-88f8-0eab
Service-VLAN/Custom-VLAN : -/-
Access interface     : GE1/0/1
User ID              : 0x48080008
VPI/VCI(for ATM)     : -/-
DHCP lease           : N/A
DHCP remain lease    : N/A
Login time           : May 9 09:10:01 2014
Online time (hh:mm:ss) : 00:16:37
Service node         : Slot 1 CPU 0
Type                 : Unclassified-IP
State                : Online

```

AAA:

```

IP pool              : N/A
Session idle time    : N/A
Session duration     : N/A, remaining: N/A
Remaining traffic    : N/A
Max multicast addresses : 4
Multicast address list : N/A

```

QoS:

```

User profile         : unis6 (active)
Session group profile : N/A
Inbound CAR          : CIR 1000bps PIR 2000bps CBS 500bit (active)
Outbound CAR         : CIR 3000bps PIR 4000bps CBS 500bit (active)

```

Flow statistic:

```

Uplink  packets/bytes : 0/0
Downlink packets/bytes : 0/0

```

ITA:

```

Level-1 Uplink  packets/bytes: 0/0
          Downlink packets/bytes: 0/0
Level-2 Uplink  packets/bytes: 0/0
          Downlink packets/bytes: 0/0

```

表1-13 display ipv6 subscriber session 命令显示信息描述表

字段	描述
Basic	IPoE会话的基本信息
Description	IPoE会话的描述信息（“-”表示没有描述信息）
Username	用户认证时使用的用户名

字段	描述
Domain	用户认证时使用的认证域名
VPN instance	用户所属的MPLS L3VPN实例，N/A表示用户属于公网
IP address	用户的IP地址
MAC address	用户的MAC地址
Service-VLAN/Customer-VLAN	用户所在的公网VLAN/私网VLAN（“-”表示没有VLAN信息）
Access interface	用户接入的接口名称
User ID	用户ID，只有用户在线后才会由系统分配，0xffffffff表示暂未分配
VPI/VCI(for ATM)	ATM的PVC信息
DHCP lease	DHCP服务器分配给用户的IP地址租约时间，单位为秒 - N/A: 表示无DHCP租约 - Unlimited: 表示租约无限长
DHCP remain lease	DHCP服务器分配给用户的IP地址租约剩余时长 只在Service node上可以查看到有效的剩余时长，非Service node上该字段显示为N/A
Login time	用户登录时间，即用户授权成功的时间，格式为设备时间，如：MM-DD hh:mm:ss YYYY
Online time (hh:mm:ss)	用户本次上线的在线时长
Service node	为用户提供认证服务的节点信息
Type	IPoE会话的创建类型 - DHCP: DHCP报文触发创建 - Unclassified-IP: 未知源IP报文触发创建 - Static: 静态配置 - NDRS: IPv6 ND RS报文触发创建
State	用户状态: - Init: 初始化 - Offline: 正在下线 - Auth: 认证中 - AuthFail: 认证失败 - AuthPass: 认证通过 - AssignedIP: 会话已具备IP地址 - Online: 用户在线 - Backup: 备份状态，表示该用户是由对端备份到本端的
AAA	IPoE会话的AAA授权信息
IP pool	AAA授权的DHCP地址池名称，N/A表示AAA未授权该属性
Session idle time	用户闲置切断时间，单位为秒，N/A表示不进行闲置切断

字段	描述
Session duration	AAA授权的IPoE会话超时时间，单位为秒 - N/A: 表示未授权会话时长 - Unlimited: 表示会话时长无限制
remaining	AAA授权的IPoE会话剩余时长 - 当 AAA 未授权 IPoE 会话超时时间时，该字段始终显示为 N/A - 当 AAA 授权 IPoE 会话超时时间时 - 如果用户通过三层以太网接口/三层以太网子接口上线，该字段始终显示具体的剩余时长或 Unlimited（表示会话时长无限制） - 如果用户通过三层聚合接口/三层聚合子接口上线，则只有在本命令中指定 Service node 所在的 slot 或接口时，才会显示具体的剩余时长或 Unlimited（表示会话时长无限制），否则显示为 N/A
Remaining traffic	授权的剩余流量，单位为字节，N/A表示未对用户指定授权流量
Max multicast addresses	AAA授权用户可加入的组播组的最大数目
Multicast address list	AAA授权用户可加入的组播组地址列表，N/A表示AAA未授权该属性
QoS	IPoE会话的QoS信息
User profile	AAA授权的User Profile名称。若未授权User profile，则显示为N/A。授权状态包括如下： - active: AAA 授权 User Profile 成功 - inactive: AAA 授权 User Profile 失败或者设备上不存在该 User Profile - 授权结果未知
Session group profile	AAA授权的Session Group Profile名称。若未授权Session Group Profile，则显示为N/A。授权状态包括如下： - active: AAA 授权 Session Group Profile 成功 - inactive: AAA 授权 Session Group Profile 失败或者设备上不存在该 Session Group Profile - 授权结果未知
Inbound CAR	入方向CAR值（CIR：入方向平均速率，单位为bps；PIR：入方向峰值速率，单位为bps；CBS：入方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： - active: 表示入方向 CAR 限速下发成功 - inactive: 表示入方向 CAR 限速下发失败
Outbound CAR	出方向CAR值（CIR：出方向平均速率，单位为bps；PIR：出方向峰值速率，单位为bps；CBS：出方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： - active: 表示出方向 CAR 限速下发成功 - inactive: 表示出方向 CAR 限速下发失败
Flow statistic:	IPoE会话的流量统计信息
Uplink packets/bytes	上行流量报文数/字节数
Downlink packets/bytes	下行流量报文数/字节数

字段	描述
ITA	IPoE会话的ITA（Intelligent Target Accounting，智能靶向计费）业务流量统计信息
Level- <i>n</i> Uplink packets/bytes	计费等级为 <i>n</i> 的上行流量报文数/字节数， <i>n</i> 的取值范围为1~8
Downlink packets/bytes	计费等级为 <i>n</i> 的下行流量报文数/字节数， <i>n</i> 的取值范围为1~8

【相关命令】

- **ip subscriber enable**

1.2.5 display ipv6 subscriber session statistics

display ipv6 subscriber session statistics 命令用来显示 IPv6 IPoE 个人用户统计信息。

【命令】

```
display ipv6 subscriber session statistics [ session-type { dhcp | ndrs | static | unclassified-ip } ] [ interface interface-type interface-number ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

session-type: 用户上线类型。不指定该参数，则表示显示所有类型的 IPv6 IPoE 个人用户统计信息。

dhcp: 表示 DHCP 用户。

ndrs: 表示 RS 报文触发认证的用户。

static: 表示静态个人用户。

unclassified-ip: 表示未知源 IP 用户。

interface *interface-type* *interface-number*: 显示指定接口上的 IPv6 IPoE 个人用户统计信息，*interface-type* *interface-number* 表示接口类型和接口编号。如果未指定本参数，将显示所有接口上 IPv4 IPoE 个人用户已经上线和正在上线的统计信息。

slot *slot-number*: 显示指定成员设备上的 IPv6 IPoE 个人用户统计信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示所有成员设备上的 IPv6 IPoE 个人用户统计信息。

【举例】

```
# 显示接口 GigabitEthernet1/0/1 上 IPv6 IPoE 个人用户统计信息。
<Sysname> display ipv6 subscriber session statistics session-type dhcp interface
gigabitethernet 1/0/1
Total                : 100
Init                 : 0
Authenticating       : 20
Authenticate fail    : 0
Authenticate pass    : 20
Assigned IP          : 10
Online               : 50
Backup               : 0
```

表1-14 display ipv6 subscriber session statistics 命令显示信息描述表

字段	描述
Total	接入的总用户数
Init	处于初始状态的用户数
Authenticating	处于正在认证状态的用户数
Authenticate fail	处于认证失败状态的用户数
Authenticate pass	处于认证成功状态的用户数
Assigned IP	处于成功分配到IP地址状态的用户数
Online	处于在线状态的用户数
Backup	处于备份状态的用户数

【相关命令】

- **reset ipv6 subscriber session**

1.2.6 display ipv6 subscriber subnet-leased

display ipv6 subscriber subnet-leased 命令用来显示 IPv6 IPoE 子网专线用户信息。

【命令】

```
display ipv6 subscriber subnet-leased [ interface interface-type
interface-number ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin

context-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上的 IPv6 IPoE 子网专线用户信息, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 将显示所有接口上的 IPv6 IPoE 子网专线用户信息。

slot *slot-number*: 显示指定成员设备上的 IPv6 IPoE 子网专线用户信息, *slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数, 将显示所有成员设备上的 IPv6 IPoE 子网专线用户信息。

【举例】

显示接口 GigabitEthernet1/0/1 上的 IPv6 IPoE 子网专线用户信息。

```
<Sysname> display ipv6 subscriber subnet-leased interface gigabitethernet 1/0/1
```

Basic:

Access interface	: GE1/0/1
VPN instance	: N/A
Username	: a
Network	: 99::/64
User ID	: 0x40000001
State	: Online
Service node	: Slot 1 CPU 0
Domain	: radius6
Login time	: May 14 20:22:14 2014
Online time (hh:mm:ss)	: 00:16:37

AAA:

IP pool	: N/A
Session idle time	: N/A
Session duration	: N/A, remaining: N/A
Remaining traffic	: N/A
Max multicast addresses	: 4
Multicast address list	: N/A

QoS:

User profile	: unis6 (active)
Session group profile	: N/A
Inbound CAR	: CIR 1000bps PIR 2000bps CBS 500bit (active)
Outbound CAR	: CIR 3000bps PIR 4000bps CBS 500bit (active)

Flow statistic:

Uplink	packets/bytes	: 0/0
Downlink	packets/bytes	: 0/0

ITA:

Level-1 Uplink	packets/bytes	: 0/0
Downlink	packets/bytes	: 0/0
Level-2 Uplink	packets/bytes	: 0/0
Downlink	packets/bytes	: 0/0

表1-15 display ipv6 subscriber subnet-leased 命令显示信息描述表

字段	描述
Basic	IPoE会话的基本信息
Access interface	用户所在的接口名称
VPN instance	用户所属的MPLS L3VPN实例，N/A表示用户属于公网
User name	用户认证时使用的用户名
Network	用户所在的子网地址
User ID	用户ID，只有用户在线后才会由系统分配，0xffffffff表示暂未分配
State	用户的认证状态 • Init: 初始化 • Offline: 正在下线 • Auth: 认证中 • AuthFail: 认证失败 • AuthPass: 认证通过 • AssignedIP: 会话已具备 IP 地址 • Online: 用户在线 • Backup: 备份状态，表示该用户是由对端备份到本端的
Service node	为用户提供认证服务的节点信息
Domain	用户认证时使用的认证域名
Login time	用户登录时间，即用户授权成功的时间，格式为设备时间，如：MM-DD hh:mm:ss YYYY
Online time (hh:mm:ss)	用户本次上线的在线时长
AAA	IPoE会话的AAA授权信息
IP pool	AAA授权的DHCP地址池名称，N/A表示AAA未授权该属性
Session idle time	用户闲置切断时间，单位为秒，N/A表示不进行闲置切断
Session duration	AAA授权的IPoE会话超时时间，单位为秒 • N/A: 表示未授权会话时长 • Unlimited: 表示会话时长无限制
remaining	AAA授权的IPoE会话剩余时长 • 当 AAA 未授权 IPoE 会话超时时间时，该字段始终显示为 N/A • 当 AAA 授权 IPoE 会话超时时间时 ◦ 如果用户通过三层以太网接口/三层以太网子接口上线，该字段始终显示具体的剩余时长或 Unlimited（表示会话时长无限制） ◦ 如果用户通过三层聚合接口/三层聚合子接口上线，则只有在本命令中指定 Service node 所在的 slot 或接口时，才会显示具体的剩余时长或 Unlimited（表示会话时长无限制），否则显示为 N/A
Remaining traffic	授权的剩余流量，单位为字节，N/A表示未对用户指定授权流量
Max multicast addresses	AAA授权用户可加入的组播组的最大数目

字段	描述
Multicast address list	AAA授权用户可加入的组播组地址列表，N/A表示AAA未授权该属性
QoS	IPoE会话的QoS信息
User profile	AAA授权的User Profile名称。若未授权User Profile，则显示为N/A。授权状态包括如下： - active: AAA 授权 User Profile 成功 - inactive: AAA 授权 User Profile 失败或者设备上不存在该 User Profile - 授权结果未知
Session group profile	AAA授权的Session Group Profile名称。若未授权Session Group Profile，则显示为N/A。授权状态包括如下： - active: AAA 授权 Session Group Profile 成功 - inactive: AAA 授权 Session Group Profile 失败或者设备上不存在该 Session Group Profile - 授权结果未知
Inbound CAR	入方向CAR值（CIR：入方向平均速率，单位为bps；PIR：入方向峰值速率，单位为bps；CBS：入方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： - active: 表示入方向 CAR 限速下发成功 - inactive: 表示入方向 CAR 限速下发失败
Outbound CAR	出方向CAR值（CIR：出方向平均速率，单位为bps；PIR：出方向峰值速率，单位为bps；CBS：出方向突发尺寸，单位为bit） 若未授权CAR，则显示为N/A。授权状态包括如下： - active: 表示出方向 CAR 限速下发成功 - inactive: 表示出方向 CAR 限速下发失败
Flow statistic:	IPoE会话的流量统计信息
Uplink packets/bytes	上行流量报文数/字节数
Downlink packets/bytes	下行流量报文数/字节数
ITA	IPoE会话的ITA（Intelligent Target Accounting，智能靶向计费）业务流量统计信息
Level- <i>n</i> Uplink packets/bytes	计费等级为 <i>n</i> 的上行流量报文数/字节数， <i>n</i> 的取值范围为1~8
Downlink packets/bytes	计费等级为 <i>n</i> 的下行流量报文数/字节数， <i>n</i> 的取值范围为1~8

【相关命令】

- ipv6 subscriber enable**

1.2.7 display ipv6 subscriber subnet-leased statistics

display ipv6 subscriber subnet-leased statistics 命令用来显示 IPv6 IPoE 子网专线用户统计信息。

【命令】

display ipv6 subscriber subnet-leased statistics [**interface** *interface-type* *interface-number*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上的 IPv6 IPoE 子网专线用户统计信息, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 将显示所有接口上 IPv4 IPoE 子网专线用户已经上线和正在上线的统计信息。

slot *slot-number*: 显示指定单板上的 IPv6 IPoE 子网专线用户统计信息, *slot-number* 表示 **slot** *slot-number*: 显示指定成员设备上的 IPv6 IPoE 子网专线用户统计信息, *slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数, 将显示所有成员设备上的 IPv6 IPoE 子网专线用户统计信息。

【举例】

显示接口 GigabitEthernet1/0/1 上的 IPv6 IPoE 子网专线用户统计信息。

```
<Sysname> display ipv6 subscriber subnet-leased statistics interface gigabitethernet 1/0/1
Total                : 100
Init                 : 0
Authenticating       : 20
Authenticate fail    : 0
Authenticate pass    : 20
Assigned IP          : 10
Online               : 50
Backup               : 0
```

表1-16 display ipv6 subscriber subnet-leased statistics 命令显示信息描述表

字段	描述
Total	接入的总用户数
Init	处于初始状态的用户数
Authenticating	处于正在认证状态的用户数
Authenticate fail	处于认证失败状态的用户数
Authenticate pass	处于认证成功状态的用户数
Assigned IP	处于成功分配到IP地址状态的用户数
Online	处于在线状态的用户数

字段	描述
Backup	处于备份状态的用户数

1.2.8 ipv6 subscriber 8021p

ipv6 subscriber 8021p 命令用来配置 IPv6 接入用户的 IP 报文的内/外层 VLAN tag 中的 802.1p 值与认证域的映射关系。

undo ipv6 subscriber 8021p 命令用来删除指定 802.1p 值与认证域的映射关系。

【命令】

ipv6 subscriber 8021p 8021p-list domain domain-name

undo ipv6 subscriber 8021p 8021p-list

【缺省情况】

未配置 IPv6 接入用户的 IP 报文的内/外层 VLAN tag 中的 802.1p 值与认证域的映射关系。

【视图】

三层以太网子接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

8021p-list: 802.1p 值列表，表示一个或多个 802.1p 值，表示方式为 **8021p-list = { 8021p-value [to 8021p-value] }&<1-8>**，其中，**8021p-value** 为指定 **8021p** 的编号，取值范围为 0~7。**&<1-8>**表示前面的参数最多可以输入 8 次。

domain domain-name: 表示与指定的 **8021p** 范围相关联的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。

【使用指导】

本命令用来配置指定 802.1p 值范围内的 IPv6 接入用户（包括 IPv6 未知源 IP 接入用户、静态 IPv6 IPoE 接入用户和 IPv6 IPoE 子网/接口专线用户）认证时使用的认证域，通过指定的认证域进行认证授权。

【举例】

在子接口 GigabitEthernet 1/0/1.100 上配置内层 VLAN TAG 中 802.1p 值范围为 2 到 5 的 IPv6 接入用户认证使用的认证域为 1pdm。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1.100
```

```
[Sysname-GigabitEthernet1/0/1.100] ipv6 subscriber service-identify 8021p second-vlan
```

```
[Sysname-GigabitEthernet1/0/1.100] ipv6 subscriber 8021p 2 to 5 domain 1pdm
```

【相关命令】

- **ipv6 subscriber service-identify**

1.2.9 ipv6 subscriber access-user log enable

ipv6 subscriber access-user log enable 命令用来开启 IPv6 IPoE 接入用户日志信息功能。

undo ipv6 subscriber access-user log enable 命令用来关闭 IPv6 IPoE 接入用户日志信息功能。

【命令】

ipv6 subscriber access-user log enable [successful-login | failed-login | logout [normal] [abnormal]] *

undo ipv6 subscriber access-user log enable [successful-login | failed-login | logout [normal] [abnormal]] *

【缺省情况】

IPv6 IPoE 接入用户日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

successful-login: 表示 IPv6 IPoE 接入用户上线成功日志功能。

failed-login: 表示 IPv6 IPoE 接入用户上线失败日志功能。

logout: 表示 IPv6 IPoE 接用户下线日志功能。

normal: 表示 IPv6 IPoE 接用户正常下线日志功能。

abnormal: 表示 IPv6 IPoE 接用户异常下线日志功能。

【使用指导】



注意

为了防止设备输出过多的 IPv6 IPoE 日志信息，一般情况下建议不要开启此功能。

IPv6 IPoE 接入用户日志是为了满足网络管理员维护的需要，对用户的上线成功、上线失败、正常下线和异常下线的信息进行记录，包括用户名、IPv6 地址、接口名称、两层 VLAN、MAC 地址、上线失败原因、下线原因等。设备生成的 IPv6 IPoE 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

配置本命令时，如果未指定任何参数，将同时开启用户的上线成功、上线失败、正常下线和异常下线日志功能。

通过 **undo** 命令关闭日志功能时，如果未指定任何参数，将同时关闭用户的上线成功、上线失败、正常下线和异常下线日志功能。

【举例】

```
# 开启 IPv6 IPoE 接入用户日志信息功能。
<Sysname> system-view
[Sysname] ipv6 subscriber access-user log enable
```

1.2.10 ipv6 subscriber dhcp domain

ipv6 subscriber dhcp domain 命令用来配置 IPv6 DHCP 个人接入用户使用的认证域。
undo ipv6 subscriber dhcp domain 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber dhcp domain domain-name
undo ipv6 subscriber dhcp domain
```

【缺省情况】

IPv6 DHCP 个人接入用户的认证域为缺省认证域。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

domain-name: 指定认证使用的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括“/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>”以及“@”字符。

【使用指导】

本命令用来配置 DHCPv6 报文触发接入的 IPv6 DHCP 个人接入用户在认证时使用的域名，该域名必须在接入设备上存在且配置完整。

配置 **ipv6 subscriber dhcp domain** 命令后，如果用户报文中携带 Option 16，Option 16 内容符合域名的格式要求，并且接口配置了 **ipv6 subscriber trust option16** 命令，则 IPoE 接入用户使用 Option 16 作为指定的认证域进行认证；否则，使用本命令指定的认证域。

如果不配置 **ipv6 subscriber dhcp domain** 命令，且 DHCPv6 报文中未携带 Option 16，则使用缺省认证域认证。

当用户需要将 Option 16 字段中的信息按字符串形式解析时，请确保 Option 16 字段内容中不出现字符串结束字符和不可见字符，否则在生成域名时将产生异常。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 上 IPv6 DHCP 个人接入用户使用的认证域为 ipoe。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dhcp domain ipoe
```

【相关命令】

- **ipv6 subscriber dhcp username**

- **ipv6 subscriber initiator dhcp enable**
- **ipv6 subscriber trust**

1.2.11 ipv6 subscriber dhcp max-session

ipv6 subscriber dhcp max-session 命令用来配置接口上允许 DHCPv6 报文触发创建的 IPv6 IPoE 会话的最大数目。

undo ipv6 subscriber dhcp max-session 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber dhcp max-session max-number
undo ipv6 subscriber dhcp max-session
```

【缺省情况】

未配置接口上允许 DHCPv6 报文触发创建的 IPv6 IPoE 会话的最大数目。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

max-number: 允许 DHCPv6 触发创建的 IPv6 IPoE 会话的最大数目，取值范围为 1~64000。

【使用指导】

DHCPv6 报文触发创建的 IPv6 IPoE 会话数目达到最大值后，后续 DHCPv6 报文不能触发创建 IPv6 IPoE 会话。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 上允许 DHCPv6 报文触发创建的 IPv6 IPoE 会话的最大数目为 100。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dhcp max-session 100
```

【相关命令】

- **display ipv6 subscriber session**
- **ipv6 subscriber initiator dhcp enable**
- **reset ipv6 subscriber session**

1.2.12 ipv6 subscriber dhcp password option16

ipv6 subscriber dhcp password option16 命令用来配置 IPv6 DHCP 个人接入用户使用 DHCPv6 报文中的 Option 16 作为认证密码。

undo ipv6 subscriber dhcp password option16 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber dhcp password option16 [ offset offset ] [ length length ]  
undo ipv6 subscriber dhcp password option16
```

【缺省情况】

IPv6 DHCP 个人接入用户未使用 DHCPv6 报文中的 Option 16 作为认证密码。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

offset offset: 表示从 Option 16 首部偏移指定字节后的内容作为认证密码, *offset* 表示字节偏移量, 取值范围为 1~63, 单位为字节。如果未指定本参数, 将从 Option 16 中起始处后的内容作为认证密码。

length length: 表示从 Option 16 首部偏移 *offset* 所处的位置开始, 取指定长度的字节作为认证密码, *length* 表示获取字节的长度, 取值范围为 1~63, 单位为字节。如果未指定本参数, 将从 Option 16 首部偏移 *offset* 所处的位置开始取剩余的所有内容作为认证密码。

【使用指导】

IPv6 DHCP 个人接入用户支持通过多种方式获取认证密码, 并按如下优先顺序选择第一个可用的认证密码进行认证:

- 同时满足如下条件时, 使用本命令配置方式获取的密码作为认证密码:
 - 接口上配置了 **ipv6 subscriber dhcp password option16** 命令;
 - 接口上配置了 **ipv6 subscriber trust option16** 命令并且 DHCPv6 报文中携带的 Option 16 中内容符合可见字符的格式要求。
- 使用 **ipv6 subscriber password** 命令配置的密码作为认证密码。
- 使用缺省字符串 **vlan** 作为认证密码。

ipv6 subscriber dhcp password option16 命令用来配置 IPv6 DHCP 用户在认证时使用的密码, 该密码必须与认证服务器上配置的密码保持一致。

当用户需要将 Option 16 字段中的信息作为认证密码时, 请确保 Option 16 字段内容中不出现字符串结束字符和不可见字符, 否则在生成用户密码时将产生异常。

【举例】

配置接口 GigabitEthernet1/0/1 上的 IPv6 DHCP 个人接入用户使用从 Option 16 首部偏移 10 个字节后的 20 个字节内容作为认证密码。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dhcp password option16 offset 10 length 20
```

【相关命令】

- **ipv6 subscriber initiator dhcp enable**

- **ipv6 subscriber password**
- **ipv6 subscriber trust**
- **ipv6 subscriber dhcp username**

1.2.13 ipv6 subscriber dhcp username

ipv6 subscriber dhcp username 命令用来配置 IPv6 DHCP 个人接入用户的认证用户名的命名规则。

undo ipv6 subscriber dhcp username 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber dhcp username include { circuit-id [ separator separator ]
| client-id [ separator separator ] | nas-port-id [ separator separator ] |
port [ separator separator ] | remote-id [ separator separator ] | second-vlan
[ separator separator ] | slot [ separator separator ] | source-mac
[ address-separator address-separator ] [ separator separator ] | subslot
[ separator separator ] | sysname [ separator separator ] | vendor-class
[ separator separator ] | vendor-specific [ separator separator ] | vlan
[ separator separator ] } *
undo ipv6 subscriber dhcp username
```

【缺省情况】

IPv6 DHCP 个人接入用户使用报文源 MAC 地址作为认证用户名。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

circuit-id: 表示以 IPv6 DHCP 报文中的 Option18 字段中的信息为用户名。

client-id: 表示以 IPv6 DHCP 报文中的 Option1 字段中的信息作为用户名。

nas-port-id: 表示以用户认证报文中的 NAS-PORT-ID 属性作为用户名。

port: 表示以用户接入的端口号作为用户名。

remote-id: 表示以 IPv6 DHCP 报文中的 Option37 字段中的信息作为用户名。

second-vlan: 表示以认证报文中的内层 VLAN 作为用户名。

slot: 表示以用户接入的槽位号作为用户名。

source-mac: 表示以用户报文的源 MAC 地址作为用户名。

address-separator address-separator: MAC 地址分隔符，可以为任意可配置的可见字符。若指定了分隔符，例如“-”，则用户名形如 xxxx-xxxx-xxxx；若不指定该参数，则用户名为 xxxxxxxxxxxx 形式。建议不要使用@作为分隔符，避免携带@字符的用户名在 AAA 服务器端不能被正确解析。

subslot: 表示以用户接入的子卡号作为用户名。

sysname: 表示以用户接入设备的设备名作为用户名。

vendor-class: 表示以 IPv6 DHCP 报文中的 Option16 字段中的信息作为用户名。

vendor-specific: 表示以 IPv6 DHCP 报文中的 Option17 字段中的信息作为用户名。

vlan: 表示以认证报文中的外层 VLAN 作为用户名。

separator separator: 当前字段分隔符，用在当前字段后面以连接后面的一个字段，可以为任意可配置的可见字符。建议不要使用@作为分隔符，避免携带@字符的用户名在 AAA 服务器端不能被正确解析。

【使用指导】

该命令用来配置 IPv6 DHCP 接入用户在认证时使用的用户名的命名规则，根据该命名规则获取的用户名必须与认证服务器上配置的用户名保持一致。此类用户进行 IPoE 认证时使用的密码由 **ipv6 subscriber password** 命令配置。

在允许的用户名类型范围内，该命令支持任意形式、任意顺序的用户名组合。例如：若配置 **ipv6 subscriber dhcp username include vendor-class vendor-specific**，则用户名为 Option16 字段内容和 Option17 字段内容的拼接，且两个字段之间无分隔符。

为保证设备对 Option 字段中的信息进行正确解析，请确保 Option 字段内容中不出现字符串结束符和不可见字符，否则可能生成错误的用户名。

【举例】

配置接口 GigabitEthernet1/0/1 上 IPv6 DHCP 个人接入用户使用 Client Identifier Option 字段中的信息作为用户名。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dhcp username include client-id
```

配置接口 GigabitEthernet1/0/1 上 IPv6 DHCP 个人接入用户使用接入设备的设备名、接入的槽位号、接入的子卡号、接入的端口号和认证报文中的外层 VLAN 信息作为用户名，所选用的字段之间均使用#作为分隔符。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dhcp username include sysname separator # slot separator # subslot separator # port separator # vlan
```

【相关命令】

- **ipv6 subscriber initiator dhcp enable**
- **ipv6 subscriber password**

1.2.14 ipv6 subscriber dscp

ipv6 subscriber dscp 命令用来配置 IPv6 接入用户的 IP 报文的 DSCP 值与用户认证域的映射关系。

undo ipv6 subscriber dscp 命令用来删除指定 DSCP 值与用户认证域的映射关系。

【命令】

```
ipv6 subscriber dscp dscp-value-list domain domain-name
```

undo ipv6 subscriber dscp dscp-value-list

【缺省情况】

未配置 IPv6 接入用户的 IP 报文的 DSCP 值与认证域的映射关系。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value-list: DSCP 值列表, 表示一个或多个 DSCP 的值, 表示方式为 **dscp-value-list** = { **dscp-value** [**to dscp-value**] } <1-8>。其中, **dscp-value** 为指定的 DSCP 的值, 取值范围为 0~63。<1-8> 表示前面的参数最多可以输入 8 次。

domain domain-name: 表示与指定的 DSCP 范围相关联的 ISP 域名, 为 1~255 个字符的字符串, 不区分大小写, 不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。

【使用指导】

本命令用来配置指定 DSCP 范围内的 IPv6 接入用户(包括 IPv6 未知源 IP 接入用户、静态 IPv6 IPoE 接入用户和 IPv6 IPoE 子网/接口专线用户)认证时使用的认证域, 通过指定的认证域进行认证授权。

【举例】

在接口 GigabitEthernet1/0/1 上配置 DSCP 值范围为 1 到 4 的 IPv6 接入用户认证使用的认证域为 dscpdm。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber service-identify dscp
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber dscp 1 to 4 domain dscpdm
```

【相关命令】

- **ipv6 subscriber service-identify**

1.2.15 ipv6 subscriber enable

ipv6 subscriber enable 命令用来在接口上开启 IPv6 IPoE 功能并指定用户的接入模式。

undo ipv6 subscriber enable 命令用来关闭接口上的 IPv6 IPoE 功能。

【命令】

ipv6 subscriber { l2-connected | routed } enable

undo ipv6 subscriber { l2-connected | routed } enable

【缺省情况】

接口上的 IPv6 IPoE 功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

l2-connected: 指定二层接入模式，表示此接口上用户通过二层网络接入。

routed: 指定三层接入模式，表示此接口上用户通过三层网络接入。

【使用指导】

只有在接口上开启了 IPv6 IPoE 功能后，其它的 IPv6 IPoE 相关配置才能生效。

不能通过重复执行本命令修改 IPoE 的接入模式。如需修改 IPoE 的接入模式，请先通过 **undo ipv6 subscriber enable** 命令关闭 IPoE 功能，再执行 **ipv6 subscriber enable** 命令。

在聚合接口视图下开启 IPv6 IPoE 功能时，必须同时通过 **service** 命令指定聚合接口下流量的业务处理板；否则会产生无法统计用户流量的现象。有关 **service** 命令的详细介绍请参见“二层技术-以太网交换命令参考”中的“以太网链路聚合”。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上开启二层接入模式的 IPv6 IPoE 功能。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber l2-connected enable
```

【相关命令】

- **service**（二层技术-以太网交换命令参考/以太网链路聚合）

1.2.16 ipv6 subscriber initiator dhcp enable

ipv6 subscriber initiator dhcp enable 命令用来在接口上开启 DHCPv6 报文触发生成 IPv6 IPoE 会话的功能。

undo ipv6 subscriber initiator dhcp enable 命令用来关闭接口上 DHCPv6 报文触发生成 IPv6 IPoE 会话的功能。

【命令】

```
ipv6 subscriber initiator dhcp enable  
undo ipv6 subscriber initiator dhcp enable
```

【缺省情况】

接口上 DHCPv6 报文触发生成 IPv6 IPoE 会话的功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

接口上开启该功能后，收到的首个 DHCP Solicit 报文或直接申请地址的 DHCP Request 报文会触发生成 IPv6 IPoE 会话；关闭该功能后，该接口上收到的 DHCPv6 报文不能触发生成 IPv6 IPoE 会话，已有的由 DHCPv6 报文触发生成的 IPv6 IPoE 会话不会被删除。

接口上可同时配置 DHCPv6 报文、IPv6 ND RS 和未知源 IPv6 报文触发生成 IPv6 IPoE 会话的功能。

【举例】

在接口 GigabitEthernet1/0/1 上开启 DHCPv6 报文触发生成 IPv6 IPoE 会话的功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber initiator dhcp enable
```

【相关命令】

- **display ipv6 subscriber session**
- **ipv6 subscriber enable**
- **ipv6 subscriber initiator ndrs enable**
- **ipv6 subscriber initiator unclassified-ip enable**
- **reset ipv6 subscriber session**

1.2.17 ipv6 subscriber initiator ndrs enable

ipv6 subscriber initiator ndrs enable 命令用来在接口上开启 IPv6 ND RS 报文触发生成 IPv6 IPoE 会话的功能。

undo ipv6 subscriber initiator ndrs enable 命令用来关闭接口上 IPv6 ND RS 报文触发生成 IPv6 IPoE 会话的功能。

【命令】

```
ipv6 subscriber initiator ndrs enable
undo ipv6 subscriber initiator ndrs enable
```

【缺省情况】

接口上 IPv6 ND RS 报文触发生成 IPv6 IPoE 会话的功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

接口上开启该功能后，收到的首个 IPv6 ND RS 报文会触发生成 IPv6 IPoE 会话；关闭该功能后，该接口上收到的 IPv6 ND RS 报文不能触发生成 IPv6 IPoE 会话，已有的由 IPv6 ND RS 报文触发生成的 IPv6 IPoE 会话不会被删除。

接口上可同时配置 DHCPv6 报文、IPv6 ND RS 和未知源 IPv6 报文触发生成 IPv6 IPoE 会话的功能。

【举例】

在接口 GigabitEthernet1/0/1 上开启 IPv6 ND RS 报文触发生成 IPv6 IPoE 会话的功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber initiator ndrs enable
```

【相关命令】

- **display ipv6 subscriber session**
- **ipv6 subscriber enable**
- **ipv6 subscriber initiator dhcp enable**
- **ipv6 subscriber initiator unclassified-ip enable**
- **reset ipv6 subscriber session**

1.2.18 ipv6 subscriber initiator unclassified-ip enable

ipv6 subscriber initiator unclassified-ip enable 命令用来在接口上开启未知源 IPv6 报文触发生成 IPv6 IPoE 会话的功能。

undo ipv6 subscriber initiator unclassified-ip enable 命令用来关闭接口上的未知源 IPv6 报文触发生成 IPv6 IPoE 会话的功能。

【命令】

```
ipv6 subscriber initiator unclassified-ip enable
undo ipv6 subscriber initiator unclassified-ip enable
```

【缺省情况】

接口上的未知源 IPv6 报文触发生成 IPv6 IPoE 会话的功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

接口开启该功能后，收到的未知源 IPv6 报文会触发生成 IPv6 IPoE 会话；关闭该功能后，该接口上收到的未知源 IPv6 报文不能触发生成 IPv6 IPoE 会话，已有的由未知源 IPv6 报文触发生成的 IPv6 IPoE 会话不会被删除。

接口上可同时配置 DHCPv6 报文、IPv6 ND RS 和未知源 IPv6 报文触发生成 IPv6 IPoE 会话的功能。

【举例】

在接口 GigabitEthernet1/0/1 上开启未知源 IPv6 报文触发生成 IPv6 IPoE 会话的功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber initiator unclassified-ip enable
```

【相关命令】

- **display ipv6 subscriber session**
- **ipv6 subscriber enable**
- **ipv6 subscriber initiator dhcp enable**
- **ipv6 subscriber initiator ndrs enable**
- **reset ipv6 subscriber session**

1.2.19 ipv6 subscriber interface-leased

ipv6 subscriber interface-leased 命令用来配置 IPv6 接口专线用户。

undo ipv6 subscriber interface-leased 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber interface-leased username name password { ciphertext | plaintext } string [ domain domain-name ]  
undo ipv6 subscriber interface-leased
```

【缺省情况】

未配置 IPv6 接口专线用户。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

username *name*: 指定用户认证时使用的用户名，其中 *name* 为 1~255 个字符的字符串，区分大小写。

password: 指定用户认证时使用的密码。

ciphertext: 以密文方式设置密码。

plaintext: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串。

domain *domain-name*: 指定认证使用的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符，如果未配置该参数，将使用缺省认证域来认证用户。关于缺省认证域的相关配置请参见“安全配置指导”中的“AAA”。

【使用指导】

一个 IPv6 IPoE 接口专线用户代表了该接口接入的所有 IPv6 用户，接口上接入的所有 IPv6 用户统一认证、授权和计费。该 IPoE 专线用户认证成功后，接口上接入的所有 IPv6 用户流量均允许通过，且共享一个 IPv6 IPoE 会话，并基于接口进行授权和计费。

每个接口只能配置一个 IPv6 IPoE 接口专线用户，并且不能通过重复执行本命令修改已配置的 IPv6 IPoE 接口专线用户的 **username**、**password** 或 **domain** 参数。如需修改这些参数，请先通过 **undo ipv6 subscriber interface-leased** 命令删除已配置的 IPv6 IPoE 接口专线用户，再执行 **ipv6 subscriber interface-leased** 命令。

同一接口下，IPoE 个人接入用户、IPoE 接口专线用户和 IPoE 子网专线用户的配置互斥，只能选择其中的一种配置。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上配置一个 IPv6 IPoE 接口专线用户：认证使用的用户名为 intuser，
认证使用的密码为明文 pw123。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber interface-leased username intuser password
plaintext pw123
```

【相关命令】

- **display ipv6 subscriber interface-leased**

1.2.20 ipv6 subscriber nas-port-id format

ipv6 subscriber nas-port-id format 命令用来配置 IPv6 IPoE 接入用户进行认证时，接入设备向 RADIUS 服务器发送的 NAS-PORT-ID 属性的封装格式。

undo ipv6 subscriber nas-port-id format 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber nas-port-id format cn-telecom { version1.0 | version2.0 }
undo ipv6 subscriber nas-port-id format
```

【缺省情况】

按 version 1.0 的格式要求填充发往 RADIUS 服务器的 NAS-PORT-ID 属性内容。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

version1.0：填充格式为 version 1.0，表示发送给 RADIUS 服务器的 NAS-PORT-ID 属性以电信 163 大后台要求的格式填充。不同接口类型的封装内容形式有所不同，具体请参见 表 1-17。其中，封装内容中各参数的含义为：

- **slot_num**：表示 BRAS 接入接口的槽位号。
- **subslot_num**：表示 BRAS 接入接口的子槽位号。
- **port_num**：表示 BRAS 接入接口的端口号。
- **vlan_id**：表示接入用户的 VLAN ID。

- *inner-vlan*: 表示接入用户的内层 VLAN ID。
- *outer-vlan*: 表示接入用户的外层 VLAN ID。
- *vpi*: 表示 BRAS 接入接口的 VPI。
- *vci*: 表示 BRAS 接入接口的 VCI。

表1-17 version 1.0 封装格式

接口类型	封装内容形式
三层以太网接口和三层聚合接口	slot=s lot_num;subslot=subs lot_num;port=port_num;vlanid=0
三层以太网子接口和三层聚合子接口（携带单层 VLAN Tag接入）	slot=s lot_num;subslot=subs lot_num;port=port_num;vlanid=vlan_id
三层以太网子接口和三层聚合子接口（携带双层 VLAN Tag接入）	slot=s lot_num;subslot=subs lot_num;port=port_num;vlanid=inner-vlan;vlanid2=outer-vlan
基于ATM链路的三层虚拟以太网接口(IPoEoA接入)	slot=s lot_num;subslot=subs lot_num;port=port_num;vpi=vpi;vci=vci

version2.0: 填充格式为version 2.0，表示发送给RADIUS服务器的NAS-PORT-ID属性以YDT 2275-2011 宽带接入用户线路（端口）标识要求的格式填充。version 2.0 封装格式的内容形式为：
{eth|trunk|atm} NAS_slot/NAS_subslot/NAS_port:svlan.cvlan
AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port。其中，各字段的含义请参见 表 1-18:

表1-18 version 2.0 封装格式

字段	描述
{eth trunk atm}	表示BRAS接入接口的类型，包括以太接口、trunk类型的以太网接口或ATM接口
NAS_slot	表示BRAS接入接口的槽位号
NAS_subslot	表示BRAS接入接口的子槽位号
NAS_port	表示BRAS接入接口的端口号
svlan	表示接入用户的SVLAN ID
cvlan	表示接入用户的CVLAN ID
AccessNodeIdentifier	表示接入节点的标识
ANI_rack	表示接入节点机架号
ANI_frame	表示接入节点机框号
ANI_slot	表示接入节点槽位号
ANI_subslot	表示接入节点子槽位号
ANI_port	表示接入节点端口号

【举例】

在接口 GigabitEthernet1/0/1 上配置设备使用 RADIUS 的 NAS-PORT-ID 属性封装格式为 version 2.0。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber nas-port-id format cn-telecom version2.0
```

【相关命令】

- **ipv6 subscriber initiator dhcp enable**
- **ipv6 subscriber trust**
- **ipv6 subscriber nas-port-id nasinfo-insert**

1.2.21 ipv6 subscriber nas-port-id nasinfo-insert

ipv6 subscriber nas-port-id nasinfo-insert 命令用来配置设备提取出 DHCPv6 报文的 Option 18 内容并和 NAS 信息一起作为 NAS-PORT-ID 属性字符串。

undo ipv6 subscriber nas-port-id nasinfo-insert 命令用来恢复缺省情况。

【命令】

ipv6 subscriber nas-port-id nasinfo-insert

undo ipv6 subscriber nas-port-id nasinfo-insert

【缺省情况】

如果收到的 DHCPv6 报文带有 Option18 选项，则直接使用该内容作为 NAS-PORT-ID 属性字符串。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

在 DHCP 中继组网环境下，接入设备能捕获用户的 DHCPv6 报文，并从报文中提取出 DHCPv6 Option18 选项信息。在配置了 NAS-PORT-ID 属性封装格式为 version 2.0 且信任 DHCP Option 18 的情况下，如果配置了本命令，则接入设备处理如下：

- 如果收到的 DHCPv6 报文带有 Option18，则从收到的 DHCPv6 报文中解析 Option18，并按 version 2.0 格式要求将提取出的 DHCPv6 报文的 Option 18 内容和 NAS 信息一起作为 RADIUS 的 NAS-PORT-ID 属性内容。
- 如果收到的 DHCPv6 报文不带 Option18，则按 version 2.0 格式要求封装，填充 NAS-PORT-ID 属性中的 NAS 信息字段（NAS_slot/NAS_subslot/NAS_port:svlan.cvlan），并将 AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port 部分修改为 0/0/0/0/0/0。

本功能对原 DHCPv6 报文中 Option18 选项不产生任何影响。

【举例】

在接口 GigabitEthernet1/0/1 上配置设备使用 DHCPv6 客户端上报的 Option18 信息，并在其中插入 NAS 信息，然后将其封装为 RADIUS 的 NAS-PORT-ID 属性。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber nas-port-id format cn-telecom version2.0
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber trust option18
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber nas-port-id nasinfo-insert
```

【相关命令】

- **ipv6 subscriber initiator dhcp enable**
- **ipv6 subscriber trust**
- **ipv6 subscriber nas-port-id format**

1.2.22 ipv6 subscriber nas-port-type

ipv6 subscriber nas-port-type 命令用来配置接口的 IPv6 IPoE 接入端口类型。

undo ipv6 subscriber nas-port-type 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber nas-port-type { 802.11 | adsl-cap | adsl-dmt | async | cable |
ethernet | g.3-fax | hdlc | idsl | isdn-async-v110 | isdn-async-v120 |
isdn-sync | piafs | sdsl | sync | virtual | wireless-other | x.25 | x.75 | xdsl }
undo ipv6 subscriber nas-port-type
```

【缺省情况】

IPv6 IPoE 接入端口类型为 Ethernet 类型。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

802.11: 符合 Wireless-IEEE 802.11 标准的接口类型，对应的编码值为 19。

adsl-cap: ADSL-CAP (Asymmetric DSL, Carrierless Amplitude Phase Modulation) 接口类型，对应的编码值为 12。

adsl-dmt: ADSL-DMT (Asymmetric DSL, Discrete Multi-Tone) 接口类型，对应的编码值为 13。

async: Async 接口类型，对应的编码值为 0。

cable: Cable 接口类型，对应的编码值为 17。

ethernet: Ethernet 接口类型，对应的编码值为 15。

g.3-fax: G.3 Fax 接口类型，对应的编码值为 10。

hdlc: HDLC 接口类型，对应的编码值为 7。

idsl: IDSL (ISDN Digital Subscriber Line) 接口类型, 对应的编码值为 14。

isdn-async-v110: ISDN Async V.110 接口类型, 对应的编码值为 4。

isdn-async-v120: ISDN Async V.120 接口类型, 对应的编码值为 3。

isdn-sync: ISDN Sync 口类型, 对应的编码值为 2。

piafs: 符合 PIAFS (PHS (Personal Handyphone System) Internet Access Forum Standard) 标准的接口类型, 对应的编码值为 6。

sdsl: SDSL (Symmetric DSL) 接口类型, 对应的编码值为 11。

sync: Sync 接口类型, 对应的编码值为 1。

virtual: Virtual 接口类型, 对应的编码值为 5。

wireless-other: Wireless-other 接口类型, 对应的编码值为 18。

x.25: X.25 接口类型, 对应的编码值为 8。

x.75: X.75 接口类型, 对应的编码值为 9。

xdsl: XDSL (Digital Subscriber Line of unknown type) 接口类型, 对应的编码值为 16。

【使用指导】

此处配置的端口接入类型值将作为向 RADIUS 服务器发送的 RADIUS 请求报文的 NAS-Port-Type 属性值, 用于向 RADIUS 服务器正确传递用户的接入端口信息。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 的 IPv6 IPoE 接入端口类型为 SDSL。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber nas-port-type dsdl
```

1.2.23 ipv6 subscriber ndrs domain

ipv6 subscriber ndrs domain 命令用来配置 IPv6 ND RS 个人接入用户使用的认证域。

undo ipv6 subscriber ndrs domain 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber ndrs domain domain-name
undo ipv6 subscriber ndrs domain
```

【缺省情况】

IPv6 ND RS 个人接入用户使用缺省认证域作为认证域。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

domain-name: 指定认证使用的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括“/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>”以及“@”字符。

【使用指导】

本命令用来配置 IPv6 ND RS 报文触发接入的 IPv6 IPoE 接入用户在认证时使用的域名，该域名必须与认证服务器上配置的域名保持一致。

配置 **ipv6 subscriber ndrs domain** 命令后，对于 IPv6 ND RS 报文触发认证的 IPoE 接入用户使用本命令指定的域名进行认证，否则使用缺省认证域认证。

【举例】

配置接口 GigabitEthernet1/0/1 上 IPv6 ND RS 接入用户使用的认证域为 ipoe。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber ndrs domain ipoe
```

【相关命令】

ipv6 subscriber initiator ndrs enable

1.2.24 ipv6 subscriber ndrs max-session

ipv6 subscriber ndrs max-session 命令用来配置接口上允许 RS 报文触发创建的 IPv6 IPoE 会话的最大数目。

undo ipv6 subscriber ndrs max-session 命令用来恢复缺省情况。

【命令】

ipv6 subscriber ndrs max-session max-number

undo ipv6 subscriber ndrs max-session

【缺省情况】

未配置接口上允许创建的 IPv6 IPoE 会话的最大数目

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

max-number: 允许 RS 触发创建的 IPv6 IPoE 会话的最大数目，取值范围为 1~64000。

【使用指导】

RS 报文触发创建的 IPv6 IPoE 会话数目达到最大值后，后续 RS 报文不能触发创建 IPv6 IPoE 会话，DHCPv6 报文、未知源 IPv6 报文等触发创建 IPv6 IPoE 会话不会受此最大值限制。

【举例】

配置接口 GigabitEthernet1/0/1 上允许 RS 报文触发创建的 IPv6 IPoE 会话的最大数目为 100。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber ndrs max-session 100
```

【相关命令】

```
display ipv6 subscriber session
ipv6 subscriber initiator ndrs enable
reset ipv6 subscriber session
```

1.2.25 ipv6 subscriber ndrs username

ipv6 subscriber ndrs username 命令用来配置 IPv6 ND RS 接入用户的认证用户名的命名规则。

undo ipv6 subscriber ndrs username 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber ndrs username include { nas-port-id [ separator separator ]
| port [ separator separator ] | second-vlan [ separator separator ] | slot
[ separator separator ] | source-mac [ address-separator address-separator ]
[ separator separator ] | subslot [ separator separator ] | sysname
[ separator separator ] | vlan [ separator separator ] } *
undo ipv6 subscriber ndrs username
```

【缺省情况】

IPv6 ND RS 接入用户采用用户报文的源 MAC 地址作为认证用户名。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

nas-port-id: 表示使用用户的 NAS-PORT-ID 属性作为用户名。

port: 表示以用户接入的端口号作为用户名。

second-vlan: 表示以认证报文中的内层 VLAN 作为用户名。

slot: 表示以用户接入的槽位号作为用户名。

source-mac: 表示使用用户报文的源 MAC 地址作为用户名。

separator separator: MAC 地址分隔符，可以为任意可配置的可见字符。若指定了分隔符，例如“-”，则用户名形如 xxxx-xxxx-xxxx；若不指定该参数，则用户名为 xxxxxxxxxxxx 形式。建议不要使用@作为分隔符，避免携带@字符的用户名在 AAA 服务器端不能被正确解析。

subslot: 表示以用户接入的子卡号作为用户名。

sysname: 表示以用户接入设备的设备名作为用户名。

vlan: 表示以认证报文中的外层 VLAN 作为用户名。

separator separator: 当前字段分隔符, 用在当前字段后面以连接后面的一个字段, 可以为任意可配置的可见字符。建议不要使用@作为分隔符, 避免携带@字符的用户名在 AAA 服务器端不能被正确解析。

【使用指导】

本命令用来配置 IPv6 RS 报文触发接入的 IPv6 IPoE 接入用户在认证时使用的用户名的命名规则, 根据该命名规则获取的用户名必须与认证服务器上配置的用户名保持一致。此类用户进行 IPoE 认证时使用的密码由 **ipv6 subscriber password** 命令配置。

在允许的用户名类型范围内, 该命令支持任意形式、任意顺序的用户名组合。例如: 若配置 **ipv6 subscriber ndrs username include nas-port-id source-mac**, 则用户名为 NAS-PORT-ID 属性字段和源 MAC 地址字段内容的拼接, 且两个字段之间无分隔符

【举例】

配置接口 GigabitEthernet1/0/1 上的 IPv6 ND RS 接入用户使用用户报文的源 MAC 地址作为用户名。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber ndrs username include source-mac
```

配置接口 GigabitEthernet1/0/1 上 IPv6 ND RS 接入用户使用接入设备的设备名、接入的槽位号、接入的子卡号、接入的端口号和认证报文中的外层 VLAN 信息作为用户名, 所选用的字段之间均使用#作为分隔符。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber ndrs username include sysname separator # slot separator # subslot separator # port separator # vlan
```

【相关命令】

ipv6 subscriber initiator ndrs enable

ipv6 subscriber password

1.2.26 ipv6 subscriber password

ipv6 subscriber password 命令用来配置 IPv6 IPoE 个人接入用户的认证密码。

undo ipv6 subscriber password 命令用来恢复缺省情况。

【命令】

ipv6 subscriber password { ciphertext | plaintext } string

undo ipv6 subscriber password

【缺省情况】

IPv6 IPoE 个人接入用户的认证密码为字符串 **vlan**。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ciphertext: 以密文方式设置密码。

plaintext: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串。

【使用指导】

ipv6 subscriber password 命令用来配置 IPv6 IPoE 个人接入用户(包括动态和静态 IPv6 IPoE 个人接入用户) 的认证密码，该密码必须与认证服务器上配置的密码保持一致。

其中，对于动态 IPv6 DHCP 个人接入用户支持通过多种方式获取认证密码，具体请参见 **ipv6 subscriber dhcp password option16** 命令。

【举例】

配置接口 GigabitEthernet1/0/1 上 IPv6 IPoE 个人接入用户认证时使用的密码为明文的 123。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber password plaintext 123
```

【相关命令】

- **ipv6 subscriber dhcp username**
- **ipv6 subscriber enable**
- **ipv6 subscriber unclassified-ip username**
- **ipv6 subscriber dhcp password option16**

1.2.27 ipv6 subscriber service-identify

ipv6 subscriber service-identify 命令用来配置 IPv6 接入用户的业务识别方式。

undo ipv6 subscriber service-identify 命令用来恢复缺省情况。

【命令】

三层以太网接口视图/三层聚合口视图

ipv6 subscriber service-identify dscp

undo ip subscriber service-identify

三层以太网子接口视图/三层聚合子接口视图

ipv6 subscriber service-identify { 8021p { second-vlan | vlan } | dscp | second-vlan | vlan }

undo ip subscriber service-identify

【缺省情况】

未配置 IPv6 接入用户的业务识别方式。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

8021p second-vlan: 表示 QinQ 模式下基于内层 VLAN Tag 中的 802.1p 值识别业务。

8021p vlan: 表示基于 VLAN Tag 中的 802.1p 值识别业务，QinQ 模式下基于外层 VLAN Tag 中的 802.1p 值识别业务。

dscp: 表示基于 DSCP 值识别业务。

second-vlan: QinQ 模式下基于内层 VLAN ID 识别业务。

vlan: 表示基于 VLAN ID 识别业务，QinQ 模式下基于外层 VLAN ID 识别业务。

【使用指导】

对于 IPv6 接入用户（包括 IPv6 未知源 IP 接入用户、静态 IPv6 IPoE 接入用户和 IPv6 IPoE 子网/接口专线用户）认证时使用的认证域由报文中携带的业务信息来决定。不同的业务特征可以对应不同的认证域，每一个接口可以指定仅识别某种类型业务的报文。例如，接口上若指定了基于 DSCP 值识别业务，且通过 **ipv6 subscriber dscp 1 domain aabcc** 命令指定了 DSCP 值 1 与认证域 aabcc 的映射关系，则 IPv6 报文 DSCP 值为 1 的用户认证时将会使用认证域 aabcc。

一个接口上只能指定一个业务识别方式。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 上的 IPv6 接入用户认证使用基于 DSCP 的业务识别方式
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber service-identify dscp
```

【相关命令】

- **ipv6 subscriber 8021p**
- **ipv6 subscriber dscp**
- **ipv6 subscriber vlan**

1.2.28 ipv6 subscriber session static

ipv6 subscriber session static 命令用来配置静态 IPv6 IPoE 会话。

undo ipv6 subscriber session static 命令用来删除指定的静态 IPv6 IPoE 会话。

【命令】

```
ipv6 subscriber session static ipv6 ipv6-address [ vlan vlan-id [ second-vlan vlan-id ] ] [ mac mac-address ] [ domain domain-name ] [ description string ]  
undo ipv6 subscriber session static ipv6 ipv6-address [ vlan vlan-id [ second-vlan vlan-id ] ]
```

【缺省情况】

未配置静态 IPv6 IPoE 会话。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6 *ipv6-address*: 表示用户的 IP 地址。

vlan *vlan-id*: 表示用户报文的外层 VLAN。其中 *vlan-id* 表示 VLAN ID, 取值范围为 1~4094。
本参数仅子接口支持, 非子接口不支持。

second-vlan *vlan-id*: 表示用户报文的内层 VLAN。其中 *vlan-id* 表示 VLAN ID, 取值范围为 1~4094。本参数仅子接口支持, 非子接口不支持。

mac *mac-address*: 表示用户的 MAC 地址, 形式为 H-H-H。

domain *domain-name*: 指定认证使用的 ISP 域名, 为 1~255 个字符的字符串, 不区分大小写, 不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。如果未指定该参数, 将使用缺省认证域来认证用户。关于缺省认证域的相关配置请参见“安全配置指导”中的“AAA”。

description *string*: 指定静态会话的描述信息, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。如果未指定该参数, 则静态会话无描述信息。

【使用指导】

静态 IPoE 会话的匹配优先级高于动态 IPoE 会话。若已经存在静态 IPoE 会话, 则与之匹配 IP 报文不会触发新的动态 IPoE 会话; 若存在一个未知源 IP 报文、DHCP 报文或 ND RS 报文触发建立的动态 IPoE 会话, 则再配置一个能与该未知源 IP 报文、DHCP 接入用户 IP 报文或 ND RS 接入用户 IP 报文匹配的静态 IPoE 会话, 会覆盖已经存在的动态 IPoE 会话。

当静态会话中指定的 IP 地址与 DHCP 地址池中可分配的 IP 地址存在交集时, 则: 对于 DHCPv6 地址池需要通过命令 **ipv6 dhcp server forbidden-address** 配置交集 IPv6 地址为不参与自动分配的 IPv6 地址。有关配置不参与自动分配 IP 地址命令的详细介绍, 请参见“三层技术-IP 业务命令参考”中的“DHCPv6”。

系统支持配置多个静态 IPoE 会话, 并根据命令中指定参数的不同分为如下三种情况:

- IPv6 (无外层 VLAN 和内层 VLAN) 相同的静态 IPv6 IPoE 会话;
- IPv6、外层 VLAN (无内层 VLAN) 两个参数相同的静态 IPv6 IPoE 会话;
- IPv6、外层 VLAN、内层 VLAN 三个参数相同的静态 IPv6 IPoE 会话。

上述三种情况的静态 IPv6 IPoE 会话每种情况最多只能存在一条, 并且不能通过重复执行本命令修改上述三种中已配置的 **mac** 和 **domain** 参数。如需修改 **mac** 和 **domain** 参数, 请先通过 **undo ipv6 subscriber session static** 命令删除指定静态 IPv6 会话对应的当前配置后再执行 **ipv6 subscriber session static** 命令。

同一接口下, 静态 IPoE 会话、接口专线用户和子网专线用户的配置互斥, 只能选择其中的一种配置。

【举例】

在接口 GigabitEthernet1/0/1 上配置一条静态 IPv6 IPoE 会话：用户 IPv6 地址为 2000::1，认证使用的认证域为 dm1。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber session static ipv6 2000::1 domain dm1
```

【相关命令】

- **display ipv6 subscriber session**

1.2.29 ipv6 subscriber subnet-leased

ipv6 subscriber subnet-leased 命令用来配置 IPv6 IPoE 子网专线用户。

undo ipv6 subscriber subnet-leased 命令用来删除指定的 IPv6 IPoE 子网专线用户。

【命令】

ipv6 subscriber subnet-leased ipv6 *ipv6-address* *prefix-length* *username name* *password { ciphertext | plaintext } string [domain domain-name]*

undo ipv6 subscriber subnet-leased ipv6 *ipv6-address* *prefix-length*

【缺省情况】

未配置 IPv6 IPoE 子网专线用户。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6 *ipv6-address*: 表示用户的 IPv6 地址。

prefix-length: IPv6 子网前缀长度，取值范围为 1~127。

username name: 指定用户认证时使用的用户名，其中 *name* 为 1~255 个字符的字符串，区分大小写。

password: 指定用户认证时使用的密码。

ciphertext: 以密文方式设置密码。

plaintext: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串。

domain domain-name: 指定认证使用的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符，如果未配置该参数，将使用缺省认证域来认证用户。关于缺省认证域的相关配置请参见“安全配置指导”中的“AAA”。

【使用指导】

一个 IPv6 IPoE 子网专线用户代表了该接口接入的所有该子网内 IPv6 用户，该子网内的所有 IPv6 用户统一认证、授权和计费。该 IPoE 专线用户认证成功后，接口上接入的所有该子网内 IPv6 用户流量均允许通过，且共享一个 IPv6 IPoE 会话，并基于子网进行授权和计费。

每个子网只能配置一个 IPv6 IPoE 子网专线用户。

同一接口下，IPoE 个人接入用户、IPoE 接口专线用户和 IPoE 子网专线用户的配置互斥，只能选择其中的一种配置。

【举例】

在接口 GigabitEthernet1/0/1 上配置一个 IPv6 IPoE 子网专线用户：用户 IPv6 地址和前缀为 2001:10::100/64，认证使用的用户名为 netuser，认证使用的密码为明文 pw123。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber subnet-leased ipv6 2001:10::100 64 username
netuser password plaintext pw123
```

【相关命令】

- **display ipv6 subscriber subnet-leased**

1.2.30 ipv6 subscriber timer quiet

ipv6 subscriber timer quiet 命令用来配置 IPv6 IPoE 用户的静默时间。

undo ipv6 subscriber timer quiet 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber timer quiet time
undo ipv6 subscriber timer quiet
```

【缺省情况】

IPv6 IPoE 用户的静默时间功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

time: IPoE 用户的静默时间，取值范围为 10~3600，单位为秒。

【使用指导】

本命令用来设置用户认证失败以后，设备需要等待的时间间隔。在静默期间，设备不对来自认证失败用户的报文进行认证处理，直接丢弃，可以防止该类用户报文持续发送给服务器认证而对设备性能造成影响。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。

【举例】

在接口 GigabitEthernet1/0/1 上配置 IPv6 IPoE 用户的静默时间为 100 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber timer quiet 100
```

【相关命令】

- **ipv6 subscriber initiator dhcp enable**
- **ipv6 subscriber initiator unclassified-ip enable**

1.2.31 ipv6 subscriber trust

ipv6 subscriber trust 命令用来配置信任 DHCPv6 报文中的指定 Option。

undo ipv6 subscriber trust 命令用来取消信任 DHCPv6 报文中指定的 Option。

【命令】

```
ipv6 subscriber trust { option16 | option18 | option37 }
undo ipv6 subscriber trust { option16 | option18 | option37 }
```

【缺省情况】

不信任 DHCPv6 报文中的任何 Option。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

- option16:** 表示信任 DHCPv6 报文中的 Option 16。
- option18:** 表示信任 DHCPv6 报文中的 Option18。
- option37:** 表示信任 DHCPv6 报文中的 Option37。

【使用指导】

DHCP 组网环境中，接入设备可以提取用户 DHCPv6 报文中的 Option 16 信息。如果接入设备信任 DHCPv6 报文中的 Option 16 信息，则：

- 在 Option 16 内容有效（无非法字符“/”、“\”、“|”、“””、“:”、“*”、“?”、“<”、“>”等），且没有域名分隔符@字符的情况下，IPoE 用户使用整个 Option 16 的内容作为指定的认证域进行认证。
- 在 Option 16 内容有效（无非法字符“/”、“\”、“|”、“””、“:”、“*”、“?”、“<”、“>”等），且其中包含了域名分隔符@字符的情况下，IPoE 用户使用@字符之后的字符串作为指定的认证域进行认证。如果在 Option 16 内容中包括多个@字符，则使用最后一个@字符之后的字符串作为 IPoE 用户的认证域名。

如果接入设备不信任 DHCPv6 报文中的 Option 16 信息，但是接口上配置了 **ipv6 subscriber dhcp domain** 命令，则 IPoE 用户使用该命令指定的认证域进行认证；否则，使用缺省认证域进行认证。

DHCP 中继组网环境中，接入设备可以提取用户 DHCPv6 报文中的指定 Option 信息。如果接入设备信任 DHCPv6 报文中的 Option 18，则：

- 接入设备在采用 version 2.0 格式封装 RADIUS NAS-PORT-ID 属性时，会根据 Option 18 选项内容封装发往 RADIUS 服务器的 NAS-PORT-ID 属性；
- 接入设备会根据 Option 18 选项的内容封装发往 RADIUS 服务器的 DSL_AGENT_CIRCUIT_ID 属性。

如果接入设备信任 DHCPv6 报文中的 Option 37，则接入设备会根据 Option 37 选项的内容封装发往 RADIUS 服务器的 DSL_AGENT_REMOTE_ID 属性。

【举例】

在接口 GigabitEthernet1/0/1 上配置设备信任 DHCPv6 报文中的 Option18。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber trust option18
```

【相关命令】

- **ipv6 subscriber dhcp domain**
- **ipv6 subscriber initiator dhcp enable**
- **ipv6 subscriber nas-port-id format**
- **ipv6 subscriber nas-port-id nasinfo-insert**

1.2.32 ipv6 subscriber unclassified-ip domain

ipv6 subscriber unclassified-ip domain 命令用来配置 IPv6 接入用户使用的认证域。

undo ipv6 subscriber unclassified-ip domain 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber unclassified-ip domain domain-name
undo ipv6 subscriber unclassified-ip domain
```

【缺省情况】

IPv6 接入用户的认证域为缺省认证域。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

domain-name：认证使用的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。

【使用指导】

该命令用来配置 IPv6 报文触发接入的 IPv6 接入用户（包括 IPv6 未知源 IP 接入用户、静态 IPv6 IPoE 接入用户和 IPv6 IPoE 子网/接口专线用户）在认证时使用的缺省域名，该域名必须在接入设备上存在且配置完整。

如果指定接口上配置了 **ipv6 subscriber service-identify**，则优先使用 **ipv6 subscriber service-identify** 指定的业务识别方式获取对应的认证域。只有在未匹配到 **ipv6 subscriber service-identify** 命令指定的认证域时，才使用 **ipv6 subscriber unclassified-ip domain** 命令指定的认证域。如果 **ipv6 subscriber unclassified-ip domain** 命令也未配置，则使用缺省认证域。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 上的 IPv6 接入用户使用的认证域为 ipoe。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber unclassified-ip domain ipoe
```

【相关命令】

- **ipv6 subscriber initiator unclassified-ip enable**
- **ipv6 subscriber service-identify**

1.2.33 ipv6 subscriber unclassified-ip max-session

ipv6 subscriber unclassified-ip max-session 命令用来配置接口上允许未知源 IPv6 报文触发创建的动态 IPv6 IPoE 会话的最大数目。

undo ipv6 subscriber unclassified-ip max-session 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber unclassified-ip max-session max-number
undo ipv6 subscriber unclassified-ip max-session
```

【缺省情况】

未配置接口上允许未知源 IPv6 报文创建的动态 IPv6 IPoE 会话的最大数目。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

max-number：允许未知源 IPv6 报文触发创建的 IPv6 IPoE 会话的最大数目，取值范围为 1～64000。

【使用指导】

未知源 IPv6 报文触发创建的 IPv6 IPoE 会话数目达到最大值后，后续未知源 IPv6 报文不能触发创建 IPv6 IPoE 会话。DHCPv6 报文触发创建 IPv6 IPoE 会话不会受此最大值限制。

【举例】

配置接口 GigabitEthernet1/0/1 上允许未知源 IPv6 报文触发创建的 IPv6 IPoE 会话的最大数目为 100。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber unclassified-ip max-session 100
```

【相关命令】

- **display ipv6 subscriber session**
- **ipv6 subscriber initiator unclassified-ip enable**
- **reset ipv6 subscriber session**

1.2.34 ipv6 subscriber unclassified-ip username

ipv6 subscriber unclassified-ip username 命令用来配置 IPv6 未知源 IP 接入用户和 IPv6 静态个人用户的认证用户名的命名规则。

undo ipv6 subscriber unclassified-ip username 命令用来恢复缺省情况。

【命令】

```
ipv6 subscriber unclassified-ip username include { nas-port-id [ separator  
separator ] | port [ separator separator ] | second-vlan [ separator  
separator ] | slot [ separator separator ] | source-ip [ address-separator  
address-separator ] [ separator separator ] | source-mac [ address-separator  
address-separator ] [ separator separator ] | subslot [ separator separator ]  
| sysname [ separator separator ] | vlan [ separator separator ] } *
```

```
undo ipv6 subscriber unclassified-ip username
```

【缺省情况】

IPv6 未知源 IP 接入用户和 IPv6 静态个人用户采用用户报文的源 IPv6 地址作为认证用户名。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

nas-port-id: 表示使用用户的 NAS-PORT-ID 属性作为用户名。

port: 表示以用户接入的端口号作为用户名。

second-vlan: 表示以认证报文中的内层 VLAN 作为用户名。

slot: 表示以用户接入的槽位号作为用户名。

source-ip: 表示使用用户报文的源 IPv6 地址作为用户名。

address-separator address-separator: IPv6 地址分隔符, 可以为任意可配置的可见字符。若指定了分隔符, 例如 “-”, 则用户名形如 1-2-3; 若不指定该参数, 则用户名形如 1::2:3。建议不要使用@作为分隔符, 避免携带@字符的用户名在 AAA 服务器端不能被正确解析。

source-mac: 表示使用用户报文的源 MAC 地址作为用户名。

address-separator address-separator: MAC 地址分隔符, 可以为任意可配置的可见字符。若指定了分隔符, 例如 “-”, 则用户名形如 xxxx-xxxx-xxxx; 若不指定该参数, 则用户名为 xxxxxxxxxxxx 形式。建议不要使用@作为分隔符, 避免携带@字符的用户名在 AAA 服务器端不能被正确解析。

subslot: 表示以用户接入的子卡号作为用户名。

sysname: 表示以用户接入设备的设备名作为用户名。

vlan: 表示以认证报文中的外层 VLAN 作为用户名。

separator separator: 当前字段分隔符, 用在当前字段后面以连接后面的一个字段, 可以为任意可配置的可见字符。建议不要使用@作为分隔符, 避免携带@字符的用户名在 AAA 服务器端不能被正确解析。

【使用指导】

本命令用来配置 IPv6 未知源 IP 接入用户和 IPv6 静态个人用户在认证时使用的用户名的命名规则, 根据该命名规则获取的用户名必须与认证服务器上配置的用户名保持一致。

在允许的用户名类型范围内, 该命令支持任意形式、任意顺序的用户名组合。例如: 若配置 **ipv6 subscriber unclassified-ip username include source-ip source-mac**, 则用户名为源 IPv6 地址字段和源 MAC 地址字段内容的拼接, 且两个字段之间无分隔符。

【举例】

配置接口 GigabitEthernet1/0/1 上的 IPv6 未知源 IP 接入用户和 IPv6 静态个人用户使用用户报文的源 IPv6 地址作为用户名。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber unclassified-ip username include source-ip
# 配置接口 GigabitEthernet1/0/1 上的 IPv6 未知源 IP 接入用户和 IPv6 静态个人用户使用接入设备的设备名、接入的槽位号、接入的子卡号、接入的端口号和认证报文中的外层 VLAN 信息作为用户名, 所选用的字段之间均使用#作为分隔符。
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber unclassified-ip username include sysname separator # slot separator # subslot separator # port separator # vlan
```

【相关命令】

- **ipv6 subscriber initiator unclassified-ip enable**
- **ipv6 subscriber password**

1.2.35 ipv6 subscriber user-detect

ipv6 subscriber user-detect 命令用来开启静态/动态 IPv6 IPoE 个人接入用户在线探测功能, 并配置其探测方式。

undo ipv6 subscriber user-detect 命令用来关闭静态/动态 IPv6 IPoE 个人接入用户在线探测功能。

【命令】

```
ipv6 subscriber user-detect { icmpv6 | nd } retry retries interval interval  
undo ipv6 subscriber user-detect
```

【缺省情况】

静态/动态 IPv6 IPoE 个人接入用户在线探测功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

icmpv6: 表示使用 ICMPv6 请求报文作为探测报文。

nd: 表示使用 ND 协议中的 NS 报文作为探测报文。

retry *retries*: 探测失败后允许重复尝试的最大次数，取值范围为 2~5。例如，*retries* 值为 2 表示连续三次失败就认为用户不在线。

interval *interval*: 探测的时间间隔，取值范围为 30~1200，单位为秒。

【使用指导】

接口上的静态/动态 IPv6 IPoE 个人接入用户上线后，设备会定时统计用户流量。若一个探测间隔（*interval*）内用户流量无变化，则该探测间隔结束后，设备将发送一次探测报文。如果设备在探测间隔内未收到用户的报文，则认为一次探测失败。

若设备首次探测失败，将继续做指定次数（*retries*）的重复探测，若全部探测尝试都失败（即一直未收到该用户报文），则认为此用户不在线，停止发送探测报文并删除用户；若设备在探测中收到用户的报文，则认为用户在线，重置探测定时器并开始下一次探测。

对于与接口在同一网段内的静态/动态 IPv6 IPoE 个人接入用户，可使用 IPv6 ND 协议中的 NS 或 ICMPv6 请求报文对用户进行探测；对于与接口不在同一网段内的静态/动态 IPv6 IPoE 个人接入用户，应使用 ICMPv6 请求报文对用户进行探测。

接口上不可同时启用两种方式对 IPv6 IPoE 个人接入用户进行探测。

【举例】

配置接口 GigabitEthernet1/0/1 上使用 IPv6 ND 协议中的 NS 报文对静态/动态 IPv6 IPoE 个人接入用户进行在线检测，探测失败后允许重复尝试 3 次，探测的时间间隔为 50 秒。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber user-detect nd retry 3 interval 50
```

【相关命令】

- **ipv6 subscriber enable**

1.2.36 ipv6 subscriber vlan

ipv6 subscriber vlan 命令用来配置 IPv6 接入用户的 IP 报文的内/外层 VLAN 值与认证域的映射关系。

undo ipv6 subscriber vlan 命令用来删除指定内/外层 VLAN 值与认证域的映射关系。

【命令】

```
ipv6 subscriber vlan vlan-list domain domain-name  
undo ipv6 subscriber vlan vlan-list
```

【缺省情况】

未配置 IPv6 接入用户的 IP 报文的内/外层 VLAN 与认证域的映射关系。

【视图】

三层以太网子接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

vlan-list: VLAN 列表，表示一个或多个 VLAN，表示方式为 **vlan-list = { vlan-id [to vlan-id] }** &<1-10>，其中，**vlan-id** 为指定 VLAN 的编号，取值范围为 1~4094。&<1-10> 表示前面的参数最多可以输入 10 次。

domain domain-name: 表示与指定的 VLAN 范围相关联的 ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。

【使用指导】

本命令用来配置指定 VLAN 范围内 IPv6 接入用户（包括 IPv6 未知源 IP 接入用户、静态 IPv6 IPoE 接入用户和 IPv6 IPoE 子网/接口专线用户）进行认证时使用的认证域，通过指定的认证域进行认证授权。

【举例】

在子接口 GigabitEthernet 1/1.100 上配置内层 VLAN ID 范围为 2 到 100 的 IPv6 接入用户认证使用的认证域为 vlandm。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1.100  
[Sysname-GigabitEthernet1/0/1.100] ipv6 subscriber service-identify second-vlan  
[Sysname-GigabitEthernet1/0/1.100] ipv6 subscriber vlan 2 to 100 domain vlandm
```

【相关命令】

- **ipv6 subscriber service-identify**

1.2.37 ipv6 subscriber whitelist enable

ipv6 subscriber whitelist enable 命令用来开启 IPv6 IPoE 白名单功能。

undo ipv6 subscriber whitelist enable 命令用来关闭 IPv6 IPoE 白名单功能。

【命令】

```
ipv6 subscriber whitelist enable
undo ipv6 subscriber whitelist enable
```

【缺省情况】

IPv6 IPoE 白名单功能处于关闭状态。

【视图】

三层以太网接口视图/三层以太网子接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启 IPv6 IPoE 白名单功能后，仅匹配到静态 IPv6 IPoE 会话的 IPv6 流量才会触发 IPoE 认证，其余流量 IPoE 不做任何处理，均直接放行。

在一些组网环境中，接口上可能需要同时开启 IPoE 和 Portal 功能，例如：监控摄像头等哑终端使用 IPoE 进行免认证上线，同时宽带拨号用户使用 Portal 进行 Web 认证上线；这种组网环境可配置 IPoE 白名单功能。当接口上同时开启 IPv6 IPoE 白名单功能和 Portal 功能时：

- 如果用户 IPv6 流量可以匹配到静态 IPv6 IPoE 会话，则按静态 IPv6 IPoE 认证流程处理。当需要对 IPv6 IPoE 用户进行免认证时，domain 认证域下的 IPv6 IPoE 认证及授权方式必须配置为 none。
- 如果用户 IPv6 流量未匹配任何静态 IPv6 IPoE 会话，则进入 Portal 认证流程处理。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上开启 IPv6 IPoE 白名单功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 subscriber whitelist enable
```

1.2.38 reset ipv6 subscriber offline statistics

reset ipv6 subscriber offline statistics 命令用来清除 IPv6 IPoE 用户下线统计信息。

【命令】

```
reset ipv6 subscriber offline statistics [ interface interface-type
interface-number ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interface interface-type interface-number: 表示清除指定接口上的 IPv6 IPoE 用户下线统计信息, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 将清除所有接口上的 IPv6 IPoE 用户下线统计信息。

【举例】

清除所有接口上的 IPv6 IPoE 用户的下线统计信息。
<Sysname> reset ipv6 subscriber offline statistics

【相关命令】

- **display ipv6 subscriber offline statistics**

1.2.39 reset ipv6 subscriber session

reset ipv6 subscriber session 命令用来清除动态个人 IPv6 IPoE 会话和重置静态 IPv6 IPoE 会话, 强制用户下线。

【命令】

reset ipv6 subscriber session [**interface interface-type interface-number**]
[**domain domain-name** | **ipv6 ipv6-address** [**vpn-instance vpn-instance-name**]
| **mac mac-address** | **username name**]

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface interface-type interface-number: 表示清除指定接口动态个人 IPv6 IPoE 会话和重置静态 IPv6 IPoE 会话, *interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数, 将清除所有接口动态个人 IPv6 IPoE 会话和重置静态 IPv6 IPoE 会话。

domain domain-name: 表示清除和重置使用指定 ISP 域认证的 IPv6 IPoE 会话, *domain-name* 为 1~255 个字符的字符串, 不区分大小写, 不能包括 “/”、“\”、“|”、“.”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。

ipv6 ipv6-address: 表示清除和重置指定 IP 地址的 IPv6 IPoE 会话, *ipv6-address* 为指定的 IPv6 地址。

vpn-instance vpn-instance-name: 表示清除和重置指定 VPN 实例的 IPv6 IPoE 会话, *vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示 IPv6 IPoE 会话位于公网中。

mac mac-address: 表示清除和重置指定源 MAC 地址的 IPv6 IPoE 会话, 形式为 H-H-H。

username name: 表示清除和重置指定用户名的 IPv6 IPoE 会话, *name* 为 1~255 个字符的字符串, 区分大小写。

【使用指导】

本命令用来清除动态个人 IPv6 IPoE 会话和重置静态 IPv6 IPoE 会话信息，并强制用户下线，如果不指定条件，则表示删除所有动态 IPv6 IPoE 会话重置所有静态 IPv6 IPoE 会话。

专线用户和静态个人用户的会话不能通过 **reset ipv6 subscriber session** 命令清除，只能通过相应的 **undo** 命令删除配置的方式清除。

【举例】

清除接口 GigabitEthernet1/0/1 上动态个人 IPv6 IPoE 会话和重置静态 IPv6 IPoE 会话，强制用户下线。

```
<Sysname> reset ipv6 subscriber session interface gigabitethernet 1/0/1
```

【相关命令】

- **display ipv6 subscriber session**

目 录

1 IP信誉	1
1.1 IP信誉配置命令	1
1.1.1 display ip-reputation attack-category	1
1.1.2 display ip-reputation exception	2
1.1.3 display ip-reputation top-hit-statistics	2
1.1.4 display ip-reputation	3
1.1.5 ip-reputation	5
1.1.6 attack-category	5
1.1.7 exception	6
1.1.8 global enable	7
1.1.9 top-hit-statistics enable	8

1 IP信誉

1.1 IP信誉配置命令

1.1.1 display ip-reputation attack-category

display ip-reputation attack-category 命令用来显示 IP 信誉特征库中的攻击分类信息。

【命令】

display ip-reputation attack-category

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

仅在 IP 信誉功能处于开启状态时，才能查看到 IP 信誉库中的攻击分类信息。

如果未配置对指定攻击分类执行的动作，则显示特征库中的缺省配置。

【举例】

显示 IP 信誉特征库中的攻击分类信息。

```
<Sysname> display ip-reputation attack-category
```

ID	Attack name	Action	Logging
1	ddos	permit	enabled
2	web	deny	disabled

图1-1 display ip-reputation attack-category 命令显示信息描述表

字段	描述
ID	攻击分类ID
Attack name	攻击分类名称
Action	对匹配上攻击分类的报文执行动作，取值包括： • permit: 放行 • deny: 丢弃
Logging	表示日志功能启用状态，取值包括： • enabled: 开启状态

字段	描述
	disabled: 关闭状态

【相关命令】

- attack-category

1.1.2 display ip-reputation exception

display ip-reputation exception 命令用来显示 IP 信誉例外 IP 地址。

【命令】

display ip-reputation exception

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

仅在 IP 信誉功能处于开启状态时，才能查看到 IP 信誉例外 IP 地址。

【举例】

```
# 显示 IP 信誉例外 IP 地址。
<Sysname> display ip-reputation exception
IP address
10.1.1.1
10.10.1.1
```

图1-2 display ip-reputation exception 命令显示信息描述表

字段	描述
IP address	表示IP信誉例外IP地址

1.1.3 display ip-reputation top-hit-statistics

display ip-reputation top-hit-statistics 命令用来显示命中 IP 信誉库的 IP 地址 Top 排名统计信息。

【命令】

display ip-reputation top-hit-statistics [*top-number*] [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

top-number: 显示命中 IP 信誉库次数排名前 *top-number* 名的 IP 地址统计信息。*top-number* 的取值范围为 10~100，缺省值为 10。

slot slot-number: 显示指定成员设备上命中 IP 信誉库次数排名前 *top-number* 的 IP 地址统计信息，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，显示所有成员设备上命中 IP 信誉库次数排名前 *top-number* 的 IP 地址统计信息。

【使用指导】

仅在命中 IP 信誉库的 IP 地址 Top 排名统计功能处于开启状态时，才能查看到排名统计信息。
本命令仅显示命中次数非零的 IP 地址排名统计信息，实际显示条目数可能小于 *top-number*。

【举例】

显示指定 slot 上的命中 IP 信誉库次数排名前 10 的 IP 地址排名统计信息。

```
<Sysname> display ip-reputation top-hit-statistics 10 slot 1
```

Slot 1:

IP address	Hit count
10.1.1.1	1000
10.1.1.2	999
10.1.1.3	996
10.1.1.4	994
10.1.1.5	994
10.1.1.6	994

图1-3 display ip-reputation top-hit-statistics 命令显示信息描述表

字段	描述
IP address	命中IP信誉库的IP地址
Hit count	命中IP信誉库的次数

1.1.4 display ip-reputation

display ip-reputation 命令用来显示 IP 信誉库中的 IP 地址信息。

【命令】

display ip-reputation ipv4 ipv4-address

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ipv4 ipv4-address: 显示 IP 信誉库中指定 IPv4 地址的信息。

【使用指导】

IP 信誉库中包含 IP 地址的攻击分类、匹配方向、匹配动作和命中 IP 信誉库次数等信息。
一个 IP 地址可对应多种攻击分类，每种攻击分类都有对应的匹配方式和匹配动作等信息。设备将根据攻击分类显示 IP 地址的相关信息。

【举例】

```
# 显示 IP 信誉库中地址为 192.168.1.1 的信息。  
<Sysname> display ip-reputation ipv4 192.168.1.1  
IP address    Attack ID    Attack name  Direction   Action      Logging     Hit count  
192.168.1.1   1           ddos         src          deny        enabled     1000  
              2           web          dst          permit      disabled
```

图1-4 display ip-reputation 命令显示信息描述表

字段	描述
IP address	表示查询的IP信誉库中的IP地址
Attack ID	表示该IP地址对应的攻击分类ID
Attack name	表示该IP地址对应的攻击分类名称
Direction	表示该IP地址被标识为特定攻击时的匹配方向，取值包括： • src: 作为源地址匹配 • dst: 作为目的地址匹配 • src/dst: 即可源地址也可作为目的地址匹配
Action	表示对匹配上该IP地址的报文执行动作，取值包括： • permit: 表示放行 • deny: 表示丢弃
Logging	表示日志功能的启用状态，取值包括： • enabled: 表示开启日志功能 • disabled: 表示关闭日志功能

字段	描述
Hit count	表示该IP地址命中IP信誉库的次数

1.1.5 ip-reputation

ip-reputation 命令用来进入 IP 信誉视图。

undo ip-reputation 命令用来删除 IP 信誉视图下的所有配置。

【命令】

ip-reputation

undo ip-reputation

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【举例】

进入 IP 信誉视图。

```
<Sysname> system-view
```

```
[Sysname] ip-reputation
```

```
[Sysname-ip-reputation]
```

1.1.6 attack-category

attack-category 命令用来配置对指定攻击分类执行的操作。

undo attack-category 命令用来恢复缺省情况。

【命令】

attack-category *attack-id* { action { deny | permit } | logging { disable | enable } }*

undo attack-category *attack-id*

【缺省情况】

未配置对指定攻击分类执行的操作，设备使用 IP 信誉特征库中的缺省配置对匹配该 IP 地址的报文执行相应的操作。

【视图】

IP 信誉视图

【缺省用户角色】

network-admin

context-admin

【参数】

attack-id: 攻击分类的编号。本参数的取值范围与 IP 信誉库特征文件有关，请以设备的实际情况为准。

action: 表示攻击分类的匹配动作。

deny: 表示动作为丢弃。

permit: 表示动作为放行。

logging: 表示 IP 信誉日志功能，即 IP 地址匹配到 IP 信誉攻击分类时，生成日志信息的功能。

disable: 表示关闭日志功能。

enable: 表示开启日志功能。

【使用指导】

本功能仅在开启 IP 信誉功能后生效。

IP 信誉库中，一个 IP 地址可对应多种攻击分类，每种攻击分类都有对应执行的动作。

当 IP 地址只属于一种攻击分类时，设备将对匹配上该 IP 地址的报文执行攻击分类对应的动作；当 IP 地址属于多种攻击分类时，设备将对匹配上该 IP 地址的报文执行多种攻击分类中优先级最高的动作。其中，动作的优先级从高到底依次为：阻断>允许。

只要 IP 地址所属的任一攻击分类开启了日志功能，则对匹配上该 IP 地址的报文执行记录日志动作。

设备仅支持以快速日志输出的方式输出 IP 信誉日志，有关快速日志输出的详细介绍，请参见“网络管理和监控命令参考”中的“快速日志输出”。

【举例】

配置 IP 信誉库中编号为 1 的攻击分类对应的动作为 deny，并开启日志功能。

```
<Sysname> system-view
[Sysname] ip-reputation
[Sysname-ip-reputation] attack-category 1 action deny logging enable
```

【相关命令】

- **display ip-reputation**
- **global enable**

1.1.7 exception

exception 命令用来配置 IP 信誉例外 IP 地址。

undo exception 命令用来删除 IP 信誉例外 IP 地址。

【命令】

```
exception ipv4 ipv4-address
undo exception ipv4 ipv4-address
```

【缺省情况】

未配置 IP 信誉例外 IP 地址。

【视图】

IP 信誉视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4 ipv4-address: 表示例外 IPv4 地址。

【使用指导】

本功能仅在开启 IP 信誉功能后生效。

若报文的源/目的 IP 地址匹配 IP 信誉例外 IP 地址，则直接放行该报文。

多次执行本命令，可配置多个例外 IP 地址。

【举例】

```
# 配置 IPv4 地址 192.168.1.1 为 IP 信誉例外 IP 地址。  
<Sysname> system-view  
[Sysname] ip-reputation  
[Sysname-ip-reputation] exception ipv4 192.168.1.1
```

【相关命令】

- **display ip-reputation exception**
- **global enable**

1.1.8 global enable

global enable 命令用来开启全局 IP 信誉功能。

undo global enable 命令用来关闭全局 IP 信誉功能。

【命令】

```
global enable  
undo global enable
```

【缺省情况】

全局 IP 信誉功能处于关闭状态。

【视图】

IP 信誉视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 开启全局 IP 信誉功能。  
<Sysname> system-view  
[Sysname] ip-reputation  
[Sysname-ip-reputation] global enable
```

1.1.9 top-hit-statistics enable

top-hit-statistics enable 命令用来开启命中 IP 信誉库的 IP 地址 Top 排名统计功能。

undo top-hit-statistics enable 命令用来关闭命中 IP 信誉库的 IP 地址 Top 排名统计功能。

【命令】

top-hit-statistics enable

undo top-hit-statistics enable

【缺省情况】

命中 IP 信誉库的 IP 地址 Top 排名统计功能处于关闭状态。

【视图】

IP 信誉视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

本功能仅在开启 IP 信誉功能后生效。

开启本功能后，设备将对命中 IP 信誉库的 IP 地址进行统计排名。关闭本功能后，统计信息将自动清空。

【举例】

开启命中 IP 信誉库的 IP 地址 Top 排名统计功能。

```
<Sysname> system-view
```

```
[Sysname] ip-reputation
```

```
[Sysname-ip-reputation] top-hit-statistics enable
```

【相关命令】

- **display ip-reputation top-hit-statistics**

目 录

1 MAC地址认证	1-1
1.1 MAC地址认证配置命令	1-1
1.1.1 display mac-authentication	1-1
1.1.2 display mac-authentication connection	1-4
1.1.3 mac-authentication	1-6
1.1.4 mac-authentication critical vlan	1-6
1.1.5 mac-authentication critical-voice-vlan	1-7
1.1.6 mac-authentication domain	1-8
1.1.7 mac-authentication guest-vlan	1-9
1.1.8 mac-authentication guest-vlan auth-period	1-10
1.1.9 mac-authentication host-mode multi-vlan	1-11
1.1.10 mac-authentication max-user	1-12
1.1.11 mac-authentication re-authenticate server-unreachable keep-online	1-12
1.1.12 mac-authentication timer	1-13
1.1.13 mac-authentication timer auth-delay	1-14
1.1.14 mac-authentication user-name-format	1-15
1.1.15 reset mac-authentication critical-vlan	1-16
1.1.16 reset mac-authentication guest-vlan	1-17
1.1.17 reset mac-authentication statistics	1-18

1 MAC地址认证

1.1 MAC地址认证配置命令

1.1.1 display mac-authentication

display mac-authentication 命令用来显示 MAC 地址认证的相关信息。

【命令】

display mac-authentication [*interface interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface interface-type interface-number: 显示全局及指定端口的 MAC 地址认证相关信息。*interface-type interface-number* 为端口类型和端口编号。若指定的端口上未使能 MAC 地址认证，则不显示该端口任何信息。

【使用指导】

如果不指定任何参数，则显示所有在线 MAC 地址认证的详细信息，主要包括全局及端口的配置信息、认证报文统计信息以及认证用户信息。

【举例】

显示 MAC 地址认证信息。

```
<Sysname> display mac-authentication
Global MAC authentication parameters:
  MAC authentication       : Enabled
  User name format        : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
    Username              : mac
    Password              : Not configured
  Offline detect period   : 300 s
  Quiet period            : 60 s
  Server timeout          : 100 s
  Authentication domain   : Not configured, use default domain
Online MAC-auth wired users   : 1

Silent MAC users:
  MAC address      VLAN ID  From port      Port index
```

```

0001-0000-0001    100    GigabitEthernet1/0/2    21
0001-0000-0003    12     GigabitEthernet1/0/4    301

```

```

GigabitEthernet1/0/1 is link-up
  MAC authentication      : Enabled
  Carry User-IP          : Disabled
  Authentication domain   : Not configured
  Auth-delay timer       : Enabled
    Auth-delay period    : 60 s
  Re-auth server-unreachable : Logoff
  Guest VLAN             : 100
  Guest VLAN auth-period : 150 s
  Critical VLAN          : Not configured
  Critical voice VLAN     : Disabled
  Host mode              : Multiple VLAN
  Max online users       : 256
  Authentication attempts : successful 2, failed 3
  Current online users    : 1
    MAC address          Auth state
    0001-0000-0001      Unauthenticated

```

表1-1 display mac-authentication 命令显示信息描述表

字段	描述
Global MAC authentication parameters	全局MAC地址认证参数
MAC authentication	MAC地址认证的开启状态
User name format	MAC地址认证使用的账号格式 - 若采用 MAC 地址账号，则显示具体的用户名格式以及是否带连字符、字母是否大小写，例如本例中“MAC address in lowercase(xx-xx-xx-xx-xx-xx)”，它表示用户名格式为六段式的 MAC 地址，其中字母为小写 - 若采用固定用户名账号，则显示“Fixed account”
Username	用户名 - 采用 MAC 地址账号时，该值显示为“mac”，无实际意义，仅表示采用 MAC 地址作为用户名和密码 - 采用固定用户名账号时，该值为配置的用户名（缺省为 mac）
Password	用户名的密码 - 采用 MAC 地址账号时，该值显示为“Not configured” - 采用固定用户名账号时，配置的值将显示为*****
Offline detect period	下线检测定时器的值
Quiet period	静默定时器的值
Server timeout	服务器连接超时定时器的值

字段	描述
Authentication domain	系统视图下指定的MAC地址认证用户使用的认证域，如果没有指定认证域，则显示Not configured, use default domain
Online MAC-auth wired users	在线有线用户和正在发起MAC地址认证的有线用户的总数
Silent MAC users	静默用户信息
MAC address	静默用户的MAC地址
VLAN ID	静默用户所在的VLAN
From port	静默用户接入的端口名称
Port index	静默用户接入的端口索引号
GigabitEthernet1/0/1 is link-up	端口GigabitEthernet1/0/1的链路状态
MAC authentication	当前端口的MAC地址认证开启状态
Carry User-IP	（暂不支持）MAC地址认证请求携带用户IP地址开启状态
Authentication domain	端口上指定的MAC地址认证用户使用的认证域
Auth-delay timer	MAC地址认证延迟功能的开启状态
Auth-delay period	配置的认证延迟时间
Re-auth server-unreachable	重认证时服务器不可达对MAC地址认证的在线用户采取的动作 - Logoff: 重认证服务器不可达，强制 MAC 地址认证在线用户下线 - Online: 重认证服务器不可达，保持 MAC 地址认证在线用户在线
Guest VLAN	端口配置的Guest VLAN，如果没有配置，则显示Not configured
Guest VLAN auth-period	进入Guest VLAN后发起重认证的时间间隔
Critical VLAN	端口配置的Critical VLAN，如果没有配置，则显示Not configured
Critical voice VLAN	端口配置MAC地址认证的Critical Voice VLAN功能的开启状态 - Enabled: 打开 - Disabled: 关闭
Host mode	相同MAC地址用户的工作模式 - 如果配置的是多 VLAN 模式，则显示 Multiple VLAN - 如果配置的是单 VLAN 模式，则显示 Single VLAN
Max online users	本端口最多可容纳的接入用户数
Authentication attempts: successful 1, failed 0	端口上MAC地址认证的统计信息，包括认证通过的次数和认证失败的次数
MAC address	接入用户的MAC地址

字段	描述
Auth state	接入用户的状态 • Authenticated: 认证成功 • Unauthenticated: 认证失败

1.1.2 display mac-authentication connection

display mac-authentication connection 命令用来显示 MAC 地址认证在线用户的详细信息。

【命令】

```
display mac-authentication connection [ interface interface-type
interface-number | slot slot-number | user-mac mac-addr | user-name
user-name ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface *interface-type interface-number*: 显示指定端口的 MAC 地址认证用户信息。其中 *interface-type interface-number* 表示绑定的端口类型和端口编号。若不指定本参数，则显示设备上所有的 MAC 地址认证用户信息。

slot *slot-number*: 显示指定成员设备上的 MAC 地址认证用户信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定本参数，则显示所有成员设备上的 MAC 地址认证用户信息。

user-mac *mac-addr*: 显示指定 MAC 地址的 MAC 地址认证用户信息。其中 *mac-addr* 表示用户的 MAC 地址，格式为 H-H-H。若不指定本参数，则显示设备上所有的 MAC 地址认证用户信息。

user-name *user-name*: 显示指定用户名的 MAC 地址认证用户信息。其中 *user-name* 表示用户名（可包含域名），为 1~55 个字符的字符串，区分大小写。若不指定本参数，则显示设备上所有的 MAC 地址认证用户信息。

【使用指导】

如果不指定任何参数，则显示所有端口上的 MAC 地址认证在线用户信息。

多台设备组成 IRF 环境下，如果不指定任何参数，则显示所有成员设备上的 MAC 地址认证在线用户信息。

【举例】

显示所有 MAC 地址认证在线用户信息。

```
<Sysname> display mac-authentication connection
```

Total connections: 1

Slot ID: 0

User MAC address: 0015-e9a6-7cfe

Access interface: GigabitEthernet1/0/1

Username: ias

Authentication domain: unis

Initial VLAN: 1

Authorization untagged VLAN: 100

Authorization tagged VLAN: N/A

Authorization ACL number/name: 3001

Authorization user profile: N/A

Termination action: Radius-request

Session timeout period: 2 s

Online from: 2013/03/02 13:14:15

Online duration: 0h 2m 15s

表1-2 display mac-authentication connection 命令显示信息描述表

字段	描述
Total connections	在线MAC地址认证用户个数
User MAC address	用户的MAC地址
Access interface	用户的接入接口名称
Username	用户名
Authentication domain	认证时所用的ISP域的名称
Initial VLAN	初始的VLAN
Authorization untagged VLAN	授权的untagged VLAN
Authorization tagged VLAN	授权的tagged VLAN
Authorization VLAN	授权的VLAN
Authorization ACL number/name	授权ACL的编号或名称。若未授权ACL，则显示为N/A 若未授权成功，在ACL编号或名称后显示“(NOT effective)”
Authorization user profile	(暂不支持) 授权用户的User profile名称
Authorization CAR	当服务器未授权用户CAR属性时，该字段显示为N/A 当服务器授权用户CAR属性，将分为以下两个字段： - Average input rate：上行平均速率，单位为 bps - Average output rate: 下行平均速率，单位为 bps
Authorization URL	授权用户的重定向URL
Termination action	服务器下发的终止动作类型： - Default: 会话超时时间到达后，强制用户下线 - Radius-Request: 会话超时时间到达后，请求 MAC 地址认证用户进行重认证 用户采用本地认证时，该字段显示为N/A

字段	描述
Session timeout period	服务器下发的会话超时时间，该时间到达之后，用户所在的会话将会被删除，之后，对该用户所采取的动作，由Termination action字段的取值决定 用户采用本地认证时，该字段显示为N/A
Online from	MAC认证用户的上线时间
Online duration	MAC认证用户的在线时长

1.1.3 mac-authentication

mac-authentication 命令用来开启端口上或全局的 MAC 地址认证。

undo mac-authentication 命令用来关闭端口上或全局的 MAC 地址认证。

【命令】

```
mac-authentication
undo mac-authentication
```

【缺省情况】

所有端口及全局的 MAC 地址认证都处于关闭状态。

【视图】

系统视图
二层以太网接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

只有全局和端口的 MAC 地址认证均开启后，MAC 地址认证配置才能在端口上生效。

【举例】

```
# 开启全局的 MAC 地址认证。
<Sysname> system-view
[Sysname] mac-authentication
# 开启端口 GigabitEthernet1/0/1 上的 MAC 地址认证。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
```

【相关命令】

- **display mac-authentication**

1.1.4 mac-authentication critical vlan

mac-authentication critical vlan 命令用来配置端口的 MAC 地址认证的 Critical VLAN。

undo mac-authentication critical vlan 命令用来恢复缺省情况。

【命令】

```
mac-authentication critical vlan critical-vlan-id  
undo mac-authentication critical vlan
```

【缺省情况】

端口上未配置 MAC 地址认证的 Critical VLAN。

【视图】

二层以太网接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

critical-vlan-id: 端口上指定的 Critical VLAN ID，取值范围为 1~4094。该 VLAN 必须已经创建。

【使用指导】

配置此功能后，当 MAC 用户认证时对应的 ISP 域下所有认证服务器都不可达的情况下被授权访问 Critical VLAN 内的资源。

禁止删除已被配置为 Critical VLAN 的 VLAN，若要删除该 VLAN，请先通过 **undo mac-authentication critical vlan** 命令取消 MAC 地址认证的 Critical VLAN 配置。

【举例】

```
# 配置端口 GigabitEthernet1/0/1 的 Critical VLAN 为 VLAN 100。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mac-authentication critical vlan 100
```

【相关命令】

- **display mac-authentication**
- **reset mac-authentication critical-vlan**

1.1.5 mac-authentication critical-voice-vlan

mac-authentication critical-voice-vlan 命令用来开启端口上 MAC 地址认证的 Critical Voice VLAN 功能。

undo mac-authentication critical-voice-vlan 命令用来关闭端口上 MAC 地址认证的 Critical Voice VLAN 功能。

【命令】

```
mac-authentication critical-voice-vlan  
undo mac-authentication critical-voice-vlan
```

【缺省情况】

端口下 MAC 地址认证的 Critical Voice VLAN 功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

端口上开启 MAC 地址认证 Critical Voice VLAN 功能后，当语音用户进行 MAC 地址认证采用的 ISP 域中的所有认证服务器都不可达时，端口将被加入到此端口上的 Voice VLAN 中。端口上语音 VLAN 的配置命令请参见“二层技术-以太网交换命令参考”中的“VLAN”。

设备通过 LLDP（Link Layer Discovery Protocol，链路层发现协议）来判断用户是否为语音用户，因此为保证 MAC 地址认证 Critical Voice VLAN 功能可以正常工作，请在开启此功能之前务必确保全局和相应端口下均已开启 LLDP 功能。有关 LLDP 功能的配置命令介绍请参见“二层技术-以太网交换命令参考”中的“LLDP”。

开启 MAC 地址认证 Critical Voice VLAN 功能前，请保证该端口上已经配置了 MAC 地址认证 Critical VLAN。若端口上的语音用户在认证时所有认证服务器都不可达，且端口暂未将其识别为语音用户，则可以将其先加入 Critical VLAN。

【举例】

开启端口 GigabitEthernet1/0/1 上 MAC 地址认证 Critical Voice VLAN 功能。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-authentication critical-voice-vlan
```

【相关命令】

- **display mac-authentication**
- **lldp enable**（二层技术-以太网交换命令参考/LLDP）
- **lldp global enable**（二层技术-以太网交换命令参考/LLDP）
- **voice-vlan enable**（二层技术-以太网交换命令参考/VLAN）

1.1.6 mac-authentication domain

mac-authentication domain 命令用来指定 MAC 地址认证用户使用的认证域。

undo mac-authentication domain 命令用来恢复缺省情况。

【命令】

mac-authentication domain *domain-name*

undo mac-authentication domain

【缺省情况】

未指定 MAC 地址认证用户使用的认证域时，使用系统缺省的认证域。缺省认证域的介绍请参见“安全命令参考/AAA”中的命令 **domain default enable**。

【视图】

系统视图

二层以太网接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain-name: ISP 域名，为 1~255 个字符的字符串，不区分大小写。

【使用指导】

不同视图下指定的认证域的生效范围不同：

- 系统视图下指定的认证域对所有开启了 MAC 地址认证的端口生效。
 - 二层以太网接口视图下指定的认证域仅对本端口有效。不同的端口可以指定不同的认证域。
- 端口上接入的 MAC 地址认证用户将按照如下先后顺序选择认证域：端口上指定的认证域 > 系统视图下指定的认证域 > 系统缺省的认证域。

【举例】

在系统视图下指定 MAC 地址认证用户使用的认证域为 domain1。

```
<Sysname> system-view
```

```
[Sysname] mac-authentication domain domain1
```

指定端口 GigabitEthernet1/0/1 上接入的 MAC 地址认证用户使用的认证域为 aabbcc。

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-authentication domain aabbcc
```

【相关命令】

- **display mac-authentication**
- **domain default enable**（安全命令参考/AAA）

1.1.7 mac-authentication guest-vlan

mac-authentication guest-vlan 命令用来配置端口的 MAC 地址认证的 Guest VLAN。

undo mac-authentication guest-vlan 命令用来恢复缺省情况。

【命令】

```
mac-authentication guest-vlan guest-vlan-id
```

```
undo mac-authentication guest-vlan
```

【缺省情况】

端口上未配置 MAC 地址认证的 Guest VLAN。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

guest-vlan-id: 端口上指定的 Guest VLAN ID, 取值范围为 1~4094。该 VLAN 必须已经创建。

【使用指导】

配置此功能后, 当 MAC 地址认证失败的情况下, 用户可以继续被授权访问的 Guest VLAN 内的资源。

禁止删除已被配置为 Guest VLAN 的 VLAN, 若要删除该 VLAN, 请先通过 **undo mac-authentication guest-vlan** 命令取消 MAC 地址认证的 Guest VLAN 配置。

【举例】

```
# 配置端口 GigabitEthernet1/0/1 的 Guest VLAN 为 VLAN 100。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan 100
```

【相关命令】

- **display mac-authentication**
- **reset mac-authentication guest-vlan**

1.1.8 mac-authentication guest-vlan auth-period

mac-authentication guest-vlan auth-period 命令用来配置设备对 Guest VLAN 中的用户进行重新认证的时间间隔。

undo mac-authentication guest-vlan auth-period 命令用来恢复缺省情况。

【命令】

```
mac-authentication guest-vlan auth-period period-value  
undo mac-authentication guest-vlan auth-period
```

【缺省情况】

设备对 Guest VLAN 中的用户进行重新认证的时间间隔为 30 秒。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

period-value: 表示设备重新发起认证的时间间隔, 取值范围为 1~3600, 单位为秒。

【使用指导】

在 MAC 地址认证中, 如果接入用户的端口上配置了 Guest VLAN, 则该端口上认证失败的用户会被加入此 Guest VLAN。用户被加入 Guest VLAN 之后, 设备将以指定的时间间隔对该用户发起重新认证, 直到该用户认证成功。

【举例】

在端口 GigabitEthernet1/0/1 上配置设备对 Guest VLAN 中的用户进行重新认证的时间间隔为 150 秒。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan auth-period 150
```

【相关命令】

- **display mac-authentication**
- **mac-authentication guest-vlan**

1.1.9 mac-authentication host-mode multi-vlan

mac-authentication host-mode multi-vlan 命令用来指定端口工作在 MAC 地址认证的多 VLAN 模式。

undo mac-authentication host-mode 命令用来恢复缺省情况。

【命令】

mac-authentication host-mode multi-vlan

undo mac-authentication host-mode

【缺省情况】

端口工作在 MAC 地址认证的单 VLAN 模式。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

端口工作在多 VLAN 模式下时,如果相同 MAC 地址的用户在属于不同 VLAN 的相同端口再次接入,设备将能够允许用户的流量在新的 VLAN 内通过,且允许该用户的报文无需重新认证而在多个 VLAN 中转发。

端口工作在单 VLAN 模式下时,在用户已上线,且没有被下发授权 VLAN 情况下,如果此用户在属于不同 VLAN 的相同端口再次接入,则设备将让原用户下线,使得该用户能够新的 VLAN 内重新开始认证。如果已上线用户被下发了授权 VLAN,则此用户在属于不同 VLAN 的相同端口再次接入时不会被强制下线。

对于接入 IP 电话类用户的端口,指定端口工作在 MAC 地址认证的多 VLAN 模式,可避免 IP 电话终端的报文所携带的 VLAN tag 发生变化后,因用户流量需要重新认证带来语音报文传输质量受干扰的问题。

【举例】

配置端口 GigabitEthernet1/0/1 工作在 MAC 地址认证的多 VLAN 模式。

```
<Sysname> system-view
```



```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication host-mode multi-vlan
```

【相关命令】

- **display mac-authentication**

1.1.10 mac-authentication max-user

mac-authentication max-user 命令用来配置端口上最多允许同时接入的 MAC 地址认证用户数。

undo mac-authentication max-user 命令用来恢复缺省情况。

【命令】

```
mac-authentication max-user max-number
undo mac-authentication max-user
```

【缺省情况】

端口上最多允许同时接入的 MAC 地址认证用户数为 4294967295。

【视图】

二层以太网接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

max-number: 端口允许同时接入的 MAC 地址认证用户数的最大值, 取值范围为 1~4294967295。

【使用指导】

由于系统资源有限, 如果当前端口上接入的用户过多, 接入用户之间会发生资源的争用, 因此适当地配置该值可以使属于当前端口的用户获得可靠的性能保障。当接入此端口的 MAC 地址认证用户数超过最大值后, 新接入的用户将被拒绝。

【举例】

```
# 配置端口 GigabitEthernet1/0/1 最多允许同时接入 32 个 MAC 地址认证用户。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication max-user 32
```

【相关命令】

- **display mac-authentication**

1.1.11 mac-authentication re-authenticate server-unreachable keep-online

mac-authentication re-authenticate server-unreachable keep-online 命令用来配置重认证服务器不可达时端口上的 MAC 地址认证用户保持在线状态。

undo mac-authentication re-authenticate server-unreachable 命令用来恢复缺省情况。

【命令】

```
mac-authentication re-authenticate server-unreachable keep-online
undo mac-authentication re-authenticate server-unreachable
```

【缺省情况】

端口上的 MAC 地址认证在线用户重认证时，若认证服务器不可达，则会被强制下线。

【视图】

二层以太网接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

配置此命令后，在对 MAC 地址认证用户重认证过程中，若设备发现认证服务器状态不可达，则保持 MAC 地址认证用户在线。

是否对 MAC 地址认证在线用户进行周期性重认证由认证服务器授权的属性所决定。认证服务器通过下发 RADIUS 属性（`session-timeout`、`Terminal-Action`）来指定用户会话超时时长以及会话中止的动作类型，它们共同决定了如何对用户进行重认证。

- 当会话中止的动作类型为要求用户进行重认证时，端口会在用户会话超时时长到达后对该用户进行重认证；
- 当会话中止的动作类型为要求用户下线时，端口会在用户会话超时时长到达强制该用户下线；
- 当认证服务器未下发用户会话超时时长时，设备不会对用户进行重认证。

【举例】

配置端口 GigabitEthernet1/0/1 上的 MAC 地址认证在线用户进行重认证时，若服务器不可达，则保持在线状态。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication re-authenticate server-unreachable
keep-online
```

【相关命令】

- **display mac-authentication**

1.1.12 mac-authentication timer

mac-authentication timer 命令用来配置 MAC 地址认证的定时器参数。

undo mac-authentication timer 命令用来恢复缺省情况。

【命令】

```
mac-authentication timer { offline-detect offline-detect-value | quiet
quiet-value | server-timeout server-timeout-value }
undo mac-authentication timer { offline-detect | quiet | server-timeout }
```

【缺省情况】

下线检测定时器的值为 300 秒，静默定时器的值为 60 秒，服务器超时定时器的值为 100 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

offline-detect *offline-detect-value* : 表示下线检测定时器。其中，*offline-detect-value* 表示下线检测定时器的值，取值范围为 60~65535，单位为秒。

quiet *quiet-value*: 表示静默定时器。其中 *quiet-value* 表示静默定时器的值，取值范围为 1~3600，单位为秒。

server-timeout *server-timeout-value* : 表示服务器超时定时器。其中，*server-timeout-value* 表示服务器超时定时器的值，取值范围为 100~300，单位为秒。

【使用指导】

MAC 地址认证过程受以下定时器的控制：

- 下线检测定时器 (**offline-detect**)：用来设置在线用户空闲超时的时间间隔。若设备在一个下线检测定时器间隔之内，没有收到某在线用户的报文，将切断该用户的连接，同时通知 RADIUS 服务器停止对其计费。
- 静默定时器 (**quiet**)：用来设置用户认证失败以后，设备需要等待的时间间隔。在静默期间，设备不对来自认证失败用户的报文进行认证处理，直接丢弃。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。
- 服务器超时定时器 (**server-timeout**)：用来设置设备同 RADIUS 服务器的连接超时时间。在用户的认证过程中，如果到服务器超时定时器超时设备一直没有收到 RADIUS 服务器的应答，则设备将在相应的端口上禁止此用户访问网络。

【举例】

设置服务器超时定时器时长为 150 秒。

```
<Sysname> system-view
```

```
[Sysname] mac-authentication timer server-timeout 150
```

【相关命令】

- **display mac-authentication**

1.1.13 mac-authentication timer auth-delay

mac-authentication timer auth-delay 命令用来开启 MAC 地址认证延迟功能，并配置 MAC 地址认证的延时时间。

undo mac-authentication timer auth-delay 命令用来恢复缺省情况。

【命令】

mac-authentication timer auth-delay *time*

undo mac-authentication timer auth-delay

【缺省情况】

MAC 地址认证延迟功能处于关闭状态，如果用户报文触发 MAC 地址认证，认证将会立刻开始。

【视图】

以太网接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

time: 延迟 MAC 地址认证的时间，取值范围为 1~180，单位为秒。

【举例】

```
# 开启 MAC 地址延迟认证功能，并指定 MAC 地址认证的延时时间为 10 秒。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication timer auth-delay 10
```

【相关命令】

- **display mac-authentication**

1.1.14 mac-authentication user-name-format

mac-authentication user-name-format 命令用来配置 MAC 地址认证用户的帐号格式。

undo mac-authentication user-name-format 命令用来恢复缺省情况。

【命令】

```
mac-authentication user-name-format { fixed [ account name ] [ password
{ cipher | simple } string ] | mac-address [ { with-hyphen [ six-section |
three-section ] | without-hyphen } [ lowercase | uppercase ] ] }
undo mac-authentication user-name-format
```

【缺省情况】

使用用户的 MAC 地址作为用户名和密码，其中字母为小写，且不带连字符“-”。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

fixed: 表示采用固定用户名账号。

account name: 指定发送给 RADIUS 服务器进行认证或者在本地进行认证的用户名。其中 *name* 为用户名，为 1~55 个字符的字符串，区分大小写，不能包括字符@，缺省为 mac。

password: 指定固定用户名的密码。

cipher: 以密文方式设置密码。

simple: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串。

mac-address: 表示使用用户的 MAC 地址作为用户名和密码。

with-hyphen [six-section | three-section]: 带连字符“-”的 MAC 地址格式，**six-section** 表示六段式 MAC 地址格式，例如 xx-xx-xx-xx-xx-xx 或 XX-XX-XX-XX-XX-XX；**three-section** 表示三段式 MAC 地址格式，例如 xxxx-xxxx-xxxx 或 XXXX-XXXX-XXXX。如果不指定任何参数，缺省采用六段式 MAC 地址格式。

without-hyphen: 不带连字符“-”的 MAC 地址格式，例如 xxxxxxxxxxxx 或 XXXXXXXXXXXXXX。

lowercase: MAC 地址中的字母为小写。

uppercase: MAC 地址中的字母为大写。

【使用指导】

若指定用户的 MAC 地址为用户名，则用户密码也为用户的 MAC 地址。这种情况下，每一个 MAC 地址认证用户都使用唯一的用户名进行认证，安全性高，但要求认证服务器端配置多个 MAC 形式的用户帐户。

若指定一个固定的用户名，则表示不论用户的 MAC 地址为何值，所有用户均使用设备上指定的一个固定用户名和密码作为身份信息进行认证。由于同一个端口下可以有多个用户进行认证，因此这种情况下端口上的所有 MAC 地址认证用户均使用同一个固定用户名账号进行认证，服务器端仅需要配置一个用户帐户即可满足所有认证用户的认证需求，适用于接入客户端比较可信的网络环境。

【举例】

配置 MAC 地址认证的用户名为 abc，密码是明文 xyz。

```
<Sysname> system-view
```

```
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
```

配置用户的 MAC 地址为用户名和密码，使用不带连字符“-”的 MAC 地址格式，其中字母大写。

```
<Sysname> system-view
```

```
[Sysname] mac-authentication user-name-format mac-address without-hyphen uppercase
```

【相关命令】

- **display mac-authentication**

1.1.15 reset mac-authentication critical-vlan

reset mac-authentication critical-vlan 命令用来清除 Critical VLAN 内的 MAC 地址认证用户。

【命令】

```
reset mac-authentication critical-vlan interface interface-type  
interface-number [ mac-address mac-address ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface *interface-type interface-number*: 表示使指定端口上的用户退出 Critical VLAN。*interface-type interface-number* 为端口类型和端口编号。

mac-address *mac-address*: 表示使指定 MAC 地址的用户退出 Critical VLAN。若不指定本参数，则表示使指定端口上的所有用户退出 Critical VLAN。

【举例】

```
# 在端口 GigabitEthernet1/0/1 上使得 MAC 地址为 1-1-1 的 MAC 地址认证用户退出 Critical VLAN。  
<Sysname> reset mac-authentication critical-vlan interface gigabitethernet 1/0/1  
mac-address 1-1-1
```

【相关命令】

- **display mac-authentication**
- **mac-authentication critical vlan**

1.1.16 reset mac-authentication guest-vlan

reset mac-authentication guest-vlan 命令用来清除 Guest VLAN 内的 MAC 地址认证用户。

【命令】

```
reset mac-authentication guest-vlan interface interface-type  
interface-number [mac-address mac-address ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface *interface-type interface-number*: 表示使指定端口上的用户退出 Guest VLAN。*interface-type interface-number* 为端口类型和端口编号。

mac-address *mac-address*: 表示使指定 MAC 地址的用户退出 Guest VLAN。若不指定本参数，则表示使指定端口上的所有用户退出 Guest VLAN。

【举例】

```
# 在端口 GigabitEthernet1/0/1 上使得 MAC 地址为 1-1-1 的 MAC 地址认证用户退出 Guest VLAN。  
<Sysname> reset mac-authentication guest-vlan interface gigabitethernet 1/0/1 mac-address  
1-1-1
```

【相关命令】

- **display mac-authentication**
- **mac-authentication guest-vlan**

1.1.17 reset mac-authentication statistics

reset mac-authentication statistics 命令用来清除 MAC 地址认证的统计信息。

【命令】

```
reset mac-authentication statistics [ interface interface-type  
interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface interface-type interface-number: 清除指定端口的 MAC 地址认证统计信息。
interface-type interface-number 为端口类型和端口编号。如果不指定本参数，则清除所有端口上的 MAC 地址认证统计信息。

【使用指导】

如果不指定任何参数，则清除所有 MAC 地址认证统计信息。

【举例】

清除以太网端口 GigabitEthernet1/0/1 上的 MAC 认证统计信息。
<Sysname> reset mac-authentication statistics interface gigabitethernet 1/0/1

【相关命令】

- **display mac-authentication**

目 录

1 服务器外联防护.....	1-1
1.1 服务器外联防护配置命令.....	1-1
1.1.1 auto-learn enable.....	1-1
1.1.2 display scd auto-learn config	1-2
1.1.3 display scd learning record	1-3
1.1.4 display scd policy.....	1-4
1.1.5 logging enable	1-6
1.1.6 permit-dest-ip.....	1-6
1.1.7 policy enable	1-7
1.1.8 protected-server	1-8
1.1.9 protocol	1-9
1.1.10 reset scd learning record	1-9
1.1.11 rule	1-10
1.1.12 scd learning	1-11
1.1.13 scd policy	1-11
1.1.14 source-ip	1-12

1 服务器外联防护

1.1 服务器外联防护配置命令

1.1.1 auto-learn enable

auto-learn enable 命令用来开启服务器外联自动学习功能。

undo auto-learn enable 命令用来关闭服务器外联自动学习功能。

【命令】

```
auto-learn enable period { one-day | one-hour | seven-day | twelve-hour }  
undo auto-learn enable
```

【缺省情况】

服务器外联自动学习功能处于关闭状态。

【视图】

服务器外联学习视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

period: 配置服务器外联自动学习的时长，达到设置的学习时长后系统自动关闭服务器外联学习功能。

one-day: 表示连续学习一天。

one-hour: 表示连续学习一小时。

seven-day: 表示连续学习七天。

twelve-hour: 表示连续学习 12 小时。

【使用指导】

当服务器外联学习视图下不存在待防护的服务器或系统正在对服务器外联行为进行学习时，无法开启自动学习功能。

不能通过重复执行本命令来修改学习时长。如需修改学习时长，请先通过 **undo auto-learn enable** 命令关闭服务器外联自动学习功能，再执行 **auto-learn enable** 命令。

【举例】

开启服务器外联自动学习功能，并配置连续学习时间为一天。

```
<Sysname> system-view  
[Sysname] scd learning  
[Sysname-scd-learning] auto-learn enable period one-day
```

【相关命令】

- **source-ip**

1.1.2 display scd auto-learn config

display scd auto-learn config 命令用来显示服务器外联学习的相关配置信息。

【命令】

display scd auto-learn config

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示服务器外联学习的相关配置信息。

```
<Sysname> display scd auto-learn config
Learning status           : Active
Learning time             : One-hour
Server address object groups : 146
Progress                  : 6%
Start time                : 2018/03/27 10:50
End time                  : 2018/03/27 11:50
```

表1-1 display scd auto-learn config 命令显示信息描述表

字段	描述
Learning status	表示服务器外联学习的状态，其取值包括如下： • Active: 表示服务器外联学习处于开启状态 • 短横杠“-”: 表示服务器外联学习处于关闭状态
Learning time	表示服务器外联学习的时间，其取值包括如下： • One-day: 表示持续学习一天 • One-hour: 表示持续学习一小时 • Seven-day: 表示持续学习 7 天 • Twelve-hour: 表示持续学习 12 个小时
Server address object groups	表示服务器外联学习中引用了几个地址对象组
Progress	表示服务器外联学习完成的进度，以百分比形式表示
Start time	表示服务器外联学习开始的时间
End time	表示服务器外联学习结束的时间

1.1.3 display scd learning record

display scd learning record 命令用来显示服务器外联学习的结果。

【命令】

display scd learning record [**protected-server** *ip-address*] [**destination-ip** *ip-address*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

protected-server *ip-address*: 表示显示有关指定待防护服务器的外联学习结果，*ip-address* 是待防护服务器的 IP 地址。

destination-ip *ip-address*: 表示显示有关指定外联 IP 地址的外联学习结果，*ip-address* 是外联的 IP 地址。

【使用指导】

管理员可以通过学习结果来判断服务器的哪些外联是正常，哪些外联是异常，可为管理员配置服务器外联防护策略提供数据依据。

若不指定任何参数，则显示服务器外联学习的所有结果。

【举例】

显示服务器外联学习的所有结果。

```
<Sysname> display scd learning record
Id      Protected server    Destination IPv4 address  Protocol  Port
1       192.168.102.1        192.168.101.21          TCP       443
Total entries: 1
```

显示有关指定待防护服务器 192.168.102.1 的外联学习结果。

```
<Sysname> display scd learning record protected-server 192.168.102.1
Id      Protected server    Destination IPv4 address  Protocol  Port
1       192.168.102.1        192.168.101.21          TCP       443
Total entries: 1
```

显示有关指定外联 IP 地址为 192.168.101.21 的外联学习结果。

```
<Sysname> display scd learning record destination-ip 192.168.101.21
Id      Protected server    Destination IPv4 address  Protocol  Port
1       192.168.102.1        192.168.101.21          TCP       443
Total entries: 1
```

表1-2 display scd learning record 命令显示信息描述表

字段	描述
ID	表示显示信息的行号
Protected server	表示被防护服务器的IP地址
Destination IPv4 address	表示服务器外联的IPv4地址
Protocol	表示服务器外联的协议
Port	表示服务器外联的目的端口号
Total entries	表示学习到表项的条数

【相关命令】

- **reset scd learning record**

1.1.4 display scd policy

display scd policy 命令用来显示服务器外联防护策略的配置信息。

【命令】

display scd policy [name *policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

name *policy-name*: 表示服务器外联防护策略的名称，为 1~63 个字符的字符串，不区分大小写。若不指定本参数，则显示所有服务器外联防护策略的摘要配置信息。

【举例】

显示所有服务器外联防护策略的摘要配置信息。

<Sysname> display scd policy

```
Id      Name      Protected server  Rules      Logging      Policy status
1       policy1    1.1.1.1          0          Disabled     Disabled
Total entries: 1
```

表1-3 display scd policy 命令显示信息描述表

字段	描述
Id	表示显示信息的行号

Name	表示服务器外联防护策略的名称
Protected server	表示被防护服务器的IP地址
Rules	表示服务器外联防护策略中配置的规则数量
Logging	表示服务器外联防护策略中日志功能的状态，其取值包括如下： • Enabled: 表示处于开启状态 • Disabled: 表示处于关闭状态
Policy status	表示服务器外联防护策略的开启状态，其取值包括如下： • Enabled: 表示处于开启状态 • Disabled: 表示处于关闭状态
Total entries	表示服务器外联防护策略的条数

显示名称为 policy1 服务器外联防护策略的详细配置信息。

```
<Sysname> display scd policy name policy1
SCD policy name: policy1
Protected server IPv4: 1.1.1.1
Logging: Enabled
Policy status: Enabled
Rule ID: 1
Permitted dest IPv4: 1.1.2.1
Protocol: TCP port 1-4
Protocol: UDP port 1,3,5,7,9,11,13,15,17,19,21,23
Protocol: ICMP
```

表1-4 display scd policy name 命令显示信息描述表

字段	描述
SCD policy name	表示服务器外联防护策略的名称
Protected server IPv4	表示被防护服务器的IP地址
Rule ID	表示服务器外联防护规则的ID
Permitted dest IPv4	表示允许服务器外联的IP地址
Protocol	表示服务器外联的协议
Logging	表示服务器外联防护策略中日志功能的状态，其取值包括如下： • Enabled: 表示处于开启状态 • Disabled: 表示处于关闭状态
Policy status	表示服务器外联防护策略的开启状态，其取值包括如下： • Enabled: 表示处于开启状态 • Disabled: 表示处于关闭状态

1.1.5 logging enable

logging enable 命令用来开启服务器外联防护策略记录日志的功能。

undo logging enable 命令用来关闭服务器外联防护策略记录日志的功能。

【命令】

```
logging enable
undo logging enable
```

【缺省情况】

服务器外联防护策略记录日志的功能处于关闭状态。

【视图】

服务器外联防护策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启此功能后，当服务器外联防护策略检测到服务器出现异常外联行为时会输出日志进行告警。此日志信息将会被交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。有关信息中心的详细描述，请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

```
# 开启服务器外联防护策略记录日志的功能。
<Sysname> system-view
[Sysname] scd policy name policy1
[Sysname-scd-policy-policy1] logging enable
```

【相关命令】

- **display scd policy**

1.1.6 permit-dest-ip

permit-dest-ip 命令用来配置服务器允许外联的 IP 地址。

undo permit-dest-ip 命令用来删除服务器允许外联的 IP 地址。

【命令】

```
permit-dest-ip ip-address
undo permit-dest-ip
```

【缺省情况】

未配置服务器允许外联的 IP 地址。

【视图】

服务器外联防护规则视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: 指定服务器允许外联的 IP 地址，点分十进制格式。目前仅支持 IPv4 类型的 IP 地址。

【使用指导】

在服务器外联防护策略中，可以通过创建多条规则为服务器配置多个允许外联的 IP 地址。如果服务器外联的 IP 地址不在所允许的范围内，则防护策略认为服务器到此 IP 地址的连接为异常外联。

同一服务器外联防护策略下不同规则中的服务器允许外联 IP 地址不能相同。

多次执行本命令，最后一次执行的命令生效。

建议首先配置服务器外联学习功能，然后参考学习结果配置允许外联的 IP 地址。可通过 **display scd learning record** 命令用来查看服务器目前外联的 IP 地址等信息。

【举例】

在编号为 1 的服务器外联防护规则中配置服务器允许外联的 IP 地址为 1.1.1.1。

```
<Sysname> system-view  
[Sysname] scd policy name policy1  
[Sysname-scd-policy-policy1] rule 1  
[Sysname-scd-policy-policy1-1] permit-dest-ip 1.1.1.1
```

【相关命令】

- **display scd policy**

1.1.7 policy enable

policy enable 命令用来开启服务器外联防护功能。

undo policy enable 命令用来关闭服务器外联防护功能。

【命令】

policy enable
undo policy enable

【缺省情况】

服务器外联防护功能处于关闭状态。

【视图】

服务器外联防护策略视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

只有开启服务器外联防护功能后，此服务器外联防护策略才能生效。

【举例】

```
# 开启服务器外联防护功能。
<Sysname> system-view
[Sysname] scd policy name policy1
[Sysname-scd-policy-policy1] policy enable
```

【相关命令】

- **display scd policy**

1.1.8 protected-server

protected-server 命令用来配置待防护服务器的 IP 地址。

undo protected-server 命令用来删除待防护服务器的 IP 地址。

【命令】

```
protected-server ip-address
undo protected-server
```

【缺省情况】

不存在待防护服务器的 IP 地址。

【视图】

服务器外联防护策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ip-address: 指定服务器外联防护策略待防护服务器的 IP 地址，点分十进制格式。目前仅支持 IPv4 类型的 IP 地址。

【使用指导】

设备仅对指定的待防护服务器发起的外联行为进行检测。

不同服务器外联防护策略中配置的待防护服务器 IP 地址不能相同。

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 配置待防护服务器的 IP 地址为 192.168.1.10。
<Sysname> system-view
[Sysname] scd policy name policy1
[Sysname-scd-policy-policy1] protected-server 192.168.1.10
```

【相关命令】

- **display scd policy**

1.1.9 protocol

protocol 命令用来配置服务器允许外联的协议。

undo protocol 命令用来删除服务器允许外联的协议。

【命令】

```
protocol { icmp | tcp port port-list | udp port port-list }  
undo protocol { icmp | tcp | udp }
```

【缺省情况】

未配置服务器允许外联的协议。

【视图】

服务器外联防护规则视图

【缺省用户角色】

network-admin
context-admin

【参数】

icmp: 表示允许外联的协议为 ICMP 协议。

tcp: 表示允许外联的协议为 TCP 协议。

udp: 表示允许外联的协议为 UDP 协议。

port port-list: 指定 TCP 或 UDP 允许外联的目的端口号列表。表示方式为 *port-list* = { *port-number* [*to port-number*] } 其中 *port-number* 表示端口号, 取值范围是 1~65535。当使用 **to** 关键字指定端口号范围时, 起始端口号必须小于或等于结束端口号。此参数一次可以配置多个, 设备会对多个连续的端口和端口段进行合并, 合并后的端口参数不能超过 20 个。

【使用指导】

如果服务器外联的协议和端口号不在所允许的范围内, 则防护策略认为服务器到此协议和端口号的连接为异常外联。

多次执行本命令, 可以指定多种允许外联的协议。

对于相同协议多次执行本命令, 最后一次执行的命令生效。

【举例】

```
# 在编号为 1 的服务器外联防护规则中配置服务器允许外联的协议为 TCP, 端口号为 80、1000-2000。  
<Sysname> system-view  
[Sysname] scd policy name policy1  
[Sysname-scd-policy-policy1] rule 1  
[Sysname-scd-policy-policy1-1] protocol tcp port 80 1000 to 2000
```

【相关命令】

- **display scd policy**

1.1.10 reset scd learning record

reset scd learning record 命令用来清除服务器外联学习的结果。

【命令】

reset scd learning record

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【举例】

清除服务器外联学习的结果。

<Sysname> reset scd learning record

【相关命令】

- **display scd learning record**

1.1.11 rule

rule 命令用来创建服务器外联防护规则，并进入服务器外联防护规则视图。如果指定的服务器外联防护规则已经存在，则直接进入服务器外联防护规则视图。

undo rule 命令用来删除指定的服务器外联防护规则。

【命令】

rule rule-id

undo rule [*rule-id*]

【缺省情况】

不存在服务器外联防护规则。

【视图】

服务器外联防护策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-id: 表示服务器外联防护规则的编号，取值范围为 1~65535。

【使用指导】

服务器外联防护规则中可以配置服务器允许外联的 IP 地址、协议和端口号，在指定范围之外的连接都认为是非法外联行为。

执行 **undo** 命令时若不指定 *rule-id* 参数，则表示删除所有的服务器外联防护规则。

【举例】

创建编号为 1 的服务器外联防护规则，并进入此服务器外联防护规则视图。

<Sysname> system-view

```
[Sysname] scd policy name policy1
[Sysname-scd-policy-policy1] rule 1
[Sysname-scd-policy-policy1-1]
```

【相关命令】

- **display scd policy**

1.1.12 scd learning

scd learning 命令用来进入服务器外联学习视图。

undo scd learning 命令用来删除服务器外联学习视图下的所有配置。

【命令】

scd learning

undo scd learning

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

服务器外联学习功能会对指定服务器主动外联的流量进行检测，识别出服务器的所有外联行为。管理员可以通过学习结果来判断服务器的哪些外联是正常，哪些外联是异常，可为管理员配置服务器外联防护策略提供数据依据。

服务器外联学习中，无法删除服务器外联学习视图下的任何配置。

【举例】

```
<Sysname> system-view
[Sysname] scd learning
[Sysname-scd-learning]
```

1.1.13 scd policy

scd policy 命令用来创建服务器外联防护策略，并进入服务器外联防护策略视图。如果指定的服务器外联防护策略已经存在，则直接进入服务器外联防护策略视图。

undo scd policy 命令用来删除指定的服务器外联防护策略。

【命令】

scd policy name *policy-name*

undo scd policy [name *policy-name*]

【缺省情况】

不存在服务器外联防护策略。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

name *policy-name*: 表示服务器外联防护策略的名称，为 1~63 个字符的字符串，不区分大小写，且全局唯一。

【使用指导】

服务器外联防护策略中可以配置监测对象、监测规则、防护开关和日志功能。当发现待保护服务器出现异常外联系行为时，设备可以对其进行告警。此功能可以满足管理员对僵尸网络或内网持续渗透等行为的检测。

执行 **undo** 命令时若不指定 **name** 参数，则表示删除所有的服务器外联防护策略。

【举例】

```
# 创建名称为 policy1 的服务器外联防护策略，并进入此服务器外联防护策略视图。  
<Sysname> system-view  
[Sysname] scd policy name policy1  
[Sysname-scd-policy-policy1]
```

【相关命令】

- **display scd policy**

1.1.14 source-ip

source-ip 命令用来配置待防护的服务器。

undo source-ip 命令用来删除指定的待防护服务器。

【命令】

source-ip *object-group-name*
undo source-ip [*object-group-name*]

【缺省情况】

未配置待防护的服务器。

【视图】

服务器外联学习视图

【缺省用户角色】

network-admin
context-admin

【参数】

object-group-name: 表示地址对象组的名称，为 1~31 个字符的字符串，不区分大小写。有关地址对象组的详细介绍，请参见“安全配置指导”中的“对象组”。

【使用指导】

服务器外联学习功能通过引用地址对象组的方式指定待防护的服务器。指定待防护服务器后系统将对此服务器的外联行为进行学习。

多次执行本命令，可引用多个不同名称的地址对象组，最多不能超过 1024 个地址对象组。

若指定的地址对象组不存在，该配置仍会配置成功，同时也会在系统中创建一个名称为指定名称的空配置地址对象组。

服务器外联学习中，无法添加或删除待防护的服务器。

执行 **undo** 命令时若不指定 *object-group-name* 参数，则表示删除所有待防护的服务器。

【举例】

配置待防护的服务器，引用地址对象组 abc。

```
<Sysname> system-view
```

```
[Sysname] scd learning
```

```
[Sysname-scd-learning] source-ip abc
```

【相关命令】

- **object-group**（安全命令参考/对象组）



UNIS 入侵检测系统

DPI 深度安全命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《DPI 深度安全命令参考》主要介绍应用层检测引擎、IPS、URL 过滤、数据过滤、文件过滤、防病毒、数据分析中心和代理策略相关等命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。

格 式	意 义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 应用层检测引擎.....	1-1
1.1 应用层检测引擎配置命令.....	1-1
1.1.1 app-profile.....	1-1
1.1.2 authentication enable	1-1
1.1.3 block-period	1-2
1.1.4 capture-limit	1-3
1.1.5 display inspect md5-verify configuration.....	1-4
1.1.6 display inspect status	1-5
1.1.7 dns-server.....	1-5
1.1.8 email-server	1-6
1.1.9 export repeating-at.....	1-7
1.1.10 export url.....	1-8
1.1.11 inspect activate.....	1-8
1.1.12 inspect block-source parameter-profile	1-9
1.1.13 inspect bypass	1-10
1.1.14 inspect cache-option maximum	1-11
1.1.15 inspect capture parameter-profile	1-11
1.1.16 inspect cpu-threshold disable.....	1-12
1.1.17 inspect email parameter-profile	1-13
1.1.18 inspect file-uncompr-len	1-14
1.1.19 inspect logging parameter-profile.....	1-15
1.1.20 inspect md5-verify all-files.....	1-15
1.1.21 inspect optimization disable.....	1-16
1.1.22 inspect packet maximum	1-18
1.1.23 inspect redirect parameter-profile	1-18
1.1.24 inspect signature auto-update proxy.....	1-19
1.1.25 inspect source-port-identify enable.....	1-20
1.1.26 inspect stream-fixed-length disable	1-21
1.1.27 inspect stream-fixed-length	1-21
1.1.28 inspect tcp-reassemble enable.....	1-22
1.1.29 inspect tcp-reassemble max-segment.....	1-23
1.1.30 log	1-24
1.1.31 log language	1-25

1.1.32 password	1-25
1.1.33 receiver	1-26
1.1.34 redirect-url	1-27
1.1.35 secure-authentication enable	1-27
1.1.36 sender	1-28
1.1.37 username	1-29

1 应用层检测引擎

1.1 应用层检测引擎配置命令

1.1.1 app-profile

app-profile 命令用来创建 DPI 应用 profile，并进入 DPI 应用 profile 视图。如果指定的 DPI 应用 profile 已经存在，则直接进入 DPI 应用 profile 视图。

undo app-profile 命令用来删除指定的 DPI 应用 profile。

【命令】

```
app-profile profile-name  
undo app-profile profile-name
```

【缺省情况】

不存在 DPI 应用 profile。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

profile-name：表示 DPI 应用 profile 的名称，为 1~63 个字符的字符串，不区分大小写，且只能为字母、数字、下划线。

【使用指导】

DPI（Deep Packet Inspection，深度报文检测）应用 profile 是一个安全业务模板，通过在 DPI 应用 profile 中引用 DPI 各业务策略（例如 IPS 策略），并将其应用于安全策略规则中来实现报文的应用层检测功能。

【举例】

```
# 创建一个名称为 abc 的 DPI 应用 profile，并进入 DPI 应用 profile 视图。  
<Sysname> system-view  
[Sysname] app-profile abc  
[Sysname-app-profile-abc]
```

1.1.2 authentication enable

authentication enable 命令用来开启发送邮件的认证功能。

undo authentication enable 命令用来关闭发送邮件的认证功能。

【命令】

```
authentication enable
undo authentication enable
```

【缺省情况】

发送邮件的认证功能处于开启状态。

【视图】

应用层检测引擎邮件动作参数 **profile** 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

当通过命令 **email-server** 指定的邮件服务器需要认证时，可以开启发送邮件的认证功能，否则不需要开启此功能。

【举例】

```
# 关闭发送邮件的认证功能。
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] undo authentication enable
```

1.1.3 block-period

block-period 命令用来配置报文源 IP 地址被阻断的时长。

undo block-period 命令用来恢复缺省情况。

【命令】

```
block-period period
undo block-period
```

【缺省情况】

报文源 IP 地址被阻断的时长为 1800 秒。

【视图】

应用层检测引擎的源阻断动作参数 **profile** 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

period: 表示报文源 IP 地址被阻断的时长，取值范围为 1~86400，单位为秒。

【使用指导】

如果设备上同时开启了黑名单过滤功能，则报文的源 IP 地址被添加到 IP 黑名单表项后的老化时间为源阻断动作参数 **profile** 中配置的阻断时长。阻断时长之内，后续来自该源 IP 地址的报文将直接被黑名单过滤功能丢弃，不再进入应用层检测引擎中检测。

如果设备上未开启黑名单过滤功能，报文的源 IP 地址仍会被添加到 IP 黑名单表项中，但 IP 黑名单功能并未生效，后续来自该源 IP 地址的报文不会被黑名单过滤功能丢弃，仍将进入应用层检测引擎中处理。

有关黑名单过滤功能的详细介绍，请参见“安全配置指导”中的“攻击检测与防范”。

【举例】

在名称为 **b1** 的应用层检测引擎源阻断动作参数 **profile** 中，配置报文源 IP 地址被阻断的时长为 3600 秒。

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile b1
[Sysname-inspect-block-source-b1] block-period 3600
```

【相关命令】

- **blacklist enable** (security zone view)（安全命令参考/攻击检测与防范）
- **blacklist global enable**（安全命令参考/攻击检测与防范）
- **inspect block-source parameter-profile**

1.1.4 capture-limit

capture-limit 命令用来配置捕获报文的最大字节数。

undo capture-limit 命令用来恢复缺省情况。

【命令】

```
capture-limit kilobytes
undo capture-limit
```

【缺省情况】

捕获报文的最大字节数为 512 千字节。

【视图】

应用层检测引擎的捕获动作参数 **profile** 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

kilobytes：表示捕获报文的最大字节数，取值范围为 0～1024，单位为千字节。

【使用指导】

捕获到的报文将被缓存到设备本地，当缓存的报文字节数达到指定上限值时，系统会将缓存的报文上传到指定的 URL 上，并清空本地缓存，然后重新开始捕获报文。如果配置捕获报文的最大字节数为 0，则系统会将捕获到的报文立刻上传到指定的 URL 上。

【举例】

```
# 在名称为 c1 的应用层检测引擎捕获动作参数 profile 中，配置捕获报文的最大值为 1024 千字节。
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-c1] capture-limit 1024
```

【相关命令】

- export repeating-at
- export url
- inspect capture parameter-profile

1.1.5 display inspect md5-verify configuration

display inspect md5-verify configuration 命令用来显示 MD5 哈希运算配置。

【命令】

```
display inspect md5-verify configuration
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 显示 MD5 哈希运算配置。
<Sysname> system-view
[Sysname] display inspect md5-verify configuration
MD5 file verification for all files: Enabled
```

表1-1 display inspect md5-verify configuration 命令显示信息描述表

字段	描述
MD5 file verification for all files	MD5哈希运算功能状态，取值包括： • Enabled：表示应用层检测引擎对所有文件进行 MD5 哈希运算 • Disabled：表示应用层检测引擎对部分文件进行 MD5 哈希运算

【相关命令】

- `inspect md5-verify all-files`

1.1.6 `display inspect status`

`display inspect status` 命令用来显示应用层检测引擎的工作状态。

【命令】

`display inspect status`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示应用层检测引擎的运行状态。

```
<Sysname> display inspect status
Chassis 0 Slot 1:
  Running status: normal
```

表1-2 `display inspect status` 命令显示信息描述表

字段	描述
Running status	应用层检测引擎的运行状态，包括如下取值： • <code>bypass by configure</code>: 因为配置原因引擎无法处理报文 • <code>bypass by cpu busy</code>: 因为 CPU 使用率过高导致引擎无法处理报文 • <code>normal</code>: 引擎工作正常

1.1.7 `dns-server`

`dns-server` 命令用来配置域名解析服务器的 IPv4 地址。

`undo dns-server` 命令用来恢复缺省情况。

【命令】

`dns-server ip-address`
`undo dns-server`

【缺省情况】

未配置域名解析服务器的 IPv4 地址。

【视图】

应用层检测引擎邮件动作参数 **profile** 视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: 表示域名服务器的 IPv4 地址，为点分十进制格式。

【使用指导】

如果配置的邮件服务器的地址为主机名格式，当设备发送日志信息邮件时，需要通过域名解析服务器获取邮件服务器 IP 地址与主机名的映射关系。

【举例】

```
# 配置域名解析的服务器地址为 192.168.0.1。
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] dns-server 192.168.0.1
```

1.1.8 email-server

email-server 命令用来配置邮件服务器的地址。

undo email-server 命令用来恢复缺省情况。

【命令】

email-server *address-string*

undo email-server

【缺省情况】

未配置邮件服务器的地址。

【视图】

应用层检测引擎的邮件动作参数 **profile** 视图

【缺省用户角色】

network-admin

context-admin

【参数】

address-string: 表示邮件服务器的地址，为 3~63 个字符的字符串，区分大小写。

【使用指导】

配置的邮件服务器地址的地址既可以是邮件服务器的 IP 地址，也可以是邮件服务器的主机名。

采用主机名时，需要确保设备能通过静态或动态域名解析方式获得邮件服务器的 IP 地址，并与之路由可达。否则邮件发送会失败。有关域名解析功能的配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

在同一个邮件动作参数 **profile** 视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 配置邮件服务器地址为 rndcas.123.com。
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] email-server rndcas.123.com
# 配置邮件服务器地址为 192.168.1.1。
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] email-server 192.168.1.1
```

1.1.9 export repeating-at

export repeating-at 命令用来配置每天定时上传捕获报文的时间。

undo export repeating-at 命令用来恢复缺省情况。

【命令】

```
export repeating-at time
undo export repeating-at
```

【缺省情况】

每天凌晨 1 点定时上传捕获报文。

【视图】

应用层检测引擎的捕获动作参数 profile 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

time: 表示每天上传捕获报文的时间，格式为 hh:mm:ss，取值范围为 00:00:00~23:59:59。

【使用指导】

每天指定的时间到达时，无论本地缓存是否达到最大值，系统将向指定的 URL 上传缓存的捕获报文，并清空本地缓存。

【举例】

```
# 在名称为 c1 的应用层检测引擎捕获动作参数 profile 中，配置每天定时上传捕获报文的时间为凌晨 2 点。
<Sysname> system-view
[Sysname] inspect capture parameter-profile c1
[Sysname-inspect-capture-c1] export repeating-at 02:00:00
```

【相关命令】

- **capture-limit**
- **export url**
- **inspect capture parameter-profile**

1.1.10 export url

export url 命令用来配置上传捕获报文的 URL。

undo export url 命令用来恢复缺省情况。

【命令】

```
export url url-string  
undo export url
```

【缺省情况】

未配置上传捕获报文的 URL。

【视图】

应用层检测引擎的捕获动作参数 profile 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

url-string: 表示用于上传捕获报文的 URL，为 1~255 个字符的字符串。

【使用指导】

本地缓存的捕获的报文字节数达到指定上限值或者每天指定的时间到达时，系统会将缓存的报文上传到指定的 URL。如果未配置上传捕获报文的 URL，则系统依然会上传捕获到的报文并清空本地缓存，但是会上传失败。

【举例】

在名称为 c1 的应用层检测引擎捕获动作参数 profile 中，配置上传捕获报文的 URL 为 tftp://192.168.100.100/upload。

```
<Sysname> system-view  
[Sysname] inspect capture parameter-profile c1  
[Sysname-inspect-capture-c1] export url tftp://192.168.100.100/upload
```

【相关命令】

- **inspect capture parameter-profile**
- **capture-limit**
- **export repeating-at**

1.1.11 inspect activate

inspect activate 命令用来激活 DPI 各业务模块的策略和规则配置。

【命令】

```
inspect activate
```

【缺省情况】

DPI 各业务模块的策略和规则被创建、修改和删除时不生效。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

当 DPI 各业务模块（比如 URL 过滤业务）的策略和规则被创建、修改和删除后，需要执行 **inspect activate** 命令来使其策略和规则配置生效。

当 DPI 各业务模块的策略和规则被创建、修改和删除且保存配置的情况下，设备重启之后，其相关的所有策略和规则配置也会生效。

执行此命令会暂时中断 DPI 业务的处理，为了避免重复执行此命令对 DPI 业务造成影响，请完成部署 DPI 各业务模块的策略和规则后统一执行此命令。

【举例】

激活 DPI 各业务模块的策略和规则配置。

```
<Sysname> system-view
```

```
[Sysname] inspect activate
```

1.1.12 inspect block-source parameter-profile

inspect block-source parameter-profile 命令用来创建应用层检测引擎的源阻断动作参数 profile，并进入源阻断动作参数 profile 视图。如果指定的源阻断动作参数 profile 已经存在，则直接进入源阻断动作参数 profile 视图。

undo inspect block-source parameter-profile 命令用来删除应用层检测引擎的源阻断动作参数 profile。

【命令】

inspect block-source parameter-profile *parameter-name*

undo inspect block-source parameter-profile *parameter-name*

【缺省情况】

不存在源阻断动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

parameter-name：表示源阻断动作参数 profile 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

进入源阻断动作参数 **profile** 视图后，可以配置对报文执行源阻断动作时采用的特定参数，比如阻断时长。

【举例】

创建名称为 **b1** 的应用层检测引擎源阻断动作参数 **profile**，并进入源阻断动作参数 **profile** 视图。

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile b1
[Sysname-inspect-block-source-b1]
```

【相关命令】

- **block-period**

1.1.13 inspect bypass

inspect bypass 命令用来关闭应用层检测引擎功能。

undo inspect bypass 命令用来开启应用层检测引擎功能。

【命令】

```
inspect bypass
undo inspect bypass
```

【缺省情况】

应用层检测引擎功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

应用层检测引擎对报文的检测是一个复杂且会占用一定的系统资源的过程。开启应用层检测功能后，如果出现 CPU 使用率过高等情况时，可以通过关闭此功能来保证设备的正常运行。

关闭应用层检测引擎功能后，系统将不会对接收到的报文进行 DPI 深度安全处理。

【举例】

关闭应用层检测引擎功能。

```
<Sysname> system-view
[Sysname] inspect bypass
```

【相关命令】

- **display inspect status**

1.1.14 inspect cache-option maximum

inspect cache-option maximum 命令用来配置应用层检测引擎缓存待检测规则的选项的最大数目。

undo cache-option 命令用来恢复缺省情况。

【命令】

```
inspect cache-option maximum max-number  
undo inspect cache-option
```

【缺省情况】

应用层检测引擎缓存待检测规则的选项的最大数目为 32。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

max-number：指定应用层检测引擎在检测报文时，对每条 TCP/UDP 流缓存待检测规则的选项的最大数目，取值范围为 1~254。

【使用指导】

应用层检测引擎中的检测规则是由各个 DPI 业务模块中的规则或特征转换而成。一个检测规则可以对应多个关键字，每个关键字可对应多个选项。仅当关键字和选项全部匹配，该检测规则才能匹配成功。

当应用层检测引擎在检测一条 TCP/UDP 数据流时，首先匹配上了一个关键字，此时还不能确定检测规则是否匹配成功，还需要对该关键字所对应的所有选项进行匹配。若当前报文不能匹配到某个选项，则需要将该选项缓存，以便后续报文与之匹配；若选项成功匹配，则不进行缓存，继续匹配下一个选项。直到所有选项均成功匹配，数据流才能与该检测规则成功匹配。

通常，使用缺省配置即可满足用户需求。但是在某些场景中，为了提高应用层检测引擎对 TCP/UDP 数据流应用或行为的识别能力和准确率，需要将应用层检测引擎当前缓存待检测选项的最大数调高，调高后，每条数据流占用的内存可能会上升。同理某些场景下，设备内存使用率偏高，可以调低此参数，提高设备性能，以保证基础的数据转发正常进行。

【举例】

配置应用层检测引擎缓存待检测规则的选项的最大数目为 4。

```
<Sysname> system-view  
[Sysname] inspect cache-option maximum 4
```

1.1.15 inspect capture parameter-profile

inspect capture parameter-profile 命令用来创建应用层检测引擎的捕获动作参数 profile，并进入捕获动作参数 profile 视图。如果指定的捕获动作参数 profile 已经存在，则直接进入捕获动作参数 profile 视图。

undo inspect capture parameter-profile 命令用来删除应用层检测引擎的捕获动作参数 profile。

【命令】

```
inspect capture parameter-profile parameter-name  
undo inspect capture parameter-profile parameter-name
```

【缺省情况】

不存在捕获动作参数 profile。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

profile-name: 捕获动作参数 profile 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

进入捕获动作参数 profile 视图后，可以配置执行报文捕获动作时采用的特定参数，比如本地缓存报文的最大值字节数。目前，仅 IPS 功能支持。

【举例】

```
# 创建名称为 c1 的应用层检测引擎捕获动作参数 profile，并进入捕获动作参数 profile 视图。  
<Sysname> system-view  
[Sysname] inspect capture parameter-profile c1  
[Sysname-inspect-capture-c1]
```

【相关命令】

- **capture-limit**
- **export repeating-at**
- **export url**

1.1.16 inspect cpu-threshold disable

inspect cpu-threshold disable 命令用来关闭 CPU 门限响应功能。

undo inspect cpu-threshold disable 命令用来开启 CPU 门限响应功能。

【命令】

```
inspect cpu-threshold disable  
undo inspect cpu-threshold disable
```

【缺省情况】

CPU 门限响应功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

应用层检测引擎对报文的检测是一个比较复杂且会占用一定系统资源的过程。当设备的 CPU 利用率较高时，应用层检测引擎 CPU 门限响应功能会启动如下机制来缓解系统资源紧张的问题。

- 当 CPU 利用率达到设备上配置的 CPU 利用率阈值时，系统会自动关闭应用层检测引擎的检测功能来保证设备的正常运行。
- 当设备的 CPU 利用率恢复到或低于设备上配置的 CPU 利用率恢复阈值时，系统会恢复应用层检测引擎的检测功能。

在系统 CPU 占用率较高的情况下，不建议用户配置此命令。

【举例】

关闭 CPU 门限响应功能。

```
<Sysname> system-view
```

```
[Sysname] inspect cpu-threshold disable
```

【相关命令】

- **display inspect status**
- **inspect bypass**
- **inspect stream-fixed-length disable**

1.1.17 inspect email parameter-profile

inspect email parameter-profile 命令用来创建应用层检测引擎的邮件动作参数 profile，并进入邮件动作参数 profile 视图。如果指定的邮件动作参数 profile 已经存在，则直接进入邮件动作参数 profile 视图。

undo inspect email parameter-profile 命令删除应用层检测引擎邮件动作参数 profile。

【命令】

```
inspect email parameter-profile parameter-name
```

```
undo inspect email parameter-profile parameter-name
```

【缺省情况】

不存在邮件动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

parameter-name: 表示邮件动作参数 **profile** 的名称, 为 1~63 个字符的字符串, 不区分大小写。

【使用指导】

进入邮件动作参数 **profile** 视图后, 可以配置执行发送邮件动作时采用的特定参数, 比如邮件服务器的地址、发件人与收件人的地址和登录邮件服务器的用户名和密码等信息。

【举例】

创建名称为 **c1** 的应用层检测引擎邮件动作参数 **profile**, 并进入邮件动作参数 **profile** 视图。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1]
```

1.1.18 inspect file-uncompr-len

inspect file-uncompr-len 命令用来配置可解压缩数据上限。

undo inspect file-uncompr-len 命令用来恢复缺省情况。

【命令】

```
inspect file-uncompr-len max-size
undo inspect file-uncompr-len
```

【缺省情况】

可解压缩数据上限为 100MB。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

max-size: 表示可解压缩数据上限, 取值范围为 1~200, 单位为 MB。

【使用指导】

可解压缩数据上限是指设备解压一个文件时可解压缩数据的最大值。到达上限后, 该文件的剩余数据不再进行解压。

如果配置的可解压缩数据过大, 当设备频繁收到过大的压缩文件时, 设备将一直解压缩一个文件, 会影响后续文件的解压缩, 并影响设备的转发性能; 如果配置的可解压缩数据过小, 设备将不能识别压缩文件中的部分内容, 从而对 DPI 业务 (例如防病毒和数据过滤业务) 的检测结果产生影响。请管理员合理配置此参数。

目前, 仅支持解压缩 ZIP 格式的文件。

【举例】

配置最大解压缩数据大小为 150MB。

```
<Sysname> system-view
```

```
[Sysname] inspect file-uncompr-len 150
```

1.1.19 inspect logging parameter-profile

inspect logging parameter-profile 命令用来创建应用层检测引擎的日志动作参数 **profile**，并进入日志动作参数 **profile** 视图。如果指定的日志动作参数 **profile** 已经存在，则直接进入日志动作参数 **profile** 视图。

undo inspect logging parameter-profile 命令用来删除应用层检测引擎的日志动作参数 **profile**。

【命令】

```
inspect logging parameter-profile parameter-name
```

```
undo inspect logging parameter-profile parameter-name
```

【缺省情况】

不存在日志动作参数 **profile**。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

profile-name: 日志动作参数 **profile** 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

进入日志动作的参数 **profile** 视图后，可以配置生成报文日志时采用的特定参数，比如输出日志的方式。

【举例】

创建名称为 **log1** 的应用层检测引擎的日志动作参数 **profile**，并进入日志动作参数 **profile** 视图。

```
<Sysname> system-view
```

```
[Sysname] inspect logging parameter-profile log1
```

```
[Sysname-inspect-logging-log1]
```

【相关命令】

- **log**

1.1.20 inspect md5-verify all-files

inspect md5-verify all-files 命令用来配置应用层检测引擎对所有文件进行 MD5 哈希运算。

undo inspect md5-verify all-files 命令用来恢复缺省情况。

【命令】

```
inspect md5-verify all-files
```

undo inspect md5-verify all-files

【缺省情况】

只对可执行文件、office 文件和压缩文件等文件进行 MD5 哈希运算。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启此功能后，应用层检测引擎将对所有文件进行 MD5 哈希运算，并将生成的 MD5 值与特征库中的 MD5 规则进行匹配。如果匹配成功，则认为该文件携带病毒。

开启此功能后将对设备业务处理性能产生影响，请管理员根据设备实际情况进行配置。

【举例】

配置应用层检测引擎对所有文件进行 MD5 哈希运算。

```
<Sysname> system-view
[Sysname] inspect md5-verify all-files
```

【相关命令】

- **display inspect md5-verify configuration**

1.1.21 inspect optimization disable

inspect optimization disable 命令用来关闭指定的应用层检测引擎的优化调试功能。

undo inspect optimization disable 命令用来开启指定的应用层检测引擎的优化调试功能。

【命令】

```
inspect optimization [ chunk | no-acsignature | raw | uncompress |
url-normalization ] disable
undo inspect optimization [ chunk | no-acsignature | raw | uncompress |
url-normalization ] disable
```

【缺省情况】

应用层检测引擎的所有优化调试功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

chunk：表示应用层检测引擎对 Chunk 格式报文进行解码的优化调试功能。

no-acssignature: 表示应用层检测引擎对没有关键字检测规则进行检测的优化调试功能。

raw: 表示应用层检测引擎对未经解码 TCP/UDP 的应用层载荷字段进行检测的优化调试功能。

uncompress: 表示应用层检测引擎对 HTTP Body 字段进行解压缩的优化调试功能。

url-normalization: 表示应用层检测引擎对 HTTP URL 字段进行正规化校准的优化调试功能。

【使用指导】

如果不指定任何参数，则表示关闭或开启应用层检测引擎的所有优化调试功能。

有关应用层检测引擎的各种优化调试功能的详细介绍如下：

- 应用层检测引擎对 **Chunk** 格式报文进行解码的优化调试功能：**Chunk** 是 HTTP 协议载荷(Body)的一种传输方式，对于以 **Chunk** 方式传输的 HTTP 协议的载荷，需要先对其进行解码以获取真正的载荷内容。但是在某些应用场景下，设备的处理性能不能满足用户基本的通信需求，这时，关闭应用层检测引擎解码 **Chunk** 格式报文的功能，可以提高设备的吞吐量。但是配置关闭应用层检测引擎解码 **Chunk** 格式报文的功能后，应用层检测引擎对某些针对安全漏洞的攻击行为不能被识别。
- 应用层检测引擎对没有关键字检测规则进行检测的优化调试功能：没有关键字的检测规则是指此规则不是基于字符串匹配进行检测，而是基于报文的端口号、错误码等字段进行检测。缺省情况下应用层检测引擎对没有关键字的检测规则进行检测，但是在某些场景下，如果设备的吞吐量较差，不能满足客户基本的通信需求，此时可以配置应用层检测引擎对没有关键字的检测规则不进行检测，以提高设备的性能，保证用户最基础的网络通信。
- 应用层检测引擎对未经解码 TCP/UDP 的应用层载荷字段进行检测的优化调试功能：有些 TCP/UDP 数据流的应用层协议（例如 HTTP、SMTP、POP3、IMAP4）涉及编码和解码处理，而对该类数据流的应用层内容的检测需要在对报文载荷进行解码之后进行。如果当前设备的处理性能不能满足用户基本的通信需求，可以通过该命令取消对未解码的应用层载荷字段的检测，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对报文载荷内容的应用或行为的识别能力会受到影响。
- 应用层检测引擎对 HTTP Body 字段进行解压缩的优化调试功能：如果报文的 HTTP Body 字段是压缩编码，应用层检测引擎需要先对 HTTP Body 字段进行解压缩后，才能对此字段的内容进行检测。但是在某些应用场景下，设备的处理性能不能满足用户基本的通信需求，这时，可以通过配置此命令来取消对 HTTP Body 字段的压缩编码进行解压缩处理，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对某些针对安全漏洞的攻击行为不能被识别。
- 应用层检测引擎对 HTTP URL 字段进行正规化校准的优化调试功能：对 HTTP URL 字段进行正规化校准功能是指把 URL 中绝对路径字调整为常规路径格式，对特殊的路径字段进行调整和正确性检查。例如报文 URL 中绝对路径部分输入的是 test/dpi/./index.html，正规化处理后是 test/index.html。但是在某些应用场景下，设备的处理性能不能满足用户基本的通信需求，这时，可以通过配置此命令来取消对 HTTP URL 字段进行正规化校准处理，以提高设备的吞吐量。但是配置此功能后，应用层检测引擎对某些针对安全漏洞的攻击行为不能被识别。

【举例】

关闭应用层检测引擎的所有优化调试功能。

```
<Sysname> system-view
```

```
[Sysname] inspect optimization disable
```

1.1.22 inspect packet maximum

inspect packet maximum 命令用来配置应用层检测引擎可检测有载荷内容的报文的最大数目。

undo inspect packet 命令用来恢复缺省情况。

【命令】

inspect packet maximum *max-number*

undo inspect packet

【缺省情况】

应用层检测引擎可检测有载荷内容的报文的最大数目为 32。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

max-number：指定应用层检测引擎检测有载荷内容的报文的最大数目，取值范围为 1～254。

【使用指导】

应用层检测引擎在对一个数据流的第一个有载荷内容的报文进行检测时，如果没有匹配上任何检测规则，则需要继续检测此数据流的第二个有载荷内容的报文，以此类推。如果直到设备设置的最大报文检测个数还未匹配上任何检测规则，则表示对此数据流匹配失败，并直接允许此数据流通过。通常，使用缺省配置即可满足应用需求。但是在某些应用场景中，应用层检测引擎在检测有载荷内容的报文的个数达到指定的个数之后，仍然不能识别当前报文应用层信息的应用或行为，此时需要调高这个参数。调高此参数后，设备的吞吐量性能会下降，但是应用识别的成功率会增加。同理在设备吞吐量较差，不能满足客户需求的应用场景中，此时需要调低这个参数，调低参数后，吞吐量会增加，但是应用识别成功率会降低。

【举例】

配置应用层检测引擎可检测有载荷内容的报文的最大数目为 16。

```
<Sysname> system-view
```

```
[Sysname] inspect packet maximum 16
```

1.1.23 inspect redirect parameter-profile

inspect redirect parameter-profile 命令用来创建应用层检测引擎的重定向动作参数 profile，并进入重定向动作参数 profile 视图。如果指定的重定向动作参数 profile 已经存在，则直接进入重定向动作参数 profile 视图。

undo inspect redirect parameter-profile 命令用来删除应用层检测引擎的重定向动作参数 profile。

【命令】

inspect redirect parameter-profile *parameter-name*

undo inspect redirect parameter-profile *parameter-name*

【缺省情况】

不存在重定向动作参数 *profile*。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

parameter-name: 重定向动作参数 *profile* 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

进入重定向动作参数 *profile* 视图后，可以配置对报文执行重定向动作时采用的特定参数，比如对报文重定向的 URL。

【举例】

创建名称为 *r1* 的应用层检测引擎重定向动作参数 *profile*，并进入重定向动作参数 *profile* 视图。

```
<Sysname> system-view  
[Sysname] inspect redirect parameter-profile r1  
[Sysname-inspect-redirect-r1]
```

1.1.24 inspect signature auto-update proxy

inspect signature auto-update proxy 命令用来配置 DPI 业务特征库在线升级所使用的代理服务器。

undo inspect signature auto-update proxy 命令用来恢复缺省情况。

【命令】

```
inspect signature auto-update proxy { domain domain-name | ip ip-address }  
[ port port-number ] [ user user-name password { cipher | simple } string ]  
undo inspect signature auto-update proxy
```

【缺省情况】

未配置 DPI 业务特征库在线升级所使用的代理服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain *domain-name*: 指定代理服务器的域名。*domain-name* 表示代理服务器的域名，为 3~63 个字符的字符串，不区分大小写。

ip ip-address: 指定代理服务器的 IP 地址，仅支持 IPv4 类型地址。

port port-number: 指定代理服务器的端口号，取值范围为 1~65535，缺省值为 80。

user user-name: 指定登录代理服务器的用户名。*user-name* 表示用户名，为 1~31 个字符的字符串，不区分大小写。

password: 指定登录代理服务器的用户密码。

cipher: 表示以密文方式设置密码。

simple: 表示以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~31 个字符的字符串，密文密码为 1~73 个字符的字符串。

【使用指导】

当 DPI 业务模块（例如 URL 过滤业务）的特征库进行在线升级时，若设备不能连接到官方网站，则可配置一个代理服务器使设备连接到官方网站上的特征库服务专区，进行特性库在线升级。有关特征库在线升级功能的详细介绍，请参见各 DPI 业务配置指导手册中的“特征库升级与回滚”。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 DPI 业务特征库在线升级所使用的代理服务器域名为 **www.abc.com**，端口号为 **8888**，登录代理服务器的用户名和密码均为 **admin**。

```
<Sysname> system-view
[Sysname] inspect signature auto-update proxy domain www.abc.com port 8888 user admin
password simple admin
```

1.1.25 inspect source-port-identify enable

inspect source-port-identify enable 命令用来开启基于源端口的应用识别功能。

undo inspect source-port-identify enable 命令用来关闭基于源端口的应用识别功能。

【命令】

```
inspect source-port-identify enable
undo inspect source-port-identify enable
```

【缺省情况】

基于源端口的应用识别功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

如果网络中的流量种类单一、源端口固定，但无法通过目的端口对其进行基于端口的应用识别或无法基于流量特征进行内容识别时，可以开启本功能，对流量进行源端口识别，将源端口为固定端口的流量识别为访问特定类型应用的流量。

开启本功能后，可能会造成应用识别结果的误报，请管理员根据组网环境的实际情况配置。

【举例】

```
# 开启基于源端口的应用识别功能。
<sysname> system-view
[sysname] inspect source-port-identify enable
```

1.1.26 inspect stream-fixed-length disable

inspect stream-fixed-length disable 命令用来关闭应用层检测引擎检测固定长度数据流功能。

undo inspect stream-fixed-length disable 命令用来开启应用层检测引擎检测固定长度数据流功能。

【命令】

```
inspect stream-fixed-length disable
undo inspect stream-fixed-length disable
```

【缺省情况】

应用层检测引擎检测固定长度数据流功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

应用层检测引擎检测固定长度数据流功能，是指应用层检测引擎只检测每条数据流首包后固定长度内的数据，不再检测超出固定长度后的数据。

【举例】

```
# 关闭应用层检测引擎检测固定长度数据流功能。
<Sysname> system-view
[Sysname] inspect stream-fixed-length disable
```

【相关命令】

- **inspect cpu-threshold disable**
- **inspect stream-fixed-length**

1.1.27 inspect stream-fixed-length

inspect stream-fixed-length 命令用来配置应用层检测引擎检测数据流的固定长度。

undo inspect stream-fixed-length 命令用来恢复缺省情况。

【命令】

```
inspect stream-fixed-length { email | ftp | http } * length
```

undo inspect stream-fixed-length

【缺省情况】

应用层检测引擎对 FTP 协议、HTTP 协议和与 E-mail 相关协议数据流的固定检测长度均为 32 千字节。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

email: 表示设置检测与 E-mail 协议相关类型数据流的固定长度，支持的 E-mail 协议包括 SMTP、POP3 和 IMAP。

ftp: 表示设置检测 FTP 协议类型数据流的固定长度。

http: 表示设置检测 HTTP 协议类型数据流的固定长度。

length: 表示设置检测指定协议类型数据流的固定长度，取值范围为 1~2048，单位为千字节。

【使用指导】

调高此参数后，设备的吞吐量性能会下降，但是应用层信息识别的成功率会提高；同理调低参数后，设备的吞吐量会增加，但是应用层信息识别的成功率会降低。

【举例】

配置应用层检测引擎检测 FTP 协议类型数据流的固定长度为 35 千字节，检测 HTTP 协议类型数据流的固定长度为 40 千字节。

```
<Sysname> system-view
```

```
[Sysname] inspect stream-fixed-length ftp 35 http 40
```

【相关命令】

- **inspect cpu-threshold disable**
- **inspect stream-fixed-length disable**

1.1.28 inspect tcp-reassemble enable

inspect tcp-reassemble enable 命令用来开启 TCP 数据段重组功能。

undo inspect tcp-reassemble enable 命令用来关闭 TCP 数据段重组功能。

【命令】

inspect tcp-reassemble enable

undo inspect tcp-reassemble enable

【缺省情况】

TCP 数据段重组功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

大量的 TCP 乱序数据段极有可能会造成应用层检测引擎对此 TCP 数据流检测失败。例如应用层检测引擎需要检测 TCP 载荷中是否包含关键字“this is a secret”，由于数据段乱序，可能含有“a secret”的数据段先到达设备，含有“this is”的数据段后到达设备，这样就会造成应用层检测引擎对此 TCP 数据流检测失败。

为了提高应用层检测引擎对 TCP 数据流检测的准确率，可以在设备上开启 TCP 数据段重组功能。当接收到乱序的 TCP 数据段时，设备会将此数据段和来自于同一条数据流的后续数据段暂时保存至缓冲区，进行 TCP 数据段重组，完成数据段重组再送往后续流程处理。

若缓冲区中已缓存的数据段数目达到最大值（可以通过 **inspect tcp-reassemble max-segment** 命令来配置）时仍无法成功重组，则设备直接将已缓存的乱序数据段和此条数据流的所有后续 TCP 数据段送往后续流程处理，不再进行 TCP 重组。这样可以降低对设备转发性能的影响。

【举例】

```
# 开启 TCP 数据段重组功能。  
<Sysname> system-view  
[Sysname] inspect tcp-reassemble enable
```

【相关命令】

- **inspect tcp-reassemble max-segment**

1.1.29 inspect tcp-reassemble max-segment

inspect tcp-reassemble max-segment 命令用来配置 TCP 重组缓冲区可缓存的 TCP 数据段最大数目。

undo inspect tcp-reassemble max-segment 命令用来恢复缺省情况。

【命令】

```
inspect tcp-reassemble max-segment max-number  
undo inspect tcp-reassemble max-segment
```

【缺省情况】

TCP 重组缓冲区可缓存的 TCP 数据段最大数目为 10。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

max-number: 表示 TCP 重组缓冲区可缓存的 TCP 数据段最大数目，取值范围为 10~50。

【使用指导】

在存在大量 TCP 乱序数据段的网络环境中，调高此参数，则可提高应用层检测引擎对 TCP 数据段检测的准确率，但是设备转发性能可能会下降。若调低此参数可避免因长时间缓存 TCP 数据段而造成设备转发性能下降，但是应用层检测引擎对 TCP 数据段检测的准确率会降低。请根据实际情况调整此参数。

本命令仅在开启 TCP 数据段重组功能后生效。

【举例】

配置 TCP 重组缓冲区中可缓存的 TCP 数据段最大数目为 20。

```
<Sysname> system-view
[Sysname] inspect tcp-reassemble max-segment 20
```

【相关命令】

- **inspect tcp-reassemble enable**

1.1.30 log

log 命令用来配置记录报文日志的方式。

undo log 命令用来取消指定的记录报文日志的方式。

【命令】

```
log { email | syslog }
undo log { email | syslog }
```

【缺省情况】

报文日志被输出到信息中心。

【视图】

应用层检测引擎的日志动作参数 profile 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

email: 表示将日志以邮件的方式发送到指定的收件人邮箱。

syslog: 表示将日志输出到信息中心。

【举例】

在名称为 log1 的应用层检测引擎日志动作参数 profile 中，配置将生成的报文日志输出到信息中心。

```
<Sysname> system-view
[Sysname] inspect logging parameter-profile log1
[Sysname-inspect-logging-log1] log syslog
```

【相关命令】

- **inspect logging parameter-profile**

1.1.31 log language

log language 命令用来配置记录 IPS 日志使用的语言为中文。

undo log language 命令用来恢复缺省情况。

【命令】

log language chinese

undo log language chinese

【缺省情况】

记录报文日志使用的语言为英文。

【视图】

应用层检测引擎的日志动作参数 profile 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

执行本命令后，设备输出的日志中，仅 IPS 日志的威胁名称字段使用中文描述，其它日志信息仍然为英文。有关 IPS 日志的详情介绍，请参见“DPI 深度安全命令参考”中的“IPS”。

【举例】

在名称为 log1 的应用层检测引擎日志动作参数 profile 中，配置记录 IPS 日志使用的语言为中文。

```
<Sysname> system-view
```

```
[Sysname] inspect logging parameter-profile log1
```

```
[Sysname-inspect-log-para-log1] log language chinese
```

【相关命令】

- **inspect logging parameter-profile**

1.1.32 password

password 命令用来配置登录邮件服务器的密码。

undo password 命令用来恢复缺省情况。

【命令】

password { cipher | simple } string

undo password

【缺省情况】

未配置登录邮件服务器的密码。

【视图】

应用层检测引擎邮件动作参数 profile 视图

【缺省用户角色】

network-admin
context-admin

【参数】

cipher: 表示以密文方式设置用户密码。

simple: 表示以明文方式设置用户密码，该密码将以密文形式存储。

string: 表示登录邮件服务器的密码。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串，区分大小写。

【使用指导】

在同一个邮件动作参数 **profile** 视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 配置登录邮件服务器的明文密码为 abc123。  
<Sysname> system-view  
[Sysname] inspect email parameter-profile c1  
[Sysname-inspect-email-c1] password simple abc123
```

【相关命令】

- **authentication enable**

1.1.1.33 receiver

receiver 命令用来配置收件人地址。

undo receiver 命令用来恢复缺省情况。

【命令】

receiver *address-string*
undo receiver

【缺省情况】

未配置收件人地址。

【视图】

应用层检测引擎邮件动作参数 **profile** 视图

【缺省用户角色】

network-admin
context-admin

【参数】

address-string: 表示收件人地址，为 3~511 个字符的字符串，区分大小写。

【使用指导】

收件人地址可以同时输入多个，且每个收件人地址之间用英文 “;” 号隔开。

【举例】

```
# 配置收件人的地址为 123@abc.com 和 nnn@abc.com。
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] receiver 123@abc.com;nnn@abc.com
```

1.1.34 redirect-url

redirect-url 命令用来配置重定向 URL。

undo redirect-url 命令用来恢复缺省情况。

【命令】

```
redirect-url url-string
undo redirect-url
```

【缺省情况】

未配置重定向 URL。

【视图】

应用层检测引擎的重定向动作参数 profile 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

url-string: 表示重定向 URL，为 9~63 个字符的字符串，区分大小写。该 URL 必须以 http:// 或 https:// 开头，例如 http://www.baidu.com。

【使用指导】

当需要把匹配成功的报文重定向到某个 Web 界面时，可以通过执行此命令来指定重定向 URL。

【举例】

```
# 配置重定向 URL 为 http://www.abc.com/upload。
<Sysname> system-view
[Sysname] inspect redirect parameter-profile r1
[Sysname-inspect-redirect-r1] redirect-url http://www.abc.com/upload
```

【相关命令】

- **inspect redirect parameter-profile**

1.1.35 secure-authentication enable

secure-authentication enable 命令用来开启安全传输登录邮件服务器密码功能。

undo secure-authentication enable 命令用来关闭安全传输登录邮件服务器密码功能。

【命令】

```
secure-authentication enable
```

undo secure-authentication enable

【缺省情况】

安全传输登录邮件服务器密码功能处于关闭状态。

【视图】

应用层检测引擎邮件动作参数 **profile** 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启此功能后，首先在设备与邮件服务器之间创建一条安全通道，再从此通道中传输登录邮件服务器的密码。

【举例】

开启安全传输登录邮件服务器密码功能。

```
<Sysname> system-view
```

```
[Sysname] inspect email parameter-profile c1
```

```
[Sysname-inspect-email-c1] secure-authentication enable
```

【相关命令】

- **authentication enable**

1.1.36 sender

sender 命令用来配置发件人地址。

undo sender 命令用来恢复缺省情况。

【命令】

sender *address-string*

undo sender

【缺省情况】

未配置发件人地址。

【视图】

应用层检测引擎邮件动作参数 **profile** 视图

【缺省用户角色】

network-admin

context-admin

【参数】

address-string: 表示发件人地址，为 3~63 个字符的字符串，区分大小写。

【使用指导】

发件人地址是指设备向目的地发送邮件时使用的源地址。

【举例】

```
# 配置发件人的地址为 abc@123.com。
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] sender abc@123.com
```

1.1.37 username

username 命令用来配置登录邮件服务器的用户名。

undo username 命令用来恢复缺省情况。

【命令】

```
username name-string
undo username
```

【缺省情况】

未配置登录邮件服务器的用户名。

【视图】

应用层检测引擎邮件动作参数 **profile** 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

name-string: 表示登录邮件服务器的用户名。为 1~63 个字符的字符串，区分大小写。

【使用指定】

在同一个邮件动作参数 **profile** 视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 配置登录邮件服务器的用户名为 han。
<Sysname> system-view
[Sysname] inspect email parameter-profile c1
[Sysname-inspect-email-c1] username han
```

【相关命令】

- **authentication enable**

目 录

1 IPS	1-1
1.1 IPS配置命令	1-1
1.1.1 action	1-1
1.1.2 attack-category	1-1
1.1.3 display ips policy	1-2
1.1.4 display ips signature	1-4
1.1.5 display ips signature { pre-defined user-defined }	1-7
1.1.6 display ips signature library	1-9
1.1.7 display ips signature user-defined parse-failed	1-10
1.1.8 ips apply policy	1-11
1.1.9 ips parameter-profile	1-12
1.1.10 ips policy	1-13
1.1.11 ips signature auto-update	1-14
1.1.12 ips signature auto-update-now	1-14
1.1.13 ips signature import snort	1-15
1.1.14 ips signature remove snort	1-17
1.1.15 ips signature rollback	1-17
1.1.16 ips signature update	1-18
1.1.17 ips signature update-log	1-20
1.1.18 object-dir	1-20
1.1.19 override-current	1-21
1.1.20 protect-target	1-22
1.1.21 severity-level	1-23
1.1.22 signature override	1-23
1.1.23 signature override all	1-25
1.1.24 update schedule	1-26

1 IPS

1.1 IPS配置命令

1.1.1 action

action 命令用来配置筛选 IPS 特征的动作属性。

undo action 命令用来恢复缺省情况。

【命令】

```
action { block-source | drop | permit | reset } *  
undo action
```

【缺省情况】

未配置动作属性筛选条件。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

block-source: 表示源阻断动作，该动作阻断符合特征的报文，并将该报文的源 IP 地址加入 IP 黑名单。

drop: 表示丢弃报文的动作。

permit: 表示允许报文通过的动作。

reset: 表示重置动作，该动作通过发送 TCP 的 reset 报文使 TCP 连接断开。

【使用指导】

可通过配置动作属性筛选出具有该属性的特征，IPS 策略将使用筛选出的特征与报文进行匹配。可同时配置多个动作，只要符合其中一个，具有该动作属性的特征将会被筛选出来。

多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 test 的 IPS 策略中配置筛选 IPS 特征的动作作为 drop 和 reset。

```
<Sysname> system-view  
[Sysname] ips policy test  
[Sysname-ips-policy-test] action drop reset
```

1.1.2 attack-category

attack-category 命令用来配置筛选 IPS 特征的攻击分类属性。

undo attack-category 命令用来删除筛选 IPS 特征的攻击分类属性。

【命令】

```
attack-category { category [ subcategory ] | all }  
undo attack-category { category [ subcategory | all ] }
```

【缺省情况】

未配置攻击分类属性筛选条件。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

category: 表示设备中已有的攻击分类名称。

subcategory: 表示设备中已有攻击分类中的子分类名称。若不指定本参数，则表示指定攻击分类中的所有子分类。

all: 表示设备中已有的所有攻击分类。

【使用指导】

可通过配置攻击分类属性筛选出具有该属性的特征，IPS 策略将使用筛选出的特征与报文进行匹配。可多次执行本命令，配置多个攻击分类。只要符合其中一个，具有该攻击分类的特征将会被筛选出来。

【举例】

在名称为 test 的 IPS 策略中，配置筛选 IPS 特征的攻击分类为 Vulnerability 攻击分类中的 SQLInjection 子分类。

```
<Sysname> system-view  
[Sysname] ips policy test  
[Sysname-ips-policy-test] attack-category Vulnerability SQLInjection
```

1.1.3 display ips policy

display ips policy 命令用来显示 IPS 策略信息。

【命令】

```
display ips policy policy-name
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

policy-name: 表示 IPS 策略名称，为 1~63 个字符的字符串，不区分大小写。

【举例】

显示 IPS 策略 aa 的策略信息。

```
<Sysname> display ips policy aa
```

```
Total signatures           :10929      failed:0
```

```
Pre-defined signatures:10925      failed:0
```

```
User-defined signatures:4         failed:0
```

Flag:

B: Block-Source D: Drop P: Permit Rs: Reset Rd: Redirect C: Capture L: Logging

Pre: predefined User: user-defined

Type	RuleID	Target	SubTarget	Severity	Direction	Category
	SubCategory	Status	Action			
Pre	1	OperationSystem	LinuxUnix	High	Server	Vulnerability
	RemoteCodeExecu	Enable	RsL			
Pre	2	OperationSystem	LinuxUnix	High	Server	Vulnerability
	MemoryCorruptio	Enable	RsL			
Pre	4	OfficeSoftware	MicrosoftOffice	High	Any	Vulnerability
	Overflow	Enable	RsL			
Pre	5	OfficeSoftware	MicrosoftOffice	High	Any	Vulnerability
	MemoryCorruptio	Enable	RsL			
Pre	6	Browser	InternetExplore	High	Any	Vulnerability
	MemoryCorruptio	Enable	RsL			
Pre	7	Browser	InternetExplore	High	Any	Vulnerability
	MemoryCorruptio	Enable	RsL			
Pre	8	ApplicationSoft	MediaPlayer	High	Any	Vulnerability
	RemoteCodeExecu	Enable	RsL			
Pre	9	ApplicationSoft	Security	High	Server	Vulnerability
	Overflow	Enable	DL			
Pre	10	Browser	InternetExplore	High	Server	Vulnerability
	InsecureLibrary	Enable	RsL			
Pre	11	Browser	InternetExplore	High	Any	InformationDis
	c SensitiveInfo	Enable	RsL			
Pre	12	OfficeSoftware	MicrosoftOffice	Critical	Any	Vulnerability
	RemoteCodeExecu	Enable	RsL			
Pre	13	OfficeSoftware	MicrosoftOffice	High	Any	Vulnerability
	MemoryCorruptio	Enable	RsL			
Pre	14	ApplicationSoft	IM	High	Server	Vulnerability
	InsecureLibrary	Enable	RsL			
Pre	15	Browser	InternetExplore	High	Any	Vulnerability
	RemoteCodeExecu	Enable	RsL			
----	More	----				

表1-1 display ips policy 命令显示信息描述表

字段	描述
Total signatures	IPS特征总数
Pre-defined signatures	预定义IPS特征数目
User-defined signatures	用户自定义IPS特征数目
Type	IPS特征的类型，包括如下取值： - Pre: 表示预定义特征 - User: 表示自定义特征
RuleID	IPS特征编号
Target	攻击对象
SubTarget	攻击子对象
Severity	IPS特征的攻击严重程度属性，从低到高分四级：Low、Medium、High、Critical
Direction	IPS特征的匹配方向，包括如下取值： - Any: 表示从服务器到客户端方向和从客户端到服务器方向上的对象 - Client: 表示从服务器到客户端方向上的对象 - Server: 表示从客户端到服务器方向上的对象
Category	IPS特征的攻击类别名称
Subcategory	IPS特征的攻击分类中的子分类名称
Status	IPS特征的状态，包括如下取值： - Enabled: 表示此特征已生效 - Disabled: 表示此特征未生效
Action	对报文的处理动作，包括如下取值： - Block-source: 表示阻断符合特征的报文，并将该报文的源 IP 地址加入 IP 黑名单 - Drop: 表示丢弃符合特征的报文 - Permit: 表示允许符合特征的报文通过 - Reset: 表示发送 TCP 的 reset 报文或 UDP 的 ICMP 端口不可达报文使 TCP 或 UDP 连接断开 - Redirect: 表示重定向符合特征的报文 - Capture: 表示捕获符合特征的报文 - Logging: 表示对符合特征的报文生成日志

【相关命令】

- ips policy

1.1.4 display ips signature

display ips signature 命令用来显示 IPS 特征信息。

【命令】

```
display ips signature [ pre-defined | user-defined ] [ direction { any |  
to-client | to-server } ] [ category category-name | fidelity { high | low |  
medium } | protocol { icmp | ip | tcp | udp } | severity { critical | high |  
low | medium } ] *
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

pre-defined: 显示预定义 IPS 特征。

user-defined: 显示自定义 IPS 特征。

direction { any | to-client | to-server }: 显示符合指定方向属性的 IPS 特征。如果未指定此参数，则显示所有方向上的 IPS 特征。

- **to-server:** 表示一个会话的客户端到服务器的方向。
- **to-client:** 表示一个会话的服务器到客户端的方向。
- **any:** 表示一个会话的两个方向。

category category-name: 显示符合指定攻击类别属性的 IPS 特征，*category-name* 是攻击类型的名称，可通过输入“?”获取支持的攻击类型名称。如果未指定此参数，则显示所有攻击类型的 IPS 特征。

fidelity { high | low | medium }: 显示符合指定可信度属性的 IPS 特征。如果未指定此参数，则显示所有可信度的 IPS 特征。可信度是指此 IPS 特征识别攻击行为准确度，且从低到高分如下三个级别：

- **low:** 可信度比较低。
- **medium:** 可信度中等。
- **high:** 可信度比较高。

protocol { icmp | ip | tcp | udp }: 显示符合指定协议属性的 IPS 特征，协议 ICMP、IP、TCP 和 UDP 协议。如果未指定此参数，则显示所有协议的 IPS 特征。

severity { critical | high | low | medium }: 显示符合指定严重级别属性的 IPS 特征。如果未指定此参数，则显示所有严重级别的 IPS 特征。严重级别是指匹配此 IPS 特征的网络攻击造成危害的严重程度，且从低到高分四个级别：

- **low:** 攻击严重程度比较低。
- **medium:** 攻击严重程度中等。
- **high:** 攻击严重程度比较高。
- **critical:** 攻击严重程度非常高。

【使用指导】

若不指定任何参数，则显示所有 IPS 特征。

【举例】

显示可信度为中等的所有 TCP 协议的预定义 IPS 特征。

```
<Sysname> display ips signature pre-defined protocol tcp fidelity medium
```

```
Pre-defined signatures:465          failed:0
```

Flag:

Pre: predefined User: user-defined

Type	Sig-ID	Direction	Severity	Fidelity	Category	Protocol
Pre	1	To-server	High	Medium	Vulnerability	TCP
Pre	2	To-server	High	Medium	Vulnerability	TCP
Pre	3	To-client	High	Medium	Vulnerability	TCP
Pre	4	To-client	High	Medium	Vulnerability	TCP
Pre	5	To-client	High	Medium	Vulnerability	TCP
Pre	6	To-client	High	Medium	Vulnerability	TCP
Pre	7	To-client	High	Medium	Vulnerability	TCP
Pre	8	To-client	High	Medium	Vulnerability	TCP
Pre	10	To-server	High	Medium	Vulnerability	TCP
Pre	11	To-client	High	Medium	Vulnerability	TCP
Pre	12	To-client	Critical	Medium	Vulnerability	TCP
Pre	13	To-client	High	Medium	Vulnerability	TCP
Pre	14	To-server	High	Medium	Vulnerability	TCP
Pre	15	To-client	High	Medium	Vulnerability	TCP
Pre	16	To-client	Critical	Medium	Vulnerability	TCP
Pre	17	To-client	High	Medium	Vulnerability	TCP
Pre	18	To-client	High	Medium	Vulnerability	TCP

---- More ----

显示攻击严重程度为比较高的所有 UDP 协议的 IPS 特征。

```
<Sysname> display ips signature severity high protocol udp
```

```
Total signatures          :7          failed:0
```

```
Pre-defined signatures:7          failed:0
```

```
User-defined signatures:0          failed:0
```

Flag:

Pre: predefined User: user-defined

Type	Sig-ID	Direction	Severity	Fidelity	Category	Protocol
Pre	9	To-server	High	Medium	Vulnerability	UDP
Pre	45	To-server	High	Medium	Vulnerability	UDP
Pre	187	Any	High	Medium	Vulnerability	UDP
Pre	196	Any	High	Medium	Vulnerability	UDP
Pre	223	To-server	High	Medium	Vulnerability	UDP
Pre	234	To-client	High	Medium	Vulnerability	UDP
Pre	338	To-client	High	Medium	Vulnerability	UDP

表1-2 display ips signature 命令显示信息描述表

字段	描述
Total signatures	IPS特征总数
failed	Snort规则导入特征库失败和特征库加载失败的特征总数
Pre-defined count	预定义IPS特征数目
User-defined count	自定义IPS特征数目
Type	IPS特征的类型，包括如下取值： - Pre: 表示预定义特征 - User: 表示自定义特征
Sig-ID	IPS特征的编号
Direction	IPS特征的方向属性，包括如下取值： - any: 表示一个会话的两个方向 - To-server: 一个会话的客户端到服务器方向 - To-client: 一个会话的服务器到客户端方向
Severity	IPS特征的攻击严重程度属性，严重程度从低到高分四个级别：Low、Medium、High、Critical
Fidelity	IPS特征的可信度属性，可信度从低到高分三个级别：Low、Medium、High
Category	IPS特征的攻击类别名称
Protocol	IPS特征的协议属性

1.1.5 display ips signature { pre-defined | user-defined }

display ips signature { pre-defined | user-defined } 命令用来显示 IPS 特征的详细信息。

【命令】

display ips signature { pre-defined | user-defined } signature-id

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

pre-defined: 显示预定义 IPS 特征的详细信息。

user-defined: 显示自定义 IPS 特征的详细信息。

signature-id: 指定 IPS 特征的编号，其中，预定义 IPS 特征的取值范围为 1~536870911；自定义 IPS 特征的取值范围为 536870913~1073741823。

【举例】

```
# 显示编号为 1 的预定义 IPS 特征的详细信息。
<Sysname> display ips signature pre-defined 1
Type           : Pre-defined
Signature ID: 1
Status          : Enabled
Action          : Reset & Logging
Name            : GNU_Bash_CVE-2014-6271_Remote_Code_Execution_Vulnerability
Protocol        : TCP
Severity        : High
Fidelity        : Medium
Direction      : To-server
Category        : Vulnerability
Reference       : CVE-2014-6271;
Description     : GNU Bash through 4.3 processes trailing strings after function definitions
                  in the values of environment variables, which allows remote attackers to execute arbitrary
                  code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature
                  in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed
                  by unspecified DHCP clients, and other situations in which setting the environment occurs
                  across a privilege boundary from Bash execution, aka "\"ShellShock.\" NOTE: the original fix
                  for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that
                  is still present after the incorrect fix.
```

表1-3 display ips signature { pre-defined | user-defined }命令显示信息描述表

字段	描述
Type	IPS特征的类型，包括如下取值： - Pre: 表示预定义特征 - User: 表示自定义特征
Signature ID	IPS特征的编号
Status	IPS特征的状态，包括如下取值： - Enabled: 表示此特征已生效 - Disabled: 表示此特未生效
Action	对报文的处理动作，包括如下取值： - Block-source: 表示阻断符合特征的报文，并将该报文的源 IP 地址加入 IP 黑名单 - Drop: 表示丢弃符合特征的报文 - Permit: 表示允许符合特征的报文通过 - Reset: 表示发送 TCP 的 reset 报文或 UDP 的 ICMP 端口不可达报文使 TCP 或 UDP 连接断开 - Capture: 表示捕获符合特征的报文 - Logging: 表示对符合特征的报文生成日志
Name	IPS特征的名称

字段	描述
Protocol	IPS特征的协议属性
Severity	IPS特征的攻击严重程度属性，严重程度从低到高分为四个级别：Low、Medium、High、Critical
Fidelity	IPS特征的可信度属性，可信度从低到高分为三个级别：Low、Medium、High
Direction	IPS特征的方向属性，包括如下取值： - any: 表示一个会话的两个方向 - To-server: 一个会话的客户端到服务器方向 - To-client: 一个会话的服务器到客户端方向
Category	IPS特征的攻击类别名称
Reference	IPS特征的参考信息
Description	IPS特征的描述信息

1.1.6 display ips signature library

display ips signature library 命令用来显示 IPS 特征库信息。

【命令】

display ips signature library

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 IPS 特征库信息。

```
<Sysname> display ips signature library
IPS signature library information:
Type      SigVersion      ReleaseTime      Size
Current   1.02              Fri Sep 13 09:05:35 2014 71594
Last      -                  -                  -
Factory   1.00              Fri Sep 11 09:05:35 2014 71394
```

表1-4 display ips signature library 命令显示信息描述表

字段	描述
Type	IPS特征库版本，包括如下取值： Current: 表示当前版本

字段	描述
	• Last: 表示上一版本 • Factory: 表示出厂版本
SigVersion	IPS特征库版本号
ReleaseTime	IPS特征库发布时间
Size	IPS特征库文件大小，单位是Bytes

1.1.7 display ips signature user-defined parse-failed

display ips signature user-defined parse-failed 命令用来显示 IPS 自定义特征解析失败的信息。

【命令】

display ips signature user-defined parse-failed

【视图】

任意视图

【缺省用户角色】

network-admin

context-admin

【举例】

显示 IPS 自定义特征解析失败的信息。

```
<Sysname> display ips signature user-defined parse-failed
```

```
LineNo  SID      Information
1       None    Error: Invalid actions.
                Tip: Only actions {alert|drop|pass|reject|sdrop|log} are supported
2       1010082 Error: Invalid signature ID.
                Tip: The signature ID must be in the range of 1 to 536870912
3       1010083 Error: Invalid protocol.
                Tip: Only protocols {tcp|udp|icmp|ip} are supported
4       1010084 Error: Invalid direction.
                Tip: Only directions {'<>'|'->'} are supported
```

表1-5 display ips signature user-defined parse-failed 命令显示信息描述表

字段	描述
LineNo	Snort规则文件中的行号
SID	自定义特征的编号
Information	自定义特征解析失败的信息，包括如下取值： • Error: 表示自定义特征解析失败的原因 • Tip: 表示 Snort 规则文件内容的修改建议

【相关命令】

- **ips signature import snort**

1.1.8 ips apply policy

ips apply policy 命令用来在 DPI 应用 profile 中引用 IPS 策略。

undo ips apply policy 命令用来删除引用的 IPS 策略。

【命令】

```
ips apply policy policy-name mode { alert | protect }  
undo ips apply policy
```

【缺省情况】

DPI 应用 profile 中未引用 IPS 策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 表示 IPS 策略名称，为 1~63 个字符的字符串，不区分大小写。

mode: 表示 IPS 策略的模式。

alert: 告警模式，表示报文匹配上该 IPS 策略中的特征后，仅可以生成日志或捕获报文，但其他动作均不能生效。

protect: 保护模式，表示报文匹配上该 IPS 策略中的特征后，设备按照特征的动作对该报文进行处理。

【使用指导】

IPS 策略仅在被 DPI 应用 profile 引用后生效。一个 DPI 应用 profile 视图下只能引用一个 IPS 策略。多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 sec 的 DPI 应用 profile 下引用 IPS 策略 ips1，且配置 IPS 模式为保护模式。

```
<Sysname> system-view  
[Sysname] app-profile sec  
[Sysname-app-profile-sec] ips apply policy ips1 mode protect
```

【相关命令】

- **app-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **ips policy**

1.1.9 ips parameter-profile

ips { block-source | capture | email | logging | redirect } parameter-profile
命令用来配置 IPS 动作引用应用层检测引擎动作参数 profile。

undo ips { block-source | capture | email | logging | redirect } parameter-profile 命令用来取消配置 IPS 动作引用应用层检测引擎动作参数 profile。

【命令】

ips { block-source | capture | email | logging | redirect } parameter-profile
parameter-name

undo ips { block-source | capture | email | logging | redirect } parameter-profile

【缺省情况】

IPS 动作未引用应用层检测引擎动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

block-source: 表示设置 IPS 源阻断动作的参数。

capture: 表示设置 IPS 捕获动作的参数。

email: 表示设置 IPS 邮件动作的参数。

logging: 表示设置 IPS 日志动作的参数。

redirect: 表示设置 IPS 重定向动作的参数。

parameter-profile *parameter-name*: 指定 IPS 动作引用的应用层检测引擎动作参数 profile。
parameter-name 表示动作参数 profile 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

每类 IPS 动作的具体执行参数由应用层检测引擎动作参数 profile 来定义，可通过引用各动作参数 profile 为 IPS 动作提供执行参数。有关应用层检测引擎动作参数 profile 的具体配置请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

如果 IPS 动作没有引用应用层检测引擎动作参数 profile，或者引用的动作参数 profile 不存在，则使用系统中各动作参数的缺省值。

【举例】

创建名称为 ips1 的应用层检测引擎源阻断动作参数 profile，配置其阻断源 IP 地址的时长为 1111 秒。

```
<Sysname> system-view
[Sysname] inspect block-source parameter-profile ips1
[Sysname-inspect-block-source-ips1] block-period 1111
[Sysname-inspect-block-source-ips1] quit
```

配置 IPS 源阻断动作引用名称为 ips1 的应用层检测引擎源阻断动作参数 profile。

```
[Sysname] ips block-source parameter-profile ips1
```

【相关命令】

- **inspect block-source parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **inspect capture parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **inspect logging parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **inspect email parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **inspect redirect parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)

1.1.10 ips policy

ips policy 命令用来创建 IPS 策略，并进入 IPS 策略视图。如果指定的 IPS 策略已经存在，则直接进入 IPS 策略视图。

undo ips policy 命令用来删除指定的 IPS 策略。

【命令】

```
ips policy policy-name
```

```
undo ips policy policy-name
```

【缺省情况】

存在 IPS 策略，名称为 default。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: 表示 IPS 策略名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

设备上存在一个名称为 default 的缺省 IPS 策略，缺省 IPS 策略和自定义 IPS 策略都使用当前系统中的所有 IPS 特征，新增 IPS 特征会自动添加到所有策略下。但是缺省 IPS 策略中的 IPS 特征的动作属性和生效状态属性不能被修改。

【举例】

创建一个名称为 ips1 的 IPS 策略，并进入 IPS 策略视图。

```
<Sysname> system-view
```

```
[Sysname] ips policy ips1
```

```
[Sysname-ips-policy-ips1]
```

1.1.11 ips signature auto-update

ips signature auto-update 命令用来开启定期自动在线升级 IPS 特征库功能，并进入自动升级配置视图。

undo ips signature auto-update 命令用来关闭定期自动在线升级 IPS 特征库功能。

【命令】

```
ips signature auto-update
undo ips signature auto-update
```

【缺省情况】

定期自动在线升级 IPS 特征库功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

如果设备可以访问 UNIS 官方网站上的特征库服务专区，可以采用定期自动在线升级方式来对设备上的 IPS 特征库进行升级。

【举例】

```
# 开启定期自动在线升级 IPS 特征库功能，并进入自动升级配置视图。
<Sysname> system-view
[Sysname] ips signature auto-update
[Sysname-ips-autoupdate]
```

【相关命令】

- **update schedule**

1.1.12 ips signature auto-update-now

ips signature auto-update-now 命令用来立即自动在线升级 IPS 特征库。

【命令】

```
ips signature auto-update-now
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```


【使用指导】

执行此命令后，将立即自动升级设备上的 IPS 特征库，且会备份当前的 IPS 特征库文件。此命令的生效与否，与是否开启了定期自动升级 IPS 特征库功能无关。

当管理员发现 UNIS 官方网站上的特征库服务专区中的 IPS 特征库有更新时，可以选择立即自动在线升级方式来及时升级 IPS 特征库版本。

【举例】

```
# 立即自动在线升级 IPS 特征库版本。
<Sysname> system-view
[Sysname] ips signature auto-update-now
```

1.1.13 ips signature import snort

ips signature import snort 命令用来导入自定义 IPS 特征。

【命令】

```
ips signature import snort file-path
```

【缺省情况】

不存在自定义 IPS 特征。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

file-path: 自定义 IPS 特征库文件的 URL，为 1~255 个字符的字符串。

【使用指导】

当需要的 IPS 特征在设备当前 IPS 特征库中不存在时，可通过编辑 Snort 格式的 IPS 特征文件，并将其导入设备中来生成所需的 IPS 特征。导入的 IPS 特征文件内容会自动覆盖系统中所有的自定义 IPS 特征。可通过 **display ips signature user-defined** 命令查看导入的 IPS 特征信息。

管理员可以采用如下几种方式导入自定义 IPS 特征库文件。

- 本地方式：使用本地保存的自定义 IPS 特征库文件导入。
- FTP/TFTP 方式：通过 FTP 或 TFTP 方式下载远程服务器上保存的自定义 IPS 特征库文件，并导入到系统中。

参数 *file-path* 的取值与自定义 IPS 特征库文件导入的操作方式有关。采用本地方式时参数 *file-path* 取值请参见 [表 1-6](#)；采用 FTP/TFTP 方式时参数 *file-path* 取值请参见 [表 1-7](#)。

表1-6 采用本地方式时参数 *file-path* 取值说明表

导入方式	参数 <i>file-path</i> 取值	说明
自定义IPS特征库文件的存储位置与当前工作路径一致	<i>filename</i>	可以执行 pwd 命令查看当前工作路径 有关 pwd 命令的详细介绍请参见“基础配置命令参

导入方式	参数 <i>file-path</i> 取值	说明
致		考”中的“文件系统管理”
自定义IPS特征库文件的存储位置与当前工作路径不一致，且在相同存储介质上	<i>filename</i>	需要先执行 cd 命令将工作路径切换至自定义IPS特征库文件所在目录下 有关 cd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
自定义IPS特征库文件的存储位置与当前工作路径不在相同存储介质上	<i>path/ filename</i>	需要先执行 cd 命令将工作路径切换至自定义IPS特征库文件所在存储介质的根目录下，再指定自定义IPS特征库文件的相对路径 有关 cd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”

表1-7 采用 FTP/TFTP 方式时参数 *file-path* 取值说明表

升级场景	参数 <i>file-path</i> 取值	说明
自定义IPS特征库文件存储在开启FTP服务的远程服务器上	<i>ftp://username:password@server/filename</i>	<i>username</i> 为登录FTP服务器的用户名， <i>password</i> 为登录FTP服务器的密码， <i>server</i> 为FTP服务器的IP地址或主机名 当FTP用户名和密码中使用了“:”、“@”和“/”三种特殊字符时，需要将这三种特殊字符替换为其对应的转义字符。“:”、“@”和“/”三种特殊字符对应的转义字符分别为“%3A或%3a”、“%40”和“%2F或%2f”
自定义IPS特征库文件存储在开启TFTP服务的远程服务器上	<i>tftp://server/filename</i>	<i>server</i> 为TFTP服务器的IP地址或主机名

编辑 Snort 格式的 IPS 特征文件需要注意的是：

Snort 文件需要遵循 Snort 公司的语法。

Snort 规则的 SID 取值范围为 1~536870911，若超出此范围，则规则无效。

如需增加 Snort 规则，则新增规则的 SID 不能与设备上旧 Snort 文件中任何规则的 SID 相同。

编辑 Snort 规则时，必须配置 msg 字段，否则 IPS 系统日志中威胁名称字段是空的。

当用户自定义 Snort 规则中的应用无法被识别时，报文无法成功匹配该规则。

【相关命令】

- **display ips signature user-defined**
- **ips signature remove snort**

【举例】

采用 TFTP 方式，将自定义 Snort 格式的 IPS 特征库文件导入设备生成自定义 IPS 特征，自定义 Snort 格式的 IPS 特征库文件的远程路径为 *tftp://192.168.0.1/snort.rules*。

```
<Sysname> system-view
```

```
[Sysname] ips signature import snort tftp://192.168.0.1/snort.rules
```

1.1.14 ips signature remove snort

ips signature remove snort 命令用来删除导入的所有自定义 IPS 特征。

【命令】

ips signature remove snort

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【举例】

```
# 删除导入的所有自定义 IPS 特征。  
<Sysname> system-view  
[Sysname] ips signature remove snort
```

【相关命令】

- **ips signature import snort**

1.1.15 ips signature rollback

ips signature rollback 命令用来回滚 IPS 特征库。

【命令】

ips signature rollback { factory | last }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

factory: 表示 IPS 特征库的出厂版本。

last: 表示 IPS 特征库的上一版本。

【使用指导】

IPS 特征库回滚是指将当前的 IPS 特征库版本回滚到指定的版本。如果管理员发现设备当前 IPS 特征库版本在检测和防御网络攻击时，误报率较高或出现异常情况，则可以对当前 IPS 特征库版本进行回滚。目前支持将设备中的 IPS 过滤特征库版本回滚到出厂版本和上一版本。

IPS 特征库版本每次回滚前，设备都会备份当前版本。多次回滚上一版本的操作将会在当前版本和上一版本之间反复切换。例如当前 IPS 特征库是 V2，上一版本是 V1，第一次执行回滚到上一版本的操作后，特征库替换成 V1 版本，再执行回滚到上一版本的操作则特征库重新变为 V2 版本。

【举例】

```
# 配置 IPS 特征库回滚到上一版本。
<Sysname> system-view
[Sysname] ips signature rollback last
```

1.1.16 ips signature update

ips signature update 命令用来手动离线升级 IPS 特征库。

【命令】

```
ips signature update [ override-current ] file-path
```

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

override-current：表示覆盖当前版本的特征库文件。如果不指定本参数，则表示当前特征库在升级之后作为备份特征库保存在设备上。

file-path：指定特征库文件的路径，为 1~255 个字符的字符串。

【使用指导】

如果设备不能访问 UNIS 官方网站上的特征库服务专区，管理员可以采用如下几种方式手动离线升级 IPS 特征库版本。

- 本地升级：使用本地保存的特征库文件升级系统上的 IPS 特征库版本。
- FTP/TFTP 升级：通过 FTP 或 TFTP 方式下载远程服务器上保存的特征库文件，并升级系统上的 IPS 特征库版本。

使用本地升级方式离线升级特征库版本时，特征库文件只能存储在当前主用设备上，否则设备升级特征库会失败。

参数 **file-path** 的取值与手动离线升级的操作方式有关。本地升级时参数 **file-path** 取值请参见 [表 1-8](#)；FTP/TFTP 升级时参数 **file-path** 取值请参见 [表 1-9](#)。

表1-8 本地升级时参数 *file-path* 取值说明表

升级场景	参数 <i>file-path</i> 取值	说明
特征库文件的存储位置与当前工作路径一致	<i>filename</i>	可以执行 pwd 命令查看当前工作路径 有关 pwd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不一致，且在相同存储介质上	<i>filename</i>	需要先执行 cd 命令将工作路径切换至特征库文件所在目录下 有关 cd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不在相同存	<i>path/ filename</i>	需要先执行 cd 命令将工作路径切换至特征库文件所在存储介质的根目录下，再指定特征库文件的相

升级场景	参数 <i>file-path</i> 取值	说明
储介质上		对路径 有关 cd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”

表1-9 FTP/TFTP 升级时参数 *file-path* 取值说明表

升级场景	参数 <i>file-path</i> 取值	说明
特征库文件存储在开启 FTP 服务的远程服务器上	<i>ftp://username:password@server/filename</i>	<i>username</i> 为登录FTP服务器的用户名， <i>password</i> 为登录FTP服务器的密码， <i>server</i> 为FTP服务器的IP地址或主机名 当FTP的用户名和密码中使用了“:”、“@”和“/”三种特殊字符时，需要将这三种特殊字符替换为其对应的转义字符。“:”、“@”和“/”三种特殊字符对应的转义字符分别为“%3A或%3a”、“%40”和“%2F或%2f”
特征库文件存储在开启 TFTP 服务的远程服务器上	<i>tftp://server/filename</i>	<i>server</i> 为TFTP服务器的IP地址或主机名



说明

当采用 FTP/TFTP 方式升级特征库时，如果指定的是服务器的主机名，则需要确保设备能通过静态或动态域名解析方式获得 FTP/TFTP 服务器的 IP 地址，并与之路由可达。否则设备升级特征库会失败。有关域名解析功能的详细配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

【举例】

```
# 配置手动离线升级 IPS 特征库，且采用 TFTP 方式，IPS 特征库文件的远程路径为
tftp://192.168.0.10/ips-1.0.2-en.dat。
<Sysname> system-view
[Sysname] ips signature update tftp://192.168.0.10/ips-1.0.2-en.dat
# 配置手动离线升级 IPS 特征库，且采用 FTP 方式，IPS 特征库文件的远程路径为
ftp://192.168.0.10/ips-1.0.2-en.dat，用户名为 user:123，密码为 user@abc/123。
<Sysname> system-view
[Sysname] ips signature update
ftp://user%3A123:user%40abc%2F123@192.168.0.10/ips-1.0.2-en.dat
# 配置手动离线升级 IPS 特征库，且采用本地方式，IPS 特征库文件的本地路径为
cfa0:/ips-1.0.23-en.dat，且当前工作路径为 cfa0:。
<Sysname> system-view
[Sysname] ips signature update ips-1.0.23-en.dat
# 配置手动离线升级 IPS 特征库，且采用本地方式，IPS 特征库文件的本地路径为
cfa0:/dpi/ips-1.0.23-en.dat，且当前工作路径为 cfa0:。
<Sysname> cd dpi
<Sysname> system-view
[Sysname] ips signature update ips-1.0.23-en.dat
```

配置手动离线升级 IPS 特征库，且采用本地方式，IPS 特征库文件的本地路径为 cfb0:/dpi/ips-1.0.23-en.dat，当前工作路径为 cfa0:。

```
<Sysname> cd cfb0:/
```

```
<Sysname> system-view
```

```
[Sysname] ips signature update dpi/ips-1.0.23-en.dat
```

1.1.17 ips signature update-log

ips signature update-log send-time 命令用来开启 IPS 特征库更新日志记录功能并配置每日发送日志的时间。

undo ips signature update-log send-time 命令用来关闭 IPS 特征库更新日志记录功能。

【命令】

ips signature update-log send-time time

undo ips signature update-log send-time

【缺省情况】

不发送 IPS 特征库更新日志。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

time：表示日志的发送时间，格式为 hh:mm:ss，取值范围为 00:00:00～23:59:59。

【使用指导】

配置本命令后，当 IPS 特征库升级或回滚成功时，设备将记录特征库变更的时间，并在每日按照配置的时间发送日志。

目前，仅支持快速输出 IPS 特征库更新日志，配置本命令后，还需要配置 IPS 快速输出日志时使用国家电网络格式（即配置 **customlog format dpi ips sgcc** 命令）并允许设备向指定的日志主机发送 IPS 模块的日志（即配置 **customlog host** 命令）。有关快速日志输出功能的详细介绍，请参见“网络管理和监控命令参考”中的“快速日志输出”。

多次执行本命令，最后一次执行的命令生效。

【举例】

开启 IPS 特征库更新日志记录功能并配置日志的发送时间为每天的 12 点 12 分 12 秒。

```
<Sysname> system-view
```

```
[Sysname] ips signature update-log send-time 12:12:12
```

1.1.18 object-dir

object-dir 命令用来配置筛选 IPS 特征的方向属性。

undo object-dir 命令用来恢复缺省情况。

【命令】

```
object-dir { client | server } *  
undo object-dir
```

【缺省情况】

未配置方向属性筛选条件。

【视图】

IPS 策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

client: 表示从服务器到客户端方向上的对象。

server: 表示从客户端到服务器方向上的对象。

【使用指导】

可通过配置方向属性筛选出具有该属性的特征，IPS 策略将使用筛选出的特征与报文进行匹配。可同时配置多个方向，只要符合其中一个，具有该方向属性的特征将会被筛选出来。

多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 test 的 IPS 策略中仅保护从服务器到客户端方向上的对象。

```
<Sysname> system-view  
[Sysname] ips policy test  
[Sysname-ips-policy-test] object-dir client
```

1.1.19 override-current

override-current 命令用来配置定期自动在线升级 IPS 特征库时覆盖当前的特征文件。

undo override-current 命令用来恢复缺省情况。

【命令】

```
override-current  
undo override-current
```

【缺省情况】

定期自动在线升级 IPS 特征库时不会覆盖当前的特征库文件，而是同时将当前的特征库文件备份为上一版本。

【视图】

自动升级配置视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

可以通过开启此功能解决升级 IPS 特征库时设备内存不足的问题。在设备剩余内存充裕的情况下，不建议配置该功能，因为 IPS 特征库升级时，如果没有备份当前特征库文件，则不能回滚到上一版本。

配置此功能后定期自动在线升级 IPS 特征库时不会将当前的特征库文件备份为上一版本。

【举例】

配置定期自动在线升级 IPS 特征库时覆盖当前的特征文件。

```
<Sysname> system-view
[Sysname] ips signature auto-update
[Sysname-ips-autoupdate] override-current
```

【相关命令】

- **ips signature auto-update**

1.1.20 protect-target

protect-target 命令用来配置筛选 IPS 特征的保护对象属性。

undo protect-target 命令用来删除筛选 IPS 特征的保护对象属性。

【命令】

```
protect-target { target [ subtarget ] | all }
undo protect-target { target [ subtarget ] | all }
```

【缺省情况】

未配置保护对象属性筛选条件。

【视图】

IPS 策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

target: 表示保护对象分类名称。

subtarget: 表示保护对象分类中的子对象名称。若不指定本参数，则表示保护某对象分类中的所有子对象。

all: 表示所有保护对象。

【使用指导】

可通过配置保护对象属性筛选出具有该属性的特征，IPS 策略将使用筛选出的特征与报文进行匹配。可多次执行本命令，配置多个保护对象。只要符合其中一个，具有该保护对象属性的特征将会被筛选出来。

【举例】

在名称为 test 的 IPS 策略中，配置筛选 IPS 特征的保护对象为 WebServer 中 WebLogic 子对象。


```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] protect-target WebServer WebLogic
```

1.1.21 severity-level

severity-level 命令用来配置筛选 IPS 特征的严重级别属性。

undo severity-level 命令用来恢复缺省情况。

【命令】

```
severity-level { critical | high | low | medium } *
undo severity-level
```

【缺省情况】

未配置严重级别属性筛选条件。

【视图】

IPS 策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

critical: 表示严重级别最高。

high: 表示严重级别高。

low: 表示严重级别低。

medium: 表示严重级别一般。

【使用指导】

严重级别是指匹配此 IPS 特征的网络攻击造成危害的严重程度。可通过配置严重级别属性筛选出具有该属性的特征，IPS 策略将使用筛选出的特征与报文进行匹配。可同时配置多个严重级别，只要符合其中一个，具有该严重级别属性的特征将会被筛选出来。

多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 test 的 IPS 策略中，配置筛选 IPS 特征的严重级别为 critical 和 medium。

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] severity-level critical medium
```

1.1.22 signature override

signature override 命令用来修改 IPS 策略中指定特征的动作和状态。

undo signature override 命令用来恢复 IPS 策略中指定特征属性中的动作和状态。

【命令】

```
signature override { pre-defined | user-defined } signature-id { { disable |  
enable } [ { block-source | drop | permit | redirect | reset } | capture |  
logging ] * }  
undo signature override { pre-defined | user-defined } signature-id
```

【缺省情况】

预定义 IPS 特征使用系统预定义的状态和动作，自定义 IPS 特征的动作和状态在管理员导入的特征库文件中定义。

【视图】

IPS 策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

pre-defined: 表示预定义的 IPS 特征。

user-defined: 表示自定义的 IPS 特征。

signature-id: IPS 特征的编号，取值范围为 1~4294967295。

disable: 表示禁用此 IPS 特征。在某些网络环境中，如果一些 IPS 特征暂时不会被用到，而且又不想将其从 IPS 策略中删除时，可以使用 **disable** 参数来禁用这些规则。

enable: 表示启用此 IPS 特征。

block-source: 表示源阻断，该动作阻断符合特征的报文，并将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名单过滤功能的详细介绍请参见“安全命令参考”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。

drop: 表示丢弃报文。

permit: 表示允许报文通过。

redirect: 表示把符合特征的报文重定向到指定的 Web 页面上。

reset: 表示通过发送 TCP 的 reset 报文使 TCP 连接断开。

capture: 表示捕获报文。

logging: 表示生成报文日志。

【使用指导】

本命令仅用于修改自定义 IPS 策略中特征的动作和状态，缺省 IPS 策略中特征的动作和状态不能被修改。

在同一个 IPS 策略视图对同一 IPS 特征多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 ips1 的 IPS 策略中，配置编号为 2 的预定义 IPS 特征的状态为开启，动作为丢弃和捕获报文，并生成日志信息。

```
<Sysname> system-view
[Sysname] ips policy ips1
[Sysname-ips-policy-ips1] signature override pre-defined 2 enable drop capture logging
```

【相关命令】

- **blacklist enable** (security zone view) (安全命令参考/攻击检测与防范)
- **blacklist global enable** (安全命令参考/攻击检测与防范)
- **ips parameter-profile**
- **ips policy**
- **signature override all**

1.1.23 signature override all

signature override all 命令用来配置 IPS 策略中所有特征的统一动作。

undo signature override all 命令用来恢复缺省情况。

【命令】

```
signature override all { { block-source | drop | permit | redirect | reset }
| capture | logging } *
undo signature override all
```

【缺省情况】

IPS 策略执行特征属性中的动作。

【视图】

IPS 策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

block-source: 表示源阻断，该动作阻断符合特征的报文，并会将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名单过滤功能的详细介绍请参见“安全命令参考”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。

drop: 表示丢弃报文。

permit: 表示允许报文通过。

redirect: 表示把符合特征的报文重定向到指定的 Web 页面上。

reset: 表示通过发送 TCP 的 reset 报文使 TCP 连接断开。

capture: 表示捕获报文。

logging: 表示生成报文日志。

【使用指导】

如果在 IPS 策略中为所有特征配置了统一动作，则设备将根据该动作对与此策略中特征匹配成功的报文进行处理。否则，设备将根据特征属性中的动作对报文进行处理。

如果在 IPS 策略中修改了指定特征的动作，则无论 IPS 策略是否为所有特征配置了统一的动作，设备都将根据修改后的动作对报文进行处理。

【举例】

配置名称为 text 的 IPS 策略中所有特征的统一动作为丢弃，并生成日志信息和捕获报文。

```
<Sysname> system-view
[Sysname] ips policy test
[Sysname-ips-policy-test] signature override all drop logging capture
```

【相关命令】

- **blacklist enable** (security zone view)（安全命令参考/攻击检测与防范）
- **blacklist global enable**（安全命令参考/攻击检测与防范）
- **ips parameter-profile**
- **signature override**

1.1.24 update schedule

update schedule 命令用来配置定期自动在线升级 IPS 特征库的时间。

undo update schedule 命令用来恢复缺省情况。

【命令】

```
update schedule { daily | weekly { fri | mon | sat | sun | thu | tue | wed } }
start-time time tingle minutes
undo update schedule
```

【缺省情况】

设备在每天 01:00:00 至 03:00:00 之间自动在线升级 IPS 特征库。

【视图】

自动升级配置视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

daily: 表示自动升级周期为每天。

weekly: 表示以一周为周期，在指定的一天进行自动升级。

fri: 表示星期五。

mon: 表示星期一。

sat: 表示星期六。

sun: 表示星期日。

thu: 表示星期四。

tue: 表示星期二。

wed: 表示星期三。

start-time time: 指定自动升级开始时间，*time* 的格式为 hh:mm:ss，取值范围为 00:00:00～23:59:59。

tingle minutes: 指定抖动时间，即实际自动升级开始时间的偏差范围，取值范围为 0～120，单位为分钟。在 **start-time** 指定时间的前后各偏移抖动时间的一半作为自动升级的时间范围，例如，指定自动升级的开始时间为 01:00:00，抖动时间为 60 分钟，则自动升级的时间范围为 00:30:00 至 01:30:00。

【举例】

配置 IPS 特征库的定期自动在线升级时间为每周一 20:30:00，抖动时间为 10 分钟。

```
<Sysname> system-view
```

```
[Sysname] ips signature auto-update
```

```
[Sysname-ips-autoupdate] update schedule weekly mon start-time 20:30:00 tingle 10
```

【相关命令】

- **ips signature auto-update**

目 录

1 URL过滤.....	1-1
1.1 URL过滤配置命令.....	1-1
1.1.1 add.....	1-1
1.1.2 category action.....	1-2
1.1.3 default-action	1-4
1.1.4 description	1-5
1.1.5 display url-filter category	1-5
1.1.6 display url-filter signature library.....	1-9
1.1.7 display url-filter statistics	1-10
1.1.8 include pre-defined	1-11
1.1.9 rename (URL filtering category view)	1-12
1.1.10 rename (URL filtering policy view).....	1-12
1.1.11 reset url-filter statistics	1-13
1.1.12 rule	1-13
1.1.13 update schedule	1-15
1.1.14 url-filter apply policy.....	1-16
1.1.15 url-filter category.....	1-17
1.1.16 url-filter copy category.....	1-18
1.1.17 url-filter copy policy.....	1-18
1.1.18 url-filter log directory root	1-19
1.1.19 url-filter log enable.....	1-20
1.1.20 url-filter log except pre-defined	1-20
1.1.21 url-filter log except user-defined	1-21
1.1.22 url-filter policy.....	1-22
1.1.23 url-filter signature auto-update	1-23
1.1.24 url-filter signature auto-update-now	1-24
1.1.25 url-filter signature rollback	1-24
1.1.26 url-filter signature update	1-25

1 URL过滤

1.1 URL过滤配置命令

1.1.1 add

add 命令用来向 URL 过滤策略中添加黑/白名单规则。

undo add 命令用来删除 URL 过滤策略中指定的或所有黑/白名单规则。

【命令】

```
add { blacklist | whitelist } [ id ] host { regex host-regex | text host-name }  
[ uri { regex uri-regex | text uri-name } ]  
undo add { blacklist | whitelist } { id | all }
```

【缺省情况】

URL 过滤策略中不存在黑/白名单规则。

【视图】

URL 过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

blacklist: 表示 URL 过滤策略的黑名单规则。

whitelist: 表示 URL 过滤策略的白名单规则。

id: 表示黑/白名单规则的编号，取值范围为 1~65535。若未指定本参数，系统将从 1 开始，自动分配一个大于现有最大编号的最小编号，步长为 1。若新编号超出了编号上限 65535，则选择当前未使用的最小编号作为新的编号。

host: 表示匹配 URL 中的主机名字段。

uri: 表示匹配 URL 中的 URI 字段。

regex regex: 表示使用正则表达式对主机名和 URI 字段进行匹配。**regex** 是正则表达式，区分大小写，只能以字母、数字和下划线开头，且至少包含连续的 3 个非通配符。其中，主机名规则的取值范围为 3~224 个字符，URI 规则的取值范围为 3~245 个字符。

text string: 表示使用文本对主机名和 URI 字段进行匹配。**string** 是指定的主机名或 URI 规则字符串。主机名规则的取值范围为 3~224 个字符，不区分大小写，且至少包含连续的 3 个非通配符，主机名只能是字母、数字、下划线“_”、连接符“-”、冒号“:”、左方括号“[”、右方括号“]”、点号“.”和星号“*”，但 URI 无此限制；URI 规则的取值范围为 3~245 个字符，不区分大小写，且至少包含连续的 3 个非通配符。

all: 表示所有的黑/白名单规则。

【使用指导】

URL 过滤黑/白名单规则功能根据应用层的信息进行 URL 过滤。如果用户 HTTP 报文中的 URL 与 URL 过滤策略中的黑名单规则匹配成功，则丢弃此报文；如果与白名单规则匹配成功，则允许此报文通过。

使用文本方式对主机名和 URI 字段进行匹配时，对星号“*”有如下的限制：

- 匹配主机名字段时，“*”只能出现在开头或结尾，表示通配符，代表 0 到多个任意字符。
- 匹配 URI 字段时，当“*”出现在开头或结尾，表示通配符，代表 0 到多个任意字符；当“*”出现在其他位置时，则作为普通字符进行匹配。

正则表达式有如下限制：

- 正则表达式中，总的分支不能超过四个。例如'abc(c|d|e|\x3D)'有效，'abc(c|onreset|onselect|onchange|style\x3D)'无效。
- 正则表达式中，括号不能嵌套，即括号中不能有括号。例如'ab((abcs*?))'无效。
- 正则表达式中，分支不支持串联，即分支后面不能有分支。例如'ab(a|b)(c|d)^\r\n]+?'无效。
- 正则表达式中，零次重复量词'*'和'?'前面必须有四个确定字符。例如'abc*'无效，'abcd*DoS\x2d\d{5}\x20\x2bxi\r\nJOIN'有效。

【举例】

在 URL 过滤策略 news 中，添加一条黑名单规则，使用以 games.com 开头的字符串对主机名字段进行匹配。

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] add blacklist 1 host text games.com*
```

1.1.2 category action

category action 命令用来配置 URL 过滤分类动作。

undo category action 命令用来删除指定的 URL 过滤分类动作。

【命令】

```
category category-name action { block-source [ parameter-profile
parameter-name ] | drop | permit | redirect parameter-profile parameter-name
| reset } [ logging [ parameter-profile parameter-name ] ]
undo category category-name
```

【缺省情况】

不存在 URL 过滤分类动作。

【视图】

URL 过滤策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

category-name: 指定 URL 过滤分类名称，包括预定义和自定义的 URL 过滤分类名称，为 1~63 个字符的字符串，不区分大小写。

action: 表示对匹配上此 URL 过滤分类中的任何一条规则的报文所采取的动作。

block-source: 表示阻断报文，并将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名单过滤功能的详细介绍请参见“安全命令参考”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。

drop: 表示丢弃报文。

permit: 表示允许报文通过。

redirect: 表示重定向动作，把符合特征的报文重定向到指定的 Web 页面上。

reset: 表示通过发送 TCP 的 reset 报文从而使 TCP 连接断开。

logging: 表示生成报文日志。

parameter-profile parameter-name: 指定 URL 过滤动作引用的应用层检测引擎动作参数 profile。*parameter-name* 是动作参数 profile 的名称，为 1~63 个字符的字符串，不区分大小写。如果 URL 过滤动作没有引用应用层检测引擎动作参数 profile，或者引用的动作参数 profile 不存在，则使用系统中各动作参数的缺省值。有关应用层检测引擎中动作参数的详细配置请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

【使用指导】

URL 过滤功能对报文的处理过程如下：

- 如果报文匹配上该 URL 过滤分类中的任何一条规则，则设备将会根据该 URL 过滤分类绑定的动作对此报文进行处理。
- 如果报文没有匹配上该 URL 过滤分类中的任何规则，但是配置了 **default-action** 命令，则设备将根据 URL 过滤策略中配置的缺省动作来对此报文进行处理。
- 如果报文没有匹配上该 URL 过滤分类中的任何规则，且也没有配置 **default-action** 命令，则设备直接允许此报文通过。

多次执行本命令，最后一次执行的命令生效。

【举例】

在 URL 过滤策略 news 中，配置 URL 过滤分类 sina 的动作为丢弃。

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] category sina action drop
```

【相关命令】

- **inspect block-source parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **inspect redirect parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **url-filter category**
- **url-filter policy**

1.1.3 default-action

default-action 命令用来配置 URL 过滤策略的缺省动作。

undo default-action 命令用来恢复缺省情况。

【命令】

```
default-action { block-source [ parameter-profile parameter-name ] | drop |  
permit | redirect parameter-profile parameter-name | reset } [ logging  
[ parameter-profile parameter-name ] ]  
undo default-action
```

【缺省情况】

未配置 URL 过滤策略的缺省动作。

【视图】

URL 过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

block-source: 表示阻断报文，并将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名单过滤功能的详细介绍请参见“安全命令参考”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。

drop: 表示丢弃报文。

permit: 表示允许报文通过。

redirect: 表示重定向动作，把符合特征的报文重定向到指定的 Web 页面上。

reset: 表示通过发送 TCP 的 reset 报文从而使 TCP 连接断开。

logging: 表示生成报文日志动作。

parameter-profile parameter-name: 指定引用的动作参数。*parameter-name* 是动作参数 *profile* 的名称，为 1~63 个字符的字符串，不区分大小写。如果不指定该参数或指定的参数不存在，则使用动作的缺省参数。这里引用的动作参数是应用层检测引擎中配置的动作参数，有关应用层检测引擎中动作参数的详细配置请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

【使用指导】

配置此命令后，当报文没有匹配上 URL 过滤策略中的规则时，设备将根据 URL 过滤策略的缺省动作对此报文进行处理。

【举例】

在名为 cmcc 的 URL 过滤策略中，配置缺省动作为丢弃。

```
<Sysname> system-view
```

```
[Sysname] url-filter policy cmcc
```

```
[Sysname-url-filter-policy-cmcc] default-action drop
```

【相关命令】

- **inspect block-source parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **inspect redirect parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **url-filter policy**

1.1.4 description

description 命令用来配置 URL 过滤分类的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

自定义的 URL 过滤分类中未配置描述信息。

【视图】

URL 过滤分类视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: URL 过滤分类的描述信息，为 1~255 个字符的字符串，可以包含空格，不区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别 URL 过滤分类的作用，有利于后期维护。

【举例】

配置 URL 过滤分类 news 的描述信息为 News information。

```
<Sysname> system-view
```

```
[Sysname] url-filter category news
```

```
[Sysname-url-filter-category-news] description News information
```

1.1.5 display url-filter category

display url-filter category 命令用来查看 URL 过滤父分类或子分类信息。

【命令】

display url-filter { category | parent-category } [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

category: 显示 URL 过滤子分类的信息。

parent-category: 显示 URL 过滤父分类的信息。仅支持预定义父分类，且父分类下仅包含预定义子分类。

verbose: 显示 URL 过滤子分类或父分类的详细信息。如果不指定该参数，则显示 URL 过滤子分类或父分类的摘要信息。

【使用指导】

URL 过滤支持两级分类，包含父分类和子分类。

【举例】

查看 URL 过滤子分类信息。

```
<Sysname> display url-filter category
```

URL category statistics:

Predefined categories: 53

Predefined rules: 2000

User-defined categories: 5

User-defined rules: 4

URL categories:

Name : 23

Name : 24

Name : 33

Name : Pre-AdvertisementsAndPop-Ups

Name : Pre-AlcoholAndTobacco

Name : Pre-Anonymizers

Name : Pre-Arts

Name : Pre-Business

Name : Pre-Chat

Name : Pre-ComputersAndTechnology

Name : Pre-CriminalActivity

Name : Pre-Cults

Name : Pre-DatingAndPersonals

Name : Pre-DownloadSites

Name : Pre-Education

Name : Pre-Entertainment

Name : Pre-FashionAndBeauty

---- More ----

查看 URL 过滤子分类的详细信息。

```
<Sysname> display url-filter category verbose
```

URL category statistics:

Predefined categories: 53

Predefined rules: 2000
User-defined categories: 5
User-defined rules: 4

URL category details:

Name: 23
Type: User defined
Severity: 1001
Rules: 1
Description:

Name: 24
Type: User defined
Severity: 1002
Rules: 1
Description:

Name: Pre-AdvertisementsAndPop-Ups
Type: Predefined
Severity: 300
Rules: 32
Description: Sites that provide advertising graphics or other ad content files such as banners and pop-ups.

Name: Pre-AlcoholAndTobacco
Type: Predefined
Severity: 960
Rules: 7
Description: Sites that promote or sell alcohol- or tobacco-related products or services.

---- More ----

表1-1 display url-filter category 命令显示信息描述表

字段	描述
URL category statistics	设备中URL过滤子分类总数，包括预定义和自定义的分类
Predefined categories	预定义URL过滤子分类数目
Predefined rules	预定义URL过滤规则数目
User-defined categories	自定义URL过滤子分类数目
User-defined rules	自定义URL过滤规则数目
URL category details	URL过滤子分类详细信息
Name	URL过滤子分类名称
Type	URL过滤子分类类型，包括如下取值： - Predefined: 预定义分类 - User defined: 自定义分类

字段	描述
Severity	URL过滤严重级别
Rules	指定URL分类下的规则数目
Description	URL过滤子分类描述信息

查看 URL 过滤父分类信息。

```
<Sysname> display url-filter parent-category
```

```
URL parent category statistics:
```

```
    Predefined parent categories: 40
```

```
    Included predefined categories: 14
```

```
URL parent categories:
```

```
    Parent category name: SearchEngineAndPortal
```

```
    Parent category name: P2PAndDownload
```

```
    Parent category name: OrdinaryDownload
```

```
    Parent category name: House
```

```
    Parent category name: EducationAndScientificResearch
```

```
    Parent category name: Finance
```

```
    Parent category name: StreamMediaAndVideo
```

```
    Parent category name: Shopping
```

```
    Parent category name: TransportationVehicle
```

```
    Parent category name: Travel
```

```
---- More ----
```

查看 URL 过滤父分类的详细信息。

```
<Sysname> display url-filter parent-category verbose
```

```
URL parent category statistics:
```

```
    Predefined parent categories: 46
```

```
    Included predefined categories: 139
```

```
URL parent category details:
```

```
    Parent category name: Pre-Adult
```

```
    Type: Predefined
```

```
    Description: Adult
```

```
    Included categories: 7
```

```
        Pre-Abortion
```

```
        Pre-AdultSuppliers
```

```
        Pre-Homosexual
```

```
        Pre-Nudity
```

```
        Pre-OtherAdult
```

```
        Pre-SexualHealth
```

```
        Pre-Vulgar
```

```
    Parent category name: Pre-Arts
```

```
    Type: Predefined
```

```
    Description: Arts
```

```
    Included categories: 1
```

```
        Pre-Arts
```

---- More ----

表1-2 display url-filter parent-category 命令显示信息描述表

字段	描述
URL parent category statistics	设备中URL过滤父分类总数，仅支持预定义的父分类
Predefined parent categories	URL过滤父分类数目
Included predefined categories	URL过滤所有父分类下包含的预定义URL过滤子分类总数
URL parent category details	URL过滤父分类详细信息
Parent category name	URL过滤父分类名称
Type	URL过滤父分类的类型，仅支持预定义类型
Description	URL过滤父分类描述信息
Included categories	指定URL过滤父分类下包含的分类数目

1.1.6 display url-filter signature library

display url-filter signature library 查看 URL 过滤特征库信息。

【命令】

display url-filter signature library

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

查看 URL 过滤特征库信息。

```
<Sysname> display url-filter signature library
```

URL filter signature library information:

Type	SigVersion	ReleaseTime	Size
Current	1.0.0	Wed Jan 21 06:43:53 2015	36096
(null)	-	-	-
Factory	1.0.0	Wed Jan 21 06:43:53 2015	36096

表1-3 display url-filter signature library 命令显示信息描述表

字段	描述
Type	URL过滤特征库版本，包括如下取值： • Current: 当前版本 • Last: 上一版本 • Factory: 出厂版本
SigVersion	URL过滤特征库版本号
ReleaseTime	URL过滤特征库发布时间
Size	URL过滤特征库文件大小，单位是Bytes

1.1.7 display url-filter statistics

display url-filter statistics 命令用来查看 URL 过滤的统计信息。

【命令】

display url-filter statistics

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 URL 规则命中统计信息。

```
<Sysname> display url-filter statistics
-----
Slot 1 :
Total HTTP requests           : 0
Total logged HTTP requests    : 0
Total HTTP logging rate       : 0/s
Total permitted HTTP requests : 0
Total denied HTTP requests    : 0
Requests that matched the blacklist : 0
Requests that matched the whitelist : 0
Requests that matched a user-defined rule : 0
Requests that matched a predefined rule : 0
Requests that matched a cached rule : 0
Requests that matched the default action : 0
Predefined URL filtering rules : 2000
-----
```


表1-4 display url-filter statistics 命令显示信息描述表

字段	描述
Total HTTP requests	HTTP报文总数
Total logged HTTP requests	打印日志的HTTP报文总数
Total HTTP logging rate	打印日志的HTTP报文的速率
Total permitted HTTP requests	HTTP报文放行个数
Total denied HTTP requests	HTTP报文拒绝个数
Requests that matched the blacklist	黑名单规则命中数
Requests that matched the whitelist	白名单规则命中数
Requests that matched a user-defined rule	自定义规则命中数
Requests that matched a predefined rule	预定义规则命中数
Requests that matched a cached rule	缓存规则命中数
Requests that matched the default action	默认动作命中数
Predefined URL filtering rules	预定义规则数量

1.1.8 include pre-defined

include pre-defined 命令用来向自定义 URL 过滤分类中添加预定义 URL 过滤分类中的规则。
undo include pre-defined 命令用来恢复缺省情况。

【命令】

include pre-defined *category-name*
undo include pre-defined

【缺省情况】

自定义 URL 过滤分类中不存在预定义 URL 过滤分类中的规则。

【视图】

URL 过滤分类视图

【缺省用户角色】

network-admin
context-admin

【参数】

category-name: 表示预定义 URL 过滤分类的名称，为 1~63 个字符的字符串，区分大小写。指定的预定义 URL 过滤分类必须已存在。

【使用指导】

当新建的 URL 过滤分类中所需的规则与已存在的预定义 URL 过滤分类中的规则比较相似时，可通过此命令灵活、快速的创建 URL 过滤分类。

一个自定义 URL 过滤分类下只能添加一个预定义 URL 过滤分类。多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 news 的 URL 过滤分类中加预定义 URL 过滤分类 pre-Arts 中的规则。

```
<Sysname> system-view
[Sysname] url-filter category news
[Sysname-url-filter-category-news] include pre-defined pre-Arts
```

1.1.9 rename (URL filtering category view)

rename 命令用来重命名 URL 过滤分类，并进入新的 URL 过滤分类视图。

【命令】

rename *new-name*

【视图】

URL 过滤分类视图

【缺省用户角色】

network-admin
context-admin

【参数】

new-name：表示新的 URL 过滤分类的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

原有 URL 过滤分类的名称被修改后，URL 过滤策略中引用的同名 URL 过滤分类的名称也会被同步修改。

【举例】

把名称为 news 的 URL 过滤分类重命名为 hello，并进入新的 URL 过滤分类视图。

```
<Sysname> system-view
[Sysname] url-filter category news
[Sysname-url-filter-category-news] rename hello
[Sysname-url-filter-category-hello]
```

1.1.10 rename (URL filtering policy view)

rename 命令用来重命名 URL 过滤策略，并进入新的 URL 过滤策略视图。

【命令】

rename *new-name*

【视图】

URL 过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

new-name: 表示新的 URL 过滤策略的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

原有 URL 过滤策略的名称被修改后，DPI 应用 profile 中引用的同名 URL 过滤策略的名称也会被同步修改。

【举例】

把名称为 news 的 URL 过滤策略重命名为 hello，并进入新的 URL 过滤策略视图。

```
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news] rename hello
[Sysname-url-filter-policy-hello]
```

1.1.11 reset url-filter statistics

reset url-filter statistics 命令用来清除 URL 过滤的统计信息。

【命令】

reset url-filter statistics

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【举例】

清除 URL 过滤的统计信息。

```
<Sysname> reset url-filter statistics
```

【相关命令】

- **display url-filter statistics**

1.1.12 rule

rule 命令用来在自定义 URL 过滤分类中创建 URL 过滤规则。

undo rule 命令用来在自定义 URL 过滤分类中删除指定的 URL 过滤规则。

【命令】

```
rule rule-id host { regex regex | text string } [ uri { regex regex | text string } ]
undo rule rule-id
```

【缺省情况】

自定义 URL 过滤分类中不存在 URL 过滤规则。

【视图】

URL 过滤分类视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-id: 指定 URL 过滤规则编号，取值范围为 1~65535。

host: 表示 URL 过滤规则匹配 URL 中的主机名字段。

uri: 表示 URL 过滤规则匹配 URL 中的 URI 字段。

regex regex: 表示 URL 过滤规则使用正则表达式对主机名和 URI 字段进行匹配。**regex** 表示正则表达式，区分大小写，只能以字母、数字和下划线开头，且至少包含连续的 3 个非通配符。其中，主机名正则表达式的取值范围为 3~224 个字符；URI 正则表达式的取值范围为 3~253 个字符。

text string: 表示 URL 过滤规则使用文本对主机名和 URI 字段进行匹配。**string** 表示主机名或 URI 规则字符串，主机名规则的取值范围为 3~224 个字符，不区分大小写，且至少包含连续的 3 个非通配符，主机名只能是字母、数字、下划线“_”、连接符“-”、冒号“:”、左方括号“[”、右方括号“]”、点号“.”和星号“*”，但 URI 无此限制；URI 规则的取值范围为 3~255 个字符，不区分大小写，且至少包含连续的 3 个非通配符。

【使用指导】

URL 过滤规则是指对用户 HTTP 报文中的 URL 进行匹配的原则，URL 过滤规则支持两种匹配方式：

- 文本匹配：使用指定的字符串对主机名和 URI 字段进行匹配。
 - 匹配主机名字段时，首先判断主机名开头或结尾位置是否含有通配符“*”，若均未出现，则 URL 中的主机名字段与规则中指定的主机名字符串必须完全一致，才能匹配成功；若“*”出现在开头位置，则该字符串或以该字符串结尾的 URL 会匹配成功；若“*”出现在结尾位置，则该字符串或以该字符串开头的 URL 会匹配成功。若“*”同时出现在开头或结尾位置，则该字符串或含有该字符串的 URL 均会匹配成功。
 - 匹配 URI 字段时，和主机名字段匹配规则一致。
- 正则表达式匹配：使用正则表达式对主机名和 URI 字段进行匹配。例如，规则中配置主机名的正则表达式为 `sina.*cn`，则主机名为 `news.sina.com.cn` 的 URL 会匹配成功。

使用文本方式对主机名和 URI 字段进行匹配时，对星号“*”有如下的限制：

- 匹配主机名字段时，“*”只能出现在开头或结尾，表示通配符，代表 0 到多个任意字符。
- 匹配 URI 字段时，当“*”出现在开头或结尾，表示通配符，代表 0 到多个任意字符；当“*”出现在其他位置时，则作为普通字符进行匹配。

正则表达式有如下限制：

- 正则表达式中，总的分支不能超过四个。例如 `'abc(c|d|e|\x3D)'` 有效，`'abc(c|onreset|onselect|onchange|style\x3D)'` 无效。
- 正则表达式中，括号不能嵌套，即括号中不能有括号。例如 `'ab((abcs*?))'` 无效。
- 正则表达式中，分支不支持串联，即分支后面不能有分支。例如 `'ab(a|b)(c|d)^\r\n]+?'` 无效。
- 正则表达式中，零次重复量词“*”和“?”前面必须有四个确定字符。例如 `'abc*'` 无效，`'abcd*DoS\x2d\d{5}\x20\x2bxi\r\nJOIN'` 有效。

【举例】

在 URL 过滤分类 news 中添加一条 URL 过滤规则，并使用以 sina.com 开头的字符串对主机名字段进行匹配。

```
<Sysname> system-view
[Sysname] url-filter category news
[Sysname-url-filter-category-news] rule 10 host text sina.com
```

【相关命令】

- **url-filter category**

1.1.13 update schedule

update schedule 命令用来配置定期自动在线升级 URL 过滤特征库的时间。

undo update schedule 命令用来恢复缺省情况。

【命令】

```
update schedule { daily | weekly { fri | mon | sat | sun | thu | tue | wed } }
start-time time tingle minutes
undo update schedule
```

【缺省情况】

设备在每天 01:00:00 至 03:00:00 之间自动在线升级 URL 过滤特征库。

【视图】

自动升级配置视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

daily: 表示自动升级周期为每天。

weekly: 表示以一周为周期，在指定的一天进行自动升级。

fri: 表示星期五。

mon: 表示星期一。

sat: 表示星期六。

sun: 表示星期日。

thu: 表示星期四。

tue: 表示星期二。

wed: 表示星期三。

start-time time: 指定自动升级开始时间，*time* 的格式为 hh:mm:ss，取值范围为 00:00～23:59:59。

tingle minutes: 指定抖动时间，即实际自动升级开始时间的偏差范围，取值范围为 0～120，单位为分钟。在 **start-time** 指定时间的前后各偏移抖动时间的一半作为自动升级的时间范围，

例如,指定自动升级的开始时间为 01:00:00,抖动时间为 60 分钟,则自动升级的时间范围为 00:30:00 至 01:30:00。

【举例】

配置 URL 过滤特征库的定期自动在线升级时间为每周日 20:30:00, 抖动时间为 10 分钟。

```
<Sysname> system-view
```

```
[Sysname] url-filter signature auto-update
```

```
[Sysname-url-filter-autoupdate] update schedule weekly sun start-time 20:30:00 tingle 10
```

【相关命令】

- **url-filter signatures auto-update**

1.1.14 url-filter apply policy

url-filter apply policy 命令用来在 DPI 应用 profile 中引用指定的 URL 过滤策略。

undo url-filter apply policy 命令用来删除引用的 URL 过滤策略。

【命令】

```
url-filter apply policy policy-name
```

```
undo url-filter apply policy
```

【缺省情况】

DPI 应用 profile 中未引用 URL 过滤策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: URL 过滤策略名称, 为 1~31 个字符的字符串, 不区分大小写。

【使用指导】

URL 过滤策略仅在被 DPI 应用 profile 引用后生效。一个 DPI 应用 profile 下只能引用一个 URL 过滤策略。多次执行本命令, 最后一次执行的命令生效。

【举例】

在名为 abc 的 DPI 应用 profile 下引用 URL 过滤策略 news。

```
<Sysname> system-view
```

```
[Sysname] app-profile abc
```

```
[Sysname-app-profile-abc]url-filter apply policy news
```

【相关命令】

- **app-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **display app-profile**
- **display url-filter policy**

1.1.15 url-filter category

url-filter category 命令用来创建 URL 过滤分类，并进入 URL 过滤分类视图。如果指定的 URL 过滤分类已经存在，则直接进入该 URL 过滤分类视图。

undo url-filter category 命令用来删除指定的 URL 过滤分类。

【命令】

url-filter category *category-name* [**severity** *severity-level*]

undo url-filter category *category-name*

【缺省情况】

只存在预定义的 URL 过滤分类，且分类名称以字符串 Pre-开头。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

category-name: 表示 URL 过滤分类的名称，为 1~63 个字符的字符串，不区分大小写。不能以字符“Pre-”开头，因为 Pre-是预定义的 URL 过滤分类名称。

severity severity-value: 表示 URL 过滤分类的严重级别属性。**severity-value** 为严重级别，取值范围为 1000~65535，创建 URL 过滤分类时必须配置此参数，数值越大表示严重级别越高，且不同的 URL 过滤分类的严重级别不能相同。

【使用指导】

为便于管理员对数目众多的 URL 过滤规则进行统一部署，URL 过滤模块提供了 URL 过滤分类功能，以便对具有相似特征的 URL 过滤规则进行归纳以及为匹配这些规则的 URL 统一指定处理动作。每个 URL 过滤分类具有一个严重级别属性，该属性值表示对属于此过滤分类 URL 的处理优先级。

URL 过滤分类包括两种类型：

- 预定义分类：根据设备中的 URL 过滤特征库自动生成，其内容和严重级别不可被修改。
- 自定义分类：由管理员手动配置，可修改其严重级别，可添加 URL 过滤规则。

当报文匹配成功的 URL 过滤规则同属于多个 URL 过滤分类时，设备将根据严重级别最高的 URL 过滤分类中指定的动作对此报文进行处理。

【举例】

创建一个名为 news 的 URL 过滤分类，指定其严重级别为 2000。

```
<Sysname> system-view
[Sysname] url-filter category news severity 2000
[Sysname-url-filter-category-news]
```

【相关命令】

- **display url-filter category**

1.1.16 url-filter copy category

url-filter copy category 命令用来复制 URL 过滤分类。

【命令】

url-filter copy category *old-name new-name severity severity-level*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

old-name: 原有分类名称。必须为已创建的自定义分类。

new-name: 新分类名称，为 1~63 个字符的字符串，不区分大小写。不能以字符“Pre-”开头，因为 Pre-是预定义的 URL 过滤分类名称。

severity severity-level: 表示 URL 过滤分类的严重级别。**severity-level** 为严重级别，取值范围为 1000~65535。数值越大表示严重级别越高，且不同的分类严重级别不能相同，如果相同，则复制失败。

【使用指导】

本命令用来复制已存在的 URL 过滤分类，可以方便用户快速创建新的 URL 过滤分类。
目前，仅支持复制自定义 URL 过滤分类。

【举例】

通过复制名称为 news 的 URL 过滤分类来创建一个名为 test 的 URL 过滤分类。

```
<Sysname> system-view
```

```
[Sysname] url-filter copy category news test severity 1001
```

```
[Sysname-url-filter-category-test]
```

【相关命令】

- **url-filter category**

1.1.17 url-filter copy policy

url-filter copy policy 命令用来复制 URL 过滤策略。

【命令】

url-filter copy policy *old-name new-name*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

old-name: 原有策略名称。为 1~31 个字符的字符串，不区分大小写。

new-name: 新策略名称。为 1~31 个字符的字符串，不区分大小写。

【使用指导】

本命令用来复制已存在的 URL 过滤策略，可以方便用户快速创建新的 URL 过滤策略。

【举例】

通过复制名称为 news 的 URL 过滤策略来创建 2 个新的 URL 过滤策略。

```
<Sysname> system-view
[Sysname] url-filter copy policy news news1
[Sysname-url-filter-policy-news_1] quit
[Sysname] url-filter copy policy news new2
[Sysname-url-filter-policy-news_2] quit
```

【相关命令】

- **url-filter policy**

1.1.18 url-filter log directory root

url-filter log directory root 命令用来配置 URL 过滤仅对网站根目录下资源的访问进行日志记录。

undo url-filter log directory root 命令用来恢复缺省情况。

【命令】

```
url-filter log directory root
undo url-filter log directory root
```

【缺省情况】

URL 过滤对网站所有路径下资源的访问均进行日志记录。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

配置此命令后，**url-filter log except pre-defined** 和 **url-filter log except user-defined** 命令将失效。

【举例】

配置 URL 过滤仅对网站根目录下资源的访问进行日志记录。

```
<Sysname> system-view
[Sysname] url-filter log directory root
```

【相关命令】

- **category action logging**
- **default-action logging**
- **url-filter log except pre-defined**
- **url-filter log except user-defined**

1.1.19 url-filter log enable

url-filter log enable 命令用来开启应用层检测引擎日志信息功能。

undo url-filter log enable 命令用来关闭应用层检测引擎日志信息功能。

【命令】

```
url-filter log enable  
undo url-filter log enable
```

【缺省情况】

应用层检测引擎日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

应用层检测引擎日志是为了满足管理员审计需求。设备生成应用层检测引擎日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

```
# 开启应用层检测引擎日志信息功能。  
<Sysname> system-view  
[Sysname] url-filter log enable
```

1.1.20 url-filter log except pre-defined

url-filter log except pre-defined 命令用来配置 URL 过滤对预定义类型网页资源的访问不进行日志记录。

undo url-filter log except pre-defined 命令用来配置 URL 过滤对预定义类型网页资源的访问进行日志记录。

【命令】

```
url-filter log except pre-defined { css | gif | ico | jpg | js | png | swf  
| xml }
```

```
undo url-filter log except pre-defined { css | gif | ico | jpg | js | png  
| swf | xml }
```

【缺省情况】

URL 过滤对所有预定义类型网页资源的访问不进行日志记录。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

css: 表示网页资源类型为 css。

gif: 表示网页资源类型为 gif。

ico: 表示网页资源类型为 ico。

jpg: 表示网页资源类型为 jpg。

js: 表示网页资源类型为 js。

png: 表示网页资源类型为 png。

swf: 表示网页资源类型为 swf。

xml: 表示网页资源类型为 xml。

【使用指导】

此命令生效的优先级低于 **url-filter log directory root** 命令, 如果已经配置 **url-filter log directory root** 命令, 则本配置不能生效。因此, 如果要本配置生效, 则需要执行 **undo url-filter log directory root** 命令。

可多次执行此命令, 指定多种不记录访问日志的预定义网页资源类型。

【举例】

配置 URL 过滤对预定义 css 类型网页资源的访问不进行日志记录。

```
<Sysname> system-view
```

```
[Sysname] url-filter log except pre-defined css
```

【相关命令】

- **category action logging**
- **default-action logging**
- **url-filter log directory root**
- **url-filter log except user-defined**

1.1.21 url-filter log except user-defined

url-filter log except user-defined 命令用来配置 URL 过滤对自定义类型网页资源的访问不进行日志记录。

undo url-filter log except user-defined 命令用来配置 URL 过滤对自定义类型网页资源的访问进行日志记录。

【命令】

```
url-filter log except user-defined text
undo url-filter log except user-defined [ text ]
```

【缺省情况】

未配置自定义类型网页资源，URL 过滤对除预定义类型之外的所有网页资源的访问均进行日志记录。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

text：表示自定义网页资源类型，取值范围为 1~63 个字符的字符串，不区分大小写。

【使用指导】

此命令生效的优先级低于 **url-filter log directory root** 命令，如果已经配置 **url-filter log directory root** 命令，则本配置不能生效。因此，如果要本配置生效，则需要执行 **undo url-filter log directory root** 命令。

可多次执行此命令，指定多种不记录访问日志的自定义网页资源类型。

执行 **undo url-filter log except user-defined** 命令时，若未指定任何参数，则表示 URL 过滤对所有自定义类型网页资源的访问均进行日志记录。

【举例】

```
# 配置 URL 过滤对自定义 html 类型网页资源的访问不进行日志记录。
<Sysname> system-view
[Sysname] url-filter log except user-defined html
```

【相关命令】

- **category action logging**
- **default-action logging**
- **url-filter log directory root**
- **url-filter log except pre-defined**

1.1.22 url-filter policy

url-filter policy 命令用来创建 URL 过滤策略，并进入 URL 过滤策略视图。如果指定的 URL 过滤策略已经存在，则直接进入 URL 过滤策略视图。

undo url-filter policy 命令用来删除指定的 URL 过滤策略。

【命令】

```
url-filter policy policy-name
```

undo url-filter policy *policy-name*

【缺省情况】

不存在 URL 过滤策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: 表示 URL 过滤策略的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

一个 URL 过滤策略中可以为每个 URL 过滤分类配置动作，也可以在 URL 过滤策略中定义 URL 过滤策略的缺省动作。

URL 过滤策略仅在被 DPI 应用 **profile** 中引用后生效。有关 DPI 应用 **profile** 的详细介绍请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

【举例】

```
# 创建一个名为 news 的 URL 过滤策略
<Sysname> system-view
[Sysname] url-filter policy news
[Sysname-url-filter-policy-news]
```

1.1.23 url-filter signature auto-update

url-filter signature auto-update 命令用来开启定期自动在线升级 URL 过滤特征库功能，并进入自动升级配置视图。

undo url-filter signature auto-update 命令用来关闭定期自动在线升级 URL 过滤特征库功能。

【命令】

```
url-filter signature auto-update
undo url-filter signature auto-update
```

【缺省情况】

定期自动在线升级 URL 过滤特征库功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果设备可以访问官方网站上的特征库服务专区，可以采用定期自动在线升级方式来对设备上的 URL 过滤特征库进行升级。

【举例】

开启定期自动在线升级 URL 过滤特征库功能，并进入自动升级配置视图。

```
<Sysname> system-view
[Sysname] url-filter signature auto-update
[Sysname-url-filter-autoupdate]
```

【相关命令】

- **update schedule**

1.1.24 url-filter signature auto-update-now

url-filter signature auto-update-now 命令用来立即自动在线升级 URL 过滤特征库。

【命令】

url-filter signature auto-update-now

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

当管理员发现官方网站上的特征库服务专区中的 URL 过滤特征库有更新时，可以选择立即自动在线升级方式来及时升级 URL 过滤特征库版本。

【举例】

立即自动在线升级 URL 过滤特征库版本。

```
<Sysname> system-view
[Sysname] url-filter signature auto-update-now
```

1.1.25 url-filter signature rollback

url-filter signature rollback 命令用来回滚 URL 过滤特征库版本。

【命令】

url-filter signature rollback { factory | last }

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

factory: 表示 URL 过滤特征库的出厂版本。

last: 表示 URL 过滤特征库的上一版本。

【使用指导】

URL 过滤特征库回滚是指将当前的 URL 过滤特征库版本回滚到指定的 URL 过滤特征库版本。如果管理员发现设备对用户访问 Web 的 URL 过滤的误报率较高或出现异常情况，则可以对当前 URL 过滤特征库版本进行回滚。目前支持将设备中的 URL 过滤特征库版本回滚到出厂版本和上一版本。

URL 过滤特征库版本每次回滚前，设备都会备份当前版本。多次回滚上一版本的操作将会在当前版本和上一版本之间反复切换。例如当前 URL 过滤特征库版本是 V2，上一版本是 V1，第一次执行回滚到上一版本的操作后，特征库替换成 V1 版本，再执行回滚上一版本的操作则特征库重新变为 V2 版本。

【举例】

配置 URL 过滤特征库回滚到上一版本。

```
<Sysname> system-view  
[Sysname] url-filter signature rollback last
```

1.1.26 url-filter signature update

url-filter signature update 命令用来手动离线升级 URL 过滤特征库。

【命令】

url-filter signature update *file-path*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

file-path: 指定特征库文件的路径，为 1~255 个字符的字符串。

【使用指导】

如果设备不能访问官方网站上的特征库服务专区，管理员可以采用如下几种方式手动离线升级 URL 过滤特征库版本。

- 本地升级：使用本地保存的特征库文件升级系统上的 URL 过滤特征库版本。
- FTP/TFTP 升级：通过 FTP 或 TFTP 方式下载远程服务器上保存的特征库文件，并升级系统上的 URL 过滤特征库版本。

使用本地升级方式离线升级特征库版本时，特征库文件只能存储在当前主用设备上，否则设备升级特征库会失败。

参数 *file-path* 的取值与手动离线升级的操作方式有关。本地升级时参数 *file-path* 取值请参见 [表 1-5](#)；FTP/TFTP 升级时参数 *file-path* 取值请参见 [表 1-6](#)。

表1-5 本地升级时参数 *file-path* 取值说明表

升级场景	参数 <i>file-path</i> 取值	说明
特征库文件的存储位置与当前工作路径一致	<i>filename</i>	可以执行 pwd 命令查看当前工作路径 有关 pwd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不一致，且在相同存储介质上	<i>filename</i>	需要先执行 cd 命令将工作路径切换至特征库文件所在目录下 有关 cd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不在相同存储介质上	<i>path/ filename</i>	需要先执行 cd 命令将工作路径切换至特征库文件所在存储介质的根目录下，再指定特征库文件的相对路径 有关 cd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”

表1-6 FTP/TFTP 升级时参数 *file-path* 取值说明表

升级场景	参数 <i>file-path</i> 取值	说明
特征库文件存储在开启FTP服务的远程服务器上	<i>ftp://username:password@server/filename</i>	<i>username</i> 为登录FTP服务器的用户名， <i>password</i> 为登录FTP服务器的密码， <i>server</i> 为FTP服务器的IP地址或主机名 当FTP的用户名和密码中使用了“:”、“@”和“/”三种特殊字符时，需要将这三种特殊字符替换为其对应的转义字符。“:”、“@”和“/”三种特殊字符对应的转义字符分别为“%3A或%3a”、“%40”和“%2F或%2f”
特征库文件存储在开启TFTP服务的远程服务器上	<i>tftp://server/filename</i>	<i>server</i> 为TFTP服务器的IP地址或主机名



说明

当采用 FTP/TFTP 方式升级特征库时，如果指定的是服务器的主机名，则需要确保设备能通过静态或动态域名解析方式获得 FTP/TFTP 服务器的 IP 地址，并与之路由可达。否则设备升级特征库会失败。有关域名解析功能的详细配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

【举例】

配置手动离线升级 URL 过滤特征库，且采用 TFTP 方式，URL 过滤特征库文件的远程路径为 *tftp://192.168.0.10/url-filter-1.0.2-en.dat*。

```
<Sysname> system-view
```

```
[Sysname] url-filter signature update tftp://192.168.0.10/url-filter-1.0.2-en.dat
```

配置手动离线升级 URL 过滤特征库，且采用 FTP 方式，URL 过滤特征库文件的远程路径为 *ftp://192.168.0.10/url-filter-1.0.2-en.dat*，用户名为 *user:123*，密码为 *user@abc/123*。


```
<Sysname> system-view
[Sysname] url-filter signature update
ftp://user%3A123:user%40abc%2F123@192.168.0.10/url-filter-1.0.2-en.dat
# 配置手动离线升级 URL 过滤特征库，且采用本地方式，URL 过滤特征库文件的本地路径为
cfa0:/url-filter-1.0.23-en.dat，且当前工作路径为 cfa0:。
<Sysname> system-view
[Sysname] url-filter signature update url-filter-1.0.23-en.dat
# 配置手动离线升级 URL 过滤特征库，且采用本地方式，URL 过滤特征库文件的本地路径为
cfa0:/dpi/url-filter-1.0.23-en.dat，且当前工作路径为 cfa0:。
<Sysname> cd dpi
<Sysname> system-view
[Sysname] url-filter signature update url-filter-1.0.23-en.dat
# 配置手动离线升级 URL 过滤特征库，且采用本地方式，URL 过滤特征库文件的本地路径为
cfb0:/dpi/url-filter-1.0.23-en.dat，当前工作路径为 cfa0:。
<Sysname> cd cfb0:/
<Sysname> system-view
[Sysname] url-filter signature update dpi/url-filter-1.0.23-en.dat
```

目 录

1 数据过滤	1
1.1 数据过滤配置命令	1
1.1.1 action	1
1.1.2 application	1
1.1.3 data-filter apply policy	2
1.1.4 data-filter keyword-group	3
1.1.5 data-filter policy	4
1.1.6 description (data-filter policy view)	5
1.1.7 description (keyword-group view)	5
1.1.8 direction	6
1.1.9 keyword-group	7
1.1.10 pattern	7
1.1.11 pre-defined-pattern	8
1.1.12 rule	9

1 数据过滤

1.1 数据过滤配置命令

1.1.1 action

action 命令用来配置数据过滤规则的动作。

undo action 命令用来恢复缺省情况。

【命令】

```
action { drop | permit } [ logging ]  
undo action
```

【缺省情况】

数据过滤规则的动作作为丢弃。

【视图】

数据过滤规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

drop: 表示丢弃报文。

permit: 表示允许报文通过。

logging: 表示生成日志信息。

【使用指导】

如果报文同时与多个规则匹配成功，则执行这些动作中优先级最高的动作，且动作优先级从高到低的顺序为：丢弃 > 允许，但是对于生成日志动作只要匹配成功的规则中存在就会执行。

【举例】

```
# 创建一个名称为 def 的数据过滤策略。  
<Sysname> system-view  
[Sysname] data-filter policy def  
# 在名称为 r1 的数据过滤规则中配置其动作为允许报文通过。  
[Sysname-data-filter-policy-def] rule r1  
[Sysname-data-filter-policy-def-rule-r1] action permit
```

1.1.2 application

application 命令用来配置数据过滤规则的应用层协议类型。

undo application 命令用来删除指定的应用层协议类型。

【命令】

```
application { all | type { ftp | http | imap | nfs | pop3 | rtmp | smb | smtp } * }  
undo application { all | type { ftp | http | imap | nfs | pop3 | rtmp | smb | smtp }  
* }
```

【缺省情况】

数据过滤规则中不存在应用层协议类型。

【视图】

数据过滤规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

all: 表示数据过滤支持的所有应用层协议。

type: 表示规则生效的协议类型。

ftp: 表示 FTP 协议。

http: 表示 HTTP 协议。

imap: 表示 IMAP 协议。

nfs: 表示 NFS 协议。

pop3: 表示 POP3 协议。

rtmp: 表示 RTMP 协议。

smb: 表示 SMB 协议。

smtp: 表示 SMTP 协议。

【使用指导】

通过配置此命令，可以根据业务应用所属的应用层协议类型来灵活控制对那些协议类型的报文进行数据过滤。

NFS 协议仅支持 NFSv3 版本；SMB 协议支持 SMBv1 和 SMBv2 版本。

【举例】

创建一个名称为 **def** 的数据过滤策略。

```
<Sysname> system-view
```

```
[Sysname] data-filter policy def
```

在名称为 **r1** 的数据过滤规则中配置其应用层协议类型为 **HTTP**。

```
[Sysname-data-filter-policy-def] rule r1
```

```
[Sysname-data-filter-policy-def-rule-r1] application type http
```

1.1.3 data-filter apply policy

data-filter apply policy 命令用来在 DPI 应用 **profile** 中引用指定的数据过滤策略。

undo data-filter apply policy 命令用来删除引用的数据过滤策略。

【命令】

```
data-filter apply policy policy-name  
undo data-filter apply policy
```

【缺省情况】

DPI 应用 profile 中未引用数据过滤策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

policy-name: 指定数据过滤策略的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

数据过滤规则仅在 DPI 应用 profile 引用后生效。一个 DPI 应用 profile 下只能引用一个数据过滤策略。

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 在名称为 abc 的 DPI 应用 profile 下引用数据过滤策略 def。  
<Sysname> system-view  
[Sysname] app-profile abc  
[Sysname-app-profile-abc] data-filter apply policy def
```

【相关命令】

- **app-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **data-filter policy**

1.1.4 data-filter keyword-group

data-filter keyword-group 命令用来创建关键字组，并进入关键字组视图。如果指定的关键字组已经存在，则直接进入关键字组视图。

undo data-filter keyword-group 命令用来删除指定的关键字组。

【命令】

```
data-filter keyword-group keywordgroup-name  
undo data-filter keyword-group keywordgroup-name
```

【缺省情况】

不存在关键字组。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

keywordgroup-name: 表示关键字组的名字，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

关键字组用来统一组织和管理设备中配置的数据过滤特征，一个关键字组中可以配置多个数据过滤特征，且特征之间是或的关系。

【举例】

```
# 创建一个名称为 kg1 的关键字组，并进入关键字组视图。  
<Sysname> system-view  
[Sysname] data-filter keyword-group kg1  
[Sysname-data-filter-keygroup-kg1]
```

1.1.5 data-filter policy

data-filter policy 命令用来创建数据过滤策略，并进入数据过滤策略视图。如果指定的数据过滤策略已经存在，则直接进入该数据过滤策略视图。

undo data-filter policy 命令用来删除指定的数据过滤策略。

【命令】

```
data-filter policy policy-name  
undo data-filter policy policy-name
```

【缺省情况】

不存在数据过滤策略。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 表示数据过滤策略的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

一个数据过滤策略中最多可创建 32 个数据过滤规则。

【举例】

```
# 创建一个名称为 def 的数据过滤策略，并进入该数据过滤策略视图。  
<Sysname> system-view  
[Sysname] data-filter policy def  
[Sysname-data-filter-policy-def]
```

【相关命令】

- **data-filter apply policy**

1.1.6 description (data-filter policy view)

description 命令用来配置数据过滤策略的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *string*

undo description

【缺省情况】

未配置数据过滤策略的描述信息。

【视图】

数据过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

string: 表示数据过滤策略的描述信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别本数据过滤策略的作用。

【举例】

配置数据过滤策略 **def** 的描述信息为 The data filter。

```
<Sysname> system-view
```

```
[Sysname] data-filter policy def
```

```
[Sysname-data-filter-policy-def] description The data filter
```

1.1.7 description (keyword-group view)

description 命令用来配置关键字组的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *string*

undo description

【缺省情况】

未配置关键字组的描述信息。

【视图】

关键字组视图

【缺省用户角色】

network-admin
context-admin

【参数】

string: 关键字组的描述信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别本关键字组的作用。

【举例】

```
# 配置关键字组 kg1 的描述信息为 The data filter keyword group。
<Sysname> system-view
[Sysname] data-filter keyword-group kg1
[Sysname-data-filter-kg1] description The data filter keyword group
```

1.1.8 direction

direction 命令用来配置数据过滤规则的匹配方向。

undo direction 命令用来恢复缺省情况。

【命令】

```
direction { both | download | upload }
undo direction
```

【缺省情况】

数据过滤规则的匹配方向为会话的上传方向。

【视图】

数据过滤规则视图

【缺省用户角色】

network-admin
context-admin

【参数】

both: 在会话的上传方向和下载方向都进行匹配。

download: 在会话的下载方向进行匹配。

upload: 在会话的上传方向进行匹配。

【使用指导】

通过配置此命令，可以根据报文传输的方向来灵活控制对哪个方向的报文进行数据过滤。

【举例】

```
# 创建一个名称为 def 的数据过滤策略。
<Sysname> system-view
[Sysname] data-filter policy def
# 在名称为 r1 的数据过滤规则中配置其匹配方向为会话的下载方向。
```



```
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1] direction download
```

1.1.9 keyword-group

keyword-group 命令用来在数据过滤规则中引用关键字组。

undo keyword-group 命令用来恢复缺省情况。

【命令】

```
keyword-group keygroup-name
undo keyword-group
```

【缺省情况】

数据过滤规则中未引用关键字组。

【视图】

数据过滤规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

keygroup-name: 表示关键字组的名称，为 1~31 个字符的字符串，不区分大小写。引用的关键字组必须存在。

【使用指导】

在数据过滤规则中通过引用关键字组来对报文的应用层信息进行关键字匹配。

在同一个数据过滤规则视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 创建一个名称为 def 的数据过滤策略。
<Sysname> system-view
[Sysname] data-filter policy def
# 在名称为 r1 的数据过滤规则中引用关键字组 kg1。
[Sysname-data-filter-policy-def] rule r1
[Sysname-data-filter-policy-def-rule-r1] keyword-group kg1
```

【相关命令】

- **data-filter keyword-group**

1.1.10 pattern

pattern 命令用来配置数据过滤特征。

undo pattern 命令用来删除指定的数据过滤特征。

【命令】

```
pattern pattern-name { regex | text } pattern-string
```

undo pattern *pattern-name*

【缺省情况】

关键字组中不存在数据过滤特征。

【视图】

关键字组视图

【缺省用户角色】

network-admin

context-admin

【参数】

pattern-name: 表示数据过滤特征的名称，为 1~31 个字符的字符串，不区分大小写。

regex pattern-string: 表示对应用层信息进行模糊匹配的正则表达式，为 3~245 个字符的字符串，区分大小写，支持所有可输入字符，且必须包含连续的 3 个非通配符。

text pattern-string: 表示对应用层信息进行精确匹配的文本，为 3~245 个字符的字符串，支持所有可输入字符，区分大小写。

【使用指导】

一个数据过滤特征只能定义为一个正则表达式字符串或一个文本字符串。

一个关键字组中可以配置 32 个数据过滤特征，且特征之间是或的关系。

正则表达式有如下限制：

- 正则表达式中，总的分支不能超过四个。例如'abc(c|d|e|\x3D)'有效，'abc(c|onreset|onselect|onchange|style\x3D)'无效。
- 正则表达式中，括号不能嵌套，即括号中不能有括号。例如'ab((abcs*?))'无效。
- 正则表达式中，分支不支持串联，即分支后面不能有分支。例如'ab(a|b)(c|d)^\r\n]+?'无效。
- 正则表达式中，零次重复量词'*'和'?'前面必须有四个确定字符。例如'abc*'无效，'abcd*DoS\x2d\d{5}\x20\x2bxi\r\nJOIN'有效。

【举例】

```
# 在关键字组 kg1 中配置一条正则表达式，内容为(?i)^.*abc.*。  
<Sysname> system-view  
[Sysname] data-filter keyword-group kg1  
[Sysname-data-filter-kgroup-kg1] pattern 1 regex (?i)^.*abc.*
```

1.1.11 pre-defined-pattern

pre-defined-pattern 命令用来启用指定类型的预定义数据过滤特征。

undo pre-defined-pattern 命令用来禁用指定类型的预定义数据过滤特征。

【命令】

```
pre-defined-pattern name { bank-card-number | credit-card-number |  
id-card-number | phone-number }  
undo pre-defined-pattern name { bank-card-number | credit-card-number |  
id-card-number | phone-number }
```

【缺省情况】

关键字组中未启用预定义特征。

【视图】

关键字组视图

【缺省用户角色】

network-admin

context-admin

【参数】

name: 表示预定义数据过滤特征的名字。

bank-card-number: 表示银行卡号类型的预定义数据过滤特征。

credit-card-number: 表示信用卡号类型的预定义数据过滤特征。

id-card-number: 表示身份证号类型的预定义数据过滤特征。

phone-number: 表示手机号类型的预定义数据过滤特征。

【使用指导】

启用指定类型的预定义数据过滤特征后，设备将对包含该特征信息的文件和内容进行识别和过滤。

可多次执行本命令，启用多种类型的预定义数据过滤特征。

【举例】

在关键字组 **kg1** 中启用手机号码类型的预定义数据过滤特征。

```
<Sysname> system-view
```

```
[Sysname] data-filter keyword-group kg1
```

```
[Sysname-data-filter-kgroup-kg1] pre-defined-pattern name phone-number
```

1.1.12 rule

rule 命令用来创建数据过滤规则，并进入数据过滤规则视图。如果指定的数据过滤规则已经存在，则直接进入数据过滤规则视图。

undo rule 命令用来删除指定的数据过滤规则。

【命令】

rule *rule-name*

undo rule *rule-name*

【缺省情况】

不存在数据过滤规则。

【视图】

数据过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-name: 表示数据过滤规则的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

在数据过滤规则中可以配置匹配报文的一系列匹配项，比如规则匹配的方向、规则生效的协议类型、规则引用的关键字组和规则的动作。

【举例】

在名称为 **def** 的数据过滤策略下创建一个名称为 **r1** 的数据过滤规则，并进入数据过滤规则视图。

```
<Sysname> system-view  
[Sysname] data-filter policy def  
[Sysname-data-filter-policy-def] rule r1  
[Sysname-data-filter-policy-def-rule-r1]
```

目 录

1 文件过滤	1
1.1 文件过滤配置命令	1
1.1.1 action	1
1.1.2 application	1
1.1.3 description (file-filter policy view)	2
1.1.4 description (filetype-group view)	3
1.1.5 direction	4
1.1.6 file-filter apply policy	5
1.1.7 file-filter false-extension action	5
1.1.8 file-filter filetype-group	6
1.1.9 file-filter policy	7
1.1.10 filetype-group	8
1.1.11 pattern	8
1.1.12 rule	9

1 文件过滤

1.1 文件过滤配置命令

1.1.1 action

action 命令用来配置文件过滤规则的动作。

undo action 命令用来恢复缺省情况。

【命令】

```
action { drop | permit } [ logging ]  
undo action
```

【缺省情况】

文件过滤规则的动作作为丢弃。

【视图】

文件过滤规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

drop: 表示丢弃报文。

permit: 表示允许报文通过。

logging: 表示生成日志信息。

【使用指导】

如果文件的扩展名信息同时与多个规则匹配成功，则执行这些动作中优先级最高的动作，且动作优先级从高到低的顺序为：丢弃 > 允许，但是对于生成日志动作只要匹配成功的规则中存在就会执行。如果文件的扩展名信息只与一个规则匹配成功，则执行此规则中的动作。

【举例】

```
# 创建一个名称为 def 的文件过滤策略。  
<Sysname> system-view  
[Sysname] file-filter policy def  
# 在名称为 ch1 的文件过滤规则中配置其动作为允许报文通过。  
[Sysname-file-filter-policy-def] rule ch1  
[Sysname-file-filter-policy-def-rule-ch1] action permit
```

1.1.2 application

application 命令用来配置文件过滤规则的应用层协议类型。

undo application 命令用来删除指定的应用层协议类型。

【命令】

```
application { all | type { ftp | http | imap | nfs | pop3 | rtmp | smb | smtp } * }  
undo application { all | type { ftp | http | imap | nfs | pop3 | rtmp | smb | smtp }  
* }
```

【缺省情况】

文件过滤规则中不存在应用层协议类型。

【视图】

文件过滤规则视图。

【缺省用户角色】

network-admin

context-admin

【参数】

all: 表示文件过滤支持的所有应用层协议。

type: 表示规则生效的协议类型。

ftp: 表示 FTP 协议。

http: 表示 HTTP 协议。

imap: 表示 IMAP 协议。

nfs: 表示 NFS 协议。

pop3: 表示 POP3 协议。

rtmp: 表示 RTMP 协议。

smb: 表示 SMB 协议。

smtp: 表示 SMTP 协议。

【使用指导】

通过配置此命令，可以根据文件传输所采用的应用层协议类型来灵活控制对哪些协议类型的报文进行文件过滤。

NFS 协议仅支持 NFSv3 版本；SMB 协议支持 SMBv1 和 SMBv2 版本。

【举例】

创建一个名称为 **def** 的文件过滤策略。

```
<Sysname> system-view
```

```
[Sysname] file-filter policy def
```

在名称为 **ch1** 的文件过滤规则中配置其应用协议类型为 HTTP。

```
[Sysname-file-filter-policy-def] rule ch1
```

```
[Sysname-file-filter-policy-def-rule-ch1] application type http
```

1.1.3 description (file-filter policy view)

description 命令用来配置文件过滤策略的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *string*
undo description

【缺省情况】

未配置文件过滤策略的描述信息。

【视图】

文件过滤策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

string: 表示文件过滤策略的描述信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别本文件过滤策略的作用，有利于后期维护。

【举例】

```
# 配置文件过滤策略 def 的描述信息为 The file filter。  
<Sysname> system-view  
[Sysname] file-filter policy def  
[Sysname-file-filter-policy-def] description The file filter
```

【相关命令】

- **file-filter policy**

1.1.4 description (filetype-group view)

description 命令用来配置文件类型组的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *string*
undo description

【缺省情况】

未配置文件类型组的描述信息。

【视图】

文件类型组视图

【缺省用户角色】

network-admin
context-admin

【参数】

string: 文件类型组的描述信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

通过合理编写描述信息，便于管理员快速理解和识别本文件类型组的作用，有利于后期维护。

【举例】

```
# 为文件类型组 abc 配置描述信息 def。  
<Sysname> system-view  
[Sysname] file-filter filetype-group abc  
[Sysname-file-filter-fgroup-abc] description def
```

【相关命令】

- **file-filter filetype-group**

1.1.5 direction

direction 命令用来配置文件过滤规则的匹配方向。

undo direction 命令用来恢复缺省情况。

【命令】

```
direction { both | download | upload }  
undo direction
```

【缺省情况】

文件过滤规则的匹配方向为上传方向。

【视图】

文件过滤规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

both: 在上传方向和下载方向都进行匹配。

download: 在下载方向进行匹配。

upload: 在上传方向进行匹配。

【使用指导】

通过配置此命令，可以根据报文传输的方向来灵活控制对那个方向的报文进行文件过滤。

对于 FTP 和 SMTP 协议上传方向和下载方向是指会话的上传和下载方向；对于 HTTP 协议上传方向是指 HTTP 协议 POST 类型的请求方法，下载方向是指 HTTP 协议 GET 类型的请求方法。

【举例】

```
# 创建一个名称为 def 的文件过滤策略。  
<Sysname> system-view  
[Sysname] file-filter policy def
```

```
# 在名称为 ch1 的文件过滤规则中配置其匹配方向为下载方向。  
[Sysname-file-filter-policy-def] rule ch1  
[Sysname-file-filter-policy-def-rule-ch1] direction download
```

1.1.6 file-filter apply policy

file-filter apply policy 命令用来在 DPI 应用 profile 中引用文件过滤策略。

undo file-filter apply policy 命令用来删除引用的文件过滤策略。

【命令】

```
file-filter apply policy policy-name  
undo file-filter apply policy
```

【缺省情况】

DPI 应用 profile 中未引用文件过滤策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

policy-name: 文件过滤策略的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

文件过滤策略仅在被 DPI 应用 profile 引用后生效。一个 DPI（Deep Packet Inspection，深度报文检测）应用 profile 下只能引用一个文件过滤策略。多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 在名称为 abc 的 DPI 应用 profile 下引用文件过滤策略 def。  
<Sysname> system-view  
[Sysname] app-profile abc  
[Sysname-app-profile-abc] file-filter apply policy def
```

【相关命令】

- **app-profile**
- **file-filter policy**

1.1.7 file-filter false-extension action

file-filter false-extension action 命令用来配置文件的真实类型与扩展名不一致时执行的动作。

undo file-filter false-extension action 命令用来恢复缺省情况。

【命令】

```
file-filter false-extension action { drop | permit }
```

undo file-filter false-extension action

【缺省情况】

文件的真实类型与扩展名不一致时执行的动作为允许。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

drop: 表示丢弃报文。

permit: 表示允许报文通过。

【使用指导】

当设备识别出的文件的真实类型和文件的扩展名不一致时，如果动作配置为允许，则根据识别出的真实的文件类型与文件过滤规则进行匹配，并执行文件过滤规则中的动作；如果动作配置为阻断，则直接对报文进行阻断，不再进行文件过滤规则的匹配。

例如，file.txt 文件可通过修改扩展名，将其改为 file.exe 文件。文件过滤将会识别出其真实的文件类型为 txt，这与该文件的扩展名不一致，设备将根据本命令中配置的动作对该文件进行处理。

【举例】

配置文件的真实类型与扩展名不一致时执行的动作为丢弃。

```
<Sysname> system-view
```

```
[Sysname] file-filter false-extension action drop
```

1.1.8 file-filter filetype-group

file-filter filetype-group 命令用来创建文件类型组，并进入文件类型组视图。如果指定的文件类型组已经存在，则直接进入文件类型组视图。

undo file-filter filetype-group 命令用来删除指定的文件类型组。

【命令】

file-filter filetype-group *group-name*

undo file-filter filetype-group *group-name*

【缺省情况】

不存在文件类型组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name: 表示文件类型组的名字，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

文件类型组用来统一组织和管理设备中配置的文件过滤特征。一个文件类型组中可以配置多个文件过滤特征，且它们之间是或的关系。

【举例】

创建一个名称为 **fg1** 的文件类型组，并进入文件类型组视图。

```
<Sysname> system-view
[Sysname] file-filter filetype-group fg1
[Sysname-file-filter-fgroup-fg1]
```

1.1.9 file-filter policy

file-filter policy 命令用来创建文件过滤策略，并进入文件过滤策略视图。如果指定的文件过滤策略已经存在，则直接进入文件过滤策略视图。

undo file-filter policy 命令用来删除指定的文件过滤策略。

【命令】

```
file-filter policy policy-name
undo file-filter policy policy-name
```

【缺省情况】

不存在文件过滤策略。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

policy-name: 文件过滤策略的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

一个文件过滤策略中最多可以定义 32 个文件过滤规则。

【举例】

创建一个名称为 **def** 的文件过滤策略，并进入该文件过滤策略视图。

```
<Sysname> system-view
[Sysname] file-filter policy def
[Sysname-file-filter-policy-def]
```

【相关命令】

- **file-filter apply policy**

1.1.10 filetype-group

filetype-group 命令用来在文件过滤规则中引用文件类型组。

undo filetype-group 命令用来恢复缺省情况。

【命令】

filetype-group *group-name*

undo filetype-group

【缺省情况】

文件过滤规则中未引用文件类型组。

【视图】

文件过滤规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name: 表示文件类型组的名称，为 1~31 个字符的字符串，不区分大小写。被引用的文件类型组必须存在。

【使用指导】

在文件过滤规则中通过引用文件类型组来对文件的扩展名信息进行精确匹配。

在同一个文件过滤规则视图下，多次执行本命令，最后一次执行的命令生效。

【举例】

创建一个名称为 **def** 的文件过滤策略。

```
<Sysname> system-view
```

```
[Sysname] file-filter policy def
```

在名称为 **ch1** 的文件过滤规则中引用文件类型组 **fg1**。

```
[Sysname-file-filter-policy-def] rule ch1
```

```
[Sysname-file-filter-policy-def-rule-ch1] filetype-group fg1
```

【相关命令】

- **file-filter filetype-group**

1.1.11 pattern

pattern 命令用来配置文件过滤特征。

undo pattern 命令用来删除指定的文件过滤特征。

【命令】

pattern *pattern-name* **text** *pattern-string*

undo pattern *pattern-name*

【缺省情况】

文件类型组中不存在文件过滤特征。

【视图】

文件类型组视图

【缺省用户角色】

network-admin

context-admin

【参数】

pattern-name: 表示文件过滤特征的名字，为 1~31 个字符的字符串，不区分大小写。

text pattern-string: 表示对文件的扩展名信息进行精确匹配的文本，**pattern-string** 是文本内容，为 1~8 个字符的字符串，不区分大小写。

【使用指导】

文件过滤特征是设备执行文件过滤功能时系统需要对文件的扩展名信息进行识别的内容。

一个文件类型组中可以配置 32 个文件过滤特征，且它们之间是或的关系。

【举例】

在文件类型组 fg1 中配置文件过滤特征为 doc。

```
<Sysname> system-view
```

```
[Sysname] file-filter filetype-group fg1
```

```
[Sysname-file-filter-fgroup-fg1] pattern 1 text doc
```

1.1.12 rule

rule 命令用来创建文件过滤规则，并进入文件过滤规则视图。如果指定的文件过滤视图已经存在，则直接进入文件过滤视图。

undo rule 命令用来删除指定的文件过滤规则。

【命令】

rule rule-name

undo rule rule-name

【缺省情况】

不存在文件过滤规则。

【视图】

文件过滤策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-name: 文件过滤规则的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

在文件过滤规则中可以配置匹配报文的一系列匹配项，比如规则匹配的方向、规则生效的协议类型、规则引用的文件类型组和规则的动作。

只有文件属性（包括文件的应用类型、传输方向和扩展名）成功匹配规则中包含的所有检测条件才算与此规则匹配成功。

一个文件过滤策略中最多可以定义 32 个文件过滤规则。

【举例】

在名称为 **def** 的文件过滤策略下创建一个名称为 **ch1** 的文件过滤规则，并进入文件过滤规则视图。

```
<Sysname> system-view  
[Sysname] file-filter policy def  
[Sysname-file-filter-policy-def]rule ch1  
[Sysname-file-filter-policy-def-rule-ch1]
```

目 录

1 防病毒	1-1
1.1 防病毒配置命令	1-1
1.1.1 anti-virus apply policy	1-1
1.1.2 anti-virus policy	1-1
1.1.3 anti-virus parameter-profile	1-2
1.1.4 anti-virus signature auto-update	1-3
1.1.5 anti-virus signature auto-update-now	1-4
1.1.6 anti-virus signature rollback	1-4
1.1.7 anti-virus signature update	1-5
1.1.8 description	1-7
1.1.9 display anti-virus signature	1-8
1.1.10 display anti-virus signature family-info	1-9
1.1.11 display anti-virus signature library	1-10
1.1.12 display anti-virus statistics	1-11
1.1.13 exception application	1-12
1.1.14 exception md5	1-13
1.1.15 exception signature	1-13
1.1.16 inspect	1-14
1.1.17 signature severity enable	1-16
1.1.18 update schedule	1-16

1 防病毒

1.1 防病毒配置命令

1.1.1 anti-virus apply policy

anti-virus apply policy 命令用来在 DPI 应用 profile 中引用防病毒策略。

undo anti-virus apply policy 命令用来删除引用的防病毒策略。

【命令】

```
anti-virus apply policy policy-name mode { alert | protect }  
undo anti-virus apply policy
```

【缺省情况】

DPI 应用 profile 中未引用防病毒策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 表示防病毒策略名称，为 1~63 个字符的字符串，不区分大小写。

mode: 表示防病毒策略的模式。

alert: 告警模式，表示报文匹配上该防病毒策略中的特征后，仅可以生成日志，但其他动作均不生效。

protect: 保护模式，表示报文匹配上该防病毒策略中的特征后，设备按照特征的动作对该报文进行处理。

【使用指导】

防病毒策略仅在被 DPI 应用 profile 引用后生效。一个 DPI 应用 profile 视图下只能引用一个防病毒策略。多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 在名称为 sec 的 DPI 应用 profile 下引用防病毒策略 abc。  
<Sysname> system-view  
[Sysname] app-profile sec  
[Sysname-app-profile-sec] anti-virus apply policy abc mode protect
```

1.1.2 anti-virus policy

anti-virus policy 命令用来创建防病毒策略，并进入防病毒策略视图。如果指定的防病毒策略已经存在，则直接进入防病毒策略视图。

undo anti-virus policy 命令用来删除指定的防病毒策略。

【命令】

```
anti-virus policy policy-name  
undo anti-virus policy policy-name
```

【缺省情况】

存在一个缺省防病毒策略，名称为 default。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

policy-name: 表示防病毒策略的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

缺省防病毒策略和自定义防病毒策略都使用当前系统中的所有病毒特征。

缺省防病毒策略不能被修改和删除。

【举例】

创建一个名称为 abc 的防病毒策略，并进入防病毒策略视图。

```
<Sysname> system-view  
[Sysname] anti-virus policy abc  
[Sysname-anti-virus-policy-abc]
```

1.1.3 anti-virus parameter-profile

anti-virus parameter-profile 命令用来配置防病毒动作引用应用层检测引擎动作参数 profile。

undo anti-virus parameter-profile 命令用来取消配置防病毒动作引用应用层检测引擎动作参数 profile。

【命令】

```
anti-virus { email | logging | redirect } parameter-profile profile-name  
undo anti-virus { email | logging | redirect } parameter-profile
```

【缺省情况】

防病毒动作未引用应用层检测引擎动作参数 profile。

【视图】

系统视图

【缺省用户角色】

```
network-admin
```

context-admin

【参数】

email: 表示设置防病毒邮件动作的参数。

logging: 表示设置防病毒日志动作的参数。

redirect: 表示设置防病毒重定向动作的参数。

parameter-profile *parameter-name*: 表示防病毒动作引用的应用层检测引擎动作参数 profile。*parameter-name* 表示动作参数 profile 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

防病毒动作的具体执行参数（例如，邮件服务器的地址、输出日志的方式和对报文重定向的 URL）由应用层检测引擎各动作参数 profile 来定义，可通过引用各动作参数 profile 为防病毒动作提供执行参数。有关应用层检测引擎动作参数 profile 的具体配置请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

如果防病毒动作没有引用应用层检测引擎动作参数 profile，或者引用的动作参数 profile 不存在，则使用系统中各动作参数的缺省值。

【举例】

创建名称为 av1 的应用层检测引擎邮件动作参数 profile，配置登录邮件服务器的明文密码为 abc123。

```
<Sysname> system-view
[Sysname] inspect email parameter-profile av1
[Sysname-inspect-email-av1] password simple abc123
[Sysname-inspect-logging-av1] quit
```

配置防病毒邮件动作引用名称为 av1 的应用层检查引擎邮件动作参数 profile。

```
[Sysname] anti-virus email parameter-profile av1
```

【相关命令】

- **inspect email parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **inspect logging parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **inspect redirect parameter-profile**（DPI 深度安全命令参考/应用层检测引擎）

1.1.4 anti-virus signature auto-update

anti-virus signature auto-update 命令用来开启定期自动在线升级病毒特征库功能，并进入自动升级配置视图。

undo anti-virus signature auto-update 命令用来关闭定期自动在线升级病毒特征库功能。

【命令】

```
anti-virus signature auto-update
undo anti-virus signature auto-update
```

【缺省情况】

定期自动在线升级病毒特征库功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果设备可以访问 UNIS 官方网站，可以采用定期自动在线升级方式来对设备上的病毒特征库进行升级。

【举例】

开启定期自动在线升级病毒特征库功能，并进入自动升级配置视图。

```
<Sysname> system-view
[Sysname] anti-virus signature auto-update
[Sysname-anti-virus-autoupdate]
```

【相关命令】

- **update schedule**

1.1.5 anti-virus signature auto-update-now

anti-virus signature auto-update-now 命令用来立即自动在线升级病毒特征库。

【命令】

anti-virus signature auto-update-now

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

执行此命令后，将立即自动升级设备上的病毒特征库，且会备份当前的病毒特征库文件。此命令的生效与否，与是否开启了定期自动升级病毒特征库功能无关。

当管理员发现 UNIS 官方网站上的特征库服务专区中的病毒特征库有更新时，可以选择立即自动在线升级方式来及时升级病毒特征库版本。

【举例】

立即自动在线升级病毒特征库版本。

```
<Sysname> system-view
[Sysname] anti-virus signature auto-update-now
```

1.1.6 anti-virus signature rollback

anti-virus signature rollback 命令用来回滚病毒特征库。

【命令】

anti-virus signature rollback { factory | last }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

factory: 表示病毒特征库的出厂版本。

last: 表示病毒特征库的上一版本。

【使用指导】

如果管理员发现设备当前病毒特征库版本在检测和防御网络攻击时，误报率较高或出现异常情况，则可以对当前病毒特征库版本进行回滚。目前支持将设备中的病毒特征库版本回滚到出厂版本和上一版本。

病毒特征库版本每次回滚前，设备都会备份当前版本。多次回滚上一版本的操作将会在当前版本和上一版本之间反复切换。例如，当前病毒特征库版本是 V2，上一版本是 V1。第一次执行回滚到上一版本的操作后，特征库替换成 V1 版本，再执行回滚上一版本的操作则特征库重新变为 V2 版本。

【举例】

配置病毒特征库回滚到上一版本。

```
<Sysname> system-view  
[Sysname] anti-virus signature rollback last
```

1.1.7 anti-virus signature update

anti-virus signature update 命令用来手动离线升级病毒特征库。

【命令】

anti-virus signature update *file-path*

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

***file-path*:** 指定病毒特征库文件的路径，为 1~255 个字符的字符串。

【使用指导】

如果设备不能访问 UNIS 官方网站上的特征库服务专区，管理员可以采用如下几种方式手动离线升级病毒特征库版本。

- 本地升级：使用本地保存的特征库文件升级系统上的病毒特征库版本。

- **FTP/TFTP 升级：**通过 FTP 或 TFTP 方式下载远程服务器上保存的特征库文件，并升级系统上的病毒特征库版本。

使用本地升级方式离线升级特征库版本时，特征库文件只能存储在当前主用设备上，否则设备升级特征库会失败。

参数 *file-path* 的取值与手动离线升级的操作方式有关。本地升级时参数 *file-path* 取值请参见 [表 1-1](#)；FTP/TFTP 升级时参数 *file-path* 取值请参见 [表 1-2](#)。

表1-1 本地升级时参数 *file-path* 取值说明表

升级场景	参数 <i>file-path</i> 取值	说明
特征库文件的存储位置与当前工作路径一致	<i>filename</i>	可以执行 pwd 命令查看当前工作路径 有关 pwd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不一致，且在相同存储介质上	<i>filename</i>	需要先执行 cd 命令将工作路径切换至特征库文件所在目录下 有关 cd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不在相同存储介质上	<i>path/ filename</i>	需要先执行 cd 命令将工作路径切换至特征库文件所在存储介质的根目录下，再指定特征库文件的相对路径 有关 cd 命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”

表1-2 FTP/TFTP 升级时参数 *file-path* 取值说明表

升级场景	参数 <i>file-path</i> 取值	说明
特征库文件存储在开启 FTP 服务的远程服务器上	<i>ftp://username:password@server/filename</i>	<i>username</i> 为登录 FTP 服务器的用户名， <i>password</i> 为登录 FTP 服务器的密码， <i>server</i> 为 FTP 服务器的 IP 地址或主机名 当 FTP 的用户名和密码中使用了“:”、“@”和“/”三种特殊字符时，需要将这三种特殊字符替换为其对应的转义字符。“:”、“@”和“/”三种特殊字符对应的转义字符分别为“%3A”或“%3a”、“%40”和“%2F”或“%2f”
特征库文件存储在开启 TFTP 服务的远程服务器上	<i>tftp://server/filename</i>	<i>server</i> 为 TFTP 服务器的 IP 地址或主机名



说明

当采用 FTP/TFTP 方式升级特征库时，如果指定的是服务器的主机名，则需要确保设备能通过静态或动态域名解析方式获得 FTP/TFTP 服务器的 IP 地址，并与之路由可达。否则设备升级特征库会失败。有关域名解析功能的详细配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

【举例】

配置手动离线升级病毒特征库，且采用 TFTP 方式，病毒特征库文件的远程路径为 tftp://192.168.0.10/av-1.0.2-en.dat。

```
<Sysname> system-view
```

```
[Sysname] anti-virus signature update tftp://192.168.0.10/av-1.0.2-en.dat
```

配置手动离线升级病毒特征库，且采用 FTP 方式，病毒特征库文件的远程路径为 ftp://192.168.0.10/av-1.0.2-en.dat，用户名为 user:123，密码为 user@abc/123。

```
<Sysname> system-view
```

```
[Sysname] anti-virus signature update
```

```
ftp://user%3A123:user%40abc%2F123@192.168.0.10/av-1.0.2-en.dat
```

配置手动离线升级病毒特征库，且采用本地方式，病毒特征库文件的本地路径为 cfa0:/av-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> system-view
```

```
[Sysname] anti-virus signature update av-1.0.23-en.dat
```

配置手动离线升级病毒特征库，且采用本地方式，病毒特征库文件的本地路径为 cfa0:/dpi/av-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> cd dpi
```

```
<Sysname> system-view
```

```
[Sysname] anti-virus signature update av-1.0.23-en.dat
```

配置手动离线升级病毒特征库，且采用本地方式，病毒特征库文件的本地路径为 cfb0:/dpi/av-1.0.23-en.dat，当前工作路径为 cfa0:。

```
<Sysname> cd cfb0:/
```

```
<Sysname> system-view
```

```
[Sysname] anti-virus signature update dpi/av-1.0.23-en.dat
```

1.1.8 description

description 命令用来配置防病毒策略描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

未配置防病毒策略描述信息。

【视图】

防病毒策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

text：防病毒策略的描述信息，为 1~255 个字符的字符串，可以包含空格，区分大小写。

【使用指导】

描述信息便于管理员快速理解和识别本防病毒策略的作用，有利于后期维护。

【举例】

```
# 配置防病毒策略 abc 的描述信息为"RD Department anti-virus policy"。
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] description "RD Department anti-virus policy"
```

1.1.9 display anti-virus signature

display anti-virus signature 命令用来显示病毒特征信息。

【命令】

```
display anti-virus signature [ [ signature-id ] [ severity { critical | high | low | medium } ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

signature-id: 表示病毒特征的 ID 号，取值范围为 1~4294967294。若不指定该参数，则显示病毒特征的总数。

severity: 指定病毒特征攻击的严重级别。

critical: 表示严重级别最高。

high: 表示严重级别比较高。

low: 表示严重级别最低。

medium: 表示严重级别中等。

【使用指导】

可以通过本命令了解病毒特征的严重级别，便于更加合理的使用 **signature severity enable** 来使相应级别的病毒特征生效。

【举例】

```
# 显示编号为 10000001 的病毒特征信息。
<Sysname> display anti-virus signature 10000001
Signature ID: 10000001
Name          : Trojan [Downloader].VBS.Agent
Severity      : Medium
```


表1-3 display anti-virus signature 命令显示信息描述表

字段	描述
Signature ID	病毒特征编号
Name	病毒特征的名称或家族名称
Severity	病毒特征的攻击严重级别属性，取值包括： - Low - Medium - High - Critical

显示病毒特征总数。

```
<Sysname> display anti-virus signature
Total count:9206
failed:0
```

表1-4 display anti-virus signature 命令显示信息描述表

字段	描述
Total count	病毒特征的总数
Failed	从病毒特征库下发应用层检测引擎失败病毒特征的个数

1.1.10 display anti-virus signature family-info

display anti-virus signature family-info 命令用来显示病毒特征家族信息。

【命令】

display anti-virus signature family-info

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

可以通过本命令帮助用户了解防病毒特征库中包含的病毒特征家族信息。

【举例】

显示病毒特征家族信息。

```
<Sysname> display anti-virus signature family-info
Total count: 6373
```

Family ID	Family name
1	Virus.Win32.Virut.ce
2	Trojan.Win32.SGeneric
3	Virus.Win32.Nimnul.a
4	Virus.Win32.Virlock.j

表1-5 display anti-virus signature family-info 命令显示信息描述表

字段	描述
Total count	病毒特征家族的总数
Family ID	病毒特征家族的编号
Family name	病毒特征家族的名称

1.1.11 display anti-virus signature library

display anti-virus signature library 命令用来显示病毒特征库信息。

【命令】

display anti-virus signature library

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示病毒特征库信息。

```
<Sysname> display anti-virus signature library
Anti-Virus signature library information:
Type      SigVersion      ReleaseTime      Size
Current   1.0.9             Wed Apr 22 09:51:13 2015  976432
Last      -                 -                 -
Factory   1.0.0             Fri Dec 31 16:00:00 1999  20016
```

表1-6 display anti-virus signature library 命令显示信息描述表

字段	描述
Type	病毒特征库版本，包括如下取值： - Current: 当前版本 - Last: 上一版本 - Factory: 出厂版本
SigVersion	病毒特征库版本号

字段	描述
ReleaseTime	病毒特征库发布时间
Size	病毒特征库大小，单位是Bytes

1.1.12 display anti-virus statistics

display anti-virus statistics 命令用来显示防病毒统计信息。

【命令】

display anti-virus statistics [**policy** *policy-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

policy *policy-name*: 表示防病毒策略名称，为 1~63 个字符的字符串，不区分大小写。若不指定此参数，则显示所有防病毒策略的统计信息。

slot *slot-number*: 显示指定成员设备上的防病毒统计信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示所有成员设备上的防病毒统计信息。

【举例】

显示指定 slot 上的防病毒统计信息。

```
<Sysname> display anti-virus statistics slot 4 cpu 1
CPU 1 on slot 4:
Total Block:    0
Total Redirect: 0
Total Alert:    0
Type           http      ftp      smtp      pop3      imap
Block          0         0         0         0         0
Redirect       0         0         0         0         0
Alert+Permit   0         0         0         0         0
```

表1-7 display anti-virus statistics 命令显示信息描述表

字段	描述
Total Block	执行阻断动作的总数
Total Redirect	执行重定向动作的总数
Total Alert	执行告警动作的总数

字段	描述
Type	动作类型，包括如下取值： - Block: 表示阻断报文并生成日志。 - Redirect: 表示将 HTTP 连接重定向到指定的 URL 并生成日志。 - Alert+Permit: 表示仅对报文进行告警，即允许报文通过并生成日志。
http	对HTTP协议类型数据处理的动作计数
ftp	对FTP协议类型数据处理的动作计数
smtp	对SMTP协议类型数据处理的动作计数
pop3	对POP3协议类型数据处理的动作计数
imap	对IMAP协议类型数据处理的动作计数

1.1.13 exception application

exception application 命令用来配置应用例外并为其指定处理动作。

undo exception application 命令用来删除指定的或所有的应用例外。

【命令】

```
exception application application-name action { alert | block | permit }
undo exception application { application-name | all }
```

【缺省情况】

不存在应用例外。

【视图】

防病毒策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

application-name: 例外应用的名称。

action: 指定例外应用的动作。

all: 表示所有的应用例外。

alert: 表示仅对病毒报文进行告警，即允许其通过并生成病毒日志。

block: 表示阻断病毒报文并生成病毒日志。

permit: 表示允许病毒报文通过。

【使用指导】

缺省情况下，设备基于应用层协议的防病毒动作对符合病毒特征的报文进行处理。当需要对某应用层协议上承载的某一具体应用采取不同的动作时，可以将此应用设置为应用例外。例如，对 HTTP

协议进行允许通过处理，但是需要对 HTTP 协议上承载的游戏类应用采取阻断动作，这时就可以把所有游戏类的应用设置为应用例外。

【举例】

```
# 配置 163Email 应用为应用例外并为其指定处理动作为告警。
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] exception application 163Email action alert
```

1.1.14 exception md5

exception md5 命令用来配置例外 MD5 值。

undo exception md5 命令用来删除例外 MD5 值。

【命令】

```
exception md5 md5-value
undo exception md5 { md5-value | all }
```

【缺省情况】

不存在例外 MD5 值。

【视图】

防病毒策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

md5-value: 表示例外 MD5 值。

all: 表示所有的例外 MD5 值。

【使用指导】

如果发现某类检测出病毒的报文被误报时，用户可以通过查看防病毒日志获取 MD5 值并执行此命令把该报文对应的 MD5 值设置为例外。当后续再有检测出符合该 MD5 值的报文通过时，设备将对其执行允许动作。

【举例】

```
# 在名为 abc 的防病毒策略中，配置例外 MD5 值为 2b9c5137769b613f0ea11bd51c324afc。
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] exception md5 2b9c5137769b613f0ea11bd51c324afc
```

1.1.15 exception signature

exception signature 命令用来配置病毒例外。

undo exception signature 命令用来删除指定的或所有的病毒例外。

【命令】

```
exception signature signature-id  
undo exception signature { signature-id | all }
```

【缺省情况】

不存在病毒例外。

【视图】

防病毒策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

signature-id: 表示病毒特征的 ID 号，取值范围为 1~4294967294。
all: 表示所有的病毒例外。

【使用指导】

如果发现某类检测出病毒的报文被误报时，可以通过执行此命令把该报文对应的病毒特征设置为病毒例外。当后续再有检测出包含此病毒特征的报文通过时，设备将对其执行允许动作。

【举例】

```
# 配置 ID 为 101000 的病毒特征为病毒例外。  
<Sysname> system-view  
[Sysname] anti-virus policy abc  
[Sysname-anti-virus-policy-abc] exception signature 101000
```

【相关命令】

- **display anti-virus signature**

1.1.16 inspect

inspect 命令用来配置病毒检测的应用层协议类型。

undo inspect 命令用来取消对指定协议的报文进行病毒检测。

【命令】

```
inspect { ftp | http | imap | nfs | pop3 | smb | smtp } [ direction { both |  
download | upload } ] [ action { alert | block | redirect } ]  
undo inspect { ftp | http | imap | nfs | pop3 | smb | smtp }
```

【缺省情况】

设备对 FTP、HTTP、SMB、NFS 和 IMAP 协议上传和下载方向传输的报文均进行病毒检测，对 POP3 协议下载方向传输的报文进行病毒检测，对 SMTP 协议上传方向传输的报文进行病毒检测。设备对 FTP、HTTP、NFS 和 SMB 协议报文的动作为阻断，对 IMAP、SMTP 和 POP3 协议报文的动作为告警。

【视图】

防病毒策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ftp: 表示 FTP 协议。

http: 表示 HTTP 协议。

imap: 表示 IMAP 协议。

nfs: 表示 NFS 协议。

pop3: 表示 POP3 协议。

smb: 表示 SMB 协议。

smtp: 表示 SMTP 协议。

direction: 表示对指定方向上的报文进行病毒检测。

both: 表示会话的上传和下载方向。

download: 表示会话的下载方向。

upload: 表示会话的上传方向。

action: 指定对报文的处理动作。

alert: 表示仅对病毒报文进行告警，即允许其通过并生成病毒日志。

block: 表示阻断病毒报文并生成病毒日志。

redirect: 表示将携带病毒的 HTTP 连接重定向到指定的 URL 并生成病毒日志，仅对上传方向生效。

【使用指导】

配置此命令后，设备可根据报文的应用层协议类型和传输方向来对其进行病毒检测，如果检测到病毒，则对此报文执行指定的动作。

因为防病毒模块所支持协议的连接请求均由客户端发起，为了使连接可以成功建立并能对此连接上的报文进行病毒检测，需要管理员在配置安全策略或安全域间实例时确保客户端所在的安全域为源安全域、服务器所在的安全域为目的安全域。

因为 POP3 协议只有下载方向，SMTP 协议只支持上传方向，所以对这两种协议类型不支持配置方向属性。

IMAP 协议只支持告警动作。

NFS 协议仅支持 NFSv3 版本；SMB 协议支持 SMBv1 和 SMBv2 版本。

【举例】

配置对基于 HTTP 协议且是下载方向上的报文进行检测病毒，动作为告警。

```
<Sysname> system-view
```

```
[Sysname] anti-virus policy abc
```

```
[Sysname-anti-virus-policy-abc] inspect http direction download action alert
```

配置不对基于 FTP 协议的报文进行病毒检测。

```
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] undo inspect ftp
```

1.1.17 signature severity enable

signature severity enable 命令用来配置有效病毒特征的最低严重级别。

undo signature severity enable 命令用来恢复缺省情况。

【命令】

```
signature severity { critical | high | medium } enable
undo signature severity enable
```

【缺省情况】

所有严重级别的病毒特征都处于生效状态。

【视图】

防病毒策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

critical: 表示严重级别最高。

high: 表示严重级别比较高。

medium: 表示严重级别中等。

【使用指导】

在仅需要对某类及其以上严重级别病毒进行防御的应用需求中，可通过配置此功能来实现此需求。配置此功能后防病毒策略中只有指定的及其以上严重级别的病毒特征会生效。

【举例】

```
# 配置仅使 High 及其以上严重级别的病毒特征生效。
<Sysname> system-view
[Sysname] anti-virus policy abc
[Sysname-anti-virus-policy-abc] signature severity high enable
```

1.1.18 update schedule

update schedule 命令用来配置定期自动在线升级病毒特征库的时间。

undo update schedule 命令用来恢复缺省情况。

【命令】

```
update schedule { daily | weekly { fri | mon | sat | sun | thu | tue | wed } }
start-time time tingle minutes
undo update schedule
```


【缺省情况】

设备在每天 02:01:00 至 04:01:00 之间自动在线升级病毒特征库。

【视图】

自动升级配置视图

【缺省用户角色】

network-admin

context-admin

【参数】

daily: 表示升级周期为每天。

weekly: 表示以一周为周期，在指定一天进行自动升级。

fri: 表示星期五。

mon: 表示星期一。

sat: 表示星期六。

sun: 表示星期日。

thu: 表示星期四。

tue: 表示星期二。

wed: 表示星期三。

start-time time: 指定自动升级开始时间，*time* 的格式为 hh:mm:ss，取值范围为 00:00:00～23:59:59。

tingle minutes: 指定抖动时间，即实际自动升级开始时间的偏差范围，取值范围为 0～120，单位为分钟。在 **start-time** 指定时间的前后各偏移抖动时间的一半作为自动升级的时间范围，例如，指定自动升级的开始时间为 01:00:00，抖动时间为 60 分钟，则自动升级的时间范围为 00:30:00 至 01:30:00。

【举例】

配置病毒特征库的定期自动在线升级时间为每周一 20:30:00，抖动时间为 10 分钟。

```
<Sysname> system-view
```

```
[Sysname] anti-virus signature auto-update
```

```
[Sysname-anti-virus-autoupdate] update schedule weekly mon start-time 20:30:00 tingle 10
```

【相关命令】

- **anti-virus signature auto-update**

目 录

1 数据分析中心.....	1-1
1.1 数据分析中心配置命令.....	1-1
1.1.1 dac email-server client-authentication enable.....	1-1
1.1.2 dac email-server dns-server	1-1
1.1.3 dac email-server password	1-2
1.1.4 dac email-server secure-authentication enable.....	1-3
1.1.5 dac email-server sender	1-4
1.1.6 dac email-server server-address	1-4
1.1.7 dac email-server username.....	1-5
1.1.8 dac report	1-6
1.1.9 dac storage	1-7
1.1.10 display dac email-server	1-8
1.1.11 display dac report.....	1-9
1.1.12 display dac storage	1-10

1 数据分析中心

1.1 数据分析中心配置命令

1.1.1 dac email-server client-authentication enable

dac email-server client-authentication enable 命令用来开启客户端身份验证功能。
undo dac email-server client-authentication enable 命令用来关闭客户端身份验证功能。

【命令】

dac email-server client-authentication enable
undo dac email-server client-authentication enable

【缺省情况】

客户端身份认证功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

如果邮件服务器（通过 **dac email-server server-address** 命令指定）需要对登录的用户进行身份验证，则需要管理员配合邮件服务器端的要求，在设备上同时开启本功能；如果服务器不需要对用户进行身份验证，则不需要开启本功能。

开启本功能后，需要同时配置登录邮件服务器的用户名和密码。

【举例】

```
# 开启客户端身份验证功能。
<Sysname> system-view
[Sysname] dac email-server client-authentication enable
```

【相关命令】

- **dac email-server password**
- **dac email-server server-address**
- **dac email-server username**

1.1.2 dac email-server dns-server

dac email-server dns-server 命令用来配置域名解析服务器的 IPv4 地址。
undo dac email-server dns-server 命令用来恢复缺省情况。

【命令】

```
dac email-server dns-server ip-address  
undo dac email-server dns-server
```

【缺省情况】

未配置域名解析服务器的 IPv4 地址。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: 表示域名服务器的 IPv4 地址，为点分十进制格式。

【使用指导】

如果配置的数据分析中心邮件服务器的地址为主机名格式，当设备发送日志信息邮件时，首先需要
通过域名解析服务器获取邮件服务器 IP 地址与主机名的映射关系。

【举例】

```
# 配置域名解析的服务器地址为 192.168.0.1。  
<Sysname> system-view  
[Sysname] dac email-server dns-server 192.168.0.1
```

1.1.3 dac email-server password

dac email-server password 命令用来配置登录邮件服务器的密码。

undo dac email-server password 命令用来恢复缺省情况。

【命令】

```
dac email-server password { cipher | simple } string  
undo dac email-server password
```

【缺省情况】

未配置登录邮件服务器的密码。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

cipher: 表示以密文方式设置用户密码。

simple: 表示以明文方式设置用户密码，该密码将以密文形式存储。

string: 表示登录邮件服务器的密码。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串，区分大小写。

【使用指导】

配置登录邮件服务器的用户名后，还需要执行本命令设置用户密码。

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 配置登录邮件服务器的明文密码为 abc123。  
<Sysname> system-view  
[Sysname] dac email-server password simple abc123
```

【相关命令】

- **dac email-server client-authentication enable**
- **dac email-server username**

1.1.4 dac email-server secure-authentication enable

dac email-server secure-authentication enable 命令用来开启安全传输登录邮件服务器的用户信息功能。

undo dac email-server secure-authentication enable 命令用来关闭安全传输登录邮件服务器的用户信息功能。

【命令】

```
dac email-server secure-authentication enable  
undo dac email-server secure-authentication enable
```

【缺省情况】

安全传输登录邮件服务器的用户信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

开启此功能后，首先在设备与邮件服务器之间创建一条安全通道，然后在此通道中传输登录邮件服务器的用户名和密码。

本功能仅在开启客户端身份验证功能后生效。

【举例】

```
# 配置数据分析中心邮件服务器开启安全传输登录邮件服务器用户信息功能。  
<Sysname> system-view  
[Sysname] dac email-server secure-authentication enable
```

【相关命令】

- **dac email-server client-authentication enable**

1.1.5 dac email-server sender

dac email-server sender 命令用来配置发件人地址。

undo dac email-server sender 命令用来恢复缺省情况。

【命令】

dac email-server sender *address-string*

undo dac email-server sender

【缺省情况】

未配置发件人地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

address-string: 表示发件人 Email 地址，为 3~63 个字符的字符串，区分大小写。

【使用指导】

发件人地址是指数据分析中心向外发送邮件时使用的 Email 地址。

【举例】

配置发件人的地址为 abc@123.com。

<Sysname> system-view

[Sysname] dac email-server sender abc@123.com

【相关命令】

- **dac email-server server-address**

1.1.6 dac email-server server-address

dac email-server server-address 命令用来配置数据分析中心的邮件服务器地址。

undo dac email-server server-address 命令用来恢复缺省情况。

【命令】

dac email-server server-address *address-string*

undo dac email-server server-address

【缺省情况】

未配置数据分析中心的邮件服务器的地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

address-string: 表示邮件服务器的地址，为 3～63 个字符的字符串，区分大小写。

【使用指导】

配置的邮件服务器地址既可以是邮件服务器的 IP 地址，也可以是邮件服务器的主机名。

配置邮件服务器地址后，还需要配置邮件服务器的发件人地址，才能发送邮件。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置数据分析中心的邮件服务器地址为 101.1.1.255。

```
<Sysname> system-view
```

```
[Sysname] dac email-server server-address 101.1.1.225
```

【相关命令】

- **dac email-server sender**

1.1.7 dac email-server username

dac email-server username 命令用来配置登录邮件服务器的用户名。

undo dac email-server username 命令用来恢复缺省情况。

【命令】

dac email-server username *username*

undo dac email-server username

【缺省情况】

未配置登录邮件服务器的用户名。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

username: 表示登录邮件服务器的用户名，为 1～63 个字符的字符串，区分大小写。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 配置登录邮件服务器的用户名为 admin。  
<Sysname> system-view  
[Sysname] dac email-server username admin
```

【相关命令】

- **dac email-server client-authentication enable**
- **dac email-server password**

1.1.8 dac report

dac report 命令用来配置数据分析中心报表订阅地址。

undo dac report 命令用来删除数据分析中心报表订阅地址。

【命令】

```
dac report type { comparison | integrated | intelligent | summary } subscriber  
mail-address  
undo dac report type { comparison | integrated | intelligent | summary }  
[ subscriber mail-address ]
```

【缺省情况】

未配置数据分析中心报表订阅地址。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

comparison: 表示对比报表。

Integrated: 表示综合报表。

intelligent: 表示智能报表。

summary: 表示汇总报表。

subscriber mail-address: 表示报表订阅的 Email 地址，为 3~63 个字符的字符串，区分大小写。

【使用指导】

每类报表最多可以配置 50 个订阅地址。

执行 **undo** 命令时，若不指定 **subscriber**，则删除指定报表类型下的所有 **subscriber**。

【举例】

```
# 向汇总报表订阅地址中添加地址 admin@qq.com。  
<Sysname> system-view  
[Sysname] dac report type summary subscriber admin@qq.com
```



```
# 删除汇总报表订阅地址中的地址 admin@qq.com。
<Sysname> system-view
[Sysname] undo dac report type summary subscriber admin@qq.com
```

1.1.9 dac storage

dac storage 命令用来配置数据分析中心存储空间。

undo dac storage 命令用来恢复缺省情况。

【命令】

```
dac storage service { audit | file-filter | threat | traffic | url-filter }
limit { hold-time time-value | usage usage-value | action { delete |
log-only } }
undo dac storage service { audit | file-filter | threat | traffic | url-filter }
limit { hold-time | usage | action }
```

【缺省情况】

各业务的数据存储时间上限为 365 天、空间上限为 20%、上限处理动作为删除。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

audit: 表示审计业务。

file-filter: 表示文件过滤业务。

threat: 表示威胁业务，包括入侵防御业务和防病毒业务。

traffic: 表示流量业务。

url-filter: 表示 URL 过滤业务。

limit: 表示对各业务的存储空间设置限制。

hold-time time-value: 表示各业务的数据存储时间上限，取值范围为 1~65535 天。

usage usage-value: 表示各业务的数据存储空间上限，即各业务数据可占用总存储空间的百分比，取值范围为 1~100。

action: 表示上限处理动作，即各业务存储的数据达到时间上限或者空间上限后，对历史数据执行的动作。包括删除和仅发送日志信息。

delete: 表示删除动作，设备将删除保存时间最长的数据以便保存新数据，并发送日志信息。删除日志信息时，设备将按天删除，且不可删除当天的日志信息。

log-only: 表示仅发送日志动作，设备不对历史数据进行操作，也不保存新数据，仅发送日志信息。

【使用指导】

数据分析中心存储空间中保存各业务的历史数据，并设置了存储空间上限和时间上限对可存储的日志进行限制。设备定时检查日志信息的存储状态，当指定业务的历史数据达到任何一种上限时，设备将根据配置的上限动作对历史数据进行操作。

仅支持在缺省 **Context** 下配置本命令。有关 **Context** 的详细介绍，请参见“虚拟化技术配置指导”中的“**Context**”。

可多次执行本命令，分别配置各业务的存储时间上限、空间上限以及上限处理动作。其中，配置的数据存储时间上限和空间上限值应高于当前已达到的值。可通过 **Web** 界面查看各业务的存储空间使用情况。

多次执行相同参数的命令，最后一次执行的命令生效。

【举例】

配置流量业务数据存储时间上限为 60 天、存储空间上限为 30%、上限处理动作为删除。

```
<Sysname> system-view
[Sysname] dac storage service traffic limit hold-time 60
[Sysname] dac storage service traffic limit usage 30
[Sysname] dac storage service traffic limit action delete
```

1.1.10 display dac email-server

display dac email-server 命令用来显示数据分析中心邮件服务器的配置信息。

【命令】

display dac email-server

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示数据分析中心邮件服务器的信息。

```
<Sysname> display dac email-server
Mail server address : 2.2.2.2
    Mail sender address : qq@11.com
    DNS server address : 1.1.1.1
    Authentication : Enable
    secure-authentication : Enable
    Username : lkx
    password : *****
```

表1-1 display dac email-server 命令显示信息描述表

字段	描述
Mail server address	邮件服务器地址
Mail sender address	发件人地址
DNS server address	DNS服务器地址
Authentication	是否开启客户端身份验证功能
Secure-authentication	是否开启安全传输登录邮件服务器的用户信息功能
Username	登录邮件服务器的用户名
Password	登录邮件服务器的密码

1.1.11 display dac report

display dac report 命令用来显示数据分析中心报表订阅信息。

【命令】

display dac report [comparison | integrated | intelligent | summary]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

comparison: 表示对比报表。
integrated: 表示综合报表。
intelligent: 表示智能报表。
summary: 表示汇总报表。

【使用指导】

如果未指定任何参数，则显示所有类型报表的订阅信息，包括各类报表的订阅地址以及相关统计信息。

【举例】

```
# 显示数据分析中心所有类型报表的订阅信息。
<Sysname> display dac report
Total subscribers:4
Summary subscribers:1
Comparison subscribers:1
```

```

Intelligent subscribers:1
Integrated subscribers:1
Report type          Subscriber email address
Summary              124@123.com
Comparison           111@123.com
Intelligent           123@123.com
Integrated            112@123.com

```

表1-2 display dac report 命令显示信息描述表

字段	描述
Total subscribers	报表订阅地址的总数量
Summary subscribers	汇总报表订阅地址的数量
Comparison subscribers	对比报表订阅地址的数量
Intelligent subscribers	智能报表订阅地址的数量
Integrated subscribers	综合报表订阅地址的数量
Report type	报表类型
Subscriber email address	报表订阅地址

1.1.12 display dac storage

display dac storage 命令用来显示数据分析中心存储空间的配置信息。

【命令】

```
display dac storage [ audit | file-filter | threat | traffic | url-filter ]
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【参数】

audit: 表示审计业务的存储空间配置信息。

file-filter: 表示文件过滤业务的存储空间配置信息。

threat: 表示威胁业务的存储空间配置信息（包含入侵防御和防病毒）。

traffic: 表示流量统计业务的存储空间配置信息。

url-filter: 表示 URL 过滤业务的存储空间配置信息。

【使用指导】

如果未指定任何参数，则显示所有业务的数据分析中心存储空间配置信息。

仅支持在缺省 Context 下执行本命令。有关 Context 的详细介绍，请参见“虚拟化技术配置指导”中的“Context”。

【举例】

显示数据分析中心所有业务的存储空间配置信息。

```
<Sysname> display dac storage
Total services          :5
```

Service	Time limit (days)	Usage limit	Action
audit	365	70%	log-only
traffic	128	50%	delete
threat	30	30%	delete
url-filter	7	10%	delete
file-filter	50	10%	delete

表1-3 display dac storage 命令显示信息描述表

字段	描述
Total services	业务类别总数量
Service	业务类型
Time limit	数据存储时间上限（单位：天）
Usage limit	数据存储空间上限（单位：百分比）
Action	达到数据存储时间/空间上限后的处理动作，取值范围为： • delete：表示删除，设备将删除保存时间最长的数据以便保存新数据，并发送日志信息。 • log-only：表示仅发送日志信息。

目 录

1 WAF	1-1
1.1 WAF配置命令	1-1
1.1.1 action	1-1
1.1.2 attack-category	1-2
1.1.3 display waf policy	1-2
1.1.4 display waf signature	1-5
1.1.5 display waf signature pre-defined	1-8
1.1.6 display waf signature library	1-9
1.1.7 object-dir	1-10
1.1.8 override-current	1-11
1.1.9 protected-target	1-11
1.1.10 severity-level	1-12
1.1.11 signature override	1-13
1.1.12 signature override all	1-14
1.1.13 update schedule	1-15
1.1.14 waf apply policy	1-16
1.1.15 waf parameter-profile	1-17
1.1.16 waf policy	1-18
1.1.17 waf signature auto-update	1-19
1.1.18 waf signature auto-update-now	1-20
1.1.19 waf signature rollback	1-20
1.1.20 waf signature update	1-21

1 WAF

1.1 WAF配置命令

1.1.1 action

action 命令用来配置筛选 WAF 特征的动作属性。

undo action 命令用来恢复缺省情况。

【命令】

```
action { block-source | drop | permit | reset } *  
undo action
```

【缺省情况】

未配置动作属性筛选条件。

【视图】

WAF 策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

block-source: 表示源阻断动作，该动作将阻断符合特征的报文，并将该报文的源 IP 地址加入 IP 黑名单。

drop: 表示丢弃报文的动作。

permit: 表示允许报文通过的动作。

reset: 表示重置动作，该动作通过发送 TCP 的 reset 报文使 TCP 连接断开。

【使用指导】

可通过配置动作分类属性筛选出具有该属性的特征，WAF 策略将使用筛选出的特征与报文进行匹配。可多次执行本命令，配置多个攻击分类。只要符合其中一个，具有该攻击分类的特征将会被筛选出来。

特征库升级过程中，不能成功执行本命令以及 **undo** 命令。

【举例】

```
# 在名为 test-policy 的 WAF 策略中配置筛选 WAF 特征的动作属性为 drop 和 reset。  
<Sysname> system-view  
[Sysname] waf policy test-policy  
[Sysname-waf-policy-test-policy] action drop reset
```

【相关命令】

- **display waf policy**

1.1.2 attack-category

attack-category 命令用来配置筛选 WAF 特征的攻击分类属性。

undo attack-category 命令用来删除筛选 WAF 特征的攻击分类属性。

【命令】

```
attack-category { category [ sub-category subcategory ] | all }  
undo attack-category { category [ sub-category subcategory | all ] }
```

【缺省情况】

未配置攻击分类属性筛选条件。

【视图】

WAF 策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

category: 表示设备中已有的攻击分类名称。不区分大小写，可通过输入“？”获取支持的攻击分类名称。

sub-category subcategory: 表示设备中已有攻击分类中的子分类名称。若不指定本参数，则表示指定攻击分类中的所有子分类。不区分大小写，可通过输入“？”获取支持的子分类名称。

all: 表示设备中已有的所有攻击分类。

【使用指导】

可通过配置攻击分类属性筛选出具有该属性的特征，WAF 策略将使用筛选出的特征与报文进行匹配。可多次执行本命令，配置多个攻击分类。只要符合其中一个，具有该攻击分类的特征将会被筛选出来。

【举例】

在名为 test-policy 的 WAF 策略中配置筛选 WAF 特征的攻击分类为 Vulnerability 攻击分类中的 SQL-Injection 子分类。

```
<Sysname> system-view  
[Sysname] waf policy test-policy  
[Sysname-waf-policy-test-policy] attack-category Vulnerability SQL-Injection
```

【相关命令】

- **display waf policy**

1.1.3 display waf policy

display waf policy 命令用来显示 WAF 策略信息。

【命令】

```
display waf policy policy-name
```


【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

policy-name: 表示 WAF 策略名称，为 1~63 个字符的字符串，不区分大小写。

【举例】

```
# 显示名为 aa 的 WAF 策略信息。
<Sysname> display waf policy aa
Protected website: a
  Domain: www.baidu.com
  IP address: 1.1.1.1
  Port: 1
Protected website: b
  Domain: www.ali.com
  IP address: 1.1.1.2
  Port: 2
Applied CC defense policy: a
Total signature count      : 100
Pre-defined signature count : 10
User-defined signature count: 90

Flags:
  B: Block-source  D: Drop  P: Permit  Rs: Reset  Rd: Redirect  C: Capture  L: Logging
Pre: pre-defined  User: user-defined

Type SigID      Target          SubTarget      Severity Direction Category
SubCategory      Status Action
Pre  23723      OperationSystem Any          High      Any      Vulnerability
RemoteCodeExecu Enable  RsL
Pre  24728      OperationSystem Any          Critical Server  Malware
Backdoor          Enable  DL
Pre  25066      OperationSystem Any          Critical Any      Malware
Backdoor          Enable  DL
Pre  25067      OperationSystem Any          Critical Server  Malware
Backdoor          Enable  RsL
Pre  25824      OperationSystem Any          Critical Server  Vulnerability
Overflow          Enable  RsL
---- More ----
```

表1-1 display waf policy 命令显示信息描述表

字段	描述
Protected website	表示WAF防护的网站
Domain	表示WAF防护网站的域名
IP address	表示WAF防护网站的ipv4地址
Port	表示WAF防护网站的端口号
Applied CC defense policy	表示WAF策略引用的CC攻击防护策略
Total signature count	WAF策略中筛选出的特征总数
Pre-defined signature count	预定义WAF特征数目
User-defined signature count	自定义WAF特征数目
Flags	标识符缩写，取值包括： • B: Block-source: 表示源阻断动作 • D: Drop: 表示丢弃 • P: Permit: 表示允许 • Rs: Reset: 表示重置 • C: Capture: 表示捕获 • L: Logging: 表示记录日志 • Pre: pre-defined: 表示预定义特征 • User: user-defined: 表示自定义特征
Type	WAF特征的类型，包括如下取值： • Pre: 表示预定义特征 • User: 表示自定义特征
SigID	WAF特征编号
Target	攻击对象
SubTarget	攻击子对象
Severity	WAF特征的攻击严重程度属性，从低到高分为四级：Low、Medium、High、Critical
Category	WAF特征的攻击类别名称
SubCategory	WAF特征的子攻击类别名称
Status	WAF特征的状态，包括如下取值： • Enabled: 表示此特征已生效 • Disabled: 表示此特征未生效
Action	对报文的处理动作，包括如下取值： • Block-source: 表示阻断符合特征的报文，并将该报文的源 IP 地址加入 IP 黑名单 • Drop: 表示丢弃符合特征的报文 • Permit: 表示允许符合特征的报文通过

字段	描述
	- Reset: 表示发送 TCP 的 reset 报文或 UDP 的 ICMP 端口不可达报文使 TCP 或 UDP 连接断开 - Redirect: 表示重定向符合特征的报文 - Capture: 表示捕获符合特征的报文 - Logging: 表示对符合特征的报文生成日志

1.1.4 display waf signature

display waf signature 命令用来显示 WAF 特征的简要信息。

【命令】

```
display waf signature [ pre-defined ] [ direction { any | to-client | to-server } ] [ category category-name | fidelity { high | low | medium } | severity { critical | high | low | medium } ] *
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

pre-defined: 显示预定义 WAF 特征。

direction { any | to-client | to-server }: 显示符合指定方向属性的 WAF 特征。如果未指定此参数，则显示所有方向上的 WAF 特征。

- any:** 表示一个会话的两个方向。
- to-server:** 表示一个会话的客户端到服务器的方向。
- to-client:** 表示一个会话的服务器到客户端的方向。

category category-name: 显示符合指定攻击类别属性的 WAF 特征，*category-name* 是攻击类型的名称，可通过输入“？”获取支持的攻击类型名称。如果未指定此参数，则显示所有攻击类型的 WAF 特征。

fidelity { high | low | medium }: 显示符合指定可信度属性的 WAF 特征。如果未指定此参数，则显示所有可信度的 WAF 特征。可信度是指此 WAF 特征识别攻击行为准确度，且从低到高分分为如下三个级别：

- low:** 可信度比较低。
- medium:** 可信度中等。
- high:** 可信度比较高。

severity { critical | high | low | medium }: 显示符合指定严重级别属性的 WAF 特征。如果未指定此参数，则显示所有严重级别的 WAF 特征。严重级别是指匹配此 WAF 特征的网络攻击造成危害的严重程度，且从低到高分四个级别：

- **low**: 攻击严重程度比较低。
- **medium**: 攻击严重程度中等。
- **high**: 攻击严重程度比较高。
- **critical**: 攻击严重程度非常高。

【使用指导】

若不指定任何参数，则显示所有 WAF 特征。

【举例】

显示可信度为中等的所有预定义 WAF 特征。

```
<Sysname> display waf signature pre-defined fidelity medium
Pre-defined signatures total:88      failed:0
```

Flag:

Pre: predefined User: user-defined

Type	SigID	Direction	Severity	Fidelity	Category	Protocol	SigName
Pre	3295	To-client	Critical	Medium	Vulnerability	TCP	
Pre	5379	To-client	Critical	Medium	Vulnerability	TCP	
Pre	6017	To-client	Critical	Medium	Vulnerability	TCP	
Pre	7453	To-server	High	Medium	Other	TCP	
Pre	10033	To-client	High	Medium	Vulnerability	TCP	
Pre	23227	To-server	Medium	Medium	Vulnerability	TCP	
Pre	23285	To-server	Medium	Medium	Vulnerability	TCP	
Pre	23309	To-server	Medium	Medium	Vulnerability	TCP	
Pre	23482	To-server	High	Medium	Vulnerability	TCP	
Pre	23530	To-server	High	Medium	Vulnerability	TCP	
Pre	23666	To-server	High	Medium	Vulnerability	TCP	
Pre	23722	To-server	Medium	Medium	Vulnerability	TCP	
Pre	23747	To-server	Medium	Medium	Vulnerability	TCP	
Pre	24346	To-client	Medium	Medium	Vulnerability	TCP	
Pre	25044	To-server	High	Medium	Vulnerability	TCP	
Pre	25086	To-server	High	Medium	Vulnerability	TCP	
Pre	25100	To-server	High	Medium	Vulnerability	TCP	

---- More ----

显示攻击严重程度为比较高的所有 WAF 特征。

```
<Sysname> display waf signature severity high
Total signatures      :45      failed:0
Pre-defined signatures total:45      failed:0
User-defined signatures total:0      failed:0
```

Flag:

Pre: predefined User: user-defined

Type	SigID	Direction	Severity	Fidelity	Category	Protocol	SigName
Pre	7453	To-server	High	Medium	Other	TCP	
Pre	10033	To-client	High	Medium	Vulnerability	TCP	
Pre	23192	To-server	High	High	Vulnerability	TCP	
Pre	23448	To-server	High	High	Vulnerability	TCP	
Pre	23474	To-server	High	Low	Vulnerability	TCP	
Pre	23482	To-server	High	Medium	Vulnerability	TCP	
Pre	23530	To-server	High	Medium	Vulnerability	TCP	
Pre	23666	To-server	High	Medium	Vulnerability	TCP	
Pre	24485	To-server	High	High	Vulnerability	TCP	
Pre	25044	To-server	High	Medium	Vulnerability	TCP	
Pre	25086	To-server	High	Medium	Vulnerability	TCP	
Pre	25100	To-server	High	Medium	Vulnerability	TCP	
Pre	30781	To-server	High	Medium	Vulnerability	TCP	
Pre	30807	To-server	High	Medium	Vulnerability	TCP	
Pre	30851	To-server	High	Medium	Vulnerability	TCP	

---- More ----

表1-2 display waf signature 命令显示信息描述表

字段	描述
Total signatures	WAF特征总数
Pre-defined signatures total	预定义WAF特征数目
User-defined signatures total	自定义WAF特征数目
Flags	标识符缩写，取值包括： - Pre: pre-defined: 表示预定义特征 - User: user-defined: 表示自定义特征
Type	WAF特征的类型，包括如下取值： - Pre: 表示预定义特征 - User: 表示自定义特征
SigID	WAF特征的编号
Direction	WAF特征的方向属性，包括如下取值： - any: 表示一个会话的两个方向 - To-server: 一个会话的客户端到服务器方向 - To-client: 一个会话的服务器到客户端方向
Severity	WAF特征的攻击严重程度属性，严重程度从低到高分四个级别：Low、Medium、High、Critical
Fidelity	WAF特征的可信度属性，可信度从低到高分三个级别：Low、Medium、High
Category	WAF特征的攻击类别名称
Protocol	WAF特征的协议属性
SigName	WAF自定义特征的名称

1.1.5 display waf signature pre-defined

display waf signature pre-defined 命令用来显示 WAF 预定义特征的详细信息。

【命令】

display waf signature pre-defined *signature-id*

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

signature-id: 指定 WAF 预定义特征的编号，取值范围为 1~536870911。

【举例】

```
# 显示编号为 3295 的预定义 WAF 特征的详细信息。
<Sysname> display waf signature pre-defined 3295
Type           : Pre-defined
Signature ID: 3295
Status         : Enable
Action         : Permit & Logging
Name           : WEB_SERVER_Possible_HTTP_503_XSS_Attempt_(Internal_Source)
Protocol       : TCP
Severity       : Critical
Fidelity       : Medium
Direction     : To-client
Category       : Vulnerability
Reference      :
Description    : WEB_SERVER_Possible_HTTP_503_XSS_Attempt_(Internal_Source)
```

表1-3 display waf signature pre-defined 命令显示信息描述表

字段	描述
Type	WAF特征的类型
Signature ID	WAF特征的编号
Status	WAF特征的状态，包括如下取值： - Enabled: 表示此特征已生效 - Disabled: 表示此特未生效
Action	对报文的处理动作，包括如下取值： - Block-source: 表示阻断符合特征的报文，并将该报文的源 IP 地址加入 IP 黑名单 - Drop: 表示丢弃符合特征的报文

字段	描述
	• Permit: 表示允许符合特征的报文通过 • Reset: 表示发送 TCP 的 reset 报文或 UDP 的 ICMP 端口不可达报文使 TCP 或 UDP 连接断开 • Capture: 表示捕获符合特征的报文 • Logging: 表示对符合特征的报文生成日志
Name	WAF特征的名称
Protocol	WAF特征的协议属性
Severity	WAF特征的攻击严重程度属性, 严重程度从低到高分为四个级别: Low、Medium、High、Critical
Fidelity	WAF特征的可信度属性, 可信度从低到高分三个级别: Low、Medium、High
Direction	WAF特征的方向属性, 包括如下取值: • Any: 表示一个会话的两个方向 • To-server: 一个会话的客户端到服务器方向 • To-client: 一个会话的服务器到客户端方向
Category	WAF特征的攻击类别名称
Reference	WAF特征的参考信息
Description	WAF特征的描述信息

1.1.6 display waf signature library

display waf signature library 命令用来显示 WAF 特征库信息。

【命令】

display waf signature library

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 WAF 特征库信息。

```
<Sysname> display waf signature library
WAF signature library information:
Type      SigVersion      ReleaseTime      Size (bytes)
Current   1.02              Fri Sep 13 09:05:35 2014  71594
Last      -                  -                  -
```

表1-4 display waf signature information 命令显示信息描述表

字段	描述
Type	WAF特征库版本，包括如下取值： • Current: 表示当前版本 • Last: 表示上一版本 • Factory: 表示出厂版本
SigVersion	WAF特征库版本号
ReleaseTime	WAF特征库发布时间
Size	WAF特征库文件大小，单位是Bytes

1.1.7 object-dir

object-dir 命令用来配置筛选 WAF 特征的方向属性。

undo object-dir 命令用来恢复缺省情况。

【命令】

```
object-dir { client | server } *  
undo object-dir
```

【缺省情况】

未配置方向属性筛选条件。

【视图】

WAF 策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

client: 表示从服务器到客户端方向上的对象。

server: 表示从客户端到服务器方向上的对象。

【使用指导】

可通过配置方向属性筛选出具有该属性的特征，WAF 策略将使用筛选出的特征与报文进行匹配。

可同时配置多个方向，只要符合其中一个，具有该方向属性的特征将会被筛选出来。

多次执行本命令，最后一次执行的命令生效。

【举例】

在名为 test-policy 的 WAF 策略中配置筛选 WAF 特征的方向属性为 client。

```
<Sysname> system-view
```

```
[Sysname] waf policy test-policy
```



```
[Sysname-waf-policy-test-policy] object-dir client
```

1.1.8 override-current

override-current 命令用来配置定期自动在线升级 WAF 特征库时覆盖当前的特征文件。

undo override-current 命令用来恢复缺省情况。

【命令】

override-current

undo override-current

【缺省情况】

定期自动在线升级 WAF 特征库时不会覆盖当前的特征库文件，而是将当前的特征库文件备份为上一版本。

【视图】

自动升级配置视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

可以通过开启此功能解决升级 WAF 特征库时设备内存不足的问题。在设备剩余内存充裕的情况下，不建议配置该功能，因为 WAF 特征库升级时，如果没有备份当前特征库文件，则不能回滚到上一版本。

【举例】

配置定期自动在线升级 WAF 特征库时覆盖当前的特征文件。

```
<Sysname> system-view
```

```
[Sysname] waf signature auto-update
```

```
[Sysname-waf-sig-autoupdate] override-current
```

【相关命令】

- **waf signature auto-update-now**

1.1.9 protected-target

protect-target 命令用来配置筛选 WAF 特征的保护对象属性。

undo protect-target 命令用来删除筛选 WAF 特征的保护对象属性。

【命令】

protected-target { *target* [**sub-target** *subtarget*] | **all** }

undo protected-target { *target* [**sub-target** *subtarget*] | **all** }

【缺省情况】

未配置保护对象属性筛选条件。

【视图】

WAF 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

target: 表示保护对象分类名称。不区分大小写，可通过输入“?”获取支持的对象分类名称。

subtarget: 表示保护对象分类中的子对象名称。若不指定本参数，则表示保护某对象分类中的所有子对象。不区分大小写，可通过输入“?”获取支持的子对象分类名称。

all: 表示所有保护对象。

【使用指导】

可通过配置保护对象属性筛选出具有该属性的特征，WAF 策略将使用筛选出的特征与报文进行匹配。可多次执行本命令，配置多个保护对象。只要符合其中一个，具有该保护对象属性的特征将会被筛选出来。

【举例】

在名为 test-policy 的 WAF 策略中配置筛选 WAF 特征的保护对象为 WebServer 中 WebLogic 子对象。

```
<Sysname> system-view
```

```
[Sysname] waf policy test-policy
```

```
[Sysname-waf-policy-test-policy] protected-target WebServer WebLogic
```

【相关命令】

- **display waf policy**

1.1.10 severity-level

severity-level 命令用来配置筛选 WAF 特征的严重级别属性。

undo severity-level 命令用来恢复缺省情况。

【命令】

```
severity-level { critical | high | low | medium } *
```

```
undo severity-level
```

【缺省情况】

未配置严重级别属性筛选条件。

【视图】

WAF 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

critical: 表示严重级别最高。

high: 表示严重级别高。

low: 表示严重级别低。

medium: 表示严重级别一般。

【使用指导】

严重级别是指匹配此 WAF 特征的网络攻击造成危害的严重程度。可通过配置严重级别属性筛选出具有该属性的特征，WAF 策略将使用筛选出的特征与报文进行匹配。可同时配置多个严重级别，只要符合其中一个，具有该严重级别属性的特征将会被筛选出来。

多次执行本命令，最后一次执行的命令生效。

【举例】

在名为 test-policy 的 WAF 策略中配置筛选 WAF 特征的严重级别为 critical 和 medium。

```
<Sysname> system-view
```

```
[Sysname] waf policy test-policy
```

```
[Sysname-waf-policy-test-policy] severity-level critical medium
```

【相关命令】

- **waf policy**

1.1.11 signature override

signature override 命令用来修改 WAF 策略中指定预定义特征的动作和状态。

undo signature override 命令用来恢复 WAF 策略中指定预定义特征属性中的动作和状态。

【命令】

```
signature override pre-defined signature-id { disable | enable }  
[ { block-source | drop | permit | redirect | reset } | capture | logging ] *  
undo signature override pre-defined signature-id
```

【缺省情况】

预定义 WAF 特征使用系统预定义的状态和动作。

【视图】

WAF 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

signature-id: WAF 预定义特征的编号，取值范围为 1~4294967295。

disable: 表示禁用此 WAF 特征。在某些网络环境中，如果一些 WAF 特征暂时不会被用到，而且又不想将其从 WAF 策略中删除时，可以使用 **disable** 参数来禁用这些规则。

enable: 表示启用此 WAF 特征。

block-source: 表示源阻断，该动作阻断符合特征的报文，并将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名单过滤功能的详细介绍请参见“安全命令参考”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。

drop: 表示丢弃报文。

permit: 表示允许报文通过。

redirect: 表示把符合特征的报文重定向到指定的 Web 页面上。

reset: 表示通过发送 TCP 的 reset 报文使 TCP 连接断开。

capture: 表示捕获报文。

logging: 表示生成报文日志。

【使用指导】

本命令用于修改 WAF 特征的动作和状态，名为 default 的缺省 WAF 策略中特征的动作和状态不能被修改。

在同一个 WAF 策略视图对同一 WAF 特征多次执行本命令，最后一次执行的命令生效。

【举例】

在名为 test-policy 的 WAF 策略中配置编号为 2 的预定义 WAF 特征的状态为开启，动作为丢弃和捕获报文，并生成日志信息。

```
<Sysname> system-view
[Sysname] waf policy test-policy
[Sysname-waf-policy-test-policy] signature override pre-defined 2 enable drop capture
logging
```

【相关命令】

- **blacklist enable** (security zone view)（安全命令参考/攻击检测与防范）
- **signature override all**

1.1.12 signature override all

signature override all 命令用来配置 WAF 策略中所有特征的统一动作。

undo signature override all 命令用来恢复缺省情况。

【命令】

```
signature override all { { block-source | drop | permit | redirect | reset }
| capture | logging } *
undo signature override all
```

【缺省情况】

WAF 策略执行特征属性中的动作。

【视图】

WAF 策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

block-source: 表示源阻断，该动作阻断符合特征的报文，并将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能，则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名单过滤功能的详细介绍请参见“安全命令参考”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。

drop: 表示丢弃报文。

permit: 表示允许报文通过。

redirect: 表示把符合特征的报文重定向到指定的 Web 页面上。

reset: 表示通过发送 TCP 的 reset 报文使 TCP 连接断开。

capture: 表示捕获报文。

logging: 表示生成报文日志。

【使用指导】

如果在 WAF 策略中为所有特征配置了统一动作，则设备将根据该动作对与此策略中特征匹配成功的报文进行处理。否则，设备将根据特征属性中的动作对报文进行处理。

如果在 WAF 策略中修改了指定特征的动作，则无论是否为所有特征配置了统一的动作，设备都将根据修改后的动作对报文进行处理。

【举例】

```
# 在名为 test-policy 的 WAF 策略中配置所有特征的统一动作为丢弃，并生成日志信息和捕获报文。  
<Sysname> system-view  
[Sysname] waf policy test-policy  
[Sysname-waf-policy-test-policy] signature override all drop logging capture
```

【相关命令】

- **blacklist enable** (security zone view)（安全命令参考/攻击检测与防范）
- **signature override**

1.1.13 update schedule

update schedule 命令用来配置定期自动在线升级 WAF 特征库的时间。

undo update schedule 命令用来恢复缺省情况。

【命令】

```
update schedule { daily | weekly { fri | mon | sat | sun | thu | tue | wed } }  
start-time time tingle minutes  
undo update schedule
```

【缺省情况】

设备在每天 01:00:00 至 03:00:00 之间自动在线升级 WAF 特征库。

【视图】

自动升级配置视图

【缺省用户角色】

network-admin

context-admin

【参数】

daily: 表示自动升级周期为每天。

weekly: 表示以一周为周期，在指定的一天进行自动升级。

fri: 表示星期五。

mon: 表示星期一。

sat: 表示星期六。

sun: 表示星期日。

thu: 表示星期四。

tue: 表示星期二。

wed: 表示星期三。

start-time time: 指定自动升级开始时间，*time* 的格式为 hh:mm:ss，取值范围为 00:00:00～23:59:59。

tingle minutes: 指定抖动时间，即实际自动升级开始时间的偏差范围，取值范围为 0～120，单位为分钟。在 **start-time** 指定时间的前后各偏移抖动时间的一半作为自动升级的时间范围，例如，指定自动升级的开始时间为 01:00:00，抖动时间为 60 分钟，则自动升级的时间范围为 00:30:00 至 01:30:00。

【举例】

配置 WAF 特征库的定期自动在线升级时间为每周一 20:30:00，抖动时间为 10 分钟。

```
<Sysname> system-view
```

```
[Sysname] waf signature auto-update
```

```
[Sysname-waf-autoupdate] update schedule weekly mon start-time 20:30:00 tingle 10
```

【相关命令】

- **waf signature auto-update**
- **waf signature auto-update-now**

1.1.14 waf apply policy

waf apply policy 命令用来在 DPI 应用 profile 中引用 WAF 策略。

undo waf apply policy 命令用来删除引用的 WAF 策略。

【命令】

```
waf apply policy policy-name mode { alert | protect }
```

```
undo waf apply policy
```

【缺省情况】

DPI 应用 profile 中未引用 WAF 策略。

【视图】

DPI 应用 profile 视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: 指定 WAF 策略名称，为 1~63 个字符的字符串，不区分大小写。

mode: 表示 WAF 策略的模式。

alert: 告警模式，表示报文匹配上该 WAF 策略中的特征后，仅可以生成日志或捕获报文，但其他动作均不能生效。

protect: 保护模式，表示报文匹配上该 WAF 策略中的特征后，设备按照特征的动作对该报文进行处理。

【使用指导】

WAF 策略仅在被 DPI 应用 profile 引用后生效。一个 DPI 应用 profile 视图下只能引用一个 WAF 策略。

多次执行本命令，最后一次执行的命令生效。

【举例】

在名称为 sec 的 DPI 应用 profile 下引用 WAF 策略 waf1，且配置 WAF 策略为保护模式。

```
<Sysname> system-view
```

```
[Sysname] app-profile sec
```

```
[Sysname-app-profile-sec] waf apply policy waf1 mode protect
```

【相关命令】

- **app-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **waf policy**

1.1.15 waf parameter-profile

waf { block-source | capture | logging | redirect } parameter-profile 命令用来配置 WAF 动作引用应用层检测引擎动作参数 profile。

undo waf { block-source | capture | logging | redirect } parameter-profile 命令用来取消配置 WAF 动作引用应用层检测引擎动作参数 profile。

【命令】

```
waf { block-source | capture | logging | redirect } parameter-profile  
parameter-name
```

```
undo waf { block-source | capture | logging | redirect } parameter-profile
```

【缺省情况】

WAF 动作未引用应用层检测引擎动作参数 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

block-source: 表示设置 WAF 源阻断动作的参数。

capture: 表示设置 WAF 捕获动作的参数。

logging: 表示设置 WAF 日志动作的参数。

redirect: 表示设置 WAF 重定向动作的参数。

parameter-profile *parameter-name*: 指定 WAF 动作引用的应用层检测引擎动作参数 **profile**。
parameter-name 表示动作参数 **profile** 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

每类 WAF 动作的具体执行参数由应用层检测引擎动作参数 **profile** 来定义，可通过引用各动作参数 **profile** 为 WAF 动作提供执行参数。有关应用层检测引擎动作参数 **profile** 的具体配置请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

如果 WAF 动作没有引用应用层检测引擎动作参数 **profile**，或者引用的动作参数 **profile** 不存在，则使用系统中各动作参数的缺省值。

【举例】

创建名称为 **waf1** 的应用层检测引擎源阻断动作参数 **profile**，配置其阻断源 IP 地址的时长为 1111 秒。

```
<Sysname> system-view
```

```
[Sysname] inspect block-source parameter-profile waf1
```

```
[Sysname-inspect-block-source-waf1] block-period 1111
```

```
[Sysname-inspect-block-source-waf1] quit
```

配置 WAF 源阻断动作引用名称为 **waf1** 的应用层检测引擎源阻断动作参数 **profile**。

```
[Sysname] waf block-source parameter-profile waf1
```

【相关命令】

- **inspect block-source parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **inspect capture parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **inspect logging parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)
- **inspect redirect parameter-profile** (DPI 深度安全命令参考/应用层检测引擎)

1.1.16 waf policy

waf policy 命令用来创建 WAF 策略，并进入 WAF 策略视图。如果指定的策略已经存在，则直接进入 WAF 策略视图。

undo waf policy 命令用来删除指定的 WAF 策略。

【命令】

```
waf policy policy-name  
undo waf policy policy-name
```

【缺省情况】

存在 WAF 策略，名称为 default。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

policy-name: 表示 WAF 策略的名称，为 1~63 个字符的字符串，不区分大小写，创建策略时策略名称不能为 default 且不能包含 “protected-website” 字符串。

【使用指导】

WAF 策略下可以配置特征过滤条件、匹配特征后执行的动作、防护的网站以及引用 CC 攻击防护策略。

名称为 default 的策略不可以被删除。

WAF 策略需要在 app-profile 中引用才生效，有关 app-profile 的详细介绍，请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

【举例】

```
# 创建名为 test-policy 的 WAF 策略，并进入该 WAF 策略视图。  
<Sysname> system-view  
[Sysname] waf policy test-policy  
[Sysname-waf-policy-test-policy]
```

【相关命令】

- **app-profile**（DPI 深度安全命令参考/应用层检测引擎）
- **display waf policy**

1.1.17 waf signature auto-update

waf signature auto-update 命令用来开启定期自动在线升级 WAF 特征库功能，并进入自动升级配置视图。

undo waf signature auto-update 命令用来关闭定期自动在线升级 WAF 特征库功能。

【命令】

```
waf signature auto-update  
undo waf signature auto-update
```

【缺省情况】

定期自动在线升级 WAF 特征库功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果设备可以访问官方网站上的特征库服务专区，可以采用定期自动在线升级方式来对设备上的 WAF 特征库进行升级。

【举例】

开启定期自动在线升级 WAF 特征库功能，并进入自动升级配置视图。

```
<Sysname> system-view
```

```
[Sysname] waf signature auto-update
```

```
[Sysname-waf-autoupdate]
```

【相关命令】

- **update schedule**

1.1.18 waf signature auto-update-now

waf signature auto-update-now 命令用来立即自动在线升级 WAF 特征库。

【命令】

waf signature auto-update-now

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

执行此命令后，将立即自动升级设备上的 WAF 特征库，且会备份当前的 WAF 特征库文件。此命令的生效与否，与是否开启了定期自动升级 WAF 特征库功能无关。

当管理员发现官方网站上的特征库服务专区中的 WAF 特征库有更新时，可以选择立即自动在线升级方式来及时升级 WAF 特征库版本。

【举例】

立即自动在线升级 WAF 特征库版本。

```
<Sysname> system-view
```

```
[Sysname] waf signature auto-update-now
```

1.1.19 waf signature rollback

waf signature rollback 命令用来回滚 WAF 特征库。

【命令】

```
waf signature rollback { factory | last }
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

factory: 表示 WAF 特征库的出厂版本。

last: 表示 WAF 特征库的上一版本。

【使用指导】

WAF 特征库回滚是指将当前的 WAF 特征库版本回滚到指定的版本。如果管理员发现设备当前 WAF 特征库版本在检测和防御网络攻击时，误报率较高或出现异常情况，则可以对当前 WAF 特征库版本进行回滚。目前支持将设备中的 WAF 过滤特征库版本回滚到出厂版本和上一版本。

WAF 特征库版本每次回滚前，设备都会备份当前版本。多次回滚上一版本的操作将会在当前版本和上一版本之间反复切换。例如当前 WAF 特征库是 V2，上一版本是 V1，第一次执行回滚到上一版本的操作后，特征库替换成 V1 版本，再执行回滚上一版本的操作则特征库重新变为 V2 版本。

【举例】

配置 WAF 特征库回滚到上一版本。

```
<Sysname> system-view
```

```
[Sysname] waf signature rollback last
```

【相关命令】

- **override-current**

1.1.20 waf signature update

waf signature update 命令用来手动离线升级 WAF 特征库。

【命令】

```
waf signature update [ override-current ] file-path
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

override-current: 表示覆盖当前版本的特征库文件。如果不指定本参数，则表示当前特征库在升级之后作为备份特征库保存在设备上。

file-path: 指定特征库文件的路径，为 1~255 个字符的字符串。

【使用指导】

如果设备不能访问官方网站上的特征库服务专区,管理员可以采用如下几种方式手动离线升级 WAF 特征库版本。

- 本地升级: 使用本地保存的特征库文件升级系统上的 WAF 特征库版本。
- FTP/TFTP 升级: 通过 FTP 或 TFTP 方式下载远程服务器上保存的特征库文件, 并升级系统上的 WAF 特征库版本。

使用本地升级方式离线升级特征库版本时, 特征库文件只能存储在当前主用设备上, 否则设备升级特征库会失败。

参数 *file-path* 的取值与手动离线升级的操作方式有关。本地升级时参数 *file-path* 取值请参见 [表 1-5](#); FTP/TFTP 升级时参数 *file-path* 取值请参见 [表 1-6](#)。

表1-5 本地升级时参数 file-path 取值说明表

升级场景	参数 file-path 取值	说明
特征库文件的存储位置与当前工作路径一致	filename	可以执行pwd命令查看当前工作路径 有关pwd命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不一致, 且在相同存储介质上	filename	需要先执行cd命令将工作路径切换至特征库文件所在目录下 有关cd命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”
特征库文件的存储位置与当前工作路径不在相同存储介质上	path/ filename	需要先执行cd命令将工作路径切换至特征库文件所在存储介质的根目录下, 再指定特征库文件的相对路径 有关cd命令的详细介绍请参见“基础配置命令参考”中的“文件系统管理”

表1-6 FTP/TFTP 升级时参数 file-path 取值说明表

升级场景	参数 file-path 取值	说明
特征库文件存储在开启FTP服务的远程服务器上	ftp://username:password@server/filename	username为登录FTP服务器的用户名, password为登录FTP服务器的密码, server为FTP服务器的IP地址或主机名 当FTP的用户名和密码中使用了“:”、“@”和“/”三种特殊字符时, 需要将这三种特殊字符替换为其对应的转义字符。“:”、“@”和“/”三种特殊字符对应的转义字符分别为“%3A或%3a”、“%40”和“%2F或%2f”
特征库文件存储在开启TFTP服务的远程服务器上	tftp://server/filename	server为TFTP服务器的IP地址或主机名



说明

当采用 FTP/TFTP 方式升级特征库时，如果指定的是服务器的主机名，则需要确保设备能通过静态或动态域名解析方式获得 FTP/TFTP 服务器的 IP 地址，并与之路由可达。否则设备升级特征库会失败。有关域名解析功能的详细配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

【举例】

配置手动离线升级 WAF 特征库，且采用 TFTP 方式，WAF 特征库文件的远程路径为 tftp://192.168.0.10/waf-1.0.2-en.dat。

```
<Sysname> system-view
```

```
[Sysname] waf signature update tftp://192.168.0.10/waf-1.0.2-en.dat
```

配置手动离线升级 WAF 特征库，且采用 FTP 方式，WAF 特征库文件的远程路径为 ftp://192.168.0.10/waf-1.0.2-en.dat，用户名为 user:123，密码为 user@abc/123。

```
<Sysname> system-view
```

```
[Sysname] waf signature update
```

```
ftp://user%3A123:user%40abc%2F123@192.168.0.10/waf-1.0.2-en.dat
```

配置手动离线升级 WAF 特征库，且采用本地方式，WAF 特征库文件的本地路径为 cfa0:/waf-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> system-view
```

```
[Sysname] waf signature update waf-1.0.23-en.dat
```

配置手动离线升级 WAF 特征库，且采用本地方式，WAF 特征库文件的本地路径为 cfa0:/dpi/waf-1.0.23-en.dat，且当前工作路径为 cfa0:。

```
<Sysname> cd dpi
```

```
<Sysname> system-view
```

```
[Sysname] waf signature update waf-1.0.23-en.dat
```

配置手动离线升级 WAF 特征库，且采用本地方式，WAF 特征库文件的本地路径为 cfb0:/dpi/waf-1.0.23-en.dat，当前工作路径为 cfa0:。

```
<Sysname> cd cfb0:/
```

```
<Sysname> system-view
```

```
[Sysname] waf signature update dpi/waf-1.0.23-en.dat
```

目 录

1 代理策略.....	1-1
1.1 代理策略配置命令.....	1-1
1.1.1 action.....	1-1
1.1.2 app-proxy ssl-decrypt-certificate delete.....	1-2
1.1.3 app-proxy ssl-decrypt-certificate import	1-2
1.1.4 app-proxy ssl-decrypt-certificate modify	1-4
1.1.5 app-proxy ssl whitelist activate.....	1-5
1.1.6 app-proxy ssl whitelist predefined-hostname enable	1-5
1.1.7 app-proxy ssl whitelist user-defined-hostname	1-6
1.1.8 app-proxy-policy.....	1-7
1.1.9 default action	1-8
1.1.10 destination-ip object-group	1-9
1.1.11 destination-zone	1-9
1.1.12 disable.....	1-10
1.1.13 display app-proxy server-certificate	1-11
1.1.14 display app-proxy ssl-decrypt-certificate.....	1-12
1.1.15 display app-proxy ssl whitelist hostname	1-15
1.1.16 display app-proxy ssl whitelist ip.....	1-16
1.1.17 display app-proxy-policy	1-17
1.1.18 rule	1-19
1.1.19 rule move	1-19
1.1.20 reset app-proxy server-certificate.....	1-20
1.1.21 reset app-proxy ssl whitelist ip	1-20
1.1.22 service.....	1-21
1.1.23 source-ip object-group	1-22
1.1.24 source-zone.....	1-23
1.1.25 user	1-24
1.1.26 user-group.....	1-25

1 代理策略

1.1 代理策略配置命令

1.1.1 action

action 命令用来配置代理策略规则的动作。

undo action 命令用来恢复缺省情况。

【命令】

```
action { no-proxy | ssl-decrypt | tcp-proxy }  
undo action
```

【缺省情况】

代理策略规则动作为 **no-proxy**。

【视图】

代理策略规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

no-proxy: 表示动作为不代理。

ssl-decrypt: 表示动作为 SSL 解密。

tcp-proxy: 表示动作为 TCP 代理。

【使用指导】

设备将根据代理策略规则的动作对命中规则的流量进行如下处理：

- 代理策略的动作配置为不代理时，设备将对命中策略的流量进行透传。
- 代理策略的动作配置为 SSL 解密时，设备将对命中策略的流量进行 SSL 代理，并基于此对 SSL 流量进行解密，并对解密后的流量进行深度安全检测。其中，SSL 代理是基于 TCP 代理实现的。
- 代理策略的动作配置为 TCP 代理时，设备将对命中策略的流量进行 TCP 代理，为客户端和服务端之间提供 TCP 层隔离，可有效地拦截恶意连接和攻击。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置代理策略规则 rule1 的动作为 SSL 解密。

```
<Sysname> system-view  
[Sysname] app-proxy-policy  
[Sysname-app-proxy-policy] rule 1 name rule1  
[Sysname-app-proxy-policy-0-rule1] action ssl-decrypt
```

【相关命令】

- **display app-proxy-policy**
- **rule**

1.1.2 app-proxy ssl-decrypt-certificate delete

app-proxy ssl-decrypt-certificate delete 命令用来删除 SSL 解密证书。

【命令】

app-proxy ssl-decrypt-certificate delete filename filename

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

filename: 表示 SSL 解密证书的文件名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

如果删除 SSL 解密证书，设备将不能签发 SSL 代理服务器证书发送到客户端，SSL 代理连接失败，设备将直接透传报文。

当证书成功导入设备后，文件类型会被改为 CER 格式，删除证书时需要将指定的证书后缀名改为.cer。

【举例】

```
# 删除 SSL 解密证书。  
<Sysname> system-view  
[Sysname] app-proxy ssl-decrypt-certificate delete aaa.cer
```

【相关命令】

- **display app-proxy ssl-decrypt-certificate**

1.1.3 app-proxy ssl-decrypt-certificate import

app-proxy ssl-decrypt-certificate import 命令用来导入 SSL 解密证书。

【命令】

app-proxy ssl-decrypt-certificate import { trusted | untrusted } { pem | p12 } filename filename

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

trusted: 表示 SSL 解密证书可以用于签发标识为可信的 SSL 代理服务器证书。用于传递真实服务器证书合法的信息给客户端。

untrusted: 表示 SSL 解密证书可以用于签发标识为不可信的 SSL 代理服务器证书。客户端不信任的 CA 证书。用于传递真实服务器证书非法的信息给客户端, 让用户感知到可能存在的安全风险。

pem: 表示导入的证书的格式为 PEM 编码。

P12: 表示导入的证书的格式为 PKCS#12 编码。

filename filename: 表示导入的证书文件的名称, 为 1~63 个字符的字符串, 不区分大小写。

【使用指导】

导入 SSL 解密证书时需要为其标识可以签发的 SSL 代理服务器证书的可信度。

当设备接收到服务器证书后, 将代替客户端对服务器的合法性进行验证, 并使用具备签发不同标识功能的 SSL 解密证书签发不同标识的 SSL 代理服务器证书向客户端传递服务器的合法性信息:

- 当服务器合法时: 设备将使用可签发可信标识的 SSL 解密证书签发一本可信 SSL 代理服务器证书, 向客户端传递此服务器合法的信息。
- 当服务器不合法时: 设备将使用可签发不可信标识的 SSL 解密证书签发一本不可信 SSL 代理服务器证书, 向客户端传递此服务器不合法的信息。

设备上只能存在一份可信 SSL 解密证书和一份不可信 SSL 解密证书, 多次执行本命令, 后续导入的可信或者不可信证书会覆盖原有的证书。

同一本 SSL 解密证书仅可导入一次, 如果需要为同一本证书标识两种可信度, 可执行 **app-proxy ssl-decrypt-certificate modify** 命令为证书添加可信度标识。

需要在客户端浏览器上安装并信任 SSL 解密证书。防止设备启用 SSL 解密功能后, 客户端通过浏览器访问 HTTPS 类网站时, 会弹出服务器证书不是由受信任机构颁发的告警信息, 甚至有些应用程序不提示告警信息就直接中断了连接, 影响用户的正常使用。

默认情况下, 火狐浏览器不共享系统中的证书库, 如果已经在其他浏览器上导入 SSL 卸载证书, 则可以通过修改火狐浏览器中的高级设置, 使其共享系统中的证书库, 不再单独导入证书, 具体操作步骤如下:

在地址栏中输入: **about:config**, 搜索框中输入: **security.enterprise_roots.enabled**, 双击选中的条目, 或者单击鼠标右键, 选择切换, 修改其值为 **true**。

导入成功后, 设备将修改证书文件类型为 CER 格式。

【举例】

导入 PKCS#12 编码格式的用于签发可信 SSL 代理服务器证书的 SSL 解密证书。

```
<Sysname> system-view
```

```
[Sysname] app-proxy ssl-decrypt-certificate import trusted p12 filename aaa.p12
```

```
Password:
```

【相关命令】

- **display app-proxy ssl-decrypt-certificate certificate**

1.1.4 app-proxy ssl-decrypt-certificate modify

app-proxy ssl-decrypt-certificate modify 命令用来添加 SSL 解密证书可签发 SSL 代理服务器证书的可信度。

undo app-proxy ssl-decrypt-certificate modify 命令用来删除 SSL 解密证书可签发 SSL 代理服务器证书的可信度。

【命令】

```
app-proxy ssl-decrypt-certificate modify { trusted | untrusted } filename  
filename
```

```
undo app-proxy ssl-decrypt-certificate modify { trusted | untrusted }
```

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

trusted: 表示 SSL 解密证书可以用于签发标识为可信的 SSL 代理服务器证书。用于传递真实服务器证书合法的信息给客户端。

untrusted: 表示 SSL 解密证书可以用于签发标识为不可信的 SSL 代理服务器证书。客户端不信任的 CA 证书。用于传递真实服务器证书非法的信息给客户端，让用户感知到可能存在的安全风险。

filename: 表示 SSL 解密证书文件的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

本命令可用于为同一本 SSL 解密证书添加可签发 SSL 代理服务器证书的可信度，即使用一本 SSL 解密证书同时签发可信和不可信的 SSL 代理服务器证书。

为 SSL 解密证书添加指定的可信度后，原指定可信度的证书将被删除。

删除 SSL 解密证书指定的可信度后，SSL 解密证书不可签发指定可信度的 SSL 代理服务器证书，但 SSL 解密证书仍然保存在设备中，不会被删除，管理员可再次为 SSL 解密证书添加可信度。

当 SSL 解密证书成功导入设备后，文件类型会被改为 CER 格式，修改证书时需要将指定的证书后缀名改为.cer。

【举例】

修改用于签发 SSL 代理服务器证书的 CA 证书为可信证书。

```
<Sysname> system-view
```

```
[Sysname] app-proxy ssl-decrypt-certificate modify trusted filename aaa.cer
```

```
[Sysname] A trusted CA certificate already exists. Overwrite the existing trusted CA  
certificate with the specified certificate? [Y/N]:
```

【相关命令】

- **display app-proxy ssl-decrypt-certificate**

1.1.5 app-proxy ssl whitelist activate

app-proxy ssl whitelist activate 命令用来激活 SSL 代理白名单的配置。

【命令】

app-proxy ssl whitelist activate

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

需要激活 SSL 代理域名白名单配置的场景如下：

- 对自定义 SSL 代理域名白名单进行添加、修改和删除操作。
- 对预定义 SSL 代理域名白名单进行启用或禁用操作。

仅支持在缺省 Context 下配置本命令。有关 Context 的详细介绍，请参见“虚拟化技术配置指导”中的“Context”。

【举例】

配置 example.com 加入 SSL 代理域名白名单，并激活配置。

```
<Sysname> system-view
[Sysname] app-proxy ssl whitelist user-defined-hostname example.com
To activate the setting, execute app-proxy ssl whitelist activate.
[sysname] app-proxy ssl whitelist activate
```

【相关命令】

- **app-proxy ssl whitelist predefined-hostname enable**
- **app-proxy ssl whitelist user-defined-hostname**

1.1.6 app-proxy ssl whitelist predefined-hostname enable

app-proxy ssl whitelist predefined-hostname enable 命令用来启用预定义 SSL 代理域名白名单。

undo app-proxy ssl whitelist predefined-hostname enable 命令用来禁用预定义 SSL 代理域名白名单。

【命令】

```
app-proxy ssl whitelist predefined-hostname { chrome-hsts [ hostname ] |  
hostname } enable  
undo app-proxy ssl whitelist predefined-hostname { chrome-hsts [ hostname ]  
| hostname } enable
```

【缺省情况】

预定义 SSL 代理域名白名单处于启用状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

chrome-hsts [*host-name*]: 表示 Chrome 浏览器强制使用 HTTPS 方式访问的域名。
host-name, 表示域名, 为 1~63 个字符的字符串, 不区分大小写。当名称中包含空格时, 需要使用双引号将名称括起来” 例如"user for test"。若不指定本参数, 则表示所有 Chrome-hsts 类型的域名。

host-name: 表示不被 Chrome 浏览器强制使用 HTTPS 方式访问的域名, 为 1~63 个字符的字符串, 不区分大小写。当名称中包含空格时, 需要使用双引号将名称括起来” 例如"user for test"。

【使用指导】

HSTS (HTTP Strict Transport Security) 国际互联网工程组织 IETF 正在推行一种新的 Web 安全协议。HSTS 的作用是强制客户端 (如浏览器) 使用 HTTPS 与服务器创建连接。当 chrome-hsts 白名单整体处于禁用状态时, 单独启用或禁用指定的 chrome-hsts 域名不生效。

当 chrome-hsts 白名单整体处于开启状态时, 可单独启用或禁用指定的 chrome-hsts 域名。

仅支持在缺省 Context 下配置本命令。有关 Context 的详细介绍, 请参见“虚拟化技术配置指导”中的“Context”。

【举例】

整体禁用预定义 SSL 代理域名白名单中的 chrome-hsts。

```
<Sysname> system-view
```

```
[sysname] undo app-proxy ssl whitelist predefined-hostname chrome-hsts enable
```

To activate the setting, execute app-proxy ssl whitelist activate.

禁用预定义 SSL 代理域名白名单中的 12306.cn。

```
<Sysname> system-view
```

```
[sysname] undo app-proxy ssl whitelist predefined-hostname 12306.cn enable
```

To activate the setting, execute app-proxy ssl whitelist activate.

【相关命令】

- **app-proxy ssl whitelist activate**
- **display app-proxy ssl whitelist**

1.1.7 app-proxy ssl whitelist user-defined-hostname

app-proxy ssl whitelist user-defined-hostname 命令用来添加自定义 SSL 代理域名白名单。

undo app-proxy ssl whitelist user-defined-hostname 命令用来删除自定义 SSL 代理域名白名单。

【命令】

app-proxy ssl whitelist user-defined-hostname host-name

```
undo app-proxy ssl whitelist user-defined-hostname { host-name | all }
```

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

host-name: 表示服务器域名，为 1~63 个字符的字符串，不区分大小写。当名称中包含空格时，需要使用双引号将名称括起来，例如"user for test"。

all: 表示删除自定义 SSL 代理域名白名单中的所有域名。

【使用指导】

设备使用 **host-name** 与 SSL 请求报文中携带的服务器证书的“DNS Name”或“Common Name”字段进行匹配，只要含有 **host-name** 的域名均会匹配成功。若匹配成功，则透传该 SSL 连接。

配置本命令后需要执行 **app-proxy ssl whitelist activate** 命令，使配置生效。

仅支持在缺省 Context 下配置本命令。有关 Context 的详细介绍，请参见“虚拟化技术配置指导”中的“Context”。

【举例】

```
# 添加名为 example.com 的自定义 SSL 代理域名白名单，并提交配置。  
<Sysname> system-view  
[Sysname] app-proxy ssl whitelist user-defined-hostname example.com  
To activate the setting, execute app-proxy ssl whitelist activate.  
[sysname] app-proxy ssl whitelist activate
```

【相关命令】

- **app-proxy ssl whitelist activate**
- **display app-proxy ssl whitelist**

1.1.8 app-proxy-policy

app-proxy-policy 命令用来进入代理策略视图。

undo app-proxy-policy 命令用来删除所有代理策略配置。

【命令】

```
app-proxy-policy  
undo app-proxy-policy
```

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

目前仅支持 IPv4 代理策略。

【举例】

```
# 进入代理策略视图。  
<Sysname> system-view  
[Sysname] app-proxy-policy  
[Sysname-app-proxy-policy]
```

【相关命令】

- **display app-proxy-policy**

1.1.9 default action

default action 命令用来配置代理策略的缺省动作。

undo default action 命令用来恢复缺省情况。

【命令】

```
default action { no-proxy | ssl-decrypt | tcp-proxy }  
undo default action
```

【缺省情况】

缺省动作为 **no-proxy**。

【视图】

代理策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

no-proxy: 表示动作为不代理。

ssl-decrypt: 表示动作为 SSL 解密。

tcp-proxy: 表示动作为 TCP 代理。

【使用指导】

配置此命令后，当报文没有匹配上代理策略中的规则时，设备将根据缺省动作对此报文进行处理。
多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 配置代理策略的缺省动作为 SSL 解密。  
<Sysname> system-view  
[Sysname] app-proxy-policy  
[Sysname-app-proxy-policy] default action ssl-decrypt
```

1.1.10 destination-ip object-group

destination-ip object-group 命令用来配置作为代理策略规则过滤条件的目的 IP 地址对象组。

undo destination-ip object-group 命令用来删除作为代理策略规则过滤条件的目的 IP 地址对象组。

【命令】

destination-ip object-group *object-group-name*

undo destination-ip object-group [*object-group-name*]

【缺省情况】

未配置作为代理策略规则过滤条件的目的 IP 地址对象组。

【视图】

代理策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-group-name: 表示目的地址对象组的名称，为 1~31 个字符的字符串，不区分大小写，且不能为字符串 any。

【使用指导】

多次执行本命令，可配置多个目的 IP 地址作为代理策略规则的过滤条件。只要一个目的 IP 地址匹配成功，则认为目的 IP 地址过滤条件匹配成功。

指定的对象组必须已存在，若指定一个不存在的对象组，配置将下发失败。

使用 **undo** 命令时若不指定本参数，则表示删除所有目的 IP 地址对象组过滤条件。有关地址对象组的详细介绍，请参见“安全配置指导”中的“对象组”。

【举例】

配置作为代理策略规则 rule1 过滤条件的目的地址对象组为 client1 和 client2。

```
<Sysname> system-view
```

```
[Sysname] app-proxy-policy
```

```
[Sysname-app-proxy-policy] rule 1 name rule1
```

```
[Sysname-app-proxy-policy-0-rule1] destination-ip object-group client1
```

```
[Sysname-app-proxy-policy-0-rule1] destination-ip object-group client2
```

【相关命令】

- **display app-proxy-policy**
- **object-group**（安全命令参考/对象组）

1.1.11 destination-zone

destination-zone 命令用来配置作为代理策略规则过滤条件的目的安全域。

undo destination-zone 命令用来删除作为代理策略规则过滤条件的目的安全域。

【命令】

```
destination-zone destination-zone-name  
undo destination-zone [ destination-zone-name ]
```

【缺省情况】

未配置作为代理策略规则过滤条件的目的安全域。

【视图】

代理策略规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

destination-zone-name: 表示目的安全域的名称，为 1~31 个字符的字符串，不区分大小写，且不能为字符串 any。

【使用指导】

多次执行本命令，可配置多个目的安全域作为代理策略规则的过滤条件。只要一个目的安全域匹配成功，则认为目的安全域过滤条件匹配成功。

如果指定的安全域不存在，配置可以成功下发，但不生效。

使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有目的安全域类型的过滤条件。有关安全域的详细介绍，请参见“基础配置指导”中的“安全域”。

【举例】

```
# 配置作为代理策略规则 rule1 过滤条件的目的安全域为 trust 和 server。  
<Sysname> system-view  
[Sysname] app-proxy-policy  
[Sysname-app-proxy-policy] rule 1 name rule1  
[Sysname-app-proxy-policy-0-rule1] destination-zone trust  
[Sysname-app-proxy-policy-0-rule1] destination-zone server
```

【相关命令】

- **display app-proxy-policy**
- **security-zone**（安全命令参考/安全域）

1.1.12 disable

disable 命令用来禁用代理策略规则。

undo disable 命令用来启用代理策略规则。

【命令】

```
disable  
undo disable
```


【缺省情况】

代理策略规则处于启用状态。

【视图】

代理策略规则视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

禁用代理策略规则后，流量不会与代理策略规则进行匹配。

多条规则处于启用状态时，流量会按序匹配这些规则，一旦匹配成功就按照当前规则所配置动作处理。

【举例】

在代理策略规则视图下，禁用代理策略规则 rule1。

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] disable
```

【相关命令】

- rule

1.1.13 display app-proxy server-certificate

display app-proxy server-certificate 命令用来显示客户端访问的服务器的证书。

【命令】

display app-proxy server-certificate [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

slot slot-number: 显示指定成员设备上客户端访问的服务器的证书，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，显示所有成员设备上客户端访问的服务器的证书。

【使用指导】

可通过本命令查看设备作为 SSL 代理客户端时接收到的客户端访问的服务器证书。

【举例】

```
# 显示指定 slot 上的客户端访问的服务器的证书。
<Sysname> display app-proxy server-certificate slot 1
Slot1:
Total server certificates: --
Certificate info: /cn=unis-https-self-signed-certificate-13a73249669cc70a
Proxy count: 198
Most recent proxy time: 2017/10/25 10:7:7
First proxy at: 2017/10/23 15:52:59
```

图1-1 display app-proxy ssl certificate 命令显示信息描述表

字段	描述
Total server certificates	客户端访问的服务器证书总数
Certificate info	证书的一些关键信息，取值包括： • Certificate Info: example.com: 表示证书中有“DNS Name”字段，example.com 是证书的“DNS Name”。 • Certificate Info: /cn=example.com: 表示证书中无“DNS Name”字段，example.com 是证书的“Common Name”。
Proxy count	进行SSL代理的次数
Most recent proxy time	最近一次进行SSL代理的时间
First proxy at	第一次进行SSL代理的时间

【相关命令】

- **reset app-proxy server-certificate**

1.1.14 display app-proxy ssl-decrypt-certificate

display app-proxy ssl-decrypt-certificate 命令用来显示 SSL 解密证书。

【命令】

display app-proxy ssl-decrypt-certificate

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 显示 SSL 解密证书。
<Sysname> display app-proxy ssl-decrypt-certificate
```

Trusted:

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

aa:31:f8:3d:06:b0:9b: Signature Algorithm: sha1WithRSAEncryption

Issuer: C=CN, ST=bj, L=cp, O=dpi, OU=sec, CN=trustca

Validity

Not Before: Sep 7 12:00:43 2017 GMT

Not After : Aug 28 12:00:43 2057 GMT

Subject: C=CN, ST=bj, L=cp, O=dpi, OU=sec, CN=trustca

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:ec:d7:73:af:03:07:07:86:e6:31:4d:e5:32:09:
20:7f:93:19:20:b2:25:c4:cc:32:8e:e4:29:fd:e0:
30:48:4c:8d:0a:83:66:28:af:6a:e0:69:81:08:58:
ca:cf:e4:3d:5a:e8:69:92:67:71:e3:c0:66:87:8e:
16:cc:6a:89:1d:d4:22:5f:93:14:47:bd:39:60:44:
3c:ee:0a:d1:8d:d4:16:84:65:e9:b7:b1:0f:6d:af:
6e:ef:21:b5:5a:02:4f:63:46:6e:8b:73:b5:95:70:
8a:ed:5d:23:8b:d8:0e:45:2d:8b:52:ab:34:6d:3b:
d5:85:ae:1c:d4:26:6e:fb:2c:1e:18:db:55:22:96:
d8:1f:1a:33:e9:ff:1f:8c:be:28:9d:de:77:d8:9b:
a7:27:0f:7e:e2:52:3e:bd:02:ee:c3:06:93:d0:16:
b0:c7:96:bb:c8:b1:96:8d:ee:ca:6e:76:63:1e:b1:
b6:fb:31:bf:d0:13:66:ad:f6:97:cf:0b:37:f7:6c:
f8:46:b6:76:f1:70:6f:24:6c:92:a6:dd:c2:3b:cf:
3c:35:c7:74:60:dd:db:a3:bf:70:b4:55:05:4b:d7:
cd:dd:c1:1b:59:0d:41:e7:95:5a:79:44:9d:b0:8b:
a7:f2:f4:67:0e:0c:4a:b6:35:97:1e:e6:99:88:fc:
c8:e9

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Alternative Name:

IP Address:1.1.1.1, DNS:trustca, email:1@3.com

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Key Usage: critical

Certificate Sign, CRL Sign

X509v3 Subject Key Identifier:

D4:35:A8:66:63:03:04:2B:CA:4E:91:06:11:F5:72:1C:26:E0:BE:33

Netscape Cert Type:

SSL CA

Netscape Comment:

example comment extension

Signature Algorithm: sha1WithRSAEncryption

```

b9:d2:eb:98:bd:f9:8d:7e:03:a8:0e:b4:29:cf:3a:a1:fd:f4:
2a:fa:56:1c:cf:40:a4:9e:7f:5a:15:6b:88:8a:dd:86:d2:03:
c3:38:49:7a:11:09:78:81:8c:8f:0a:3b:fb:d6:60:59:c4:0b:
12:0e:38:b0:92:f3:2e:b5:96:ab:d3:a4:2d:cb:ef:fd:a0:97:
d0:63:43:8e:91:1f:f1:fc:39:c8:cf:e5:ee:4b:e7:8c:8b:f8:
3b:ff:5e:dc:00:df:5b:2f:98:53:f2:c7:da:fa:b8:2e:92:dd:
33:6a:80:df:0e:22:62:62:5d:2f:6c:eb:4c:80:c4:56:c9:00:
01:a6:82:60:e4:32:69:f7:7b:8f:6c:93:e5:c3:64:65:fe:aa:
e1:0b:10:92:bd:ea:2f:2f:e5:b6:fd:b5:5b:df:34:c8:5d:5a:
91:9a:0d:89:10:76:b8:ed:28:ef:6a:c4:7b:48:d7:88:57:7c:
cf:4e:c8:38:84:ad:54:6d:3f:40:a0:38:d7:36:61:23:7a:82:
62:34:41:3d:cc:b2:ee:4a:23:f1:7d:12:e2:23:26:10:df:c8:
a1:6f:00:00:b7:c2:1f:ce:1b:63:60:e0:63:33:e0:59:31:78:
bc:27:99:b6:27:40:95:da:1b:37:07:75:2f:99:97:56:33:f5:
4f:ad:14:31

```

图1-2 display app-proxy pki certificate 命令显示信息描述表

字段	描述
Trusted	证书的可信度，取值包括： - Trusted: 客户端信任的证书 - Untrusted: 客户端不信任的证书
Certificate	证书的信息
Data	证书的数据
Version	证书的版本
Serial Number	证书的序列号
Signature Algorithm	证书的签名算法
Issuer	证书的颁发者
Validity	证书的有效期
Subject	证书的主题
Subject Public Key Info	证书的主题公钥信息
Public Key Algorithm	公钥算法
Public-Key	公钥信息
Modulus	密钥模数
Exponent	密钥指数
X509v3 extensions	X.509v3证书扩展项
X509v3 Subject Alternative Name	主题的备用名称
IP Address	实体的IP地址
DNS	实体的DNS名

字段	描述
email	实体的电子邮箱地址
X509v3 Basic Constraints	基本约束，指出一个证书是否是CA证书
X509v3 Key Usage	密钥用法，指出有效用途
X509v3 Subject Key Identifier	主题密钥标识符
Netscape Cert Type	Netscape证书类型，可以用于指定网景软件的密钥用途
Netscape Comment	Netscape注释，在某些浏览器中可以用于展示注释信息

1.1.15 display app-proxy ssl whitelist hostname

display app-proxy ssl whitelist hostname 命令用来显示 SSL 代理域名白名单。

【命令】

display app-proxy ssl whitelist hostname { predefined | user-defined }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

user-defined: 表示显示自定义 SSL 代理域名白名单。

predefined: 表示显示预定义 SSL 代理域名白名单。

【使用指导】

仅支持在缺省 Context 下配置本命令。有关 Context 的详细介绍，请参见“虚拟化技术配置指导”中的“Context”。

【举例】

显示自定义 SSL 代理域名白名单。

```
<Sysname> display app-proxy ssl whitelist hostname user-defined
Hostname
example1.com
example2.com
```

显示预定义 SSL 代理域名白名单。

```
<Sysname> display app-proxy ssl whitelist hostname predefined
Chrome HSTS-defined hostnames:
  status      Hostname
  enabled     2mdn.net
```

```

enabled    accounts.firefox.com
enabled    aclu.org
enabled    activiti.alfresco.com
enabled    adamkostecki.de
enabled    advocate.com
enabled    adsfund.org
enabled    aie.de
enabled    airbnb.com
enabled    aladdinschools.appspot.com
enabled    alexsexton.com
enabled    alpha.irccloud.com
enabled    android.com
enabled    ansdell.net
enabled    anycoin.me
enabled    apadvantage.com
enabled    api.intercom.io
enabled    api.lookout.com
enabled    api.mega.co.nz
enabled    api.recurly.com
enabled    api.simple.com
---- More ----

```

图1-3 display app-proxy ssl whitelist 命令显示信息描述表

字段	描述
Chrome HSTS-defined hostnames	表示Chrome浏览器强制使用HTTPS方式访问的域名
Hostname	表示域名
Status	表示域名白名单的生效状态，取值包括： - Enabled：表示启用 - Disabled：表示禁用

【相关命令】

- **app-proxy ssl whitelist predefined-hostname enable**
- **app-proxy ssl whitelist user-defined-hostname**

1.1.16 display app-proxy ssl whitelist ip

display app-proxy ssl whitelist ip 命令用来显示 SSL 代理 IP 地址白名单。

【命令】

display app-proxy ssl whitelist ip { all [slot slot-number] | ip-address }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

all: 显示 SSL 代理 IP 地址白名单的所有 IP 地址。
ip-address: 显示 SSL 代理 IP 地址白名单中指定的 IP 地址。
slot slot-number: 显示指定成员设备上 SSL 代理 IP 地址白名单，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，显示所有成员设备上 SSL 代理 IP 地址白名单。

【举例】

显示指定 slot 上的所有 SSL 代理 IP 地址白名单。
<Sysname> display app-proxy ssl whitelist ip all slot 1
Slot 1:
IP address Port
10.1.1.1 443
10.10.1.1 443

图1-4 display app-proxy ssl whitelist ip 命令显示信息描述表

字段	描述
IP address	SSL代理白名单的IP地址
Port	SSL代理白名单的IP地址对应的端口号

1.1.17 display app-proxy-policy

display app-proxy-policy 命令用来显示代理策略的配置信息。

【命令】

display app-proxy-policy [rule rule-name]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

rule rule-name: 表示代理策略规则的名称，为 1~63 个字符的字符串，不区分大小写。若不指定本参数，则显示所有代理策略规则的配置。

【举例】

```
# 显示代理策略的配置信息。
<Sysname> display app-proxy-policy
Default action: ssl-decrypt
Rule with ID 0 and name rule0:
  Action: ssl-decrypt
  Status: Enabled
  Match criteria:
    Source security zones: trust
    Destination security zones: trust
    Source IP address object groups: srcobj
    Destination IP address object groups: destobj
    Service object groups: serviceobj
    Users: user1
    User groups: usergroup1

Rule with ID 2 and name rule2:
  Action: ssl-decrypt
  Status: Enabled
  Match criteria:
    source-zone: trust
    destination-zone: Untrust
```

图1-5 display app-proxy-policy 命令显示信息描述表

字段	描述
Default action	表示代理策略的缺省动作，取值包括： - no-proxy: 表示不代理 - ssl-decrypt: 表示 SSL 解密 - tcp-proxy: 表示 TCP 代理
Rule with ID <i>rule-id</i> and name <i>rule-name</i>	表示代理策略规则，ID为 <i>rule-id</i> ，名称为 <i>rule-name</i>
Action	对匹配上代理策略规则的报文执行动作，取值包括： - no-proxy: 表示不代理 - ssl-decrypt: 表示 SSL 解密 - tcp-proxy: 表示 TCP 代理
Source security zones	表示规则过滤条件中的源安全域名称
Destination security zones	表示规则过滤条件中的目的安全域名称
Source IP address object groups	表示规则过滤条件中的源IP地址对象组名称
Destination IP address object groups	表示规则过滤条件中的目的IP地址对象组名称
Service object groups	表示规则过滤条件中的服务对象组名称
Users	表示规则过滤条件中的用户名称

字段	描述
User groups	表示规则过滤条件中的用户组名称

1.1.18 rule

rule 命令用来创建代理策略规则，并进入代理策略规则视图。如果指定的代理策略规则已经存在，则直接进入代理策略规则视图。

undo rule 命令用来删除指定的代理策略规则。

【命令】

```
rule { rule-id | [ rule-id ] name rule-name }
undo rule { rule-id | name rule-name }
```

【视图】

代理策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

rule-id: 表示代理策略规则的编号，取值范围为 1~65535。若未指定本参数，系统将从 1 开始，自动分配一个大于现有最大编号的最小编号，步长为 1。如果现有最大编号已经达到规格上限，则选择当前未使用的最小编号作为新的编号。

name rule-name: 表示代理策略规则的名称，为 1~63 个字符的字符串，不区分大小写，创建规则时必须配置名称，规则名称不能为 default。

【举例】

```
# 创建名为 rule1 的代理策略规则。
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-1-rule1]
```

【相关命令】

- **display app-proxy-policy**

1.1.19 rule move

rule move 命令用来移动代理策略规则。

【命令】

```
rule move rule-id before insert-rule-id
```

【视图】

代理策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

rule-id: 表示待移动代理策略规则编号，取值范围为 1～65535。

insert-rule-id: 表示移动到指定编号的规则之前，取值范围为 1～65536。配置最大编号时，表示待移动代理策略规则移动到所有规则之后。

【使用指导】

如果待移动规则与参考规则相同或不存在，则不执行任何移动操作。

【举例】

```
# 移动代理策略规则 5 到规则 2 之前。  
<Sysname> system-view  
[Sysname] app-proxy-policy  
[Sysname-app-proxy-policy] rule move 5 before 2
```

【相关命令】

- **rule**

1.1.20 reset app-proxy server-certificate

reset app-proxy server-certificate 命令用来清除客户端访问的服务器的证书。

【命令】

reset app-proxy server-certificate

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 清除客户端访问的服务器的证书。  
<Sysname> reset app-proxy server-certificate
```

【相关命令】

- **display app-proxy server-certificate**

1.1.21 reset app-proxy ssl whitelist ip

reset app-proxy ssl whitelist ip 命令用来清除 SSL 代理 IP 地址白名单。

【命令】

reset app-proxy ssl whitelist

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【举例】

清除 SSL 代理 IP 地址白名单。

```
<Sysname> reset app-proxy ssl whitelist ip
```

【相关命令】

- **display app-proxy ssl whitelist ip**

1.1.22 service

service object-group 命令用来配置作为代理策略规则过滤条件的服务对象组。

undo service object-group 命令用来删除作为代理策略规则过滤条件的服务对象组。

【命令】

```
service object-group { object-group-name }
```

```
undo service object-group [ object-group-name ]
```

【缺省情况】

未配置作为代理策略规则过滤条件的服务对象组。

【视图】

代理策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-group-name: 服务对象组的名称，为 1~31 个字符的字符串，不区分大小写，且不能为 any。

【使用指导】

多次执行本命令，可配置多个服务对象组作为代理策略规则的过滤条件。只要一个服务对象组匹配成功，则认为服务对象组过滤条件匹配成功。

只支持服务对象组中配置四层及其以下的协议类型，若引用的服务组配置了其他协议类型，该服务组不生效。

指定的服务对象组必须已存在，若指定一个不存在的对象组，配置将下发失败。

使用 **undo** 命令时若不指定任何参数，则表示删除此规则中所有服务类型的过滤条件。

【举例】

配置作为代理策略规则 rule1 过滤条件的服务对象组为 tcp 和 ftp。

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] service object-group tcp
[Sysname-app-proxy-policy-0-rule1] service object-group ftp
```

【相关命令】

- **display app-proxy-policy**
- **object-group**（安全命令参考/对象组）

1.1.23 source-ip object-group

source-ip object-group 命令用来配置作为代理策略规则过滤条件的源 IP 地址对象组。

undo source-ip object-group 命令用来删除作为代理策略规则过滤条件的源 IP 地址对象组。

【命令】

```
source-ip object-group object-group-name
undo source-ip object-group [ object-group-name ]
```

【缺省情况】

未配置作为代理策略规则过滤条件的源 IP 地址对象组。

【视图】

代理策略规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

object-group-name: 表示源地址对象组的名称，为 1~31 个字符的字符串，不区分大小写，且不能为字符串 any。

【使用指导】

多次执行本命令，可配置多个源 IP 地址作为代理策略规则的过滤条件。只要一个源 IP 地址匹配成功，则认为源 IP 地址过滤条件匹配成功。

指定的对象组必须已存在，若指定一个不存在的对象组，配置将下发失败。

使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有源 IP 地址类型的过滤条件。有关地址对象组的详细介绍，请参见“安全配置指导”中的“对象组”。

【举例】

配置作为代理策略规则 rule1 过滤条件的源地址对象组为 server1 和 server2。

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] source-ip object-group server1
[Sysname-app-proxy-policy-0-rule1] source-ip object-group server2
```

【相关命令】

- **display app-proxy-policy**
- **object-group**（安全命令参考/对象组）

1.1.24 source-zone

source-zone 命令用来配置作为代理策略规则过滤条件的源安全域。

undo source-zone 命令用来删除作为代理策略规则过滤条件的源安全域。

【命令】

source-zone *source-zone-name*

undo source-zone [*source-zone-name*]

【缺省情况】

未配置作为代理策略规则过滤条件的源安全域。

【视图】

代理策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

source-zone-name: 表示源安全域的名称，为 1~31 个字符的字符串，不区分大小写，且不能为字符串 any。

【使用指导】

多次执行本命令，可配置多个源安全域作为代理策略规则的过滤条件，只要一个源安全域匹配成功，则认为源安全域过滤条件匹配成功。

如果指定的安全域不存在，配置可以成功下发，但不生效。

使用 **undo** 命令时若不指定此参数，则表示删除此规则中所有源安全域类型的过滤条件。有关安全域的详细介绍，请参见“安全配置指导”中的“安全域”。

【举例】

配置作为代理策略规则 rule1 过滤条件的源安全域为 trust 和 server。

```
<Sysname> system-view
```

```
[Sysname] app-proxy-policy
```

```
[Sysname-app-proxy-policy] rule 1 name rule1
```

```
[Sysname-app-proxy-policy-0-rule1] source-zone trust
```

```
[Sysname-app-proxy-policy-0-rule1] source-zone server
```

【相关命令】

- **display app-proxy-policy**
- **security-zone**（安全命令参考/安全域）

1.1.25 user

user 命令用来配置作为代理策略规则过滤条件的用户。

undo user 命令用来删除作为代理策略规则过滤条件的用户。

【命令】

```
user user-name [ domain domain-name ]
undo user [ username [ domain domain-name ] ]
```

【缺省情况】

未配置作为代理策略规则过滤条件的用户。

【视图】

代理策略规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

username: 表示用户的名称，为 1~55 个字符的字符串，区分大小写，不能是 a、al 和 all，且不能包含特殊字符 “\”、“|”、“/”、“:”、“*”、“?”、“<”、“>” 和 “@”。

domain domain-name: 表示身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“:”、“*”、“?”、“<”、“>” 和 “@” 字符。

【使用指导】

多次执行配置命令，可配置多个用户作为规则的过滤条件，只要一个用户匹配成功，则认为用户过滤条件匹配成功。

若指定的用户或身份识别域不存在或者用户和身份识别域不匹配，配置可以成功下发，但不生效。

使用 **undo** 命令时若不指定 **username**，则表示删除此规则中所有用户过滤条件。

使用 **undo** 命令时若不指定 **domain-name**，则表示删除此规则中所有身份识别域之外的用户过滤条件。

【举例】

配置作为代理策略规则 rule1 过滤条件的用户为 usera 和 userb，身份识别域均为 test。

```
<Sysname> system-view
[Sysname] app-proxy-policy
[Sysname-app-proxy-policy] rule 1 name rule1
[Sysname-app-proxy-policy-0-rule1] user usera domain test
[Sysname-app-proxy-policy-0-rule1] user userb domain test
```

【相关命令】

- **display app-proxy-policy**
- **user-identity enable**（安全命令参考/用户身份识别与管理）
- **user-identity static-user**（安全命令参考/用户身份识别与管理）

1.1.26 user-group

user-group 命令用来配置作为代理策略规则过滤条件的用户组。

undo user-group 命令用来删除作为代理策略规则过滤条件的用户组。

【命令】

user-group *user-group-name* [**domain** *domain-name*]

undo user-group [*user-group-name* [**domain** *domain-name*]]

【缺省情况】

未配置作为代理策略规则过滤条件的用户组。

【视图】

代理策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-group-name: 表示用户组的名称，为 1~200 个字符的字符串，不区分大小写。

domain domain-name: 表示在指定的身份识别域中匹配此用户组，**domain-name** 是身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符。

【使用指导】

多次执行配置命令，可配置多个用户组作为规则的过滤条件，只要一个用户组匹配成功，则认为用户组过滤条件匹配成功。

若指定的用户组不存在，配置可以成功下发，但不生效。

使用 **undo** 命令时若不指定 **user-group-name**，则表示删除此规则中所有用户组过滤条件。有关用户组的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

使用 **undo** 命令时若不指定 **domain-name**，则表示删除此规则中所有身份识别域之外的用户组过滤条件。

【举例】

配置作为代理策略规则 rule1 过滤条件的用户组为 groupa 和 groupb，身份识别域均为 test。

```
<Sysname> system-view
```

```
[Sysname] app-proxy-policy
```

```
[Sysname-app-proxy-policy] rule 1 name rule1
```

```
[Sysname-app-proxy-policy-0-rule1] user-group groupa domain test
```

```
[Sysname-app-proxy-policy-0-rule1] user-group groupb domain test
```

【相关命令】

- **display app-proxy-policy**
- **user-group**（安全命令参考/AAA）



UNIS 入侵检测系统

上网行为管理命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《上网行为管理命令参考》主要介绍带宽管理、应用审计与管理相关的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项中选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下

格 式	意 义
	的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 带宽管理.....	1-1
1.1 带宽管理配置命令.....	1-1
1.1.1 action.....	1-1
1.1.2 application	1-1
1.1.3 bandwidth	1-2
1.1.4 bandwidth average enable.....	1-3
1.1.5 bandwidth { per-ip per-user }.....	1-4
1.1.6 connection-limit count	1-5
1.1.7 connection-limit rate	1-6
1.1.8 destination-address.....	1-7
1.1.9 destination-zone	1-8
1.1.10 disable.....	1-9
1.1.11 display traffic-policy statistics bandwidth	1-9
1.1.12 display traffic-policy statistics connection-limit	1-12
1.1.13 display traffic-policy statistics rule-hit.....	1-14
1.1.14 dscp.....	1-15
1.1.15 profile name.....	1-15
1.1.16 profile reference-mode	1-16
1.1.17 profile rename	1-17
1.1.18 remark dscp.....	1-18
1.1.19 reset traffic-policy statistics bandwidth	1-19
1.1.20 reset traffic-policy statistics connection-limit	1-20
1.1.21 reset traffic-policy statistics rule-hit.....	1-21
1.1.22 rule copy	1-22
1.1.23 rule move	1-22
1.1.24 rule	1-23
1.1.25 rule rename	1-24
1.1.26 service.....	1-25
1.1.27 source-address.....	1-26
1.1.28 source-zone.....	1-26
1.1.29 statistics bandwidth enable	1-27
1.1.30 statistics connection-limit enable	1-28
1.1.31 statistics rule-hit enable	1-29

1.1.32 time-range	1-29
1.1.33 traffic-policy	1-30
1.1.34 traffic-priority	1-30
1.1.35 user	1-31
1.1.36 user-group	1-32

1 带宽管理

1.1 带宽管理配置命令

1.1.1 action

action 命令用来配置带宽策略规则的动作。

undo action 命令用来恢复缺省情况。

【命令】

```
action qos profile profile-name  
undo action
```

【缺省情况】

带宽策略规则中没有配置动作，即对匹配上该规则的流量不进行带宽管理，直接允许通过。

【视图】

带宽策略规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

profile-name: 表示对匹配成功的流量进行限流，即对此流量应用带宽通道，进而对该流量进行带宽管理。*profile-name* 是带宽通道的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

如果流量成功匹配了某条带宽策略规则，则设备将会根据该带宽策略规则中指定的动作对此流量进行控制和管理，即按照引用的带宽通道对此流量进行限流。

【举例】

```
# 在带宽策略规则 rule1 中，配置动作为应用带宽通道 profile1。  
<Sysname> system-view  
[Sysname] traffic-policy  
[Sysname-traffic-policy] rule name rule1  
[Sysname-traffic-policy-rule-rule1] action qos profile profile1
```

【相关命令】

- **profile name**

1.1.2 application

application 命令用来配置作为带宽管理规则过滤条件的应用。

undo application 命令用来删除作为带宽管理规则过滤条件的应用。

【命令】

```
application { app application-name | app-group application-group-name }  
undo application { app application-name | app-group application-group-name }
```

【缺省情况】

不存在应用过滤条件。

【视图】

带宽策略规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

app *application-name*: 是应用的名称，为 1~63 个字符的字符串，不区分大小写。

app-group *application-group-name*: 是应用组的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

在一个带宽策略规则中可以同时指定多个应用作为匹配报文的参数或依据，配置本参数后，设备可以根据业务的应用类型来对流量进行带宽管理。例如，可以根据邮箱、P2P 下载、即时通讯和 Web 等应用对流经设备的流量实施带宽管理。

若指定传输层协议类型为 dccp、sctp 和 udp-lite 的自定义应用，带宽管理功能对这些自定义应用将不进行任何限制。有关自定义应用的详细介绍，请参见“安全命令参考”中的“APR”。

【举例】

在带宽策略规则 rule1 中，配置作为带宽管理规则过滤条件的应用为 P2P_General_TCP_Communications。

```
<Sysname> system-view  
[Sysname] traffic-policy  
[Sysname-traffic-policy] rule name rule1  
[Sysname-traffic-policy-rule-rule1] application app P2P_General_TCP_Communications
```

【相关命令】

- **app-group**（安全命令参考/APR）
- **nbar application**（安全命令参考/APR）
- **port-mapping**（安全命令参考/APR）

1.1.3 bandwidth

bandwidth 命令用来配置每规则的保证带宽和最大带宽。

undo bandwidth 命令用来删除每规则的保证带宽和最大带宽。

【命令】

```
bandwidth { downstream | total | upstream } { guaranteed | maximum }  
bandwidth-value
```


undo bandwidth { downstream | total | upstream } { guaranteed | maximum }

【缺省情况】

未配置每规则的保证带宽和最大带宽。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

downstream: 表示对下行流量进行控制，即对 Server 访问 Client 的流量进行控制。

total: 表示对每规则的上下行总体流量进行控制。

upstream: 表示对上行流量进行控制，即对 Client 访问 Server 的流量进行控制。

guaranteed: 表示设置保证带宽。

maximum: 表示设置最大带宽，最大带宽不小于保证带宽。

bandwidth-value: 表示带宽值，取值范围为 8~100000000，单位为 kbps。

【使用指导】

为父子规则配置带宽通道时，应遵循如下原则：

- 子规则引用的带宽通道中的每规则最大带宽不能大于父规则引用的带宽通道中的每规则最大带宽。
- 父规则引用的带宽通道中的每规则保证带宽不能小于子规则引用的带宽通道中的每规则保证带宽之和。
- 子规则与父规则不能引用同一个带宽通道。

接口期望带宽的缺省值较小时，在流量较大的情况下，很容易出现丢包现象，这时可以将此接口的期望带宽值调大。比如 Tunnel 口的默认带宽是 64kbps，流量比较大的情况下，易出现丢包现象，这时可将 Tunnel 接口的期望带宽值调大。

【举例】

创建带宽通道 profile1。

```
<Sysname> system-view
```

```
[Sysname] traffic-policy
```

```
[Sysname-traffic-policy] profile name profile1
```

配置每规则的上行流量的最大带宽为 10000kbps、下行流量的最大带宽为 10000kbps、上行流量的保证带宽为 5000kbps、下行流量的保证带宽为 5000kbps。

```
[Sysname-traffic-policy-profile-profile1] bandwidth upstream maximum 10000
```

```
[Sysname-traffic-policy-profile-profile1] bandwidth downstream maximum 10000
```

```
[Sysname-traffic-policy-profile-profile1] bandwidth upstream guaranteed 5000
```

```
[Sysname-traffic-policy-profile-profile1] bandwidth downstream guaranteed 5000
```

1.1.4 bandwidth average enable

bandwidth average enable 命令用来开启最大带宽动态均分功能。

undo bandwidth average enable 命令用来关闭最大带宽动态均分功能。

【命令】

```
bandwidth average enable
undo bandwidth average enable
```

【缺省情况】

最大带宽动态均分功能处于关闭状态。

【视图】

带宽通道视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启此功能后，设备会基于每规则的最大带宽和在线的 IP 数量，动态的为每一个 IP 均分最大带宽，充分利用闲置的带宽资源。

只有配置了每规则的最大带宽后，才能开启此功能。

【举例】

```
# 创建带宽通道 profile1。
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
# 配置在带宽通道 profile1 中开启最大带宽动态均分功能。
[Sysname-traffic-policy-profile-profile1] bandwidth total maximum 10000
[Sysname-traffic-policy-profile-profile1] bandwidth average enable
```

【相关命令】

- **bandwidth { downstream | total | upstream } maximum**

1.1.5 bandwidth { per-ip | per-user }

bandwidth { per-ip | per-user } 命令用来配置每 IP 或每用户的最大带宽。

undo bandwidth { per-ip | per-user } 命令用来删除指定的最大带宽。

【命令】

```
bandwidth { downstream | total | upstream } { guaranteed | maximum } { per-ip | per-user } bandwidth-value
undo bandwidth { downstream | total | upstream } { guaranteed | maximum } { per-ip | per-user }
```

【缺省情况】

未配置每 IP 或每用户的保证带宽和最大带宽。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

downstream: 表示对下行流量进行控制，即对 Server 访问 Client 的流量进行控制。

total: 表示对总体流量进行控制，不区分上下行流量。

upstream: 表示对上行流量进行控制，即对 Client 访问 Server 的流量进行控制。

guaranteed: 表示设置保证带宽。

maximum: 表示设置最大带宽。

per-ip: 指定每 IP 的最大带宽。

per-user: 指定每用户的最大带宽。

bandwidth-value: 表示带宽值，取值范围为 8~100000000，单位为 kbps。

【使用指导】

此命令可以用来对带宽通道中的每 IP 或每用户进行最大带宽限制，实现更加精细化的带宽管理。

配置的每 IP 或每用户的最大带宽不能大于带宽通道整体的最大带宽。

配置每 IP 或每用户的最大带宽或保证带宽时，需要注意的是：

- 配置的每 IP 或每用户的最大带宽不能大于带宽通道整体的最大带宽。
- 配置的每 IP 或每用户的保证带宽不能大于带宽通道整体的保证带宽。
- 配置的每 IP 或每用户的保证带宽不能大于配置的每 IP 或每用户的最大带宽。

【举例】

创建带宽通道 profile1。

```
<Sysname> system-view
```

```
[Sysname] traffic-policy
```

```
[Sysname-traffic-policy] profile name profile1
```

配置每个 IP 的上行/下行最大流量带宽。

```
[Sysname-traffic-policy-profile-profile1] bandwidth upstream maximum per-ip 10000
```

```
[Sysname-traffic-policy-profile-profile1] bandwidth downstream maximum per-ip 10000
```

1.1.6 connection-limit count

connection-limit count 命令用来配置最大连接数。

undo connection-limit count 命令用来删除指定的最大连接数。

【命令】

connection-limit count { per-rule | per-ip | per-user } connection-number

undo connection-limit count { per-rule | per-ip | per-user }

【缺省情况】

未配置最大连接数。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

per-rule connection-number: 指定带宽策略规则的最大连接数。

per-ip: 指定每 IP 的最大连接数。

per-user: 指定每用户的最大连接数。

connection-number: 表示最大连接数，取值范围为 1~12000000。

【使用指导】

带宽通道中即可以配置整体的最大连接数限制，也可以配置基于每 IP 或每用户的最大连接数限制。

每 IP 或每用户的最大连接数不能大于带宽通道整体的最大连接数。

在同一个带宽通道视图下对于 **per-ip** 和 **per-user** 不可以同时存在，但是 **per-rule** 可以与 **per-ip** 或 **per-user** 同时存在。

【举例】

创建带宽通道 profile1。

```
<Sysname> system-view
```

```
[Sysname] traffic-policy
```

```
[Sysname-traffic-policy] profile name profile1
```

配置带宽策略规则的最大连接数为 1000。

```
[Sysname-traffic-policy-profile-profile1] connection-limit count per-rule 1000
```

配置每 IP 的最大连接数为 500。

```
[Sysname-traffic-policy-profile-profile1] connection-limit count per-ip 500
```

1.1.7 connection-limit rate

connection-limit rate 命令用来配置最大新建连接速率。

undo connection-limit rate 命令用来删除指定的最大新建连接速率。

【命令】

connection-limit rate { per-rule | per-ip | per-user } connection-rate

undo connection-limit rate { per-rule | per-ip | per-user }

【缺省情况】

未配置最大新建连接速率限制。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

per-rule connection-rate: 指定带宽策略规则的最大新建连接速率。

per-ip: 指定每 IP 的最大新建连接速率。

per-user: 指定每用户的最大新建连接速率。

connection-rate: 表示最大新建连接速率，取值范围为 1~12000000，单位为每秒连接数。

【使用指导】

带宽通道中即可以配置整体的最大新建连接速率，也可以配置基于每 IP 或每用户的最大新建连接速率。

每 IP 或每用户的最大新建连接速率不能大于带宽通道整体的最大新建连接速率。

在同一个带宽通道视图下对于 **per-ip** 和 **per-user** 不可以同时存在，但是 **per-rule** 可以与 **per-ip** 或 **per-user** 同时存在。

【举例】

```
# 创建带宽通道 profile1。
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
# 配置带宽策略规则的最大新建连接速率为 1000。
[Sysname-traffic-policy-profile-profile1] connection-limit rate per-rule 1000
# 配置每用户的最大新建连接速率为 500。
[Sysname-traffic-policy-profile-profile1] connection-limit rate per-user 500
```

1.1.8 destination-address

destination-address 命令用来配置作为带宽管理规则过滤条件的目的 IP 地址。

undo destination-address 命令用来删除作为带宽管理规则过滤条件的目的 IP 地址。

【命令】

destination-address address-set object-group-name

undo destination-address address-set object-group-name

【缺省情况】

不存在目的 IP 地址过滤条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-group-name: IPv4/IPv6 地址对象组的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

可以引用多个 IPv4 或 IPv6 地址对象组中指定的 IP 地址或网段来作为匹配报文目的 IP 地址的参数或依据。

在进行配置回滚前，请检查带宽策略规则引用的地址对象组的配置。若与回滚配置中的地址对象组名称相同但类型不同，将导致该配置回滚失败。

【举例】

在带宽策略规则 rule1 中，配置作为带宽管理规则过滤条件的目的 IP 地址为 IPv4 地址对象组 obgroup2 中指定的 IP 地址。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] destination-address address-set obgroup2
```

【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.9 destination-zone

destination-zone 命令用来配置作为带宽管理规则过滤条件的目的安全域。

undo destination-zone 命令用来删除作为带宽管理规则过滤条件的目的安全域。

【命令】

```
destination-zone destination-zone-name
undo destination-zone destination-zone-name
```

【缺省情况】

不存在目的安全域过滤条件。

【视图】

带宽策略规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

destination-zone-name：表示安全域的名称，为 1~31 个字符的字符串，不区分大小写。

【举例】

在带宽策略规则 rule1 中，配置作为带宽管理规则过滤条件的目的安全域为 zone2。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] destination-zone zone2
```

【相关命令】

- **security-zone name**（安全命令参考/安全域）

1.1.10 disable

disable 命令用来关闭带宽策略规则。

undo disable 命令用来恢复缺省情况。

【命令】

disable
undo disable

【缺省情况】

带宽策略规则处于开启状态。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

如果在某些组网环境中某条带宽策略规则暂时不会被用到，则可以使用此命令来关闭此条带宽策略规则。关闭带宽策略规则后，此规则不参与对流量的匹配，但依然可以对其进行复制、重命名和移动。

【举例】

```
# 关闭带宽策略规则 rule1。  
<Sysname> system-view  
[Sysname] traffic-policy  
[Sysname-traffic-policy] rule name rule1  
[Sysname-traffic-policy-rule-rule1] disable
```

1.1.11 display traffic-policy statistics bandwidth

display traffic-policy statistics bandwidth 命令用来显示带宽管理的流量统计信息。

【命令】

```
display traffic-policy statistics bandwidth { downstream | total | upstream }  
{ per-ip { ipv4 [ ipv4-address ] | ipv6 [ ipv6-address ] } rule rule-name |  
per-rule [ name rule-name ] | per-user [ user user-name ] rule rule-name }  
[ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin

context-operator

【参数】

downstream: 显示对下行流量的统计信息。

total: 显示对上行和下行流量之和的统计信息。

upstream: 显示对上行流量的统计信息。

per-ip: 以 IP 地址为单元显示匹配指定带宽策略规则的流量统计信息。

ipv4: 以 IPv4 类型的地址为单元显示匹配指定带宽策略规则的流量统计信息。

ipv4-address: 显示指定 IPv4 地址流量的统计信息，若不指定本参数，则以 IPv4 类型的地址为单元显示匹配指定带宽策略规则的所有流量统计信息。

ipv6: 以 IPv6 类型的地址为单元显示匹配指定带宽策略规则的流量统计信息。

ipv6-address: 显示指定 IPv6 地址流量的统计信息，若不指定本参数，则以 IPv6 类型的地址为单元显示匹配指定带宽策略规则的所有流量统计信息。

rule rule-name: 显示指定带宽策略规则中 IP 地址流量的统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1~63 个字符的字符串，不区分大小写。

per-rule: 以带宽策略规则为单元显示带宽管理的流量统计信息。

name rule-name: 显示指定带宽策略规则流量的统计信息，带宽策略规则的名称为 1~63 个字符的字符串，不区分大小写。若不指定本参数，则以带宽策略规则为单元显示带宽管理的所有流量统计信息。

per-user: 以用户为单元显示匹配指定带宽策略规则的流量统计信息。

user user-name: 显示指定用户流量的统计信息。*user-name* 为用户的名称，取值范围为 1~55 个字符的字符串，不区分大小写。若不指定本参数，则以用户为单元显示匹配指定带宽策略规则的所有流量统计信息。

rule rule-name: 显示指定带宽策略规则中用户流量的统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1~63 个字符的字符串，不区分大小写。

slot slot-number: 显示指定成员设备上带宽管理的流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上带宽管理的流量统计信息。

【使用指导】

通过查看带宽策略规则流量的统计信息，可判断带宽策略功能是否有效。

【举例】

以带宽策略规则为单元显示带宽策略规则 **traffic-rule** 上行流量的统计信息。

```
<Sysname> display traffic-policy statistics bandwidth upstream per-rule name traffic-rule
Slot 1:
```

Codes: PP(Passed Packets), PB(Passed Bytes), DP(Dropped Packets), DB(Dropped Bytes),
PR(Passed Rate:kbps), DR(Drop Rate:kbps), FPP(Final Passed Packets), FPB(Final Passed Bytes),
FPR(Final Passed Rate:kbps)

Rule name	State	Profile name	PP	PB	DP	DB	PR	DR	FPP	FPB	FPR
traffic-rule	Enabled	profile1	726	7550	4	2961	703	497	595	6632	664.1


```
# 以 IPv4 类型的地址为单元显示匹配带宽策略规则 traffic-rule 的所有上行流量的统计信息。
<Sysname> display traffic-policy statistics bandwidth upstream per-ip ipv4 rule traffic-rule
Slot 1:
Codes: PP(Passed Packets), PB(Passed Bytes), DP(Dropped Packets), DB(Dropped Bytes),
PR(Passed Rate:kbps), DR(Drop Rate:kbps), FPP(Final Passed Packets), FPB(Final Passed Bytes),
FPR(Final Passed Rate:kbps)
-----
Rule name      State   IP      PP    PB      DP    DB    PR      DR    FPP      FPB      FPR
-----
traffic-rule   Enabled 1.1.1.1 726   75502   4     2961  703.3  497   595      6632   664.1
-----
traffic-rule2  Enabled 1.1.1.5 756   74502   4     2901  712    488   595      6632   664.1
-----
traffic-rule3  Enabled 1.1.1.8 756   74502   4     2951  712    488   595      6632   664.1
-----
```

表1-1 display traffic-policy statistics bandwidth 命令显示信息描述表

字段	描述
Codes	标识符缩写，取值包括： - PP(Passed Packets)：带宽策略放行报文的包数 - PB(Passed Bytes)：带宽策略放行报文的字节数 - DP(Dropped Packets)：丢弃报文的包数 - DB(Dropped Bytes)：丢弃报文的字节数 - PR(Passed Rate:kbps)：带宽策略放行报文的速率，单位为 kbps - DR(Drop Rate:kbps)：丢弃报文的速率，单位为 kbps - FPP(Final Passed Packets)：带宽策略和接口带宽共同实际放行的包数 - FPB(Final Passed Bytes)：带宽策略和接口带宽共同实际放行的字节数 - FPR(Final Passed Rate:kbps)：带宽策略和接口带宽共同实际放行的速率，单位为 kbps 说明：只有指定最小一级带宽策略规则，才能显示FPP、FPB和FPR三项参数的数值，否则此三项参数显示的数值为零。
Rule name	带宽策略规则的名称
State	带宽策略规则的状态，取值包括： - Enabled：表示此规则已启用 - Disabled：表示此规则已禁用
Profile name	带宽通道的名称
User ID	用户的ID号
User name	用户的名称
IP	IP地址

1.1.12 display traffic-policy statistics connection-limit

display traffic-policy statistics connection-limit 命令用来显示带宽管理的连接数限制统计信息。

【命令】

```
display traffic-policy statistics connection-limit { per-ip { ipv4 [ ipv4-address ] | ipv6 [ ipv6-address ] } rule rule-name | per-rule [ name rule-name ] | per-user [ user user-name ] rule rule-name } } [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

per-ip: 以 IP 地址为单元显示匹配指定带宽策略规则的连接数限制统计信息。

ipv4: 以 IPv4 类型的地址为单元显示匹配指定带宽策略规则的连接数限制统计信息。

ipv4-address: 显示指定 IPv4 地址的连接数限制统计信息，若不指定本参数，则以 IPv4 类型的地址为单元显示匹配指定带宽策略规则的所有连接数限制统计信息。

ipv6: 以 IPv6 类型的地址为单元显示匹配指定带宽策略规则的连接数限制统计信息。

ipv6-address: 显示指定 IPv6 地址的连接数限制统计信息，若不指定本参数，则以 IPv6 类型的地址为单元显示匹配指定带宽策略规则的所有连接数限制统计信息。

rule rule-name: 显示指定带宽策略规则中 IP 地址的连接数限制统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1~63 个字符的字符串，不区分大小写。

per-rule: 以带宽策略规则为单元显示带宽管理的连接数限制统计信息。

name rule-name: 显示指定带宽策略规则的连接数限制统计信息，带宽策略规则的名称为 1~63 个字符的字符串，不区分大小写。若不指定本参数，则以带宽策略规则为单元显示带宽管理的所有连接数限制统计信息。

per-user: 以用户为单元显示匹配指定带宽策略规则的连接数限制统计信息。

user user-name: 显示指定用户的连接数限制统计信息。*user-name* 为用户的名称，取值范围为 1~55 个字符的字符串，不区分大小写。若不指定本参数，则以用户为单元显示匹配指定带宽策略规则的所有连接数限制统计信息。

rule rule-name: 显示指定带宽策略规则中用户的连接数限制统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1~63 个字符的字符串，不区分大小写。

slot slot-number: 显示指定成员设备上带宽管理的连接数限制统计信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上带宽管理的连接数限制统计信息。

【使用指导】

通过查看带宽管理的连接数限制统计信息，可判断带宽策略功能是否有效。

【举例】

以带宽策略规则为单元显示带宽策略规则 traffic-rule 的连接数限制统计信息。

```
<Sysname> display traffic-policy statistics connection-limit per-rule name traffic-rule
Slot 1:
Codes: CC(Current Connection), RC(Rejective Connection), CL(Current Limit), RRC(Rate
Rejective Connection), RR(Rejective Rate), PR(Pass Rate)
-----
Rule name      State      Profile name  CC        RC        CL        RRC        RR        PR
-----
traffic-rule   Enabled   profile1     200       300       200       200       300       200
-----
```

以用户为单元显示匹配带宽策略规则 traffic-rule 的所有连接数限制统计信息。

```
<Sysname> display traffic-policy statistics connection-limit per-user rule traffic-rule
Slot 1:
Codes: CC(Current Connection), RC(Rejective Connection), CL(Current Limit), RRC(Rate
Rejective Connection), RR(Rejective Rate), PR(Pass Rate)
-----
Rule name      State      Profile name  User ID   User name  CC   RC   CL   RRC   RR   PR
-----
traffic-rule   Enabled   profile1     0x3d     user1     200  300  200  200  300  200
-----
```

表1-2 display traffic-policy statistics connection-limit 命令显示信息描述表

字段	描述
Codes	标识符缩写，取值包括： - CC (current connections)：当前连接数 - RC (rejected connections)：达到最大连接数后，拒绝的连接数 - CL (connection limit)：配置的连接数限制 - RRC(Rate Rejective Connection)：达到最大新建连接速率后，拒绝的连接数 - RR(Rejective Rate)：拒绝新建连接的速率，单位为每秒连接数 - PR(Pass Rate)：放行新建连接的速率，单位为每秒连接数
Rule name	带宽策略规则的名称
State	带宽策略规则的状态，取值包括： - Enabled：表示此规则已启用 - Disabled：表示此规则已禁用
Profile name	带宽通道的名称
User ID	用户的ID号
User name	用户的名称

IP	IP地址

1.1.13 display traffic-policy statistics rule-hit

display traffic-policy statistics rule-hit 命令用来显示带宽策略规则的命中统计信息。

【命令】

display traffic-policy statistics rule-hit [**rule** *rule-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

rule *rule-name*: 显示指定带宽策略规则的命中统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1~63 个字符的字符串，不区分大小写。若不指定本参数，则显示带宽策略中所有规则的命中统计信息。

slot *slot-number*: 显示指定成员设备上带宽策略规则的命中统计信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则显示所有成员设备上带宽策略规则的命中统计信息。

【举例】

显示带宽策略中所有规则的命中统计信息。

```
<Sysname> display traffic-policy statistics rule-hit
Slot 1:
```

Rule ID	Rule name	State	Profile ID	Profile name	Hit
201	traffic-rule	Enabled	21	profile1	11111
202	traffic-rule1	Enabled	22	profile2	11112
203	traffic-rule2	Enabled	23	profile1	11565

表1-3 display traffic-policy statistics rule-hit 命令显示信息描述表

字段	描述
Rule ID	带宽策略规则的ID号

Rule name	带宽策略规则的名称
State	带宽策略规则的状态，取值包括： • Enabled: 表示此规则已启用 • Disabled: 表示此规则已禁用
Profile ID	带宽通道的ID号
Profile name	带宽通道的名称
Hit	带宽策略规则被匹配的次数

1.1.14 dscp

dscp 命令用来配置作为带宽管理规则过滤条件的 DSCP 优先级。

undo dscp 命令用来删除作为带宽管理规则过滤条件的 DSCP 优先级。

【命令】

dscp *dscp-value*

undo dscp *dscp-value*

【缺省情况】

不存在 DSCP 优先级过滤条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value: 表示报文DSCP优先级，取值仅可以是关键字，关键字如 [表 1-4](#) 所示。

【举例】

在带宽策略规则 **rule1** 中，配置作为带宽管理规则过滤条件的 DSCP 优先级为 **af11**。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] dscp af11
```

1.1.15 profile name

profile name 命令用来创建带宽通道，并进入带宽通道视图。如果指定的带宽通道已经存在，则直接进入带宽通道视图。

undo profile name 命令用来删除指定的带宽通道。

【命令】

```
profile name profile-name  
undo profile name profile-name
```

【缺省情况】

不存在带宽通道。

【视图】

带宽策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

profile-name: 带宽通道的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

带宽通道定义了实施带宽管理的对象所能够使用的带宽资源，带宽通道将被带宽策略规则引用。

【举例】

```
# 创建一个名为 profile1 的带宽通道，并进入该带宽通道视图。  
<Sysname> system-view  
[Sysname] traffic-policy  
[Sysname-traffic-policy] profile name profile1  
[Sysname-traffic-policy-profile-profile1]
```

【相关命令】

- **action**

1.1.16 profile reference-mode

profile reference-mode 命令用来配置带宽通道的引用方式。

undo profile reference-mode 命令用来恢复缺省情况。

【命令】

```
profile reference-mode { per-rule | rule-shared }  
undo profile reference-mode
```

【缺省情况】

带宽通道的引用方式为策略独占。

【视图】

带宽通道视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

per-rule: 表示策略独占，每一个引用带宽通道的带宽策略规则均单独受到该带宽通道的约束，即与该带宽策略规则匹配成功的流量，独享带宽通道中的带宽限制和连接数限制。

rule-shared: 表示策略共享，所有引用某带宽通道的带宽策略规则均共同受到该带宽通道的约束，即与多条带宽策略规则匹配成功的多条流量，共享带宽通道中的带宽限制和连接数限制。

【使用指导】

带宽通道被带宽策略规则引用后，此带宽通道中的带宽限制和连接数限制就会在带宽策略中生效，其限制方式包括策略独占和策略共享两种。

【举例】

```
# 创建带宽通道 profile1。
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
# 配置带宽通道 profile1 被带宽策略规则引用的方式为策略共享。
[Sysname-traffic-policy-profile-profile1] profile reference-mode rule-shared
```

1.1.17 profile rename

profile rename 命令用来重命名带宽通道

【命令】

profile rename *old-name new-name*

【视图】

带宽策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

old-name: 表示带宽通道原来的名称，为 1~63 个字符的字符串，不区分大小写。

new-name: 表示带宽通道新的名称，为 1~63 个字符的字符串，不区分大小写。新的名称不能为设备中已存在的带宽通道名称。

【举例】

```
# 创建带宽通道 profile1。
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
[Sysname-traffic-policy-profile-profile1] quit
# 把带宽通道 profile1 重命名为 profile2。
[Sysname-traffic-policy] profile rename profile1 profile2
```

1.1.18 remark dscp

remark dscp 命令用来重标记报文的 DSCP 优先级。

undo remark dscp 命令用来恢复缺省情况。

【命令】

remark dscp *dscp-value*

undo remark dscp

【缺省情况】

不修改报文的 DSCP 优先级。

【视图】

带宽通道视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value: 表示报文DSCP优先级，取值仅可以是关键字，关键字如 [表 1-4](#) 所示。

表1-4 DSCP 关键字与值的对应表

关键字	DSCP 值（二进制）	DSCP 值（十进制）
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40

关键字	DSCP 值（二进制）	DSCP 值（十进制）
cs6	110000	48
cs7	111000	56
ef	101110	46

【使用指导】

优先级重标记是指修改报文中 DSCP（Differentiated Services Code Point）字段的值。DSCP 字段也称为 DSCP 优先级，是网络设备进行流量分类的依据。位于报文传输路径上的各个网络设备，可以通过 DSCP 优先级来区分流量，进而对不同 DSCP 优先级的流量采取差异化的处理。

【举例】

```
# 创建带宽通道 profile1。
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] profile name profile1
# 重标记报文的 DSCP 优先级为 af22
[Sysname-traffic-policy-profile-profile1] remark dscp af22
```

1.1.19 reset traffic-policy statistics bandwidth

reset traffic-policy statistics bandwidth 命令用来清除带宽管理的流量统计信息。

【命令】

```
reset traffic-policy statistics bandwidth { downstream | total | upstream }
{ per-ip { ipv4 [ ipv4-address ] | ipv6 [ ipv6-address ] } rule rule-name |
```

per-rule [*name rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* }

```
[ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

downstream: 清除对下行流量的统计信息。

upstream: 清除对上行流量的统计信息。

total: 清除对上行和下行流量之和的统计信息。

per-ip: 以 IP 地址为单元清除匹配指定带宽策略规则的流量统计信息。

ipv4: 以 IPv4 类型的地址为单元清除匹配指定带宽策略规则的流量统计信息。

ipv4-address: 清除指定 IPv4 地址流量的统计信息，若不指定本参数，则以 IPv4 类型的地址为单元清除匹配指定带宽策略规则的所有流量统计信息。

ipv6: 以 IPv6 类型的地址为单元清除匹配指定带宽策略规则的流量统计信息。

ipv6-address: 清除指定 IPv6 地址流量的统计信息，若不指定本参数，则以 IPv6 类型的地址为单元清除匹配指定带宽策略规则的所有流量统计信息。

rule rule-name: 清除指定带宽策略规则中 IP 地址流量的统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1~63 个字符的字符串，不区分大小写。

per-rule: 以带宽策略规则为单元清除带宽管理的流量统计信息。

name rule-name: 清除指定带宽策略规则流量的统计信息，带宽策略规则的名称为 1~63 个字符的字符串，不区分大小写。若不指定本参数，则清除带宽管理的所有流量统计信息。

per-user: 以用户为单元清除匹配指定带宽策略规则的流量统计信息。

user user-name: 清除指定用户流量的统计信息。*user-name* 为用户的名称，取值范围为 1~55 个字符的字符串，不区分大小写。若不指定本参数，则以用户为单元清除匹配指定带宽策略规则的所有流量统计信息。

rule rule-name: 清除指定带宽策略规则中用户流量的统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1~63 个字符的字符串，不区分大小写。

slot slot-number: 清除指定成员设备上带宽管理的流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则清除所有成员设备上带宽管理的流量统计信息。

【举例】

以带宽策略规则为单元清除指定 slot 上匹配带宽策略规则 traffic-rule 的流量统计信息。

```
<Sysname> reset traffic-policy statistics bandwidth upstream per-rule name traffic-rule slot 1
```

1.1.20 reset traffic-policy statistics connection-limit

reset traffic-policy statistics connection-limit 命令用来清除带宽管理的连接数限制统计信息。

【命令】

```
reset traffic-policy statistics connection-limit { per-ip { ipv4  
[ ipv4-address ] | ipv6 [ ipv6-address ] } rule rule-name | per-rule [ name  
rule-name ] | per-user [ user user-name ] rule rule-name } } [ slot  
slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

per-ip: 以 IP 地址为单元清除匹配指定带宽策略规则的连接数限制统计信息。

ipv4: 以 IPv4 类型的地址为单元清除匹配指定带宽策略规则的连接数限制统计信息。

ipv4-address: 清除指定 IPv4 地址的连接数限制统计信息，若不指定本参数，则以 IPv4 类型的地址为单元清除匹配指定带宽策略规则的所有连接数限制统计信息。

ipv6: 以 IPv6 类型的地址为单元清除匹配指定带宽策略规则的连接数限制统计信息。

ipv6-address: 清除指定 IPv6 地址的连接数限制统计信息，若不指定本参数，则以 IPv6 类型的地址为单元清除匹配指定带宽策略规则的所有连接数限制统计信息。

rule rule-name: 清除指定带宽策略规则中 IP 地址的连接数限制统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1~63 个字符的字符串，不区分大小写。

per-rule: 以带宽策略规则为单元清除带宽管理的连接数限制统计信息。

name rule-name: 清除指定带宽策略规则的连接数限制统计信息，带宽策略规则的名称为 1~63 个字符的字符串，不区分大小写。若不指定本参数，则以带宽策略规则为单元清除带宽管理的所有连接数限制统计信息。

per-user: 以用户为单元清除匹配指定带宽策略规则的连接数限制统计信息。

user user-name: 清除指定用户的连接数限制统计信息。*user-name* 为用户的名称，取值范围为 1~55 个字符的字符串，不区分大小写。若不指定本参数，则以用户为单元清除匹配指定带宽策略规则的所有连接数限制统计信息。

rule rule-name: 清除指定带宽策略规则中用户的连接数限制统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1~63 个字符的字符串，不区分大小写。

slot slot-number: 清除指定成员设备上带宽管理的连接数限制统计信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则清除所有成员设备上带宽管理的连接数限制统计信息。

【举例】

以带宽策略规则为单元清除指定 slot 上匹配带宽策略规则 traffic-rule 的连接数限制统计信息。

```
<Sysname> reset traffic-policy statistics connection-limit per-rule name traffic-rule slot 1
```

1.1.21 reset traffic-policy statistics rule-hit

reset traffic-policy statistics rule-hit 命令用来清除带宽策略规则被命中次数的统计信息。

【命令】

```
reset traffic-policy statistics rule-hit [ rule rule-name ] [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule rule-name: 清除指定带宽策略规则被命中次数的统计信息。*rule-name* 为带宽策略规则的名称，取值范围为 1~63 个字符的字符串，不区分大小写。若不指定本参数，则清除带宽策略中所有规则被命中次数的统计信息。

slot slot-number: 清除指定成员设备上带宽策略规则的命中统计信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则清除所有成员设备上带宽策略规则的命中统计信息。

【举例】

清除指定 slot 上带宽策略规则 **traffic-rule** 的命中统计信息。

```
<Sysname> reset traffic-policy statistics rule-hit rule traffic-rule slot 1
```

1.1.22 rule copy

rule copy 命令用来复制带宽策略规则。

【命令】

```
rule copy rule-name new-rule-name
```

【视图】

带宽策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

rule-name: 表示被复制带宽策略规则的名称，为 1~63 个字符的字符串，不区分大小写。

new-rule-name: 表示新建带宽策略规则的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

当新建的带宽策略规则和已存在的带宽策略规则比较相似时，可通过复制已经存在的带宽策略规则来创建新的带宽策略规则。

复制带宽策略规则时，需要注意的是：

- 如果被复制的带宽策略规则中含有子带宽策略规则，则只会复制父带宽策略规则的内容。
- 通过复制创建的新策略规则紧跟在被复制的带宽策略规则之后。

【举例】

通过复制带宽策略规则 **rule1**，创建一个新的带宽策略规则 **rule2**。

```
<Sysname> system-view  
[Sysname] traffic-policy  
[Sysname-traffic-policy] rule copy rule1 rule2
```

1.1.23 rule move

rule move 命令用来移动带宽策略规则的排列顺序。

【命令】

```
rule move rule-name1 { after | before } rule-name2
```

【视图】

带宽策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

rule-name1: 表示需要被移动的带宽策略规则的名称, 为 1~63 个字符的字符串, 不区分大小写。
after: 表示把带宽策略规则 **rule-name1** 移动到带宽策略规则 **rule-name2** 的后面。
before: 表示把带宽策略规则 **rule-name1** 移动到带宽策略规则 **rule-name2** 的前面。
rule-name2: 表示移动目标的带宽策略规则的名称, 为 1~63 个字符的字符串, 不区分大小写。

【使用指导】

设备根据带宽策略规则在设备上显示的顺序从上到下对流量进行匹配, 一旦匹配上某个带宽策略规则便结束此匹配过程, 并根据该规则中指定的动作对此流量进行处理; 如果流量没有匹配上任何规则, 则允许该流量通过。为了使设备上部署的带宽管理功能达到更好、更严谨的效果, 因此配置带宽策略规则时要遵循“先精细后宽泛”的原则。如果发现设备中已配置的带宽策略规则之间的顺序不符合这个原则, 则可以使用 **rule move** 命令来调整带宽策略规则之间的顺序。

只有不同父带宽策略规则之间和相同父带宽策略规则下的子带宽策略规则之间才可以相互调整顺序。

【举例】

```
# 创建带宽策略规则 rule1。
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] quit
# 创建带宽策略规则 rule2。
[Sysname-traffic-policy] rule name rule2
[Sysname-traffic-policy-rule-rule2] quit
# 将带宽策略规则 rule1 的配置顺序移动到带宽策略规则 rule2 之后。
[Sysname-traffic-policy] rule move rule1 after rule2
```

1.1.24 rule

rule 命令用来创建或进入带宽策略规则视图。如果指定的带宽策略规则已经存在, 则直接进入带宽策略规则视图。

undo rule 命令用来删除指定的带宽策略规则。

【命令】

```
rule rule-id
rule [ rule-id ] name rule-name [ parent parent-rule-name ]
undo rule { rule-id | name rule-name }
```

【缺省情况】

不存在带宽策略规则。

【视图】

带宽策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-id: 表示带宽策略规则的编号，取值范围为 1~65534。若未指定本参数，系统将从上一次分配的编号开始，以步长为 1，自动分配一个未使用过的新编号。若新编号超出了编号上限(65534)，则选择当前未使用的最小编号作为新的编号。

rule-name: 表示带宽策略规则的名称，为 1~63 个字符的字符串，不区分大小写，且全局唯一。创建规则时必须配置规则名称。

parent parent-rule-name: 指定带宽策略规则的父规则。**parent-rule-name** 表示父规则的名称，为 1~63 个字符的字符串，不区分大小写。指定的父规则必须已经存在，否则创建该带宽策略规则时失败。

【使用指导】

带宽策略中可以配置多个带宽策略规则，这些规则用于定义匹配流量的匹配项以及流量控制的动作。设备根据这些规则在设备上显示的顺序从上到下对流量进行匹配，一旦流量匹配上某条规则便结束此匹配过程，并根据该规则中指定的动作对此流量进行处理；如果流量没有匹配上任何规则，则允许该流量通过。

当创建带宽策略规则时，如果需要继承其他带宽策略规则中的匹配项属性，则可以在创建带宽策略规则时为其指定父带宽策略规则。

创建带宽策略规则时，需要注意的是：

- 第四级带宽策略规则不能再作为父带宽策略规则。
- 只能在创建带宽策略规则时指定带宽策略规则的父带宽策略规则，不能为已存在的带宽策略规则添加或修改父带宽策略规则。

【举例】

创建一个名称为 rule1，规则 ID 为 111 的带宽策略规则，并进入该带宽策略规则视图。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule 111 name rule1
[Sysname-traffic-policy-rule-111-rule1]
```

1.1.25 rule rename

rule rename 命令用来重命名带宽策略规则。

【命令】

rule rename *old-rule-name* *new-rule-name*

【视图】

带宽策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

old-rule-name: 表示带宽策略规则的原有名称，为 1~63 个字符的字符串，不区分大小写。

new-rule-name: 表示带宽策略规则的新名称，为 1~63 个字符的字符串，不区分大小写。

【举例】

```
# 创建带宽策略规则 rule1。
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] quit
# 把带宽策略规则 rule1 重命名为 rule2。
[Sysname-traffic-policy] rule rename rule1 rule2
```

1.1.26 service

service 命令用来配置作为带宽策略规则过滤条件的服务。

undo service 命令用来删除作为带宽管理规则过滤条件的服务。

【命令】

```
service object-group-name
undo service [object-group-name ]
```

【缺省情况】

不存在服务过滤条件。

【视图】

带宽策略规则视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

object-group-name: 表示服务对象组的名称，为 1~31 个字符的字符串，不区分大小写。如果不指定该参数，则删除所有服务过滤条件。

【使用指导】

可以引用多个服务对象组作为匹配报文的参数或依据。

配置 **undo service** 命令时，如果不指定服务对象组或者指定的服务对象组是名称为 **any** 的系统默认对象组，则表示删除所有服务过滤条件。

【举例】

```
# 在带宽策略规则 rule1 中，指定匹配报文的 service 为设备上预定义的服务对象组 FTP。
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] service ftp
```


【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.27 source-address

source-address 命令用来配置作为带宽管理规则过滤条件的源 IP 地址。

undo source-address 命令用来删除作为带宽管理规则过滤条件的源 IP 地址。

【命令】

source-address address-set *object-group-name*

undo source-address address-set *object-group-name*

【缺省情况】

不存在源 IP 地址过滤条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-group-name: 表示 IPv4/IPv6 地址对象组的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

可以引用多个 IPv4 或 IPv6 地址对象组中指定的 IP 地址来作为匹配报文源 IP 地址的参数或依据。

在进行配置回滚前，请检查带宽策略规则引用的地址对象组的配置。若与回滚配置中的地址对象组名称相同但类型不同，将导致该配置回滚失败。

【举例】

在带宽策略规则 rule1 中，配置作为带宽管理规则过滤条件的源 IP 地址为 IPv4 地址对象组 obgroup1 中指定的 IP 地址。

```
<Sysname> system-view
```

```
[Sysname] traffic-policy
```

```
[Sysname-traffic-policy] rule name rule1
```

```
[Sysname-traffic-policy-rule-rule1] source-address address-set obgroup1
```

【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.28 source-zone

source-zone 命令用来配置作为带宽管理规则过滤条件的源安全域。

undo source-zone 命令用来删除作为带宽管理规则过滤条件的源安全域。

【命令】

```
source-zone source-zone-name  
undo source-zone source-zone-name
```

【缺省情况】

不存在源安全域过滤条件。

【视图】

带宽策略规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

source-zone-name: 表示安全域的名称，为 1~31 个字符的字符串，不区分大小写。

【举例】

在带宽策略规则 rule1 中，配置作为带宽管理规则过滤条件的源安全域为 zone1。

```
<Sysname> system-view  
[Sysname] traffic-policy  
[Sysname-traffic-policy] rule name rule1  
[Sysname-traffic-policy-rule-rule1] source-zone zone1
```

【相关命令】

- **security-zone name**（安全命令参考/安全域）

1.1.29 statistics bandwidth enable

statistics bandwidth enable 命令用来开启带宽管理流量统计功能。

undo statistics bandwidth enable 命令用来关闭带宽管理流量统计功能。

【命令】

```
statistics bandwidth enable  
undo statistics bandwidth enable
```

【缺省情况】

带宽管理流量统计功能处于关闭状态。

【视图】

带宽策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

开启本功能后，带宽管理业务将对匹配带宽策略规则的流量进行统计，统计信息可通过 **display traffic-policy statistics bandwidth** 命令查看。

开启本功能将对设备处理性能产生影响，请根据设备实际情况进行配置。

【举例】

开启带宽管理流量统计功能。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] statistics bandwidth enable
```

【相关命令】

- **display traffic-policy statistics bandwidth**

1.1.30 statistics connection-limit enable

statistics connection-limit enable 命令用来开启带宽管理连接数限制统计功能。

undo statistics connection-limit enable 命令用来关闭带宽管理连接数限制统计功能。

【命令】

```
statistics connection-limit enable
undo statistics connection-limit enable
```

【缺省情况】

带宽管理连接数限制统计功能处于关闭状态。

【视图】

带宽策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启本功能后，带宽管理业务将对匹配带宽策略规则的连接数限制信息进行统计，统计信息可通过 **display traffic-policy statistics connection-limit** 命令查看。

开启本功能将对设备处理性能产生影响，请根据设备实际情况进行配置。

【举例】

开启带宽管理连接数限制统计功能。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] statistics connection-limit enable
```

【相关命令】

- **display traffic-policy statistics connection-limit**

1.1.31 statistics rule-hit enable

statistics rule-hit enable 命令用来开启带宽管理规则命中统计功能。

undo statistics rule-hit enable 命令用来关闭带宽管理规则命中统计功能。

【命令】

```
statistics rule-hit enable
undo statistics rule-hit enable
```

【缺省情况】

带宽管理规则命中统计功能处于关闭状态。

【视图】

带宽策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启本功能后，带宽管理业务将对带宽策略规则的命中情况进行统计，统计信息可通过 **display traffic-policy statistics rule-hit** 命令查看。

开启本功能将对设备处理性能产生影响，请根据设备实际情况进行配置。

【举例】

```
# 开启带宽管理规则命中统计功能。
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] statistics rule-hit enable
```

【相关命令】

- **display traffic-policy statistics rule-hit**

1.1.32 time-range

time-range 命令用来指定带宽策略规则的生效时间。

undo time-range 命令用来恢复缺省情况。

【命令】

```
time-range time-range-name
undo time-range
```

【缺省情况】

带宽策略规则在任何时间下都生效。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin
context-admin

【参数】

time-range-name: 指定时间段的名称，为 1~32 个字符的字符串，不区分大小写。

【举例】

在带宽策略规则 **rule1** 中，指定带宽策略规则的生效时间为时间段 **work-time** 中配置的时间。

```
<Sysname> system-view  
[Sysname] traffic-policy  
[Sysname-traffic-policy] rule name rule1  
[Sysname-traffic-policy-rule-rule1] time-range work-time
```

【相关命令】

- **time-range** (ACL 命令参考/时间段)

1.1.33 traffic-policy

traffic-policy 命令用来进入带宽策略视图。

undo traffic-policy 命令用来删除带宽策略中的所有配置。

【命令】

```
traffic-policy  
undo traffic-policy
```

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

带宽策略视图下可以完成对带宽策略规则的创建、复制、移动和重命名等操作。

【举例】

```
# 进入带宽策略视图。  
<Sysname> system-view  
[Sysname] traffic-policy  
[Sysname-traffic-policy]
```

1.1.34 traffic-priority

traffic-priority 命令用来配置流量优先级。

undo traffic-priority 命令用来恢复缺省情况。

【命令】

```
traffic-priority priority-value  
undo traffic-priority
```

【缺省情况】

流量优先级为 1。

【视图】

带宽通道视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

priority-value: 表示流量优先级，取值范围为 1~7，数值越大优先级越高。

【使用指导】

当多个带宽通道中的流量同时从某个接口发送时，如果此接口发生阻塞，则优先级高的流量优先被发送。优先级相同的流量将会自由竞争出接口的带宽资源。

【举例】

```
# 创建带宽通道 profile1。  
<Sysname> system-view  
[Sysname] traffic-policy  
[Sysname-traffic-policy] profile name profile1  
# 配置流量优先级为 7。  
[Sysname-traffic-policy-profile-profile1] traffic-priority 7
```

1.1.35 user

user 命令用来配置作为带宽管理规则过滤条件的用户名。

undo user 命令用来删除作为带宽管理规则过滤条件的用户名。

【命令】

```
user user-name [ domain domain-name ]  
undo user user-name [ domain domain-name ]
```

【缺省情况】

不存在用户过滤条件。

【视图】

带宽策略规则视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

user-name: 指定用户的名称，为 1~55 个字符的字符串，区分大小写。不能是 a、al 和 all，且不能包含特殊字符 “\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和 “@”。

domain domain-name: 表示在指定的身份识别域中匹配此用户。**domain-name** 是身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包含特殊字符 “\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和 “@”。若不指定此参数，则表示在不属于任何身份识别域的用户中匹配此用户。有关身份识别域的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

【使用指导】

本命令可以实现基于用户的精细化带宽管理。此功能可以有效解决在移动互联网中，用户 IP 地址不断变化带来的带宽管理不方便的问题，即以不变的用户名应对变化的 IP 地址，将流量的源 IP 地址识别为用户。

【举例】

在带宽策略规则 rule1 中，配置作为带宽管理规则过滤条件的用户名为 managers。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] user managers
```

引用用户名为 user1，身份识别域为 dpi 的用户作为带宽策略规则的匹配条件。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name myrule
[Sysname-traffic-policy-rule-myrule] user user1 domain dpi
```

【相关命令】

- **local-user**（安全命令参考/AAA）
- **user-identity enable**（安全命令参考/用户身份识别与管理）
- **user-identity static-user**（安全命令参考/用户身份识别与管理）

1.1.36 user-group

user-group 命令用来配置作为带宽管理规则过滤条件的用户组。

undo user-group 命令用来删除作为带宽管理规则过滤条件的用户组。

【命令】

```
user-group user-group-name [ domain domain-name ]
undo user-group user-group-name [ domain domain-name ]
```

【缺省情况】

不存在用户组过滤条件。

【视图】

带宽策略规则视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-group-name: 指定用户组的名称，为 1~200 个字符的字符串，不区分大小写。

domain domain-name: 表示在指定的身份识别域中匹配此用户组。**domain-name** 是身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包含特殊字符 “/”、“\”、“|”、“.”、“*”、“?”、“<”、“>” 以及 “@”。若不指定此参数，则表示在不属于任何身份识别域的用户组中匹配此用户组。有关身份识别域的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

【使用指导】

本命令可以实现基于用户组的精细化带宽管理。此功能可以有效解决在移动互联网中，用户 IP 地址不断变化带来的带宽管理不方便的问题，即以不变的用户组应对变化的 IP 地址，将流量的源 IP 地址识别为用户组。

【举例】

在带宽策略规则 rule1 中，配置作为带宽管理规则过滤条件的用户组为 mak。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name rule1
[Sysname-traffic-policy-rule-rule1] user-group mak
```

引用用户组名为 usergroup1，域为 dpi 的用户组作为带宽策略规则的匹配条件。

```
<Sysname> system-view
[Sysname] traffic-policy
[Sysname-traffic-policy] rule name myrule
[Sysname-traffic-policy-rule-myrule] user-group usergroup1 domain dpi
```

【相关命令】

- **user-group**（安全命令参考/AAA）
- **user-identity enable**（安全命令参考/用户身份识别与管理）

目 录

1 应用审计与管理.....	1-1
1.1 应用审计与管理配置命令.....	1-1
1.1.1 application	1-1
1.1.2 description	1-2
1.1.3 destination-address.....	1-2
1.1.4 destination-zone	1-3
1.1.5 disable	1-4
1.1.6 keyword.....	1-5
1.1.7 keyword-group name.....	1-5
1.1.8 policy copy	1-6
1.1.9 policy default-action	1-6
1.1.10 policy move	1-7
1.1.11 policy name	1-8
1.1.12 policy rename.....	1-9
1.1.13 rule	1-9
1.1.14 rule default-action	1-11
1.1.15 rule match-method	1-12
1.1.16 service.....	1-13
1.1.17 source-address.....	1-14
1.1.18 source-zone.....	1-14
1.1.19 time-range	1-15
1.1.20 uapp-control.....	1-16
1.1.21 user	1-16
1.1.22 user-group.....	1-17

1 应用审计与管理



说明

本特性会解析出用户报文中的敏感信息和私密信息，请保证将本特性仅用于合法用途。

1.1 应用审计与管理配置命令

1.1.1 application

application 命令用来配置作为应用审计与管理策略过滤条件的应用。

undo application 命令用来删除作为应用审计与管理策略过滤条件的应用。

【命令】

```
application { app application-name | app-group application-group-name }  
undo application { app application-name | app-group application-group-name }
```

【缺省情况】

不存在应用过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

app application-name: 表示应用的名称，为 1~63 个字符的字符串，不区分大小写。

app-group application-group-name: 表示应用组的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

仅在免审计和阻断类型的策略中可配置此命令。

多次执行本命令，可配置多个应用作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理阻断策略 mypolicy2 过滤条件的应用为 app1 和 app2，应用组为 group1 和 group2。

```
<Sysname> system-view  
[Sysname] uapp-control  
[Sysname-uapp-control] policy name mypolicy2 deny  
[Sysname-uapp-control-policy-mypolicy2] application app app1
```

```
[Sysname-uapp-control-policy-mypolicy2] application app app2
[Sysname-uapp-control-policy-mypolicy2] application app-group group1
[Sysname-uapp-control-policy-mypolicy2] application app-group group2
```

【相关命令】

- **app-group**（安全命令参考/APR）
- **nbar application**（安全命令参考/APR）
- **port-mapping**（安全命令参考/APR）

1.1.2 description

description 命令用来配置关键字组的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

不存在关键字组的描述信息。

【视图】

关键字组视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

text：表示关键字组的描述信息，为 1~255 个字符的字符串，区分大小写。

【举例】

```
# 配置关键字组的描述信息为 account limit。
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] keyword-group name mykeywordgroup
[Sysname-uapp-control-keyword-group-mykeywordgroup] description account limit
```

1.1.3 destination-address

destination-address 命令用来配置作为应用审计与管理策略过滤条件的目的 IP 地址。

undo destination-address 命令用来删除作为应用审计与管理策略过滤条件的目的 IP 地址。

【命令】

```
destination-address { ipv4 | ipv6 } object-group-name
undo destination-address { ipv4 | ipv6 } object-group-name
```

【缺省情况】

不存在目的 IP 地址过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4: 表示指定 IPv4 地址对象组。

ipv6: 表示指定 IPv6 地址对象组。

object-group-name: 表示地址对象组的名称，为 1~31 个字符的字符串，不区分大小写，且必须已存在。

【使用指导】

多次执行本命令，可配置多个目的 IPv4/IPv6 地址对象组作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的目的 IPv4 地址。

```
<Sysname> system-view
```

```
[Sysname] uapp-control
```

```
[Sysname-uapp-control] policy name mypolicy1 audit
```

```
[Sysname-uapp-control-policy-mypolicy1] destination-address ipv4 obgroup3
```

```
[Sysname-uapp-control-policy-mypolicy1] destination-address ipv4 obgroup4
```

【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.4 destination-zone

destination-zone 命令用来配置作为应用审计与管理策略过滤条件的目的安全域。

undo destination-zone 命令用来删除作为应用审计与管理策略过滤条件的目的安全域。

【命令】

destination-zone *destination-zone-name*

undo destination-zone *destination-zone-name*

【缺省情况】

不存在目的安全域过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

destination-zone-name: 表示安全域的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

多次执行本命令，可配置多个目的安全域作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的目的安全域为 zone3 和 zone4。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] destination-zone zone3
[Sysname-uapp-control-policy-mypolicy1] destination-zone zone4
```

【相关命令】

- **security-zone name**（安全命令参考/安全域）

1.1.5 disable

disable 命令用来关闭应用审计与管理策略。

undo disable 命令用来开启应用审计与管理策略。

【命令】

```
disable
undo disable
```

【缺省情况】

应用审计与管理策略处于开启状态。

【视图】

应用审计与管理策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

如果在某些组网环境中某条应用审计与管理策略暂时不会被用到，则可以使用此命令来关闭此条应用审计与管理策略。关闭应用审计与管理策略后，此策略将不能对流量进行匹配，但依然可以对其进行复制、重命名和移动的操作。

【举例】

```
# 关闭应用审计与管理策略 mypolicy1。
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1
[Sysname-uapp-control-policy-mypolicy1] disable
```

1.1.6 keyword

keyword 命令用来配置关键字。

undo keyword 命令用来删除指定的关键字。

【命令】

keyword *keyword-value*

undo keyword *keyword-value*

【缺省情况】

不存在关键字。

【视图】

关键字组视图

【缺省用户角色】

network-admin

context-admin

【参数】

keyword-value: 表示关键字，为 1~63 个字符的字符串，区分大小写。

【举例】

配置应用审计与管理的关键字为 keywordname。

```
<Sysname> system-view
```

```
[Sysname] uapp-control
```

```
[Sysname-uapp-control] keyword-group name mykeywordgroup
```

```
[Sysname-uapp-control-keyword-group-mykeywordgroup] keyword keywordname
```

1.1.7 keyword-group name

keyword-group name 命令用来创建关键字组，并进入关键字组视图。如果指定的关键字组已经存在，则直接进入关键字组视图。

undo keyword-group name 命令用来删除指定的关键字组。

【命令】

keyword-group name *keyword-group-name*

undo keyword-group name *keyword-group-name*

【缺省情况】

不存在关键字组。

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin

context-admin

【参数】

keyword-group-name: 表示关键字组的名称，为 1~63 个字符的字符串，不区分大小写。

【举例】

```
# 创建名称为 mykeywordgroup 的关键字组，并进入关键字组视图。  
<Sysname> system-view  
[Sysname] uapp-control  
[Sysname-uapp-control] keyword-group name mykeywordgroup  
[Sysname-uapp-control-keyword-group-mykeywordgroup]
```

1.1.8 policy copy

policy copy 命令用来复制应用审计与管理策略。

【命令】

policy copy *policy-name* *new-policy-name*

【缺省情况】

不存在应用审计与管理策略。

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 表示被复制应用审计与管理策略的名称，为 1~63 个字符的字符串，不区分大小写。

new-policy-name: 表示新建应用审计与管理策略的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

当需要新建的应用审计与管理策略和已存在的策略比较相似时，可通过复制已经存在的策略来快速的创建新的应用审计与管理策略。

【举例】

```
# 复制应用审计与管理策略 policy1，复制后的策略名称为 policy2。  
<Sysname> system-view  
[Sysname] uapp-control  
[Sysname-uapp-control] policy copy policy1 policy2
```

1.1.9 policy default-action

policy default-action 命令用来配置应用审计与管理策略的缺省动作。

【命令】

policy default-action { deny | permit }

【缺省情况】

应用审计与管理策略的缺省动作是允许。

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin

context-admin

【参数】

deny: 表示阻断报文。

permit: 表示允许报文通过。

【使用指导】

若报文未与任何一个应用审计与管理策略匹配成功，则设备将根据应用审计与管理策略的缺省动作对报文进行处理。

【举例】

配置应用审计与管理策略的缺省动作为丢弃。

```
<Sysname> system-view
```

```
[Sysname] uapp-control
```

```
[Sysname-uapp-control] policy default-action deny
```

1.1.10 policy move

policy move 命令用来移动应用审计与管理策略的位置。

【命令】

```
policy move policy-name1 { after | before } policy-name2
```

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name1: 表示需要被移动的应用审计与管理策略的名称，为 1~63 个字符的字符串，不区分大小写。

after: 表示把应用审计与管理策略 ***policy-name1*** 移动到应用审计与管理策略 ***policy-name2*** 的后面。

before: 表示把应用审计与管理策略 ***policy-name1*** 移动到应用审计与管理策略 ***policy-name2*** 的前面。

policy-name2: 表示移动目标的应用审计与管理策略的名称，为 1~63 个字符的字符串，不区分大小写。

【举例】

```
# 创建应用审计与管理策略，名称为 policy1。
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name policy1 audit
[Sysname-uapp-control-policy-policy1] quit
# 创建应用审计与管理策略，名称为 policy2。
[Sysname-uapp-control] policy name policy2 audit
[Sysname-uapp-control-policy-policy2] quit
# 移动应用审计与管理策略 policy1 到 policy2 之后。
[Sysname-uapp-control] policy move policy1 after policy2
```

1.1.11 policy name

policy name 命令用来创建应用审计与管理策略，并进入应用审计与管理策略视图。如果指定的应用审计与管理策略已经存在，则直接进入应用审计与管理策略视图。

undo policy name 命令用来删除指定的应用审计与管理策略。

【命令】

```
policy name policy-name [ audit | deny | noaudit ]
undo policy name policy-name
```

【缺省情况】

不存在应用审计与管理策略。

【视图】

应用审计与管理视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

policy-name: 表示应用审计与管理策略的名称，为 1~63 个字符的字符串，不区分大小写，且名称必须全局唯一。

audit: 表示审计类型的策略。

deny: 表示阻断类型的策略。

noaudit: 表示免审计类型的策略。

【使用指导】

本命令用来创建应用审计与管理策略，创建策略时必须指定策略类型，应用审计与管理策略分为如下三类：

- 审计策略：对匹配策略中所有过滤条件的报文，根据审计规则对此报文进行审计。
- 免审计策略：对匹配策略中所有过滤条件的报文进行免审计。
- 阻断策略：对匹配策略中所有过滤条件的报文进行阻断。

每类策略中具体可配置的内容不同，其中 **application** 命令只能在免审计和阻断类型的策略下配置，**rule**、**rule default-action** 和 **rule match-method** 命令只能在审计类型的策略下配置。

【举例】

创建一个名称为 **mypolicy1** 的应用审计与管理策略，并对用户的应用行为进行审计，并进入应用审计与管理策略视图。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1]
```

1.1.12 policy rename

policy rename 命令用来重命名应用审计与管理策略。

【命令】

policy rename *old-policy-name new-policy-name*

【视图】

应用审计与管理视图

【缺省用户角色】

network-admin
context-admin

【参数】

old-policy-name: 表示应用审计与管理策略的原有名称，为 1~63 个字符的字符串，不区分大小写。

new-policy-name: 表示应用审计与管理策略的新名称，为 1~63 个字符的字符串，不区分大小写。

【举例】

```
# 创建应用审计与管理策略，名称为 policy1。
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name policy1 audit
[Sysname-uapp-control-policy-policy1] quit
# 修改应用审计与管理策略 policy1 的名称为 policy2
[Sysname-uapp-control] policy rename policy1 policy2
```

1.1.13 rule

rule 命令用来配置应用审计与管理策略的审计规则。

undo rule id 命令用来删除指定的审计规则。

【命令】

```
rule rule-id { app app-name | app-category app-category-name | any } behavior
{ behavior-name | any } bhcontent { bhcontent-name | any } { keyword { equal
| exclude | include | unequal } { keyword-group-name | any } | integer { equal
| greater | greater-equal | less | less-equal | unequal } { number } } action
{ deny | permit } [ audit-logging ]
undo rule rule-id
```

【缺省情况】

不存在审计规则。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

rule-id: 表示审计规则 ID，取值范围为 1~64。

app app-name: 表示对指定的应用进行审计。

app-category app-category-name: 表示对指定的应用分类进行审计。

any: 表示对所有应用和应用分类进行审计。

behavior behavior-name: 表示对指定应用或应用分类的某一具体行为进行审计。
behavior-name 是行为名称。

any 表示所有行为。

bhcontent bhcontent-name: 表示对该行为中的某一具体内容进行审计。*bhcontent-name* 是行为内容。

any 表示所有行为内容。

keyword: 表示行为内容的匹配方式为字符串形式的关键字。

- **equal**: 表示审计规则对行为内容的匹配方式为与关键字完全相等。
- **exclude**: 表示审计规则对行为内容的匹配方式为不包含关键字。
- **include**: 表示审计规则对行为内容的匹配方式为包含关键字。
- **unequal**: 表示审计规则对行为内容的匹配方式为与关键字不相等。

keyword-group-name: 表示审计规则引用的关键字组。

any 表示对指定应用或应用分类行为的所有内容进行审计。

integer: 表示行为内容的匹配方式为数字。

- **equal**: 表示对等于指定数字的行为内容进行审计。
- **greater**: 表示对大于指定数字的行为内容进行审计。
- **greater-equal**: 表示对大于等于指定数字的行为内容进行审计。
- **less**: 表示对小于指定数字的行为内容进行审计。
- **less-equal**: 表示对小于等于指定数字的行为内容进行审计。

- **unequal:** 表示对不等于指定数字的行为内容进行审计。
- number:** 表示审计规则使用的数字，取值范围为 0~4294967295。
- action:** 表示审计规则的动作，即对与审计规则匹配成功的报文执行的动作。
- **deny:** 表示审计规则动作为阻断报文。
 - **permit:** 表示审计规则动作为允许报文通过。
 - **audit-logging:** 表示审计规则动作为生成审计日志。若未配置本参数，则与此审计规则匹配成功的报文不会生成审计日志。

【使用指导】

审计规则用来对用户的具体应用行为进行更加精细化控制。

当报文与策略中配置的所有过滤条件均匹配成功后，会根据审计规则对此报文进行更加精细化的审计。

仅在审计类型的策略中可配置此命令。

对于微信和 QQ，仅支持对整个应用进行阻断，不支持对指定的行为和内容进行阻断。

【举例】

创建一个名称为 mypolicy1 的应用审计与管理审计策略。

```
<Sysname> system-view
```

```
[Sysname] uapp-control
```

```
[Sysname-uapp-control] policy name mypolicy1 audit
```

创建第一条审计规则：对 QQ 应用行为是登录，行为内容为账号且包含关键字 1234 的用户报文进行放行审计，并生成审计日志。

```
[Sysname-uapp-control-policy-mypolicy1] rule 1 app qq behavior Login bhcontent Account keyword include mykeywd1 action permit audit-logging
```

创建第二条审计规则：对 QQ 应用行为是登录，行为内容为账号但不等于数字 785 的用户报文进行放行审计，但不生成审计日志。

```
[Sysname-uapp-control-policy-mypolicy1] rule 2 app qq behavior Login bhcontent Account integer unequal 785 action permit
```

创建第三条审计规则：对 IM 应用组行为是登录，行为内容为账号且包含关键字 0 的用户报文进行阻断，并生成审计日志。

```
[Sysname-uapp-control-policy-mypolicy1] rule 3 app-category IM behavior Login bhcontent Account keyword include mykeywd2 action deny audit-logging
```

【相关命令】

- **keyword**
- **keyword-group name**

1.1.14 rule default-action

rule default-action 命令用来配置审计规则的缺省动作。

【命令】

```
rule default-action { deny | permit }
```

【缺省情况】

审计规则的缺省动作为允许。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

deny: 表示阻断匹配审计规则的报文。

permit: 表示允许匹配审计规则的报文通过。

【使用指导】

若报文未与策略中的任何一条审计规则匹配成功，则设备将根据该策略中审计规则的缺省动作对报文进行处理。

【举例】

配置审计规则的缺省动作为阻断。

```
<Sysname> system-view
```

```
[Sysname] uapp-control
```

```
[Sysname-uapp-control] policy name mypolicy1 audit
```

```
[Sysname-uapp-control-policy-mypolicy1] rule default-action deny
```

1.1.15 rule match-method

rule match-method 命令用来配置审计规则的匹配模式。

【命令】

```
rule match-method { all | in-order }
```

【缺省情况】

审计规则的匹配模式为顺序匹配。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

all: 表示审计规则匹配模式为全匹配。

in-order: 表示审计规则匹配模式为顺序匹配。

【使用指导】

顺序匹配表示审计规则按照规则 ID 从小到大的顺序进行逐一匹配，一旦报文与某条审计规则匹配成功就结束此匹配过程，并根据该审计规则中的动作对此报文进行相应处理。

全匹配表示审计规则按照审计规则 ID 从小到大的顺序进行匹配，若报文与其条动作为允许的规则匹配成功，则继续匹配后续规则直到最后一条规则；若报文与某条动作为阻断的规则匹配成功，则

不再进行后续规则的匹配。设备将根据所有匹配成功的审计规则中优先级最高的动作（阻断的优先级高于允许）对此报文进行相应处理。

【举例】

```
# 配置审计规则的匹配模式为全匹配。
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] rule match-method all
```

1.1.16 service

service 命令用来配置作为应用审计与管理策略过滤条件的服务。

undo service 命令用来删除作为应用审计与管理策略过滤条件的服务。

【命令】

```
service service-name
undo service [service-name ]
```

【缺省情况】

不存在服务过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

service-name: 是服务对象组的名称，为 1~31 个字符的字符串，不区分大小写，且必须已存在。如果不指定该参数，则删除所有服务过滤条件。

【使用指导】

多次执行本命令，可配置多个服务作为应用审计与管理策略的过滤条件。

配置 **undo service** 命令时，如果指定的服务对象组为 **any**，则表示删除所有服务过滤条件。

【举例】

```
# 配置应用审计与管理审计策略 mypolicy1 过滤条件的服务为 dns-tcp 和 dns-udp。
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] service dns-tcp
[Sysname-uapp-control-policy-mypolicy1] service dns-udp
```

【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.17 source-address

source-address 命令用来配置作为应用审计与管理策略过滤条件的源 IP 地址。

undo source-address 命令用来删除作为应用审计与管理策略过滤条件的源 IP 地址。

【命令】

source-address { **ipv4** | **ipv6** } *object-group-name*

undo source-address { **ipv4** | **ipv6** } *object-group-name*

【缺省情况】

不存在源 IP 地址过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4: 表示指定 IPv4 地址对象组。

ipv6: 表示指定 IPv6 地址对象组。

object-group-name: 表示地址对象组的名称，为 1~31 个字符的字符串，不区分大小写，且必须已存在。

【使用指导】

多次执行本命令，可配置多个源 IP/IPv6 地址对象组作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的源 IP 地址。

```
<Sysname> system-view
```

```
[Sysname] uapp-control
```

```
[Sysname-uapp-control] policy name mypolicy audit
```

```
[Sysname-uapp-control-policy-mypolicy] source-address ipv4 obgroup1
```

```
[Sysname-uapp-control-policy-mypolicy] source-address ipv4 obgroup2
```

【相关命令】

- **object-group**（安全命令参考/对象组）

1.1.18 source-zone

source-zone 命令用来配置作为应用审计与管理策略过滤条件的源安全域。

undo source-zone 命令用来删除作为应用审计与管理策略过滤条件的源安全域。

【命令】

source-zone *source-zone-name*

undo source-zone *source-zone-name*

【缺省情况】

不存在源安全域过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

source-zone-name: 表示安全域的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

多次执行本命令，可配置多个源安全域作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的源安全域为 zone1 和 zone2。

```
<Sysname> system-view
```

```
[Sysname] uapp-control
```

```
[Sysname-uapp-control] policy name mypolicy1 audit
```

```
[Sysname-uapp-control-policy-mypolicy1] source-zone zone1
```

```
[Sysname-uapp-control-policy-mypolicy1] source-zone zone2
```

【相关命令】

- **security-zone name**（安全命令参考/安全域）

1.1.19 time-range

time-range 命令用来配置应用审计与管理策略的生效时间。

undo time-range 命令用来恢复缺省情况。

【命令】

time-range *time-range-name*

undo time-range

【缺省情况】

应用审计与管理策略在任何时间下都生效。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

time-range-name: 表示时间段的名称，为 1~32 个字符的字符串，不区分大小写。

【举例】

配置应用审计与管理审计策略 mypolicy1 的生效时间段为 work-time。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] time-range work-time
```

【相关命令】

- **time-range** (ACL 命令参考/时间段)

1.1.20 uapp-control

uapp-control 命令用来进入应用审计与管理视图。

undo uapp-control 命令用来删除应用审计与管理策略中的所有配置。

【命令】

```
uapp-control
undo uapp-control
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

在应用审计与管理视图下可完成应用审计与管理策略的创建、复制、移动和重命名以及关键字组的创建。应用审计与管理策略分为三种类型：审计（**audit**），免审计（**noaudit**）和阻断（**deny**），其中免审计和阻断类型的策略用来做粗粒度的应用审计与管理，审计类型的策略用来做精细化的应用审计与管理。

【举例】

进入应用审计与管理视图。

```
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control]
```

1.1.21 user

user 命令用来配置作为应用审计与管理策略过滤条件的用户。

undo user 命令用来删除作为应用审计与管理策略过滤条件的用户。

【命令】

```
user user-name [ domain domain-name ]
undo user user-name [ domain domain-name ]
```


【缺省情况】

不存在用户过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-name: 表示身份识别用户的账户名称，为 1~55 个字符的字符串，区分大小写，不能是 a、al 和 all，且不能包含特殊字符 “\”、“|”、“/”、“:”、“*”、“?”、“<”、“>” 和 “@”。

domain domain-name: 表示在指定的身份识别域中匹配此用户。**domain-name** 是身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包含特殊字符 “\”、“|”、“/”、“:”、“*”、“?”、“<”、“>” 和 “@”。若不指定此参数，则表示在不属于任何身份识别域的用户中匹配此用户。

有关身份识别域的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

【使用指导】

多次执行本命令，可配置多个用户作为应用审计与管理策略的过滤条件。

【举例】

```
# 配置应用审计与管理策略 mypolicy1 过滤条件的用户为 managers1 和 managers2。
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] user managers1
[Sysname-uapp-control-policy-mypolicy1] user managers2
# 引用用户名为 managers1，身份识别域为 dpi 的用户作为应用审计与管理策略的过滤条件。
<Sysname> system-view
[Sysname] uapp-control
[Sysname-uapp-control] policy name mypolicy1 audit
[Sysname-uapp-control-policy-mypolicy1] user managers1 domain dpi
```

【相关命令】

- **user-identity enable**（安全命令参考/用户身份识别与管理）

1.1.22 user-group

user-group 命令用来配置作为应用审计与管理策略过滤条件的用户组。

undo user-group 命令用来删除作为应用审计与管理策略过滤条件的用户组。

【命令】

user-group *user-group-name* [**domain** *domain-name*]

undo user-group *user-group-name* [**domain** *domain-name*]

【缺省情况】

不存在用户组过滤条件。

【视图】

应用审计与管理策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-group-name: 表示身份识别用户组的名称，为 1~200 个字符的字符串，不区分大小写。

domain domain-name: 表示在指定的身份识别域中匹配此用户组。**domain-name** 是身份识别域的名称，为 1~255 个字符的字符串，不区分大小写，不能包含特殊字符“/”、“\”、“|”、“:”、“*”、“?”、“<”、“>”以及“@”。若不指定此参数，则表示在不属于任何身份识别域的用户组中匹配此用户组。有关身份识别域的详细介绍，请参见“安全配置指导”中的“用户身份识别与管理”。

【使用指导】

多次执行本命令，可配置多个用户组作为应用审计与管理策略的过滤条件。

【举例】

配置应用审计与管理审计策略 mypolicy1 过滤条件的用户组为 group1 和 group2。

```
<Sysname> system-view
```

```
[Sysname] uapp-control
```

```
[Sysname-uapp-control] policy name mypolicy1 audit
```

```
[Sysname-uapp-control-policy-mypolicy1] user-group group1
```

```
[Sysname-uapp-control-policy-mypolicy1] user-group group2
```

引用用户组名为 group1，域为 dpi 的用户组作为应用审计与管理审计策略规则的匹配条件。

```
<Sysname> system-view
```

```
[Sysname] uapp-control
```

```
[Sysname-uapp-control] policy name mypolicy1 audit
```

```
[Sysname-uapp-control-policy-mypolicy1] user-group group1 domain dpi
```

【相关命令】

- **user-identity enable**（安全命令参考/用户身份识别与管理）



UNIS 入侵检测系统

接口管理命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《接口管理命令参考》主要介绍接口批量配置、以太网接口、LoopBack 接口、NULL 接口和 InLoopBack 接口相关的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。

格 式	意 义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 接口批量配置	1-1
1.1 接口批量配置命令	1-1
1.1.1 display interface range	1-1
1.1.2 interface range	1-1
1.1.3 interface range name	1-3

1 接口批量配置

1.1 接口批量配置命令

1.1.1 display interface range

display interface range 命令用来显示通过 **interface range name** 命令创建的批量接口的信息。

【命令】

display interface range [*name name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

name name: 设备上已创建的批量接口的别名，为 1~32 个字符的字符串，区分大小写。不指定该参数时，显示当前设备中所有通过 **interface range name** 命令已创建的批量接口的信息。

【举例】

显示当前设备中所有通过 **interface range name** 命令创建的批量接口的信息。

```
<Sysname> display interface range  
Interface range name t2 GigabitEthernet1/0/1 GigabitEthernet1/0/2  
Interface range name test GigabitEthernet1/0/3 GigabitEthernet1/0/4
```

以上显示信息表明：批量接口 **t2** 下绑定了接口 **GigabitEthernet1/0/1** 和 **GigabitEthernet1/0/2**，批量接口 **test** 下绑定了接口 **GigabitEthernet1/0/3** 和 **GigabitEthernet1/0/4**。

【相关命令】

- **interface range name**

1.1.2 interface range

interface range 命令用来绑定一组接口，并进入接口批量配置视图。

【命令】

interface range *interface-list*

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface-list: 接口列表，表示方式为 **interface-list = { interface-type interface-number1 [to interface-type interface-number2] }**<1-24>。其中 **interface-type interface-number** 表示接口类型和接口编号。<1-24>表示前面的参数最多可以输入 24 次。**interface-type interface-number2** 的值要大于等于 **interface-type interface-number1** 的值。选中的接口必须位于同一接口卡或子卡上。

【使用指导】

当多个接口需要配置某功能（比如 **shutdown**）时，需要逐个进入接口视图，在每个接口执行一遍命令，比较繁琐。**interface range** 命令提供了一种批量配置方式。使用该命令可以将不同类型的接口进行绑定，并进入接口批量配置视图。

在接口批量配置视图下，只能执行接口列表中第一个接口支持的命令，不能执行第一个接口不支持但其它成员接口支持的命令。（接口列表中的第一个接口指的是执行 **interface range** 命令时指定的第一个接口）。在接口批量配置视图下，输入问号并回车，将显示该视图下支持的所有命令。

在接口批量配置视图下执行命令，会在绑定的所有接口下执行该命令：

- 当命令执行完成后，系统提示配置失败并保持在接口批量配置视图。
 - 如果配置失败的接口是接口列表的第一个接口，则表示列表中的所有接口都未配置该命令。
 - 如果配置失败的接口是其它接口，则表示除了提示失败的接口外，其它接口都已经配置成功。
- 如果命令执行完成后，退回到系统视图，则表示：
 - 接口视图和系统视图下都支持该命令。
 - 在列表中的某个接口上配置失败，在系统视图下配置成功。
 - 列表中位于这个接口后面的接口不再执行该命令。

此时，可到列表中各接口的视图下使用 **display this** 命令验证配置效果，同时如果不需要在系统视图下配置该命令的话，请使用相应的 **undo** 命令取消该配置。

在接口批量配置视图下，执行 **display this** 命令，将显示接口列表中第一个接口当前生效的配置。

批量配置接口时有如下限制：

- 设置为接口列表的第一个接口之前，需要确保可以通过 **interface interface-type { interface-number | interface-number.subnumber }** 命令进入该接口视图。
- 聚合口加入批量接口时，建议不要将该聚合口的成员接口也加入，否则在批量接口配置视图下执行某些配置命令时，可能会导致聚合分裂。
- 批量接口包含的接口数量没有上限，仅受系统资源限制。接口数量较多时，在批量接口配置视图下执行命令等待的时间将较长。

【举例】

关闭接口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4。

```
<Sysname> system-view
```

```
[Sysname] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[Sysname-if-range] shutdown
```

1.1.3 interface range name

interface range name name interface interface-list 命令用来绑定一组接口，为这组接口指定一个别名，并使用该别名进入接口批量配置视图。

interface range name name（不带 **interface** 参数时）命令用来使用别名进入接口批量配置视图。

undo interface range name 命令用来取消接口绑定，删除接口别名。

【命令】

```
interface range name name [ interface interface-list ]
undo interface range name name
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

name：批量接口的别名，为 1~32 个字符的字符串，区分大小写。

interface-list：接口列表，表示方式为 **interface-list = { interface-type interface-number [to interface-type interface-number] }&<1-24>**。其中 **interface-type interface-number** 表示接口类型和接口编号。**&<1-24>**表示前面的参数最多可以输入 24 次。**interface-type interface-number2** 的值要大于等于 **interface-type interface-number1** 的值。选中的接口必须位于同一接口卡或子卡上。

【使用指导】

interface range name 和 **interface range** 命令都能提供接口批量配置功能，它们的差别在于：**interface range name** 命令在绑定接口的时候可以定义一个别名，可以进行多次绑定，给不同的绑定定义不同的别名，以示区别，方便记忆。并且，后续可以使用别名直接进入接口批量配置视图，不再需要输出一长串的接口列表，配置起来更简便。用户可以使用 **display interface range** 命令来查看绑定了哪些接口。

在接口批量配置视图下，只能执行接口列表中第一个接口支持的命令，不能执行第一个接口不支持但其它成员接口支持的命令。（接口列表中的第一个接口指的是执行 **interface range** 命令时指定的第一个接口）。在接口批量配置视图下，输入问号并回车，将显示该视图下支持的所有命令。

在接口批量配置视图下执行命令，会在绑定的所有接口下执行该命令：

- 当命令执行完成后，系统提示配置失败并保持在接口批量配置视图。
 - 如果配置失败的接口是接口列表的第一个接口，则表示列表中的所有接口都没有配置该命令。
 - 如果配置失败的接口是其它接口，则表示除了提示失败的接口外，其它接口都已经配置成功。

- 如果命令执行完成后，退回到系统视图，则表示：
 - 在接口视图和系统视图下都支持该命令。
 - 在列表中的某个接口上配置失败，在系统视图下配置成功。
 - 列表中位于这个接口后面的接口不再执行该命令。

此时，可到列表中各接口的视图下使用 **display this** 命令验证配置效果，同时如果不需要在系统视图下配置该命令的话，请使用相应的 **undo** 命令取消该配置。

在接口批量配置视图下，执行 **display this** 命令，将显示接口列表中第一个接口当前生效的配置。

批量配置接口时有如下限制：

- 设置为接口列表的第一个接口之前，需要确保可以通过 **interface interface-type { interface-number | interface-number.subnumber }** 命令进入该接口视图。
- 聚合口加入批量接口时，建议不要将该聚合口的成员接口也加入，否则在批量接口配置视图下执行某些配置命令时，可能会导致聚合分裂。
- 批量接口包含的接口数量没有上限，仅受系统资源限制。接口数量较多时，在批量接口配置视图下执行命令等待的时间将较长。
- 系统中支持的批量接口别名的个数没有上限，仅受系统资源限制。推荐用户配置 1000 个以下，配置数量过多，可能引起该特性执行效率降低。

【举例】

将 5 个以太网接口 GigabitEthernet1/0/1～GigabitEthernet1/0/4 定义为 myEthPort，并进入批量接口视图。

```
<Sysname> system-view
```

```
[Sysname] interface range name myEthPort interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4
```

```
[Sysname-if-range-myEthPort]
```

进入 myEthPort 别名对应的批量接口配置视图。

```
<Sysname> system-view
```

```
[Sysname] interface range name myEthPort
```

```
[Sysname-if-range-myEthPort]
```

【相关命令】

- **display interface range**

目 录

1 以太网接口	1-1
1.1 以太网接口通用配置命令	1-1
1.1.1 bandwidth	1-1
1.1.2 broadcast-suppression	1-1
1.1.3 combo enable	1-3
1.1.4 dampening	1-4
1.1.5 default	1-5
1.1.6 description	1-6
1.1.7 display counters	1-6
1.1.8 display counters rate	1-8
1.1.9 display ethernet statistics	1-9
1.1.10 display interface	1-11
1.1.11 display packet-drop	1-21
1.1.12 duplex	1-22
1.1.13 flow-control	1-23
1.1.14 flow-interval	1-24
1.1.15 interface	1-24
1.1.16 jumboframe enable	1-25
1.1.17 loopback	1-26
1.1.18 multicast-suppression	1-27
1.1.19 port link-mode	1-28
1.1.20 reset counters interface	1-28
1.1.21 reset ethernet statistics	1-29
1.1.22 reset packet-drop interface	1-30
1.1.23 shutdown	1-30
1.1.24 speed	1-31
1.1.25 sub-interface rate-statistic	1-32
1.1.26 unicast-suppression	1-33
1.2 二层以太网接口的配置命令	1-34
1.2.1 display storm-constrain	1-34
1.2.2 mdix-mode	1-36
1.2.3 storm-constrain	1-36
1.2.4 storm-constrain control	1-37

1.2.5 storm-constrain enable log.....	1-38
1.2.6 storm-constrain enable trap	1-39
1.2.7 storm-constrain interval.....	1-39
1.3 三层以太网接口/子接口的配置命令	1-40
1.3.1 mac-address	1-40
1.3.2 mac-address-filter enable	1-41
1.3.3 mtu.....	1-42

1 以太网接口

1.1 以太网接口通用配置命令

1.1.1 bandwidth

bandwidth 命令用来配置接口的期望带宽。

undo bandwidth 命令用来恢复缺省情况。

【命令】

bandwidth *bandwidth-value*

undo bandwidth

【缺省情况】

接口的期望带宽 = 接口的波特率 ÷ 1000 (kbps)。

【视图】

以太网接口视图

以太网子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

bandwidth-value: 表示接口的期望带宽，取值范围为 1~400000000，单位为 kbps。

【使用指导】

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 的期望带宽为 1000kbps。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bandwidth 1000
# 设置以太网子接口 GigabitEthernet1/0/1.1 的期望带宽为 1000kbps。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] bandwidth 1000
```

【相关命令】

- **Speed**

1.1.2 broadcast-suppression

broadcast-suppression 命令用来开启端口广播风暴抑制功能，并设置广播风暴抑制阈值。

undo broadcast-suppression 命令用来关闭端口广播风暴抑制功能。

【命令】

```
broadcast-suppression { ratio | pps max-pps | kbps max-kbps }  
undo broadcast-suppression
```

【缺省情况】

所有接口不对广播流量进行抑制。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ratio: 指定以太网接口允许通过的最大广播流量占该接口带宽的百分比，取值范围为 0~100。数值越小，允许通过的广播流量也越小。

pps max-pps: 指定以太网接口每秒允许转发的最大广播包数，单位为 pps (packets per second, 每秒转发的报文数)，取值范围为 0~1.4881×接口带宽。

kbps max-kbps: 指定以太网接口每秒允许转发的最大广播流量，单位为 kbps (kilobits per second, 每秒转发的千比特数)，取值范围为 0~接口带宽。

【使用指导】

本命令设置的是接口允许通过的最大广播报文流量。当接口上的广播流量超过用户设置的值后，系统将丢弃超出广播流量限制的报文，从而使接口广播流量所占的比例控制在限定的范围内，以便保证业务的正常运行。

执行 **broadcast-suppression** 或 **storm-constrain** 命令都能开启端口的广播风暴抑制功能，**storm-constrain** 命令通过软件对广播报文进行抑制，对设备性能有一定影响，**broadcast-suppression** 通过芯片物理上对广播报文进行抑制，相对 **storm-constrain** 来说，对设备性能影响较小。请不要同时配置 **broadcast-suppression** 和 **storm-constrain** 命令，以免配置冲突，导致抑制效果不确定。

当风暴抑制阈值配置为 **pps** 或 **kbps** 时，设备可能会根据芯片支持的步长，将配置值转换成步长的倍数。所以，端口下配置的抑制阈值可能与实际生效抑制阈值不一致，请注意查看设备的提示信息。

【举例】

在以太网接口 GigabitEthernet1/0/1 上，每秒最多允许 10000kbps 广播报文通过，对超出该范围的广播报文进行抑制。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] broadcast-suppression kbps 10000
```

```
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

以上信息表示：用户配置的值 10000kbps，因为芯片支持的步长为 64，所以实际生效的值为 10048kbps (64 的 157 倍)。

【相关命令】

- **multicast-suppression**
- **unicast-suppression**

1.1.3 combo enable



注意

- 在 Bootware 菜单中，Combo 接口的光接口不可用。
- 当光口处于激活状态时，仅支持自协商和 1000 Mbps 两种接口速率，全双工和自协商两种双工模式。因此，电口处于激活状态时所做的其他接口速率和双工模式配置，切换成光口时不会生效。

combo enable 命令用来激活 Combo 接口中的电口或者光口。

【命令】

combo enable { copper | fiber }

本命令的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	不支持
T5000-G30	支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	不支持
T1000-CN60/T1000-CN80	不支持

【缺省情况】

电口处于激活状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

copper: 表示该 Combo 接口的电口被激活，请使用双绞线连接。

fiber: 表示该 Combo 接口的光口被激活，请使用光纤连接。

【使用指导】

Combo 接口是一个逻辑接口，一个 Combo 接口物理上对应设备面板上一个电口和一个光口。电口与其对应的光口是光电复用关系，两者不能同时工作（当激活其中的一个接口时，另一个接口就自动处于关闭状态），用户可根据组网需求选择使用电口或光口。

请根据设备面板上的标识了解设备上有哪些 Combo 接口以及每个 Combo 接口的编号。

【举例】

```
# 指定 GigabitEthernet1/0/1 端口的电口被激活。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] combo enable copper
# 指定 GigabitEthernet1/0/1 端口的光口被激活。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] combo enable fiber
```

1.1.4 dampening

dampening 命令用来开启接口的 dampening 功能。

undo dampening 命令用来恢复缺省情况。

【命令】

```
dampening [ half-life reuse suppress max-suppress-time ]
undo dampening
```

【缺省情况】

接口的 dampening 功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

half-life: 半衰期，取值范围为 1~120，单位为秒，缺省值为 54。

reuse: 启用值，取值范围为 200~20000，缺省值为 750，必须要小于 **suppress** 的值。

suppress: 抑制门限，取值范围为 200~20000，缺省值为 2000。

max-suppress-time: 最大抑制时间，取值范围为 1~255，单位为秒，缺省值为半衰期的 3 倍，即 162。

【使用指导】

配置本命令时，各参数之间应满足以下关系，请根据该关系来选择参数的取值：

- 最大惩罚值 = $2^{(\text{最大抑制时间}/\text{半衰期})} \times \text{启用值}$ ，其中最大惩罚值不可配。
- 抑制值的配置值 ≤ 最大惩罚值 ≤ 抑制值可配的最大值

本命令对使用 **shutdown** 命令手动关闭的接口无效。手工 **shutdown** 接口时，dampening 的惩罚值恢复为初始值 0。

接口在抑制期发生 up 事件，通过 **display interface** 命令、MIB 网管或 Web 网管等方式查看时，该接口的状态仍然为 down。

【举例】

按照缺省值开启接口 GigabitEthernet1/0/1 的 dampening 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dampening
# 开启接口 GigabitEthernet1/0/1 的 dampening 功能，配置半衰期为 2 秒，启用值为 800，抑制门
限为 3000，最大抑制时间为 5 秒。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dampening 2 800 3000 5
```

【相关命令】

- **display interface**

1.1.5 default

default 命令用来恢复当前接口的缺省配置。

【命令】

default

【视图】

以太网接口视图

以太网子接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】



注意

接口下的某些配置恢复到缺省情况后，会对设备上当前运行的业务产生影响。建议您在执行该命令前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

【举例】

将以太网接口 GigabitEthernet1/0/1 恢复为缺省配置。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] default
This command will restore the default settings. Continue? [Y/N]:y
# 将以太网子接口 GigabitEthernet1/0/1.1 恢复为缺省配置。
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] default
This command will restore the default settings. Continue? [Y/N]:y
```

1.1.6 description

description 命令用来设置当前接口的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description text

undo description

【缺省情况】

接口的描述信息为“接口名 Interface”，例如：GigabitEthernet1/0/1 Interface。

【视图】

以太网接口视图

以太网子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: 接口的描述信息，为 1~255 个字符的字符串，区分大小写。

【举例】

设置以太网接口 GigabitEthernet1/0/1 的描述信息为“lan-interface”。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] description lan-interface
```

设置以太网子接口 GigabitEthernet1/0/1.1 的描述信息为“subinterface1/0/1.1”。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1.1
```

```
[Sysname-GigabitEthernet1/0/1.1] description subinterface1/0/1.1
```

1.1.7 display counters

display counters 命令用来显示接口的流量统计信息。

【命令】

```
display counters { inbound | outbound } interface [ interface-type  
[ interface-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

inbound: 显示输入报文的流量统计信息。
outbound: 显示输出报文的流量统计信息。
interface-type: 指定接口类型。
interface-number: 指定接口编号。

【使用指导】

可通过命令 **reset counters interface** 清除以太网接口的统计信息。
如果不指定接口类型，则显示所有可统计的接口的流量统计信息。
如果指定接口类型而不指定接口编号，则显示该类型下所有接口的流量统计信息。
如果同时指定接口类型和接口编号，则显示指定接口的报文流量统计信息。

【举例】

```
# 显示接口的报文输入流量统计信息。
<Sysname> display counters inbound interface
Interface          Total (pkts)    Broadcast (pkts)  Multicast (pkts)  Err (pkts)
GE1/0/1             100             100                0                  0
GE1/0/2             Overflow         Overflow           Overflow           Overflow

Overflow: More than 14 digits (7 digits for column "Err").
--: Not supported.
```

表1-1 display counters 命令显示信息描述表

字段	描述
Interface	接口名称缩写
Total (pkts)	接口接收或发送报文的总数（单位为包）
Broadcast (pkts)	接口接收或发送广播报文的总数（单位为包）
Multicast (pkts)	接口接收或发送组播报文的总数（单位为包）
Err (pkts)	接口接收或发送错误报文的总数（单位为包）
Overflow: More than 14 digits (7 digits for column "Err").	当某个统计信息的值为 Overflow 时，表示该项数据的长度超过了显示范围： - 对于 Err 项，Overflow 表示数据的长度超过了 7 位十进制数 - 对于其它项，Overflow 表示数据的长度超过了 14 位十进制数
--: Not supported.	当某个统计信息的值为“--”时，表示设备不支持该项数据的统计

【相关命令】

- **reset counters interface**

1.1.8 display counters rate

display counters rate 命令用来显示最近一个统计周期内处于 up 状态的接口的报文速率统计信息。

【命令】

display counters rate { inbound | outbound } interface [interface-type [interface-number]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

inbound: 显示报文接收速率统计信息。

outbound: 显示报文发送速率统计信息。

interface-type: 指定接口类型。

interface-number: 指定接口编号。

【使用指导】

如果不指定 **interface-type** 和 **interface-number**，则显示所有可统计的接口类型中最近一个统计周期内处于 up 状态的接口的报文速率统计信息。

如果指定 **interface-type** 而不指定 **interface-number**，则显示该类型下最近一个统计周期内处于 up 状态接口的报文速率统计信息。

如果同时指定 **interface-type** 和 **interface-number**，则显示指定接口在最近一个统计周期内报文速率统计信息。如果该接口在最近一个统计周期内一直处于 down 状态，则提示接口不支持该操作。

统计周期可以通过 **flow-interval** 命令来配置。

【举例】

显示接口的报文接收速率统计信息。

```
<Sysname> display counters rate inbound interface
```

Usage: Bandwidth utilization in percentage

Interface	Usage (%)	Total (pps)	Broadcast (pps)	Multicast (pps)
GE1/0/1	0	0	--	--

Overflow: More than 14 digits.

--: Not supported.

表1-2 display counters rate 命令显示信息描述表

字段	描述
Interface	接口名称缩写
Usage (%)	在最近一个统计周期内，接口的带宽利用率（单位为百分比）
Total (pps)	在最近一个统计周期内，接口接收或发送所有类型报文的平均速率（单位为包/秒）
Broadcast (pps)	在最近一个统计周期内，接口接收或发送广播报文的平均速率（单位为包/秒）
Multicast (pps)	在最近一个统计周期内，接口接收或发送组播报文的平均速率（单位为包/秒）
Overflow: More than 14 digits.	当某个统计信息的值为Overflow时，表示该项数据的长度超过了14位十进制数
--: Not supported.	当某个统计信息的值为“--”时，则表示设备不支持该项数据的统计

【相关命令】

- flow-interval
- reset counters interface

1.1.9 display ethernet statistics

display ethernet statistics 命令用来显示以太网软件模块收发报文的统计信息。

【命令】

display ethernet statistics slot slot-number

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备的统计信息，*slot-number* 表示设备在 IRF 中的成员编号。

【举例】

显示指定 slot 上的以太网软件模块收发报文的统计信息。

```
<Sysname> display ethernet statistics slot 1
ETH receive packet statistics:
  Totalnum      : 10447      ETHIINum       : 4459
  SNAPNum       : 0          RAWNum         : 0
  LLCNum        : 0          UnknownNum     : 0
  ForwardNum    : 4459      ARP             : 0
```

```

MPLS          : 0          ISIS          : 0
ISIS2         : 0          IP            : 0
IPV6          : 0

ETH receive error statistics:
NullPoint     : 0          ErrIfindex    : 0
ErrIfcb       : 0          IfShut     : 0
ErrAnalyse    : 5988       ErrSrcMAC   : 5988
ErrHdrLen     : 0

ETH send packet statistics:
L3OutNum      : 211        VLANOutNum  : 0
FastOutNum    : 155        L2OutNum   : 0

ETH send error statistics:
MbufRelayNum  : 0          NullMbuf    : 0
ErrAdjFwd     : 0          ErrPrepend  : 0
ErrHdrLen     : 0          ErrPad      : 0
ErrQoSTrs     : 0          ErrVLANTrs  : 0
ErrEncap      : 0          ErrTagVLAN  : 0
IfShut        : 0          IfErr       : 0

```

表1-3 display ethernet statistics 命令显示信息描述表

字段	描述
ETH receive packet statistics	以太网软件模块接收到的以太网报文的统计信息： • Totalnum: 接收报文的总个数 • ETHIINum: 接收的 ETHII 封装格式报文个数 • SNAPNum: 接收的 SNAP 封装格式报文个数 • RAWNum: 接收的 RAW 封装格式报文个数 • ISISNum: 接收的 ISIS 封装格式报文个数 • LLCNum: 接收的 LLC 封装格式报文个数 • UnknowNum: 接收的未知封装格式报文个数 • ForwardNum: 二层转发或上送 CPU 的报文个数 • ARP: 接收的 ARP 报文个数 • MPLS: 接收的 MPLS 报文个数 • ISIS: 接收的 ISIS 报文个数 • ISIS2: 接收的 ISIS2 报文个数 • IP: 接收的 IP 报文个数 • IPv6: 接收的 IPv6 报文个数

字段	描述
ETH receive error statistics	以太网软件模块接收错误的以太网报文的统计信息（可能是包本身包含错误或者是接收动作出错了）： • NullPoint: 接收报文时指针为空的报文的个数 • ErrIfindex: 接收报文时接口索引错误的报文个数 • ErrIfcb: 接收报文时接口控制块错误的报文个数 • IfShut: 接收报文时接口 shutdown 的报文个数 • ErrAnalyse: 接收报文时报文解析错误的报文个数 • ErrSrcMAC: 接收的包含源 MAC 地址错误的报文个数 • ErrHdrLen: 接收的包含报文头长度错误的报文个数
ETH send packet statistics	以太网软件模块发送的以太网报文的统计信息： • L3OutNum: 通过三层以太网接口发送的报文总个数 • VLANOutNum: 通过 VLAN 接口发送的报文总个数 • FastOutNum: 快速发送的报文总个数 • L2OutNum: 通过二层以太网接口发送的报文总个数 • MbufRelayNum: 透传发送的报文总个数
ETH send error statistics	以太网软件模块发送的错误以太网报文的统计信息： • NullMbuf: 发送报文时空指针错误的报文个数 • ErrAdjFwd: 发送报文时邻接表错误的报文个数 • ErrPrepend: 发送报文时扩展错误的报文个数 • ErrHdrLen: 发送的包含报文头长度错误的报文个数 • ErrPad: 发送报文时填充错误的报文个数 • ErrVLANTrs: 发送报文时 VLAN 发送失败的报文个数 • ErrEncap: 发送报文时封装链路头失败的报文个数 • ErrTagVLAN: 发送报文时封装 VLAN TAG 失败的报文个数 • IfShut: 发送报文时端口 shutdown 的报文个数 • IfErr: 发送报文时出接口错误的报文个数

【相关命令】

- **reset ethernet statistics**

1.1.10 display interface

display interface 命令用来显示接口的运行状态和相关信息。

【命令】

```
display interface [ interface-type [ interface-number | interface-number.subnumber ] ] [ brief [ description | down ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-type: 指定接口类型。

interface-number: 指定接口编号。

interface-number.subnumber: 指定子接口编号。其中 **interface-number** 为主接口编号；**subnumber** 为子接口编号，取值范围为 1~4094。

brief: 显示接口的概要信息。不指定该参数时，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果某接口的描述信息超过 27 个字符，不指定该参数时，只显示描述信息中的前 27 个字符，超出部分不显示。

down: 显示当前物理状态为 down 的接口的信息以及 down 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【使用指导】

如果不指定接口类型和接口编号，则显示所有接口的信息。

如果仅指定接口类型，则显示所有该类型接口的信息。

【举例】

查看三层以太网接口 GigabitEthernet1/0/1 的运行状态和相关信息。

```
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: Administratively DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/0/1 Interface
Maximum transmission unit: 1500
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
IPv6 packet frame type: Ethernet II, hardware address: 3822-d666-bd0c
Media type is twisted pair, loopback not set, promiscuous mode set
Speed Negotiation, Duplex Negotiation, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Last link flapping: Never
Last clearing of counters: Never
Current system time:2078-11-09 17:58:38
Last time when physical state changed to up:-
Last time when physical state changed to down:2078-11-01 21:21:23
Peak input rate: 0 bytes/sec, at 00-00-00 00:00:00
Peak output rate: 0 bytes/sec, at 00-00-00 00:00:00
Last 300 second input: 0 packets/sec 0 bytes/sec -%
Last 300 second output: 0 packets/sec 0 bytes/sec -%
Input (total): 0 packets, 0 bytes
```

```

        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input (normal): 0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants, - throttles
        0 CRC, 0 frame, 0 overruns, 0 aborts
        0 ignored, - parity errors
Output (total): 0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output (normal): 0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, 0 underruns, - buffer failures
        0 aborts, 0 deferred, 0 collisions, 0 late collisions
        0 lost carrier, 0 no carrier
# 查看二层以太网接口 GigabitEthernet1/0/1 的运行状态和相关信息。
<Sysname> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: 000c-2963-b767
Description: GigabitEthernet1/0/1 Interface
Loopback is not set
Media type is twisted pair, port hardware type is 1000_BASE_T_AN_SFP
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
MDI type: Automdix
Port link-type: Access
    Tagged VLANs:    None
    UnTagged VLANs: 1
Last link flapping: 6 hours 39 minutes 25 seconds
Last clearing of counters:  14:34:09 Tue 11/01/2011
Current system time:2017-12-09 10:59:08
Last time when physical state changed to up:-
Last time when physical state changed to down:2017-12-09 10:59:07
    Peak input rate: 0 bytes/sec, at 2013-07-17 22:06:19
    Peak output rate: 0 bytes/sec, at 2013-07-17 22:06:19
    Last 300 second input:  0 packets/sec 0 bytes/sec -%
    Last 300 second output: 0 packets/sec 0 bytes/sec -%
Input (total): 0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input (normal): 0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses

```

Input: 0 input errors, 0 runs, 0 giants, 0 throttles
 0 CRC, 0 frame, 0 overruns, 0 aborts
 0 ignored, 0 parity errors
 Output (total): 0 packets, 0 bytes
 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, 0 buffer failures
 0 aborts, 0 deferred, 0 collisions, 0 late collisions
 0 lost carrier, 0 no carrier

表1-4 display interface 命令显示信息描述表

字段	描述
GigabitEthernet1/0/1	接口GigabitEthernet1/0/1的相关信息
Current state	接口的物理状态，状态可能为： - Administratively DOWN: 表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 - DOWN: 表示该接口的管理状态为开启，但物理状态为关闭（可能因为没有物理连线或者线路故障） - DOWN (Link-Aggregation interface down): 表示该接口所属的聚合接口已经通过 shutdown 命令被关闭 - DOWN (Tunnel-Bundle administratively down): 表示该接口所属的 Tunnel-Bundle 接口已经通过 shutdown 命令被关闭 - DOWN (Monitor-Link uplink down): Monitor Link 联动而导致接口被关闭 - ETH-rddc Shutdown: 表示该接口被冗余组模块关闭，即接口状态为冗余关闭 - mac-address moving down: 由于 MAC 地址迁移抑制导致接口被关闭 - MAD ShutDown: 当 IRF 分裂后，处于 Recovery 状态的 IRF 会将除了保留接口外的所有接口状态设置为 MAD ShutDown - Storm-Constrain: 表示端口上因为组播或广播报文中某类报文的流量大于其上限阈值而被关闭 - STP DOWN: 表示接口由于触发了 STP BPDU 保护而自动关闭 - UP: 该端口的管理状态和物理状态均为开启
Line protocol state	接口的链路层协议状态。其值由链路层经过参数协商决定，取值为： - UP: 表示数据链路层协议状态为开启 - UP(spoofing): 表示该接口的数据链路层协议状态为开启，但实际可能没有对应的链路，或者所对应的链路不是永久存在而是按需建立。通常 NULL、LoopBack 等接口会具有该属性 - DOWN: 表示数据链路层协议状态为关闭 - DOWN(<i>protocols</i>): 表示接口的数据链路层被一个或者多个协议模块关闭。<i>protocols</i> 为 LAGG 和 BFD 的任意组合： - LAGG: 表示聚合接口中没有选中的成员端口而关闭接口的数据链路层 - BFD: 表示由于 BFD 模块检测到链路故障而关闭接口的数据链路层
Description	接口的描述信息
Bandwidth	接口的期望带宽

字段	描述
Maximum transmission unit	接口的MTU
Internet protocol processing: Disabled	接口未配置IP地址，不能处理IP报文
Internet address: <i>ip-address/mask-length</i> (Type)	接口IP地址。<i>Type</i>表示地址获取方式，取值如下： - Primary: 手动配置的主地址 - Sub: 手动配置的从地址。当配置了主地址时，仅显示主地址；仅配置从地址时，才显示本信息 - Unnumbered: 借用其他接口的IP地址 - MAD: 成员设备上配置的MAD IP地址，详细介绍请参见“虚拟化技术配置指导”中的“IRF”  说明 <i>Type</i>的取值情况与接口类型有关，请以实际情况为准
IP packet frame type	IPv4报文发送帧格式
hardware address	接口的MAC地址
IPv6 packet frame type	IPv6报文发送帧格式
Media type is	接口的介质类型
Port hardware type is	接口的硬件类型
Port priority	接口优先级
Loopback is set internal	以太网接口正在进行对内环回测试，该显示信息与用户的配置有关
Loopback is set external	对以太网接口进行对外环回测试，该显示信息与用户的配置有关
Loopback is not set	接口上未配置环回测试，该显示信息与用户的配置有关
10Mbps-speed mode	接口速率为10Mbps，该显示信息与用户的配置以及链路参数的协商结果有关
100Mbps-speed mode	接口速率为100Mbps，该显示信息与用户的配置以及链路参数的协商结果有关
1000Mbps-speed mode	接口速率为1000Mbps，该显示信息与用户的配置以及链路参数的协商结果有关
10Gbps-speed mode	接口速率为10Gbps，该显示信息与用户的配置以及链路参数的协商结果有关
40Gbps-speed mode	接口速率为40Gbps，该显示信息与用户的配置以及链路参数的协商结果有关
Unknown-speed mode	速率未知，可能因为速率协商失败或者接口物理未连通
half-duplex mode	接口工作在半双工模式，该显示信息与用户的配置以及链路参数的协商结果有关
full-duplex mode	接口工作在全双工模式，该显示信息与用户的配置以及链路参数的协商结果有关
unknown-duplex mode	未知双工模式，可能因为双工模式协商失败或者接口物理未连通
Link speed type is autonegotiation	当用户配置了 speed auto 时显示该信息
Link speed type is force link	当用户使用 speed 命令配置了具体的速率时显示该信息，例如1000M等
link duplex type is autonegotiation	当用户配置了 duplex auto 时显示该信息

字段	描述
link duplex type is force link	当用户使用 duplex 命令配置了具体的双工模式时显示该信息，例如 half 或者 full
Flow-control is not enabled	未配置流量控制功能，该显示信息与用户的配置以及链路参数的协商结果有关
Maximum frame length	接口允许通过的最大以太网帧长度
Allow jumbo frame to pass	允许长帧通过
Broadcast max-	广播风暴抑制阈值，可能为 ratio （百分比）、 pps 或者 kbps ，与用户的配置有关
Multicast max-	组播风暴抑制阈值，可能为 ratio （百分比）、 pps 或者 kbps ，与用户的配置有关
Unicast max-	未知单播风暴抑制阈值，可能为 ratio （百分比）、 pps 或者 kbps ，与用户的配置有关
PVID	接口所在的缺省VLAN ID
MDI type	网线类型，取值为 automdix 、 mdi 或 mdix ，与用户的配置有关
Port link-type	链路类型，取值为 access 、 trunk 或 hybrid ，与用户的配置有关
Tagged VLANs	通过该接口后携带Tag的VLAN
UnTagged VLANs	通过该接口后不再携带Tag的VLAN
VLAN Passing	该接口实际可以通过的VLAN（接口允许通过并且已创建的VLAN）
VLAN permitted	接口允许通过的VLAN报文
Trunk port encapsulation	Trunk接口的封装格式
Last link flapping	接口最近一次物理状态改变到现在的时长。 Never 表示接口从设备启动后一直处于 down 状态（没有改变过）
Last clearing of counters	最近一次使用 reset counters interface 命令清除接口下的统计信息的时间（如果从设备启动一直没有执行 reset counters interface 命令清除过该接口下的统计信息，则显示 Never ）
Current system time	当前系统时间，时间显示格式为YYYY/MM/DD HH:MM:SS 如果配置了时区，时间显示格式为YYYY/MM/DD HH:MM:SS UTC±HH:MM:SS
Last time when physical state changed to up	最近一次接口物理状态变为UP的时刻 “-”表示接口物理状态没有发生过变化
Last time when physical state changed to down	最近一次接口物理状态变为DOWN的时刻 “-”表示接口物理状态没有发生过变化
Last 300 second input: 0 packets/sec 0 bytes/sec 0% Last 300 second output: 0 packets/sec 0 bytes/sec 0%	端口在最近300秒接收和发送报文的平均速率，单位分别为数据包/秒和字节/秒，以及实际速率和接口带宽的百分比 如果值显示为“-”，则表示不支持该统计项
Input(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口接收的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项

字段	描述
Input(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口接收的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口接收的正常单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
input errors	端口接收的错误报文的统计值
runts	接收到的超小帧的数量 超小帧是指长度小于64字节、格式正确且包含有效的CRC字段的帧
giants	接收到的超大帧的数量 超大帧是指有效长度大于端口允许通过最大报文长度的帧： - 对于禁止长帧通过的以太网端口，超大帧是指有效长度大于 1518 字节（不带 VLAN Tag）或大于 1522 字节（带 VLAN Tag 报文）的帧 - 对于允许长帧通过的以太网端口，超大帧是指有效长度大于指定最大长帧长度的帧
throttles	接收到的长度为非整数字节的帧的个数
CRC	接收到的CRC校验错误、长度正常的帧的数量
frame	接收到的CRC校验错误、且长度不是整数字节的帧的数量
overruns	当端口的接收速率超过接收队列的处理能力时，导致报文被丢弃
aborts	接收到的非法报文总数，非法报文包括： - 报文碎片：长度小于 64 字节（长度可以为整数或非整数）且 CRC 校验错误的帧 - jabber 帧：有效长度大于端口允许通过的最大报文长度，且 CRC 校验错误的帧（长度可以为整数字节数或非整数字节数）。如对于禁止长帧通过的以太网端口，jabber 帧是指大于 1518（不带 VLAN Tag）或 1522（带 VLAN Tag）字节，且 CRC 校验错误的帧；对于允许长帧通过的以太网端口，jabber 帧是指有效长度大于指定最大长帧长度，且 CRC 校验错误的帧 - 符号错误帧：报文中至少包含 1 个错误的符号 - 操作码未知帧：报文是 MAC 控制帧，但不是 Pause 帧 - 长度错误帧：报文中 802.3 长度字段与报文实际长度（46~1500 字节）不匹配
ignored	由于端口接收缓冲区不足等原因而丢弃的报文数量
parity errors	接收到的奇偶校验错误的帧的数量
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送报文的统计值，包括正常报文、异常报文和正常PAUSE帧的报文数、字节数 端口发送的单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	端口发送的正常报文的统计值，包括正常报文和正常PAUSE帧的报文数、字节数 端口发送的正常单播报文、广播报文、组播报文和PAUSE帧的数量 如果值显示为“-”，则表示不支持该统计项
output errors	各种发送错误的报文总数

字段	描述
underruns	当端口的发送速率超过了发送队列的处理能力，导致报文被丢弃，是一种非常罕见的硬件异常
buffer failures	由于端口发送缓冲区不足而丢弃的报文数量
aborts	发送失败的报文总数，即报文已经开始发送，但由于各种原因（如冲突）而导致发送失败
deferred	延迟报文的数量，延迟报文是指发送前检测到冲突而被延迟发送的报文
collisions	冲突帧的数量，冲突帧是指在发送过程中检测到冲突的而停止发送的报文
late collisions	延迟冲突帧的数量，延迟冲突帧是指帧的前512 bits已经被发送，由于检测到冲突，该帧被延迟发送
lost carrier	（暂不支持）载波丢失，一般适用于串行WAN接口，发送过程中，每丢失一个载波，此计数器加一
no carrier	（暂不支持）无载波，一般适用于串行WAN接口，当试图发送帧时，如果没有载波出现，此计数器加一
Peak input rate	接口输入流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间
Peak output rate	接口输出流量的峰值速率大小（单位为bytes/sec）以及峰值产生的时间

显示所有接口的概要信息。

```
<Sysname> display interface brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
```

Interface	Link	Protocol	Primary IP	Description
GE1/0/1	DOWN	DOWN	--	
Loop0	UP	UP(s)	2.2.2.9	
NULL0	UP	UP(s)	--	
Vlan1	UP	UP	--	
Vlan999	UP	UP	192.168.1.42	

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
```

```
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
```

Interface	Link	Speed	Duplex	Type	PVID	Description
GE1/0/2	DOWN	auto	A	A	1	
GE1/0/3	UP	1G(a)	F(a)	A	1	aaaaaaaaaaaaaaaaaaaaaaaaaaaaa

显示接口 GigabitEthernet1/0/1 的概要信息，包括用户配置的全部描述信息。

```
<Sysname> display interface gigabitethernet 1/0/1 brief description
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
```



```

Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface          Link Speed  Duplex Type PVID Description
GE1/0/1            UP    1G(a)   F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

```

显示当前物理状态为 down 的接口的信息以及 down 的原因。

```

<Sysname> display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
GE1/0/1             DOWN Not connected
Vlan2               DOWN Not connected

```

```

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
GE1/0/2             DOWN Not connected

```

表1-5 display interface brief 命令显示信息描述表

字段	描述
Brief information on interfaces in route mode:	三层模式下（route）接口的概要信息，即三层接口的概要信息
Link: ADM - administratively down; Stby - standby	- 如果某接口的 Link 属性值为“ADM”，则表示该接口被管理员通过 shutdown 命令关闭，需要在该接口下执行 undo shutdown 命令才能恢复接口本身的物理状态 - 如果某接口的 Link 属性值为“Stby”，则表示该接口是一个处于 Standby 状态的备份接口，使用 display interface-backup state 命令可以查看该备份接口对应的主接口
Protocol: (s) - spoofing	如果某接口的 Protocol 属性值中带有“(s)”，则表示该接口的数据链路层协议状态显示为 UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的。通常 NULL、LoopBack 等接口会具有该属性
Interface	接口名称缩写
Link	接口物理连接状态，取值为： - UP: 表示接口物理上是连通的 - DOWN: 表示接口物理上不通 - ADM: 表示接口被管理员通过 shutdown 命令关闭，需要执行 undo shutdown 命令才能恢复接口本身的物理状态 - Stby: 表示该接口是一个处于 Standby 状态的备份接口
Protocol	接口数据链路层协议状态，取值为： - UP: 表示接口的数据链路层协议状态为开启 - DOWN: 表示接口的数据链路层协议状态为关闭 - UP(s): 表示接口的数据链路层协议状态显示为 UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的。通常 NULL、LoopBack 等接口会取该值
Primary IP	接口主 IP 地址。取值为“--”时，表示接口尚未配置 IP 地址

字段	描述
Description	接口的描述信息
Brief information of interfaces in bridge mode:	二层模式下（bridge）的接口概要信息，即二层接口的概要信息
Speed: (a) - auto	如果某接口的Speed属性值为“(a)”，则表示该接口的速率是通过自动协商获取的 如果某接口的Speed属性值为“auto”，则表示该接口的速率是通过自动协商获取的，但协商还未开始
Duplex: (a)/A - auto; H - half; F - full	如果某接口的Duplex属性值为“(a)”或者“A”，则表示该接口的Duplex属性是通过自动协商获取的；取值为“H”则表示为半双工；取值为“F”则表示为全双工 当显示为“A”时表示该接口的Duplex属性是通过自动协商获取的，但协商还未开始
Type: A - access; T - trunk; H - hybrid	接口的链路类型： • A: 表示 Access 链路类型 • H: 表示 Hybrid 链路类型 • T: 表示 Trunk 链路类型
Speed	接口的速率，单位为bps
Duplex	接口的双工模式，取值为： • A: 表示双工模式由自动协商结果决定 • F: 表示全双工 • F(a): 表示自由协商的结果为全双工 • H: 表示半双工 • H(a): 表示自由协商的结果为半双工
Type	接口的链路类型： • A: 表示 Access 链路类型 • H: 表示 Hybrid 链路类型 • T: 表示 Trunk 链路类型
PVID	接口所在的缺省VLAN ID

字段	描述
Cause	接口物理连接状态为down的原因，取值为： • Administratively: 表示本链路被手工关闭了（配置了 shutdown 命令），需要执行 undo shutdown 命令才能恢复真实的物理状态 • DOWN (Link-Aggregation interface down): 聚合接口被关闭后，该聚合接口的所有成员端口的状态会显示为 DOWN，down 的原因会显示为 DOWN (Link-Aggregation interface down) • DOWN (Loopback detection down): 由于环路检测模块检测到环路而自动关闭接口 • DOWN (Monitor-Link uplink down): 由于 Monitor Link 模块检测到上行链路 down 而自动关闭接口 • MAD ShutDown: 当 IRF 分裂后，处于 Recovery 状态的 IRF 会将除了保留接口外的所有接口状态设置为 DOWN，down 的原因会显示为 MAD ShutDown • Not connected: 表示没有物理连接（可能没有插网线或者网线故障） • Storm-Constrain: 表示端口上因为组播或广播报文中某类报文的流量大于其上限阈值而被关闭 • STP DOWN: 由于触发了 STP BPDU 保护而自动关闭接口 • Standby: 表示接口处于备份状态

【相关命令】

- **reset counters interface**

1.1.11 display packet-drop

display packet-drop 命令用来显示接口丢弃的报文的信息。

【命令】

```
display packet-drop { interface [ interface-type [ interface-number ] ] | summary }
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

interface-type: 指定接口类型。

interface-number: 指定接口编号。

summary: 将所有接口丢弃报文的统计信息累计后再显示。

【使用指导】

如果不指定接口类型和接口编号，显示所有接口丢弃的报文的信息。
如果仅指定接口类型，显示该类型所有接口丢弃的报文的信息。

【举例】

```
# 显示接口 GigabitEthernet1/0/1 丢弃报文的信息。
<Sysname> display packet-drop interface gigabitethernet 1/0/1
GigabitEthernet1/0/1:
Packets dropped due to full GBP or insufficient bandwidth: 301
Packets dropped due to Fast Filter Processor (FFP): 261
Packets dropped due to STP non-forwarding state: 0
Packets dropped due to rate-limit: 143
Packets dropped due to broadcast-suppression: 301
Packets dropped due to unicast-suppression: 215
Packets dropped due to multicast-suppression: 241
Packets dropped due to Tx packet aging: 246
# 将所有接口丢弃报文的统计信息累计后再显示。
<Sysname> display packet-drop summary
All interfaces:
Packets dropped due to full GBP or insufficient bandwidth: 301
Packets dropped due to Fast Filter Processor (FFP): 261
Packets dropped due to STP non-forwarding state: 0
Packets dropped due to rate-limit: 143
Packets dropped due to broadcast-suppression: 301
Packets dropped due to unicast-suppression: 215
Packets dropped due to multicast-suppression: 241
Packets dropped due to Tx packet aging: 246
```

表1-6 display packet-drop 命令显示信息描述表

字段	描述
Packets dropped due to full GBP or insufficient bandwidth	由于芯片缓存满或者带宽不够导致的丢包数
Packets dropped due to Fast Filter Processor (FFP)	由于数据包被过滤所导致的丢包数
Packets dropped due to STP non-forwarding state	由于STP协议状态为discarding导致的丢包数
Packets dropped due to rate-limit	由于速率限制导致的丢包数
Packets dropped due to broadcast-suppression	由于广播抑制导致的丢包数
Packets dropped due to unicast-suppression	由于未知单播抑制导致的丢包数
Packets dropped due to multicast-suppression	由于组播抑制导致的丢包数
Packets dropped due to Tx packet aging	由于出方向报文超时导致的丢包数

1.1.12 duplex

duplex 命令用来设置以太网接口的双工模式。

undo duplex 命令用来恢复缺省情况。

【命令】

```
duplex { auto | full | half }  
undo duplex
```

【缺省情况】

以太网接口的双工模式为 **auto**（自协商）状态。

【视图】

以太网接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

auto: 接口与对端接口自动协商双工状态。
full: 全双工状态，接口在发送数据包的同时可以接收数据包。
half: 半双工状态，接口同一时刻只能发送数据包或接收数据包。

【举例】

```
# 将以太网接口 GigabitEthernet1/0/1 接口设置为全双工状态。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] duplex full
```

1.1.13 flow-control

flow-control 命令用来开启以太网接口的流量控制功能。

undo flow-control 命令用来关闭以太网接口流量控制功能。

【命令】

```
flow-control  
undo flow-control
```

【缺省情况】

以太网接口的流量控制功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

配置 **flow-control** 命令后，设备具有发送和接收流量控制报文的能力：

- 当本端发生拥塞时，设备会向对端发送流量控制报文。
- 当本端收到对端的流量控制报文后，会停止报文发送。

只有本端和对端设备都开启了流量控制功能，才能实现对本端以太网接口的流量控制。

【举例】

开启以太网接口 GigabitEthernet1/0/1 的流量控制功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-control
```

1.1.14 flow-interval

flow-interval 命令用来配置接口统计报文信息的时间间隔。

undo flow-interval 命令用来恢复缺省情况。

【命令】

```
flow-interval interval
undo flow-interval
```

【缺省情况】

接口统计报文信息的时间间隔为 300 秒。

【视图】

以太网接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interval: 接口统计信息的时间间隔值，取值范围为 5~300，单位为秒，步长为 5（即取值必须为 5 的整数倍）。

【使用指导】

Context 中的共享接口不支持该命令。

【举例】

设置以太网接口 GigabitEthernet1/0/1 的统计信息时间间隔为 100 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-interval 100
```

1.1.15 interface

interface 命令用来进入接口视图或创建子接口并进入子接口视图。如果指定的子接口已经存在，则直接进入子接口视图。

【命令】

interface *interface-type* { *interface-number* | *interface-number.subnumber* }

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type: 指定接口类型。

interface-number: 指定接口编号。

interface-number.subnumber: 指定子接口编号。其中 *interface-number* 为主接口编号；*subnumber* 为子接口编号，取值范围为 1~4094。

【举例】

进入以太网接口 GigabitEthernet1/0/1 视图。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1]
```

创建以太网子接口 GigabitEthernet1/0/1.1 并进入该子接口的视图。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1.1
```

```
[Sysname-GigabitEthernet1/0/1.1]
```

1.1.16 jumboframe enable

jumboframe enable 命令用来允许超长帧通过。

undo jumboframe enable 命令用来禁止超长帧通过。

undo jumboframe enable size 命令用来恢复缺省情况。

【命令】

jumboframe enable [*size*]

undo jumboframe enable [*size*]

【缺省情况】

以太网接口上允许通过的超长帧的最大长度为 9216 字节。

【视图】

二层以太网接口视图

三层以太网接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

size: 以太网接口上允许通过的超长帧的最大长度，单位为字节，取值范围为 1～9216。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 允许超长帧通过以太网接口 GigabitEthernet1/0/1。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] jumboframe enable
```

1.1.17 loopback



说明

开启环回功能后，接口将不能正常转发数据包，请按需配置。

loopback 命令用来开启以太网接口的环回功能。

undo loopback 命令用来关闭以太网接口的环回功能。

【命令】

```
loopback { external | internal }  
undo loopback
```

【缺省情况】

以太网接口的环回功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

external: 开启以太网接口的外部环回功能。

internal: 开启以太网接口的内部环回功能。

【使用指导】

开启环回功能后，接口将自动切换到全双工模式，关闭环回功能后会自动恢复原有双工模式。

shutdown 和 **loopback** 命令互斥，后配置的失败。

【举例】

```
# 开启以太网接口 GigabitEthernet1/0/1 的内部环回功能。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1
```



```
[Sysname-GigabitEthernet1/0/1] loopback internal
```

1.1.18 multicast-suppression

multicast-suppression 命令用来开启端口组播风暴抑制功能，并设置组播风暴抑制阈值。

undo multicast-suppression 命令用来关闭端口组播风暴抑制功能。

【命令】

multicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo multicast-suppression

【缺省情况】

所有接口不对组播流量进行抑制。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ratio: 指定以太网接口允许通过的最大组播流量占该接口带宽的百分比。取值范围为 0~100。数值越小，则允许通过的组播流量也越小。

pps max-pps: 指定以太网接口每秒最多通过的组播包包数，取值范围为 0~1.4881×接口带宽。

kbps max-kbps: 指定以太网接口每秒最多通过的组播流量，单位为 kbps，取值范围为 0~接口带宽。

【使用指导】

本命令设置的是接口允许通过的最大组播报文流量。当接口上的组播流量超过用户设置的值后，系统将丢弃超出组播流量限制的报文，从而使接口组播流量所占的比例控制在限定的范围内，以便保证业务的正常运行。

执行 **multicast-suppression** 或 **storm-constrain** 命令都能开启端口的组播风暴抑制功能，**storm-constrain** 命令通过软件对组播报文进行抑制，对设备性能有一定影响，**multicast-suppression** 通过芯片物理上对组播报文进行抑制，相对 **storm-constrain** 来说，对设备性能影响较小。请不要同时配置 **multicast-suppression** 和 **storm-constrain** 命令，以免配置冲突，导致抑制效果不确定。

当风暴抑制阈值配置为 **pps** 或 **kbps** 时，设备可能会根据芯片支持的步长，将配置值转换成步长的倍数。所以，端口下配置的抑制阈值可能与实际生效抑制阈值不一致，请注意查看设备的提示信息。

【举例】

在以太网接口 GigabitEthernet1/0/1 上，每秒最多允许 10000kbps 组播报文通过，对超出该范围的组播报文进行抑制。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] multicast-suppression kbps 10000
```

```
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

以上信息表示：用户配置的值为 10000kbps，因为芯片支持的步长为 64，所以实际生效的值为 10048kbps（64 的 157 倍）。

【相关命令】

- **broadcast-suppression**
- **unicast-suppression**

1.1.19 port link-mode

port link-mode 命令用来切换以太网接口的工作模式。

undo port link-mode 命令用来恢复缺省情况。

【命令】

```
port link-mode { bridge | route }  
undo port link-mode
```

【缺省情况】

以太网接口工作在三层模式。

【视图】

以太网接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

bridge：工作在二层模式。

route：工作在三层模式。

【使用指导】

基于业务板的硬件构造，设备上的某些接口只能作为二层以太网接口；某些接口只能作为三层以太网接口；某些接口比较灵活，工作模式可以通过命令行设置。如果将工作模式设置为二层模式（**bridge**），则作为一个二层以太网接口使用，如果将工作模式设置为三层模式（**route**），则作为一个三层以太网接口使用。

接口模式切换后，除了 **shutdown** 和 **combo enable** 命令，该以太网接口下的其它所有命令都将恢复到新模式下的缺省情况。

【举例】

```
# 使接口 GigabitEthernet1/0/1 工作在二层模式。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] port link-mode bridge
```

1.1.20 reset counters interface

reset counters interface 命令用来清除接口的统计信息。

【命令】

reset counters interface [*interface-type* [*interface-number*]]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type: 指定接口类型。

interface-number: 指定接口编号。

【使用指导】

在某些情况下，需要统计一定时间内某接口的流量，这就需要在统计开始前清除该接口原有的统计信息，重新进行统计。

如果不指定 *interface-type* 和 *interface-number*，则清除所有接口的统计信息。

如果指定 *interface-type* 而不指定 *interface-number*，则清除所有该类型接口的统计信息。

【举例】

清除以太网接口 GigabitEthernet1/0/1 的统计信息。

```
<Sysname> reset counters interface gigabitethernet 1/0/1
```

【相关命令】

- **display interface**
- **display counters interface**
- **display counters rate interface**

1.1.21 reset ethernet statistics

reset ethernet statistics 命令用来清除以太网软件模块收发报文的统计信息。

【命令】

reset ethernet statistics [*slot slot-number*]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot slot-number: 清除指定成员设备的统计信息，*slot-number* 表示设备在 IRF 中的成员编号。不指定该参数时，表示所有成员设备。

【举例】

清除指定 slot 上的以太网软件模块收发报文的统计信息。

```
<Sysname> reset ethernet statistics slot 1
```

【相关命令】

- **display ethernet statistics**

1.1.22 reset packet-drop interface

reset packet-drop interface 命令用来清除接口丢弃报文的统计信息。

【命令】

```
reset packet-drop interface [ interface-type [ interface-number ] ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type: 指定接口类型。

interface-number: 指定接口编号。

【使用指导】

如果不指定接口类型和接口编号，则清除所有接口丢弃的报文的信息。

如果仅指定接口类型，则清除所有该类型接口丢弃的报文的信息。

【举例】

清除以太网接口 GigabitEthernet1/0/1 丢弃报文的统计信息。

```
<Sysname> reset packet-drop interface gigabitethernet 1/0/1
```

清除所有接口丢弃报文的统计信息。

```
<Sysname> reset packet-drop interface
```

【相关命令】

- **display packet-drop**

1.1.23 shutdown

shutdown 命令用来关闭以太网接口/子接口。

undo shutdown 命令用来打开以太网接口/子接口。

【命令】

shutdown

undo shutdown

【缺省情况】

以太网接口/子接口处于开启状态。

【视图】

以太网接口视图

以太网子接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

在某些特殊情况下（例如修改接口的工作参数），接口相关配置不能立即生效，需要关闭再打开接口后，才能生效。

shutdown 和 **loopback** 命令互斥，后配置的失败。

【举例】

关闭以太网接口 GigabitEthernet1/0/1 后打开该接口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] shutdown
[Sysname-GigabitEthernet1/0/1] undo shutdown
```

关闭以太网子接口 GigabitEthernet1/0/1.1 后打开该接口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1.1
[Sysname-GigabitEthernet1/0/1.1] shutdown
[Sysname-GigabitEthernet1/0/1.1] undo shutdown
```

1.1.24 speed

speed 命令用来设置以太网接口的速率。

undo speed 命令用来恢复缺省情况。

【命令】

```
speed { 10 | 100 | 1000 | 10000 | 40000 | auto }
undo speed
```

【缺省情况】

以太网接口速率处于自协商状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

10: 表示接口速率为 10Mbps。

100: 表示接口速率为 100Mbps。

1000: 表示接口速率为 1000Mbps。

10000: 表示接口速率为 10000Mbps。

40000: 表示接口速率为 40000Mbps。

本参数的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	不支持
T5000-G30	支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	不支持
T1000-CN60/T1000-CN80	不支持

auto: 表示接口速率处于自协商状态。

【使用指导】

对于以太网电口来说，使用 **speed** 命令设置端口速率，目的是使其与对端进行速率匹配。

对于光口来说，使用 **speed** 命令设置端口速率，目的是使其与可插拔光模块进行速率匹配。

不同类型的接口支持配置的参数不同，具体情况请在相关接口视图下执行 **speed ?** 命令查看。

【举例】

将以太网接口 GigabitEthernet1/0/1 的速率设置为自协商获得。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] speed auto
```

1.1.25 sub-interface rate-statistic

sub-interface rate-statistic 命令用来开启以太网接口/子接口的速率统计功能。

undo sub-interface rate-statistic 命令用来关闭接口/子接口的速率统计功能。

【命令】

sub-interface rate-statistic

undo sub-interface rate-statistic

【缺省情况】

以太网接口/子接口的速率统计功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启本功能后可能需要耗费大量系统资源，请谨慎使用。

【举例】

开启 GigabitEthernet1/0/1 接口的子接口速率统计功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sub-interface rate-statistic
This configuration may make a negative effect on the performance. Are you sure to continue?
[Y/N]:y
```

1.1.26 unicast-suppression

unicast-suppression 命令用来开启端口未知单播风暴抑制功能，并设置未知单播风暴抑制阈值。

undo unicast-suppression 命令用来关闭端口未知单播风暴抑制功能。

【命令】

```
unicast-suppression { ratio | pps max-pps | kbits max-kbps }
undo unicast-suppression
```

【缺省情况】

所有接口不对未知单播流量进行抑制。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ratio: 指定以太网接口最大未知单播流量占该接口带宽的百分比。取值范围为 0~100。数值越小，则允许通过的未知单播流量也越小。

pps max-pps: 指定以太网接口每秒最多通过的未知单播包包数，取值范围为 0~1.4881×接口带宽。

kbits max-kbps: 指定以太网接口每秒通过的未知单播流量，单位为 kbps，取值范围为 0~接口带宽。

【使用指导】

本命令设置的是接口允许通过的最大未知单播报文流量。当接口上的未知单播流量超过用户设置的值后，系统将丢弃超出未知单播流量限制的报文，从而使接口未知单播流量所占的比例降低到限定的范围，保证网络业务的正常运行。

当风暴抑制阈值配置为 **pps** 或 **kbits** 时，设备可能会根据芯片支持的步长，将配置值转换成步长的倍数。所以，端口下配置的抑制阈值可能与实际生效抑制阈值不一致，请注意查看设备的提示信息。

【举例】

在以太网接口 GigabitEthernet1/0/1 上，每秒最多允许 10000kbps 未知单播报文通过，对超出该范围的未知单播报文进行抑制。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] unicast-suppression kbps 10000
The actual value is 10048 on port GigabitEthernet1/0/1 currently.
```

以上信息表示：用户配置的值 10000kbps，因为芯片支持的步长为 64，所以实际生效的值为 10048kbps（64 的 157 倍）。

【相关命令】

- **broadcast-suppression**
- **multicast-suppression**

1.2 二层以太网接口的配置命令

1.2.1 display storm-constrain

display storm-constrain 命令用来显示接口流量控制信息。

【命令】

```
display storm-constrain [ broadcast | multicast ] [ interface interface-type interface-number ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

broadcast：只显示广播报文流量控制信息。

multicast：只显示组播报文流量控制信息。

interface *interface-type* *interface-number*：显示指定接口的报文流量控制信息。
interface-type interface-number 指定接口类型和接口编号。不指定该参数时，显示所有接口报文的流量控制信息。

【使用指导】

不指定 **broadcast** 和 **multicast** 参数时，则显示所有类型报文的流量控制信息。

【举例】

显示系统当前所有接口的流量控制信息。

```
<Sysname> display storm-constrain
```


Abbreviation: BC - broadcast; MC - multicast; UC - unicast;
FW - forwarding

Flow Statistic Interval: 5 (in seconds)

Port	Type	Lower	Upper	Unit	Mode	Status	Trap	Log	StateChg
GE1/0/1	MC	100	200	kbps	shutdown	shutdown	off	on	10

表1-7 display storm-constrain 命令显示信息描述表

字段	描述
Flow Statistic Interval	流量统计的时间间隔，单位为秒
Port	接口名称缩写
Type	进行流量阈值控制的报文类型： - BC: broadcast, 表示广播报文 - MC: multicast, 表示组播报文 - UC: unicast, 表示未知单播报文（暂不支持）
Lower	用户配置的流量控制下限阈值或百分比
Upper	用户配置的流量控制上限阈值或百分比
Unit	用户配置的流量阈值的单位，为pps、kbps或百分比
Mode	用户配置的流量阈值超过上限的控制动作： - block 表示阻塞方式 - shutdown 表示关闭方式 - N/A 表示未配置控制动作
Status	接口报文转发状态，取值为： - FW 表示该端口处于正常转发状态 - shutdown 表示端口已被关闭 - block 表示该端口对该类报文直接丢弃
Trap	Trap信息输出开关： - on 表示打开 - off 表示关闭
Log	Log信息输出开关： - on 表示打开 - off 表示关闭
StateChg	接口报文转发状态切换次数 当StateChg达到65535次时，会自动跳转到0，重新计数

1.2.2 mdix-mode



说明

光口不支持本命令。

mdix-mode 命令用来设置以太网接口的 MDIX 模式。

undo mdix-mode 命令用来恢复缺省情况。

【命令】

```
mdix-mode { automdix | mdi | mdix }  
undo mdix-mode
```

【缺省情况】

以太网接口的 MDIX 模式为 **automdix**。

【视图】

二层以太网接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

automdix: 两端设备通过协商来决定引脚 1 和 2 是发送还是接收信号，引脚 3 和 6 是接收还是发送信号。

mdi: 使用引脚 1 和 2 发送信号，使用引脚 3 和 6 接收信号。

mdix: 使用引脚 1 和 2 接收信号，使用引脚 3 和 6 发送信号。

【举例】

设置以太网接口 GigabitEthernet1/0/1 的 MDIX 模式为 **automdix**。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mdix-mode automdix
```

1.2.3 storm-constrain

storm-constrain 命令用来开启端口流量阈值控制功能，并设置上限阈值与下限阈值。

undo storm-constrain 命令用来关闭端口流量阈值控制功能。

【命令】

```
storm-constrain { broadcast | multicast } pps upperlimit lowerlimit  
undo storm-constrain { all | broadcast | multicast }
```

【缺省情况】

端口流量阈值控制功能处于关闭状态，即不对端口的报文流量进行抑制。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

all: 取消端口所有类型（组播和广播）报文流量阈值配置。

broadcast: 设置端口广播报文流量阈值。

multicast: 设置端口组播报文流量阈值。

pps: 以包每秒为单位统计流量。

upperlimit: 端口报文流量的上限阈值。当和 **pps** 一起使用时，该参数的取值范围为 0~1.4881×接口带宽。

lowerlimit: 端口报文流量的下限阈值。当和 **pps** 一起使用时，该参数的取值范围为 0~1.4881×接口带宽。

【使用指导】

执行本命令后，设备就会周期性地对接口收到的指定类型的报文进行统计，如果流量超过上限阈值，则采取一定的措施。其中，通过 **storm-constrain interval** 命令可以配置统计周期，通过 **storm-constrain control** 命令可以配置流量超过上限阈值时采取的控制方式。

执行 **storm-constrain** 与 **broadcast-suppression**、**multicast-suppression**、**unicast-suppression** 命令都能开启端口的风暴抑制功能。**storm-constrain** 命令通过软件对报文流量进行抑制，对设备性能有一定影响，**broadcast-suppression**、**multicast-suppression**、**unicast-suppression** 通过芯片物理上对报文流量进行抑制，相对 **storm-constrain** 来说，对设备性能影响较小。对于某种类型的报文流量，请不要同时配置这两种方式，以免配置冲突，导致抑制效果不确定。

配置时，**upperlimit** 值必须大于 **lowerlimit** 值，建议不要配成相等值。

【举例】

对 GigabitEthernet1/0/1 端口配置广播报文流量阈值，上限阈值为 200pps、下限阈值为 150pps。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] storm-constrain broadcast pps 200 150
```

【相关命令】

- **storm-constrain control**
- **storm-constrain interval**

1.2.4 storm-constrain control

storm-constrain control 命令用来设置端口组播或者广播流量超过上限阈值时采取的控制方式。

undo storm-constrain control 命令用来恢复缺省情况。

【命令】

```
storm-constrain control { block | shutdown }  
undo storm-constrain control
```

【缺省情况】

不对端口流量进行控制。

【视图】

二层以太网接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

block: block 方式，即：当端口上组播或广播报文中某类报文的流量大于其上限阈值时，端口将暂停转发该类报文（其它类型报文照常转发），端口处于阻塞状态，但仍会统计该类报文的流量。当该类报文的流量小于其下限阈值时，端口将自动恢复对此类报文的转发。

shutdown: shutdown 方式，即：当端口上组播或广播报文中某类报文的流量大于其上限阈值时，端口将被关闭，系统停止转发所有报文。当该类报文的流量小于其下限阈值时，端口状态不会自动恢复，此时可通过执行 **undo shutdown** 命令或取消端口上流量阈值的配置来恢复。

【举例】

```
# 配置 GigabitEthernet1/0/1 端口，当流量超过上限阈值时，采用 block 方式控制。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] storm-constrain control block
```

【相关命令】

- **storm-constrain**
- **storm-constrain control**

1.2.5 storm-constrain enable log

storm-constrain enable log 命令用来配置端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Log 信息。

undo storm-constrain enable log 命令用来禁止端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Log 信息。

【命令】

```
storm-constrain enable log  
undo storm-constrain enable log
```

【缺省情况】

端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Log 信息。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

context-admin

【举例】

当 GigabitEthernet1/0/1 端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Log 信息。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] storm-constrain enable log
```

1.2.6 storm-constrain enable trap

storm-constrain enable trap 命令用来配置端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Trap 信息。

undo storm-constrain enable trap 命令用来禁止端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Trap 信息。

【命令】

storm-constrain enable trap

undo storm-constrain enable trap

【缺省情况】

端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Trap 信息。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

context-admin

【举例】

当 GigabitEthernet1/0/1 端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Trap 信息。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] storm-constrain enable trap
```

1.2.7 storm-constrain interval

storm-constrain interval 命令用来配置端口流量阈值控制模块流量统计的时间间隔。

undo storm-constrain interval 命令用来恢复缺省情况。

【命令】

```
storm-constrain interval interval  
undo storm-constrain interval
```

【缺省情况】

端口流量统计的时间间隔为 10 秒。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

interval: 端口流量统计的时间间隔，取值范围为 1~300，单位为秒。为了保持网络状态的稳定，建议设置的时间间隔不低于 10 秒。

【使用指导】

本命令设置的时间间隔专门为 **storm-constrain** 命令服务的，不同于 **flow-interval** 命令设置的时间间隔。虽然同样是统计端口流量，但是功能是分开的。

【举例】

```
# 配置端口流量统计时间间隔为 60 秒。  
<Sysname> system-view  
[Sysname] storm-constrain interval 60
```

【相关命令】

- **storm-constrain**
- **storm-constrain control**

1.3 三层以太网接口/子接口的配置命令

1.3.1 mac-address

mac-address 命令用来配置以太网接口的 MAC 地址。

undo mac-address 命令用来恢复缺省情况。

【命令】

```
mac-address mac-address  
undo mac-address
```

【缺省情况】

未配置以太网接口的 MAC 地址。

【视图】

三层以太网接口视图

三层以太网子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

mac-address: MAC 地址，形式为 H-H-H。

【使用指导】

配置三层以太网子接口 MAC 地址时，子接口与主接口 MAC 地址不可使用同一地址。

【举例】

```
# 配置三层以太网接口 GigabitEthernet1/0/1 的 MAC 地址为 0001-0001-0001。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mac-address 1-1-1
```

1.3.2 mac-address-filter enable

mac-address-filter enable 命令用来开启目的 MAC 地址过滤功能。

undo mac-address-filter enable 命令用来关闭目的 MAC 地址过滤功能。

【命令】

mac-address-filter enable
undo mac-address-filter enable

【视图】

系统视图

【缺省情况】

目的 MAC 地址过滤功能处于开启状态。

【缺省用户角色】

network-admin

【使用指导】

开启目的 MAC 地址过滤功能后，若三层以太网接口、三层以太网子接口、三层以太网聚合接口和三层以太网冗余接口收到报文的目的 MAC 地址是该接口的 MAC 地址，则接收此报文，并进行后续处理；否则，直接丢弃此报文。

关闭目的 MAC 地址过滤功能后，三层以太网接口、三层以太网子接口、三层以太网聚合接口和三层以太网冗余接口不检查收到报文的目的 MAC 地址，直接接收该报文，并进行后续处理。通常情况下使用缺省配置即可。

此功能只对三层以太网接口、三层以太网子接口、三层以太网聚合接口和三层以太网冗余接口生效。

目的 MAC 地址过滤功能与配置冗余接口 MAC 地址功能互斥，不能同时配置。关于冗余接口 MAC 地址的详细介绍请参见“可靠性命令参考”中的“以太网冗余接口”。

【举例】

```
# 开启目的 MAC 地址过滤功能。  
<Sysname> system-view  
[Sysname] mac-address-filter enable
```

1.3.3 mtu

mtu 命令用来设置三层以太网接口/子接口的 MTU 值。

undo mtu 命令用来恢复缺省情况。

【命令】

```
mtu size  
undo mtu
```

【缺省情况】

三层以太网接口/子接口的 MTU 值为 1500 字节。

【视图】

三层以太网接口视图
三层以太网子接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

size: 以太网接口允许通过的 MTU 的大小，取值范围取决于接口的类型，单位为字节。

【举例】

```
# 设置三层以太网接口 GigabitEthernet1/0/1 的最大传输单元为 1430 字节。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] mtu 1430  
# 设置三层以太网子接口 GigabitEthernet1/0/1.1 的最大传输单元为 1430 字节。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1.1  
[Sysname-GigabitEthernet1/0/1.1] mtu 1430
```


目 录

1 LoopBack接口、NULL接口和InLoopBack接口	1-1
1.1 LoopBack接口、NULL接口和InLoopBack接口配置命令	1-1
1.1.1 bandwidth	1-1
1.1.2 default	1-1
1.1.3 description	1-2
1.1.4 display interface inloopback	1-3
1.1.5 display interface loopback	1-5
1.1.6 display interface null	1-8
1.1.7 interface loopback	1-9
1.1.8 interface null	1-10
1.1.9 reset counters interface loopback	1-11
1.1.10 reset counters interface null	1-11
1.1.11 shutdown	1-12

1 LoopBack接口、NULL接口和InLoopBack接口

1.1 LoopBack接口、NULL接口和InLoopBack接口配置命令

1.1.1 bandwidth

bandwidth 命令用来配置接口的期望带宽。

undo bandwidth 命令用来恢复缺省情况。

【命令】

bandwidth *bandwidth-value*

undo bandwidth

【缺省情况】

LoopBack 接口的期望带宽为 0kbps。

【视图】

LoopBack 接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

bandwidth-value: 表示接口的期望带宽，取值范围为 1~400000000，单位为 kbps。

【使用指导】

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

【举例】

配置 LoopBack0 的期望带宽为 1000kbps。

```
<Sysname> system-view
```

```
[Sysname] interface loopback 0
```

```
[Sysname-LoopBack0] bandwidth 1000
```

1.1.2 default

default 命令用来恢复接口的缺省配置。

【命令】

default

【视图】

LoopBack 接口视图

NULL 接口视图

【缺省用户角色】

network-admin
context-admin

【使用指导】



注意

接口下的某些配置恢复到缺省情况后，会对设备上当前运行的业务产生影响。建议您在执行该命令前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

【举例】

```
# 将 LoopBack0 恢复为缺省配置。  
<Sysname> system-view  
[Sysname] interface loopback 0  
[Sysname-LoopBack0] default
```

1.1.3 description

description 命令用来设置接口的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text  
undo description
```

【缺省情况】

接口的描述信息为“接口名 Interface”，比如：LoopBack0 Interface。

【视图】

LoopBack 接口视图
NULL 接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

text: 接口的描述信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

当设备上存在多个接口时，可以根据接口的连接信息或用途来配置接口的描述信息，以便区别和管理各接口。

配置的描述信息可通过命令行 **display interface** 查看。

【举例】

```
# 设置 LoopBack0 的描述信息为 “for RouterID”。
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] description for RouterID
```

1.1.4 display interface inloopback

display interface inloopback 命令用来显示 InLoopBack 接口的相关信息。

【命令】

display interface [inloopback [0]] [brief [description | down]]

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

inloopback [0]: InLoopBack 接口的编号。如果不指定 **inloopback** 参数，将显示所有接口的相关信息。

brief: 显示接口的概要信息。不指定该参数时，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果某接口的描述信息超过 27 个字符，不指定该参数时，只显示描述信息中的前 27 个字符，超出部分不显示。对于 InLoopBack 接口，因为其描述信息只能为 InLoopBack0 Interface，不能配置，所以，该参数对 InLoopBack 接口无意义。

down: 显示当前物理状态为 down 的接口的信息以及 down 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【使用指导】

因为设备只支持一个 InLoopBack 接口 InLoopBack0，所以不管是否指定 **0** 参数，显示的都是 InLoopBack0 的相关信息。

【举例】

```
# 显示指定接口 InLoopBack0 的相关信息。
<Sysname> display interface inloopback
InLoopBack0
Current state: UP
Line protocol state: UP(spoofing)
Description: InLoopBack0 Interface
Maximum transmission unit: 1536
Physical: InLoopBack
```

Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
 Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
 Input: 0 packets, 0 bytes, 0 drops
 Output: 0 packets, 0 bytes, 0 drops

表1-1 display interface inloopback 命令显示信息描述表

字段	描述
Current state	接口当前的物理层状态。始终为UP，表示接口能收发报文
Line protocol state	链路层协议状态。始终为UP(spoofing)，表示接口的链路层协议状态为UP，但实际可能没有对应的链路，或者对应的链路不是永久存在，而是按需建立的
Description	接口的描述信息。只能为InLoopBack0 Interface，不可配置
Maximum transmission unit	接口的MTU
Physical: InLoopBack	接口的物理类型是InLoopBack
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最近300秒钟的平均输入速率（只有接口支持统计功能时才显示该信息）： - bytes/sec 表示平均每秒输入的字节数 - bits/sec 表示平均每秒输入的比特数 - packets/sec 表示平均每秒输入的包数
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最近300秒钟的平均输出速率（只有接口支持统计功能时才显示该信息）： - bytes/sec 表示平均每秒输出的字节数 - bits/sec 表示平均每秒输出的比特数 - packets/sec 表示平均每秒输出的包数
Input: 0 packets, 0 bytes, 0 drops	接口输入的报文数，输入的字节数，输入报文中丢弃的报文数（只有接口支持统计功能时才显示这些信息）
Output: 0 packets, 0 bytes, 0 drops	接口输出的报文数，输入的字节数，输入报文中丢弃的报文数（只有接口支持统计功能时才显示这些信息）

显示 InLoopBack 接口的概要信息。

```
<Sysname> display interface inloopback 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
InLoop0            UP    UP(s)    --
```

表1-2 display interface inloopback brief 命令显示信息描述表

字段	描述
Brief information on interfaces in route mode:	InLoopBack接口的概要信息

字段	描述
Link: ADM - administratively down; Stby - standby	- 如果某接口的 Link 属性值为“ADM”，则表示该接口被管理员通过 shutdown 命令关闭，需要在该接口下执行 undo shutdown 命令才能恢复接口本身的物理状态 - 如果某接口的 Link 属性值为“Stby”，则表示该接口是一个处于 Standby 状态的备份接口
Protocol: (s) - spoofing	如果某接口的 Protocol 属性值中带有(s)，则表示该接口的数据链路层协议状态显示为UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的。通常NULL、LoopBack、InLoopBack等接口会具有该属性
Interface	接口名称缩写
Link	接口物理连接状态。取值为UP，表示本链路物理上是连通的
Protocol	接口数据链路层协议状态，取值为UP(s)
Primary IP	接口IP地址 因为InLoopBack接口下不能配置命令行，所以该项对InLoopBack接口无意义
Description	接口的描述信息。因为InLoopBack接口下不能配置命令行，所以该项对InLoopBack接口无意义

1.1.5 display interface loopback

display interface loopback 命令用来显示 LoopBack 接口的相关信息。

【命令】

```
display interface [ loopback [ interface-number ] ] [ brief [ description | down ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

loopback [interface-number]: LoopBack 接口的编号，取值范围为已创建的 LoopBack 接口的编号。如果不指定 **loopback** 参数，将显示所有接口的相关信息。如果不指定 **interface-number** 参数，将显示所有已创建的 LoopBack 接口的相关信息。

brief: 显示接口的概要信息。不指定该参数时，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果某接口的描述信息超过 27 个字符，不指定该参数时，只显示描述信息中的前 27 个字符，超出部分不显示。

down: 显示当前物理状态为 down 的接口的信息以及 down 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【使用指导】

display interface loopback 命令用来显示 Loopback 接口的相关信息。只有创建 LoopBack 接口后，才支持该命令。

【举例】

显示 LoopBack0 接口的相关信息。

```
<Sysname> display interface loopback 0
LoopBack0
Current state: UP
Line protocol state: UP(spoofing)
Description: LoopBack0 Interface
Bandwidth: 1000 kbps
Maximum transmission unit: 1536
Internet protocol processing: Disabled
Physical: Loopback
Last clearing of counters: Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

表1-3 display interface loopback 命令显示信息描述表

字段	描述
Current state	接口当前的物理层状态 - UP: 表示接口能收发报文 - Administratively DOWN: 表示接口被手工关闭了，即在接口下配置了 shutdown 命令
Line protocol state	链路层协议状态: UP(spoofing)，表示接口的链路层协议状态为UP，但实际可能没有对应的链路，或者对应的链路不是永久存在，而是按需建立的
Description	接口的描述信息
Bandwidth	接口的期望带宽，只有当取值不为0时，才显示该字段
Maximum transmission unit	接口的MTU
Internet protocol processing: Disabled	表示不能处理三层报文（接口没有配置IP地址时，显示该信息）
Internet address: <i>ip-address/mask-length (Type)</i>	接口IP地址。 <i>Type</i> 表示地址获取方式，取值如下： - Primary: 手动配置的主地址 - Sub: 手动配置的从地址。当配置了主地址时，仅显示主地址；仅配置从地址时，才显示本信息 - Unnumbered: 借用其他接口的 IP 地址 - MAD: 成员设备上配置的 MAD IP 地址，详细介绍请参见“虚拟化技术命令参考”中的“IRF”  说明 <i>Type</i> 的取值情况与接口类型有关，请以实际情况为准

字段	描述
Physical: Loopback	接口的物理类型是Loopback
baudrate	波特率，单位为kbps
Last clearing of counters	最近一次使用 reset counters interface 命令清除接口下的统计信息的时间（如果从设备启动一直没有执行 reset counters interface 命令清除过该接口下的统计信息，则显示Never）
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最近300秒钟的平均输入速率（只有接口支持统计功能时才显示该信息）： - bytes/sec 表示平均每秒输入的字节数 - bits/sec 表示平均每秒输入的比特数 - packets/sec 表示平均每秒输入的包数
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最近300秒钟的平均输出速率（只有接口支持统计功能时才显示该信息）： - bytes/sec 表示平均每秒输出的字节数 - bits/sec 表示平均每秒输出的比特数 - packets/sec 表示平均每秒输出的包数
Input: 0 packets, 0 bytes, 0 drops	接口输入的报文数，输入的字节数，输入报文中丢弃的报文数（只有接口支持统计功能时才显示这些信息）
Output: 0 packets, 0 bytes, 0 drops	接口输出的报文数，输入的字节数，输入报文中丢弃的报文数（只有接口支持统计功能时才显示这些信息）

显示 LoopBack 接口的概要信息。

```
<Sysname> display interface loopback brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
Loop0              UP    UP(s)    --          forLAN1
```

显示当前物理状态为 down 的 LoopBack 接口的信息以及 down 的原因。

```
<Sysname> display interface loopback brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
Loop0              ADM  Administratively
```

表1-4 display interface loopback brief 命令显示信息描述表

字段	描述
Brief information on interfaces in route mode:	LoopBack接口的概要信息

字段	描述
Link: ADM - administratively down; Stby - standby	- 如果某接口的 Link 属性值为“ADM”，则表示该接口被管理员通过 shutdown 命令关闭，需要在该接口下执行 undo shutdown 命令才能恢复接口本身的物理状态 - 如果某接口的 Link 属性值为“Stby”，则表示该接口是一个处于 Standby 状态的备份接口
Protocol: (s) - spoofing	如果某接口的 Protocol 属性值中带有(s)，则表示该接口的数据链路层协议状态显示为UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的。通常NULL、LoopBack等接口会具有该属性
Interface	接口名称缩写
Link	接口物理连接状态，取值可能为： - UP：表示接口物理上是连通的 - DOWN：表示接口物理上不通 - ADM：表示接口被管理员通过 shutdown 命令关闭，需要执行 undo shutdown 命令才能恢复接口本身的物理状态
Protocol	接口数据链路层协议状态，取值为UP(s)
Primary IP	接口主IP地址
Description	接口的描述信息
Cause	接口物理连接状态为down的原因，取值为Administratively时，表示本链路被手工关闭了（配置了 shutdown 命令），需要执行 undo shutdown 命令才能恢复真实的物理状态

【相关命令】

- interface loopback**
- reset counters interface loopback**

1.1.6 display interface null

display interface null 命令用来显示 NULL 接口的相关信息。

【命令】

display interface [null [0]] [brief [description | down]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

null [0]: NULL 接口的编号。如果不指定 **null** 参数，将显示所有接口的相关信息。

brief: 显示接口的概要信息。不指定该参数时，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果某接口的描述信息超过 27 个字符，不指定该参数时，只显示描述信息中的前 27 个字符，超出部分不显示；指定该参数时，可以显示全部描述信息。

down: 显示当前物理状态为 **down** 的接口的信息以及 **down** 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【使用指导】

因为设备只支持一个 Null 接口 Null0，所以不管是否指定 **0** 参数，显示的都是 Null0 的相关信息。

【举例】

显示指定接口 NULL0 的相关信息。

```
<Sysname> display interface null 0
NULL0
Current state: UP
Line protocol state: UP(spoofing)
Description: NULL0 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV, baudrate: 1000000 kbps
Last clearing of counters: Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

显示 NULL 接口的概要信息。

```
<Sysname> display interface null 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
NULL0              UP    UP(s)    --
```

display interface null命令显示信息描述请参见 [表 1-3](#) 和 [表 1-4](#)。

【相关命令】

- **interface null**
- **reset counters interface null**

1.1.7 interface loopback

interface loopback 命令用来创建 LoopBack 接口，并进入 LoopBack 接口视图。如果指定的 LoopBack 接口已经存在，则直接进入该 LoopBack 接口视图。

undo interface loopback 命令用来删除指定的 LoopBack 接口。

【命令】

```
interface loopback interface-number  
undo interface loopback interface-number
```

【缺省情况】

不存在 LoopBack 接口。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface-number: LoopBack 接口的编号，取值范围为 0~1023。

【使用指导】

LoopBack 接口创建后，物理层和链路层永远处于 up 状态，除非手工关闭该接口。因此，使用 LoopBack 接口建立连接，能够避免连接受接口物理状态的影响，从而提高连接的可靠性。比如，将 LoopBack 接口作为建立 FTP 连接时的源接口。

【举例】

```
# 创建接口 LoopBack0。  
<Sysname> system-view  
[Sysname] interface loopback 0  
[Sysname-LoopBack0]
```

1.1.8 interface null

interface null 命令用来进入 NULL 接口的视图。

【命令】

```
interface null 0
```

【缺省情况】

设备只支持一个 NULL 接口——NULL0，用户不能创建也不能删除。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

0: NULL 接口的编号。

【举例】

```
# 进入接口 NULL0 的视图。  
<Sysname> system-view  
[Sysname] interface null 0  
[Sysname-NULL0]
```

1.1.9 reset counters interface loopback

reset counters interface loopback 命令用来清除 LoopBack 接口的统计信息。

【命令】

```
reset counters interface [ loopback [ interface-number ] ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

loopback [*interface-number*]：逻辑接口编号。*interface-number* 为 LoopBack 接口的编号。如果不指定，则清除所有接口的统计信息；如果指定 **loopback** 参数，而不指定 *interface-number* 参数，则清除所有 LoopBack 接口的统计信息。

【使用指导】

如果要统计一定时间内接口的流量来判断接口和链路工作是否正常，可以使用该命令先清除接口原有的统计信息，然后让接口自动重新统计。

只有创建 LoopBack 接口后，才支持该命令。

【举例】

```
# 清除接口 LoopBack0 的统计信息。  
<Sysname> reset counters interface loopback 0
```

【相关命令】

- **display interface loopback**

1.1.10 reset counters interface null

reset counters interface null 命令用来清除 NULL 接口的统计信息。

【命令】

```
reset counters interface [ null [ 0 ] ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
```

context-admin

【参数】

null [0]: NULL 接口的编号。如果不指定 **null** 参数，则清除所有接口的统计信息。

【使用指导】

如果要统计一定时间内接口的流量来判断接口工作是否正常，可以使用该命令先清除接口原有的统计信息，然后让接口自动重新统计。

【举例】

清除接口 NULL0 的统计信息。

```
<Sysname> reset counters interface null 0
```

【相关命令】

- **display interface null**

1.1.11 shutdown

shutdown 命令用来关闭 LoopBack 接口。

undo shutdown 命令用来开启 LoopBack 接口。

【命令】

shutdown

undo shutdown

【缺省情况】

LoopBack 接口处于开启状态。

【视图】

LoopBack 接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

执行 **shutdown** 命令会导致使用该接口建立的链路中断，不能通信，请谨慎使用。

【举例】

关闭接口 LoopBack0。

```
<Sysname> system-view
```

```
[Sysname] interface loopback 0
```

```
[Sysname-LoopBack0] shutdown
```



UNIS 入侵检测系统

二层技术-以太网交换命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《二层技术-以太网交换命令参考》主要介绍 MAC 地址表、二层转发、以太网链路聚合、VLAN、环路检测和 LLDP 的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。

格 式	意 义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 MAC地址表	1-1
1.1 MAC地址表配置命令	1-1
1.1.1 display mac-address	1-1
1.1.2 display mac-address aging-time	1-2
1.1.3 display mac-address mac-learning	1-3
1.1.4 mac-address (interface view)	1-4
1.1.5 mac-address (system view)	1-5
1.1.6 mac-address mac-learning enable	1-6
1.1.7 mac-address mac-learning priority	1-8
1.1.8 mac-address max-mac-count	1-9
1.1.9 mac-address max-mac-count enable-forwarding	1-9
1.1.10 mac-address timer	1-10
1.1.11 snmp-agent trap enable mac-address	1-11

1 MAC地址表

1.1 MAC地址表配置命令

1.1.1 display mac-address

display mac-address 命令用来显示 MAC 地址表信息。

【命令】

```
display mac-address [ mac-address [ vlan vlan-id ] | [ [ dynamic | static ]  
[ interface interface-type interface-number ] | blackhole ] [ vlan vlan-id ]  
[ count ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

mac-address: 显示指定 MAC 地址的 MAC 地址表项，*mac-address* 的格式为 H-H-H。在配置时，用户可以省去 MAC 地址中每段开头的“0”，例如输入“f-e2-1”即表示输入的 MAC 地址为“000f-00e2-0001”。

vlan *vlan-id*: 显示指定 VLAN 的 MAC 地址表项。*vlan-id* 的取值范围为 1~4094。

dynamic: 显示动态 MAC 地址表项。

static: 显示静态 MAC 地址表项。

interface *interface-type* *interface-number*: 显示指定接口的 MAC 地址表项。*interface-type* *interface-number* 为接口类型和接口编号。

blackhole: 显示黑洞 MAC 地址表项。

count: 显示 MAC 地址表项的数量。如果配置本参数，将仅显示符合条件的（由 **count** 前面的参数决定）MAC 地址表项的数量，而不显示 MAC 地址表项的具体内容。如果不指定本参数，则显示符合条件的 MAC 地址表的具体内容。

【使用指导】

使用本命令可以查看静态、动态和黑洞 MAC 地址表项，表项内容主要包括 MAC 地址、VLAN ID、接口等信息。

如果不指定任何参数，将显示所有的 MAC 地址表项信息。

对于聚合接口，需要有选中端口，该聚合接口对应的动态 MAC 地址才能在 MAC 地址表项中显示。

【举例】

显示 VLAN 100 的 MAC 地址表项的信息。

```
<Sysname> display mac-address vlan 100
```

MAC Address	VLAN ID	State	Port/Nickname	Aging
0033-0033-0033	100	Blackhole	N/A	N
0000-0000-0002	100	Static	GE1/0/3	N
00e0-fc00-5829	100	Learned	GE1/0/4	Y

显示 MAC 地址表项的数量。

```
<Sysname> display mac-address count
```

1 mac address(es) found.

表1-1 display mac-address 命令显示信息描述表

字段	描述
MAC Address	MAC地址
VLAN ID	MAC地址对应接口所属的VLAN
State	MAC地址表项的状态，包括： - Static：表示该表项是静态 MAC 地址表项 - Learned：动态 MAC 地址表项。可以手工配置也可以由设备学习获得 - Blackhole：表示该表项是黑洞 MAC 地址表项 - Drop aging：表示该表项是可老化的 MAC 地址表项，收到该 MAC 地址报文会被丢弃 - Drop no-aging：表示该表项是不可老化的 MAC 地址表项，收到该 MAC 地址报文会被丢弃 - Vlan-interface：表示该表项是 VLAN 虚接口 MAC 地址表项
Port/Nickname	MAC地址对应的接口名称或Nickname（设备仅显示，不支持该参数）。如果显示为接口名称，表示发往该MAC地址的报文将从此接口发出（黑洞MAC地址表项此处显示为N/A）
Aging	老化时间，该表项有两种取值： - Y：表示该表项会被老化 - N：表示该表项不会被老化
<i>n</i> mac address(es) found	共有 <i>n</i> 个MAC地址表项

【相关命令】

- **mac-address**
- **mac-address timer**

1.1.2 display mac-address aging-time

display mac-address aging-time 命令用来显示 MAC 地址表动态表项的老化时间。

【命令】

display mac-address aging-time

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 MAC 地址表中动态表项的老化时间。
<Sysname> display mac-address aging-time
MAC address aging time: 300s.

【相关命令】

- **mac-address timer**

1.1.3 display mac-address mac-learning

display mac-address mac-learning 命令用来显示 MAC 地址学习功能的开启状态。

【命令】

display mac-address mac-learning [**interface** *interface-type*
interface-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface interface-type interface-number: 显示指定接口的 MAC 地址学习状态。
interface-type interface-number 为接口类型和接口编号。如果不指定本参数，则显示全局和所有接口的 MAC 地址学习状态。

【举例】

显示全局和所有接口的 MAC 地址学习状态。
<Sysname> display mac-address mac-learning
Global MAC address learning status: Enabled.

Port	Learning Status
GE1/0/1	Enabled
GE1/0/2	Enabled

表1-2 display mac-address mac-learning 命令显示信息描述表

字段	描述
Global MAC address learning status	全局的MAC地址学习状态：Enabled为开启，Disabled为禁止
Port	接口名称
Learning Status	接口的MAC地址学习状态：Enabled为开启，Disabled为禁止

【相关命令】

- **mac-address mac-learning enable**

1.1.4 mac-address (interface view)

mac-address 命令用来在接口下添加或者修改 MAC 地址表项。

undo mac-address 命令用来删除接口下的 MAC 地址表项。

【命令】

```
mac-address { dynamic | static } mac-address vlan vlan-id
undo mac-address { dynamic | static } mac-address vlan vlan-id
```

【缺省情况】

接口下未配置任何 MAC 地址表项。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

dynamic: 动态 MAC 地址表项。

static: 静态 MAC 地址表项。

mac-address: MAC 地址，格式为 H-H-H，不支持组播 MAC 地址、全 0 的 MAC 地址和全 F 的 MAC 地址。在配置时，用户可以省去 MAC 地址中每段开头的“0”，例如输入“f-e2-1”即表示输入的 MAC 地址为“000f-00e2-0001”。

vlan vlan-id: 当前接口所属的 VLAN。*vlan-id* 为指定 VLAN 的编号，取值范围为 1~4094。该 VLAN 必须已经创建。

【使用指导】

一般情况下，设备通过源 MAC 地址学习过程自动建立 MAC 地址表。为了提高接口安全性，网络管理员可手工在 MAC 地址表中加入特定 MAC 地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。手工配置的静态 MAC 地址表项优先级高于自动生成的表项。

如果不保存配置，设备重启后所有表项都会丢失；如果保存配置，静态 MAC 地址表项不会丢失，动态 MAC 地址表项会丢失。

【举例】

在端口 GigabitEthernet1/0/1 下增加静态 MAC 地址表项 000f-e201-0101，该端口属于 VLAN 2。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2
```

在接口 Bridge-Aggregation1 下增加静态 MAC 地址表项 000f-e201-0102，该接口属于 VLAN 1。

```
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1
```

【相关命令】

- **display mac-address**
- **mac-address** (system view)

1.1.5 mac-address (system view)

mac-address 命令用来添加或者修改 MAC 地址表项。

undo mac-address 命令用来删除 MAC 地址表项。

【命令】

```
mac-address { dynamic | static } mac-address interface interface-type  
interface-number vlan vlan-id
```

```
mac-address blackhole mac-address vlan vlan-id
```

```
undo mac-address [ [ dynamic | static ] mac-address interface interface-type  
interface-number vlan vlan-id ]
```

```
undo mac-address [ blackhole | dynamic | static ] [ mac-address ] vlan vlan-id
```

```
undo mac-address [ dynamic | static ] interface interface-type  
interface-number
```

【缺省情况】

未配置任何 MAC 地址表项。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

dynamic: 动态 MAC 地址表项。

static: 静态 MAC 地址表项。

blackhole: 黑洞 MAC 地址表项。当报文的源 MAC 地址或目的 MAC 地址与黑洞 MAC 地址表项匹配时，该报文被丢弃。

mac-address: MAC 地址，格式为 H-H-H，不支持组播 MAC 地址、全 0 的 MAC 地址和全 F 的 MAC 地址。在配置时，用户可以省去 MAC 地址中每段开头的“0”，例如输入“f-e2-1”即表示输入的 MAC 地址为“000f-00e2-0001”。

vlan vlan-id: 指定接口所属的 VLAN。*vlan-id* 为指定 VLAN 的编号，取值范围为 1~4094。该 VLAN 必须已经创建。

interface interface-type interface-number : 出接口。*interface-type interface-number* 为接口类型和接口编号。

【使用指导】

通过本命令可以添加或者修改如下类型的 MAC 地址表项：

动态 MAC 地址：设备通过源 MAC 地址学习过程自动建立 MAC 地址表或者由用户手工配置。

静态 MAC 地址：为了提高接口安全性，网络管理员可手工在 MAC 地址表中加入特定 MAC 地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。手工配置的静态 MAC 地址表项优先级高于自动生成的表项。

黑洞 MAC 地址：用于丢弃指定源 MAC 地址或目的 MAC 地址的报文。

用户手工配置的静态 MAC 地址表项或黑洞 MAC 地址表项不会被动态 MAC 地址表项覆盖，而动态 MAC 地址表项可以被静态 MAC 地址表项和黑洞 MAC 地址表项覆盖。

删除 MAC 地址表项时，需要注意：

- 执行 **undo mac-address** 命令时若不指定任何参数，将删除所有单播 MAC 地址表项和静态组播 MAC 地址表项。
- 可以删除指定 VLAN 的所有 MAC 地址表项（包括单播 MAC 地址表项和静态组播 MAC 地址表项）；可以选择删除动态 MAC 地址表项、静态 MAC 地址表项、黑洞 MAC 地址表项；可以按接口删除单播 MAC 地址表项，但不能按接口删除组播 MAC 地址表项。

如果不保存配置，设备重启后所有表项都会丢失；如果保存配置，静态 MAC 地址表项和黑洞 MAC 地址表项不会丢失，动态表项会丢失。

【举例】

添加静态地址表项，目的 MAC 地址为 000f-e201-0101，出接口为 GigabitEthernet1/0/1，且该接口属于 VLAN 2。

```
<Sysname> system-view
```

```
[Sysname] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2
```

【相关命令】

- **display mac-address**
- **mac-address** (interface view)

1.1.6 mac-address mac-learning enable

mac-address mac-learning enable 命令用来打开设备全局、接口或者 VLAN 的 MAC 地址学习功能。

undo mac-address mac-learning enable 命令用来关闭设备全局、接口或者 VLAN 的 MAC 地址学习功能。

【命令】

```
mac-address mac-learning enable
undo mac-address mac-learning enable
```

【缺省情况】

MAC 地址学习功能处于开启状态。

【视图】

系统视图
二层以太网接口视图
二层聚合接口视图
VLAN 视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

有时为了保证设备的安全，需要关闭 MAC 地址学习功能。常见的危及设备安全的情况是：非法用户使用大量源 MAC 地址不同的报文攻击设备，导致设备 MAC 地址表资源耗尽，造成设备无法根据网络的变化更新 MAC 地址表。关闭 MAC 地址学习功能可以有效防止这种攻击。

关闭 MAC 地址学习功能时，需要注意：

- 关闭 MAC 地址学习功能后，设备就学不到新地址，从而影响设备及时刷新 MAC 地址表。用户可以根据实际情况关闭接口的 MAC 地址学习功能。
- 关闭全局的 MAC 地址学习功能后，接口将不再学习新的 MAC 地址。
- 关闭 MAC 地址学习功能可能会导致广播，因此在关闭接口的 MAC 地址学习功能的同时，一般还要使用接口广播风暴抑制功能。有关广播风暴抑制功能的介绍，请参见“接口管理配置指导”中的“以太网接口”。
- 在开启全局的 MAC 地址学习功能的前提下，用户可以关闭设备上单个接口的 MAC 地址学习功能。
- 关闭 MAC 地址学习功能后，对于已经存在的动态 MAC 地址表项，待老化时间超时后将自然老化。

【举例】

```
# 关闭全局 MAC 地址学习功能。
<Sysname> system-view
[Sysname] undo mac-address mac-learning enable
# 关闭 VLAN 10 的 MAC 地址学习功能。
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] undo mac-address mac-learning enable
# 关闭端口 GigabitEthernet1/0/1 的 MAC 地址学习功能。
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo mac-address mac-learning enable
```

【相关命令】

- **display mac-address mac-learning**

1.1.7 mac-address mac-learning priority

mac-address mac-learning priority 命令用来配置接口的 MAC 地址学习优先级。

undo mac-address mac-learning priority 命令用来恢复缺省情况。

【命令】

```
mac-address mac-learning priority { high | low }
undo mac-address mac-learning priority
```

【缺省情况】

MAC 地址学习优先级为低优先级。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

high: 配置 MAC 地址学习优先级为高优先级。

low: 配置 MAC 地址学习优先级为低优先级。

【使用指导】

接口的 MAC 地址学习功能分为两个优先级：高优先级和低优先级。对于高优先级的接口，可以学习任何 MAC 地址；对于低优先级的接口，在学习 MAC 地址时需要查看高优先级接口是否已经学到该 MAC 地址，如果已经学到，则不允许学习该 MAC 地址。

为了预防攻击，避免下行接口学到网关等上层设备的 MAC 地址，可以进行如下配置：

- 将上行接口的 MAC 地址学习优先级配置为高优先级。
- 将下行接口的 MAC 地址学习优先级配置为低优先级。

【举例】

配置端口 GigabitEthernet1/0/1 的 MAC 地址学习优先级为高优先级。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address mac-learning priority high
```

配置接口 Bridge-Aggregation1 的 MAC 地址学习优先级为高优先级。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] mac-address mac-learning priority high
```

1.1.8 mac-address max-mac-count

mac-address max-mac-count 命令用来配置接口的 MAC 地址数学习上限。

undo mac-address max-mac-count 命令用来恢复缺省情况。

【命令】

mac-address max-mac-count *count*

undo mac-address max-mac-count

【缺省情况】

接口的 MAC 地址数学习上限仅受设备硬件能力的限制。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

count: 接口的 MAC 地址数学习上限，为 0 即表示不允许该接口学习 MAC 地址。取值范围为 0～4096。

【使用指导】

通过配置接口的 MAC 地址数学习上限，用户可以控制设备维护的 MAC 地址表的表项数量。如果 MAC 地址表过于庞大，可能导致设备的转发性能下降。当接口学习到的 MAC 地址数达到上限时，该接口将不再对 MAC 地址进行学习。

【举例】

配置端口 GigabitEthernet1/0/1 的 MAC 地址数学习上限为 200。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 200
```

【相关命令】

- **mac-address**
- **mac-address max-mac-count enable-forwarding**

1.1.9 mac-address max-mac-count enable-forwarding

mac-address max-mac-count enable-forwarding 命令用来配置当达到接口的 MAC 地址数学习上限时，允许转发源 MAC 地址不在 MAC 地址表里的报文。

undo mac-address max-mac-count enable-forwarding 命令用来配置当达到接口的 MAC 地址数学习上限时，禁止转发源 MAC 地址不在 MAC 地址表里的报文。

【命令】

```
mac-address max-mac-count enable-forwarding
undo mac-address max-mac-count enable-forwarding
```

【缺省情况】

当达到接口的 MAC 地址数学习上限时，允许转发源 MAC 地址不在 MAC 地址表里的报文。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin
context-admin

【举例】

配置端口 GigabitEthernet1/0/1 的 MAC 地址数学习上限为 200，当端口学习的 MAC 地址数达到 200 时，禁止转发源 MAC 地址不在 MAC 地址表里的报文。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 200
[Sysname-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding
```

【相关命令】

- **mac-address**
- **mac-address max-mac-count**

1.1.10 mac-address timer

mac-address timer 命令用来配置动态 MAC 地址表项的老化时间。

undo mac-address timer 命令用来恢复缺省情况。

【命令】

```
mac-address timer { aging seconds | no-aging }
undo mac-address timer
```

【缺省情况】

动态 MAC 地址表项的老化时间为 300 秒。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

aging seconds: 动态 MAC 地址表项的老化时间，单位为秒，设备支持的取值范围为 10~1400。

no-aging: 不老化。

【使用指导】

用户配置的老化时间过长或者过短，都可能影响设备的运行性能：

- 如果用户配置的老化时间过长，设备可能会保存许多过时的 MAC 地址表项，从而耗尽 MAC 地址表资源，导致设备无法根据网络的变化更新 MAC 地址表。
- 如果用户配置的老化时间太短，设备可能会删除有效的 MAC 地址表项，可能导致设备广播大量的数据报文，影响设备的运行性能。

所以用户需要根据实际情况，配置合适的老化时间来有效的实现 MAC 地址老化功能。

【举例】

```
# 配置动态 MAC 地址表项的老化时间为 500 秒。  
<Sysname> system-view  
[Sysname] mac-address timer aging 500
```

【相关命令】

- **display mac-address aging-time**

1.1.11 snmp-agent trap enable mac-address

snmp-agent trap enable mac-address 命令用来开启 MAC 地址表的告警功能。

undo snmp-agent trap enable mac-address 命令用来关闭 MAC 地址表的告警功能。

【命令】

```
snmp-agent trap enable mac-address  
undo snmp-agent trap enable mac-address
```

【缺省情况】

MAC 地址表的告警功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

开启 MAC 地址表的告警功能后，MAC 地址表模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，请通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

关闭 MAC 地址表的告警功能后，设备将只发送日志信息到信息中心模块，此时请配置信息中心的输出规则和输出方向来查看 MAC 地址表模块的日志信息。

有关 SNMP 和信息中心的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”和“信息中心”。

目前 MAC 地址表模块仅有 MAC 地址迁移上报的告警功能，所以打开或关闭 MAC 地址迁移上报的告警功能，就相当于打开或关闭 MAC 地址表所有的告警功能。

【举例】

关闭 MAC 地址迁移的告警功能。

```
<Sysname> system-view
```

```
[Sysname] undo snmp-agent trap enable mac-address
```

目 录

1 以太网链路聚合	1-1
1.1 以太网链路聚合配置命令	1-1
1.1.1 bandwidth	1-1
1.1.2 default	1-1
1.1.3 description	1-2
1.1.4 display interface	1-3
1.1.5 display lacp system-id	1-8
1.1.6 display link-aggregation load-sharing mode	1-9
1.1.7 display link-aggregation load-sharing path	1-10
1.1.8 display link-aggregation member-port	1-13
1.1.9 display link-aggregation summary	1-15
1.1.10 display link-aggregation verbose	1-17
1.1.11 interface bridge-aggregation	1-20
1.1.12 interface route-aggregation	1-21
1.1.13 jumboframe enable	1-22
1.1.14 lacp edge-port	1-23
1.1.15 lacp mode	1-23
1.1.16 lacp period short	1-24
1.1.17 lacp system-priority	1-25
1.1.18 link-aggregation auto-aggregation enable	1-25
1.1.19 link-aggregation global load-sharing mode	1-26
1.1.20 link-aggregation ignore vlan	1-27
1.1.21 link-aggregation lacp traffic-redirect-notification enable	1-28
1.1.22 link-aggregation load-sharing mode	1-29
1.1.23 link-aggregation load-sharing mode local-first	1-30
1.1.24 link-aggregation mode	1-31
1.1.25 link-aggregation port-priority	1-31
1.1.26 link-aggregation selected-port maximum	1-32
1.1.27 link-aggregation selected-port minimum	1-33
1.1.28 link-delay	1-34
1.1.29 mtu	1-35
1.1.30 port link-aggregation group	1-36
1.1.31 reset counters interface	1-37

1.1.32 reset lacp statistics	1-37
1.1.33 shutdown	1-38

1 以太网链路聚合

1.1 以太网链路聚合配置命令

1.1.1 bandwidth

bandwidth 命令用来配置接口的期望带宽。

undo bandwidth 命令用来恢复缺省情况。

【命令】

bandwidth *bandwidth-value*

undo bandwidth

【缺省情况】

接口的期望带宽 = 接口的波特率 ÷ 1000 (kbps)。

【视图】

二层聚合接口视图

三层聚合接口视图

三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

bandwidth-value: 表示接口的期望带宽，取值范围为 1~400000000，单位为 kbps。

【使用指导】

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

【举例】

```
# 配置二层聚合接口 1 的期望带宽为 10000kbps。
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] bandwidth 10000
# 配置三层聚合接口 1 的期望带宽为 10000kbps。
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] bandwidth 10000
```

1.1.2 default

default 命令用来恢复聚合接口的缺省配置。

【命令】

default

【视图】

二层聚合接口视图

三层聚合接口视图

三层聚合子接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】



注意

接口下的某些配置取消后，会对现有功能产生影响，建议您在执行该命令前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

【举例】

将二层聚合接口 1 恢复为缺省配置。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] default
```

将三层聚合接口 1 恢复为缺省配置。

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] default
```

1.1.3 description

description 命令用来配置接口的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

接口的描述信息为“接口名 Interface”，比如接口 Bridge-Aggregation1 的缺省描述信息为：Bridge-Aggregation1 Interface。

【视图】

二层聚合接口视图
三层聚合接口视图
三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

text: 表示接口的描述信息，为 1~255 个字符的字符串，区分大小写。

【举例】

```
# 配置二层聚合接口 1 的描述信息为 “connect to the lab”。
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] description connect to the lab
# 配置三层聚合接口 1 的描述信息为 “connect to the lab”。
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] description connect to the lab
```

1.1.4 display interface

display interface 命令用来显示聚合接口的相关信息。

【命令】

```
display interface [ { bridge-aggregation | route-aggregation }
[ interface-number ] ] [ brief [ description | down ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

bridge-aggregation: 显示二层聚合接口的相关信息。

route-aggregation: 显示三层聚合接口的相关信息。

interface-number: 表示聚合接口的编号，取值范围为已创建的聚合接口的编号。

brief: 显示接口的概要信息。如果未指定该参数，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果某接口的描述信息超过 27 个字符，不指定该参数时，只显示描述信息中的前 27 个字符，超出部分不显示；指定该参数时，可以显示全部描述信息。

down: 显示当前物理状态为 down 的接口的信息以及 down 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【使用指导】

如果未指定聚合接口的类型，将显示所有接口的相关信息。

如果指定了聚合接口的类型而未指定聚合接口编号，将显示所有已创建的该类型聚合接口的相关信息。

【举例】

显示二层聚合接口 1 的详细信息。

```
<Sysname> display interface bridge-aggregation 1
Bridge-Aggregation1
Current state: UP
IP packet frame type: Ethernet II, hardware address: 000f-e207-f2e0
Description: Bridge-Aggregation1 Interface
Bandwidth: 1000 kbps
2Gbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
PVID: 1
Port link-type: Access
Tagged VLANs:   None
Untagged VLANs: 1
Last clearing of counters: Never
  Last 300 seconds input:  6900 packets/sec 885160 bytes/sec    0%
  Last 300 seconds output: 3150 packets/sec 404430 bytes/sec    0%
Input (total): 5364747 packets, 686688416 bytes
    2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input (normal): 5364747 packets, 686688416 bytes
    2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input: 0 input errors, 0 runts, 0 giants, 0 throttles
    0 CRC, 0 frame, 0 overruns, - aborts
    - ignored, - parity errors
Output (total): 1042508 packets, 133441832 bytes
    1042306 unicasts, 0 broadcasts, 202 multicasts, - pauses
Output (normal): 1042508 packets, 133441832 bytes
    1042306 unicasts, 0 broadcasts, 202 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
    0 aborts, 0 deferred, 0 collisions, 0 late collisions
    - lost carrier, - no carrier
```

显示三层聚合接口 1 的详细信息。

```
<Sysname> display interface route-aggregation 1
Route-Aggregation1
Current state: UP
Line protocol state: UP
```

```

Description: Route-Aggregation1 Interface
Bandwidth: 1000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 0000-0000-0000
IPv6 packet frame type: Ethernet II, hardware address: 0000-0000-0000
Port priority: 0
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Last clearing of counters: Never
  Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
  Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 drops
  0 packets output, 0 bytes, 0 drops

```

显示二层聚合接口 1 的概要信息。

```

<Sysname> display interface bridge-aggregation 1 brief
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface          Link Speed  Duplex Type PVID Description
BAGG1              UP   auto    A     A    1

```

显示三层聚合接口 1 的概要信息。

```

<Sysname> display interface route-aggregation 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
RAGG1              UP    UP      --

```

表1-1 display interface 命令显示信息描述表

字段	描述
Bridge-Aggregation1	二层聚合接口名
Route-Aggregation1	三层聚合接口名
Current state	接口的状态： - Administratively DOWN: 表示该接口已被 shutdown 命令关闭，其管理状态为关闭 - DOWN: 表示该接口的管理状态为开启，但其物理状态为关闭（可能由于没有物理连线或线路故障） - UP: 表示该接口的管理状态和物理状态均为开启
IP packet frame type	IPv4报文帧格式

字段	描述
hardware address	接口的MAC地址
Description	接口的描述信息
Bandwidth	接口的期望带宽值，当该参数的取值为0时，不显示该参数
Port priority	接口优先级
Output queue - Urgent queuing: Size/Length/Discards	输出队列（紧急队列中当前的消息数/最大可容纳的消息数/已丢弃的消息数）
Output queue - Protocol queuing: Size/Length/Discards	输出队列（协议队列中当前的消息数/最大可容纳的消息数/已丢弃的消息数）
Output queue - FIFO queuing: Size/Length/Discards	输出队列（先进先出队列中当前的消息数/最大可容纳的消息数/已丢弃的消息数）
Unknown-speed mode, unknown-duplex mode	接口的速率和双工模式均未知
Link speed type is autonegotiation, link duplex type is autonegotiation	接口的速率和双工模式都是通过自协商确定的
PVID	接口缺省VLAN的编号
Port link-type	接口的链路类型，取值可能为access、trunk或hybrid
Tagged VLANs	通过该接口后携带Tag的VLAN
Untagged VLANs	通过该接口后不再携带Tag的VLAN
Last clearing of counters	最后一次使用 reset counters interface 命令清除接口统计信息的时间。如果从设备启动一直没有执行 reset counters interface 命令清除过该接口下的统计信息，则显示Never
Last 300 seconds input/output rate	接口在最近300秒接收/发送报文的平均速率
Input/Output (total)	接口接收/发送的全部报文的统计值
Input/Output (normal)	接口接收/发送的正常报文的统计值
Line protocol state	接口数据链路层协议状态： - UP - DOWN
Maximum transmission unit	接口的最大传输单元
Internet protocol processing: Disabled	接口未配置IP地址，不能处理IP报文
Internet address: <i>ip-address/mask-length</i> (<i>Type</i>)	接口IP地址。<i>Type</i>表示地址获取方式，取值如下： - Primary: 手动配置的主地址 - Sub: 手动配置的从地址。当配置了主地址时，仅显示主地址；仅配置从地址时，才显示本信息 - Unnumbered: 借用其他接口的IP地址 - MAD: 成员设备上配置的MAD IP地址，详细介绍请参见“虚拟化技术命令参考”中的“IRF”  说明 <i>Type</i>的取值情况与接口类型有关，请以实际情况为准

字段	描述
Brief information on interfaces in route mode	三层接口的概要信息
Brief information on interfaces in bridge mode	二层接口的概要信息
Link: ADM - administratively down; Stby - standby	接口的物理连接状态： • ADM: 表示该接口已被管理员通过 shutdown 命令关闭，在该接口下执行 undo shutdown 命令才能恢复其物理状态 • Stby: 表示该接口是一个处于 Standby 状态的备份接口
Speed: (a) - auto	如果某接口的Speed属性值为“(a)”，则表示该接口的速率是通过自动协商获取的 如果某接口的Speed属性值为“auto”，则表示该接口的速率是通过自动协商获取的，但协商还未开始
Duplex: (a)/A - auto; H - half; F - full	接口的双工模式： • (a)/A: 表示双工模式都是通过自协商确定的 • H: 表示双工模式为半双工 • F: 表示双工模式为全双工
Type: A - access; T - trunk; H - hybrid	接口的链路类型： • A: 表示 Access 类型 • H: 表示 Hybrid 类型 • T: 表示 Trunk 类型
Protocol: (s) - spoofing	如果某接口的Protocol属性值中带有“(s)”字符串，则表示该接口的数据链路层协议状态显示为UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的
Interface	接口名称的缩写
Link	接口物理连接状态，取值为： • UP: 表示接口物理上是连通的 • DOWN: 表示接口物理上是不通的 • ADM: 表示接口被管理员通过 shutdown 命令关闭，需要执行 undo shutdown 命令才能恢复接口本身的物理状态 • Stby: 表示该接口是一个处于 Standby 状态的备份接口
Speed	接口的速率（单位为bps）
Duplex	接口的双工模式
Type	接口的链路类型 • A: 表示 Access 链路类型 • H: 表示 Hybrid 链路类型 • T: 表示 Trunk 链路类型

字段	描述
Protocol	接口数据链路层协议状态，取值为： - UP：表示接口的数据链路层协议状态为开启 - DOWN：表示接口的数据链路层协议状态为关闭 - UP(s)：表示接口的数据链路层协议状态显示为 UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的
Primary IP	接口的主IP地址
Cause	接口物理连接状态为down的原因

1.1.5 display lacp system-id

display lacp system-id 命令用来显示本端系统的设备 ID。

【命令】

display lacp system-id

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

使用 **lacp system-priority** 命令可以改变系统的 LACP 优先级，但通过该命令输入的是十进制的优先级数值。而当使用 **display lacp system-id** 命令显示时，系统会自动将其转换为十六进制的优先级数值。

【举例】

显示本端系统的设备 ID。

```
<Sysname> display lacp system-id
Actor System ID: 0x8000, 0000-fc00-6504
```

表1-2 display lacp system-id 命令显示信息描述表

字段	描述
Actor System ID: 0x8000, 0000-fc00-6504	本端系统的设备ID（由系统的LACP优先级和系统的MAC地址共同构成）：系统的LACP优先级为0x8000，系统的MAC地址为0000-FC00-6504

【相关命令】

- lacp system-priority**

1.1.6 display link-aggregation load-sharing mode

display link-aggregation load-sharing mode 命令用来显示全局或聚合组内采用的聚合负载分担类型。

【命令】

```
display link-aggregation load-sharing mode [ interface  
[ { bridge-aggregation | route-aggregation } interface-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

bridge-aggregation: 显示二层聚合接口所对应聚合组内采用的聚合负载分担类型。

route-aggregation: 显示三层聚合接口所对应聚合组内采用的聚合负载分担类型。

interface-number: 聚合接口的编号。必须是当前已经创建的聚合接口编号。

【使用指导】

如果未指定参数 **interface**，则显示全局采用的聚合负载分担类型。

如果仅指定参数 **interface** 而未指定具体的聚合接口类型，则显示所有聚合接口所对应聚合组内采用的聚合负载分担类型。

只有在设备上创建了二层聚合接口、三层聚合接口之后，才能指定 **bridge-aggregation** 或 **route-aggregation** 参数。

【举例】

显示全局采用的聚合负载分担类型（缺省情况）。

```
<Sysname> display link-aggregation load-sharing mode  
Link-aggregation load-sharing mode:  
Layer 2 traffic: packet type-based sharing  
Layer 3 traffic: packet type-based sharing
```

显示全局采用的聚合负载分担类型（非缺省情况）。

```
<Sysname> display link-aggregation load-sharing mode  
Link-aggregation load-sharing mode:  
destination-mac address, source-mac address
```

显示二层聚合接口 1 所对应聚合组内采用的聚合负载分担类型（缺省情况）。

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 1  
Bridge-Aggregation1 load-sharing mode:  
Layer 2 traffic: packet type-based sharing  
Layer 3 traffic: packet type-based sharing
```

显示二层聚合接口 1 所对应聚合组内采用的聚合负载分担类型（非缺省情况）。

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 1
Bridge-Aggregation1 load-sharing mode:
destination-mac address, source-mac address
```

显示三层聚合接口 1 所对应聚合组内采用的聚合负载分担类型（缺省情况）。

```
<Sysname> display link-aggregation load-sharing mode interface route-aggregation 1
Route-Aggregation1 load-sharing mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

显示三层聚合接口 1 所对应聚合组内采用的聚合负载分担类型（非缺省情况）。

```
<Sysname> display link-aggregation load-sharing mode interface route-aggregation 1
Route-Aggregation1 load-sharing mode:
destination-mac address, source-mac address
```

表1-3 display link-aggregation load-sharing mode 命令显示信息描述表

字段	描述
Link-aggregation load-sharing mode	全局采用的聚合负载分担类型： - 缺省情况下显示：二层报文、三层报文采用的聚合负载分担类型 - 非缺省情况下显示：用户配置后采用的聚合负载分担类型
Bridge-Aggregation1 load-sharing mode	二层聚合接口1所对应聚合组内采用的聚合负载分担类型： - 缺省情况下显示：全局采用的聚合负载分担类型 - 非缺省情况下显示：用户配置后采用的聚合负载分担类型
Route-Aggregation1 load-sharing mode	三层聚合接口1所对应聚合组内采用的聚合负载分担类型： - 缺省情况下显示：全局采用的聚合负载分担类型 - 非缺省情况下显示：用户配置后采用的聚合负载分担类型
Layer 2 traffic: destination-mac address, source-mac address	二层报文缺省采用的聚合负载分担类型：按照源MAC地址和目的MAC地址进行负载分担
Layer 2 traffic: packet type-based sharing	二层报文缺省采用的聚合负载分担类型：按照产品自定义方式进行负载分担
Layer 3 traffic: destination-ip address, source-ip address	三层报文缺省采用的聚合负载分担类型：按照源IP地址和目的IP地址进行负载分担
Layer 3 traffic: packet type-based sharing	三层报文缺省采用的聚合负载分担类型：按照产品自定义方式进行负载分担
destination-mac address, source-mac address	用户配置后采用的聚合负载分担类型：按照源MAC地址和目的MAC地址进行负载分担

1.1.7 display link-aggregation load-sharing path

display link-aggregation load-sharing path 命令用来显示聚合组内采用的聚合负载分担的选路信息。

【命令】

```
display link-aggregation load-sharing path interface { bridge-aggregation  
| route-aggregation } interface-number ingress-port interface-type  
interface-number [ route ] { { destination-ip ip-address | destination-ipv6  
ipv6-address } | { source-ip ip-address | source-ipv6 ipv6-address } |  
destination-mac mac-address | destination-port port-id | ethernet-type  
type-number | ip-protocol protocol-id | source-mac mac-address | source-port  
port-id | vlan vlan-id } * slot slot-number
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

bridge-aggregation: 显示二层聚合接口相关信息。

route-aggregation: 显示三层聚合接口相关信息。

interface-number: 聚合接口的编号。取值范围为已创建的聚合接口的编号。

ingress-port interface-type interface-number: 指定报文入接口。**interface-type** 表示接口类型，只能指定物理接口。**interface-number** 表示接口编号。

route: 显示进行三层转发的报文的选路信息。不指定该参数时，显示进行二层转发的报文的选路信息。

destination-ip ip-address: 显示指定目的 IPv4 地址的报文的选路信息。

destination-ipv6 ipv6-address: 显示指定目的 IPv6 地址的报文的选路信息。

source-ip ip-address: 显示指定源 IPv4 地址的报文的选路信息。

source-ipv6 ipv6-address: 显示指定源 IPv6 地址的报文的选路信息。

destination-mac mac-address: 显示指定目的 MAC 地址的报文的选路信息，**mac-address** 的格式为 H-H-H。

destination-port port-id: 显示指定目的端口的报文的选路信息，**port-id** 表示端口号，取值范围为 1~65535。

ethernet-type type-number: 以太网层封装类型，**type-number** 表示封装类型的编号，取值范围为 1~65535。

ip-protocol protocol-id: 显示指定 IP 协议类型的报文的选路信息。**protocol-id** 表示协议号，取值范围为 0~255。

source-mac mac-address: 显示指定源 MAC 地址的报文的选路信息，**mac-address** 的格式为 H-H-H。

source-port port-id: 显示指定源端口的报文的选路信息，**port-id** 表示端口号，取值范围为 1~65535。

vlan *vlan-id*: 显示指定 VLAN 的报文的选路信息。*vlan-id* 的取值范围为 1~4094。

slot *slot-number*: 显示指定成员设备的选路信息，*slot-number* 表示成员设备所在的槽位号。

【使用指导】

通过本命令可以显示聚合组内报文选择物理出接口时所使用的参数。

显示聚合组内指定特征报文的物理出接口时，本命令指定的参数不一定会被显示。例如通过本命令指定的参数为目的 MAC 地址和目的 IP 地址，但是通过目的 MAC 地址就可以找到报文的出接口，则在计算选路信息时实际使用的参数中不显示目的 IP 地址。

选择报文出接口时需要使用的参数，本命令没有指定，则取设备的缺省值。如果没有缺省值，则按照 0 处理。

本命令只对逐流的负载分担和按照报文类型的负载分担有效，使用逐包的负载分担时不建议使用本命令获取选路信息。

【举例】

显示特征为入接口 GigabitEthernet1/0/1，目的 MAC 地址 0000-fc00-0001，源 MAC 地址 0000-fc00-0002，源 IP 地址 10.100.0.2，目的 IP 地址 10.100.0.1 的报文指定出聚合接口 Bridge-Aggregation 1 时，进行二层转发选择的物理出端口信息。

```
<Sysname> display link-aggregation load-sharing path interface bridge-aggregation 1
ingress-port gigabitethernet 1/0/1 destination-mac 0000-fc00-0001 source-mac 0000-fc00-0002
source-ip 10.100.0.2 destination-ip 10.100.0.1 slot 1
Load sharing mode: destination-mac, source-mac, source-ip, destination-ip
Unspecified parameters are set to 0.
Load-sharing parameters:
  Ingress port: GigabitEthernet1/0/1
  Destination MAC: 0000-fc00-0001
  Source MAC: 0000-fc00-0002
  Destination IP: 10.100.0.1
  Source IP: 10.100.0.2
Egress port: GigabitEthernet1/0/3
```

表1-4 display link-aggregation load-sharing path 命令显示信息描述表

字段	描述
Load sharing mode:	聚合组采用的负载分担类型： • destination-mac: 按照目的 MAC 地址负载分担 • source-mac: 按照源 MAC 地址负载分担 • destination-ip: 按照目的 IP 地址负载分担 • source-ip: 按照源 IP 地址负载分担 • destination-port: 按照目的端口负载分担 • source-port: 按照源端口负载分担 • ingress-port: 按照入端口负载分担 • vlan: 按照报文所属的 VLAN 负载分担 • packet type-based sharing: 按照报文类型自动选择负载分担类型，如果没有配置负载分担类型也显示此值

字段	描述
Unspecified parameters are set to 0	未指定的参数默认值为0
Load sharing parameters	计算选路信息时实际使用的参数
Ingress port	报文入接口
Ethernet type	报文以太网封装类型
Destination MAC	报文目的MAC地址
Source MAC	报文源MAC地址
Destination IP	报文目的IP
Source IP	报文源IP
Destination port	报文目的端口
Source port	报文源端口
IP protocol	报文IP协议类型
VLAN	报文所属VLAN
Egress port	根据报文特征所选择的路径，如果找不到出端口显示“N/A”

1.1.8 display link-aggregation member-port

display link-aggregation member-port 命令用来显示成员端口上链路聚合的详细信息。

【命令】

display link-aggregation member-port [*interface-list* | **auto**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-list: 成员端口列表，表示一个或多个成员端口。表示方式为 *interface-list* = *interface-type* *interface-number1* [**to** *interface-type* *interface-number2*]。其中，*interface-type* 为接口类型，*interface-number1* 和 *interface-number2* 为接口编号。*interface-number2* 的值要大于等于 *interface-number1* 的值。

auto: 显示所有自动聚合成员端口的链路聚合的详细信息。

【使用指导】

由于静态聚合组无法获知对端信息,因此静态聚合组只显示本端的端口编号、端口优先级和操作 Key 的值。

【举例】

显示静态聚合组内成员端口 GigabitEthernet1/0/1 上链路聚合的详细信息。

```
<Sysname> display link-aggregation member-port gigabitethernet 1/0/1
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

GigabitEthernet1/0/1:

Aggregate Interface: Bridge-Aggregation1

Port Number: 1

Port Priority: 32768

Oper-Key: 1

显示动态聚合组内成员端口 GigabitEthernet1/0/2 上链路聚合的详细信息。

```
<Sysname> display link-aggregation member-port gigabitethernet 1/0/2
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

GigabitEthernet1/0/2:

Aggregate Interface: Bridge-Aggregation2

Local:

Port Number: 2

Port Priority: 32768

Oper-Key: 2

Flag: {ACDEF}

Remote:

System ID: 0x8000, 000f-e267-6c6a

Port Number: 26

Port Priority: 32768

Oper-Key: 2

Flag: {ACDEF}

Received LACP Packets: 5 packet(s)

Illegal: 0 packet(s)

Sent LACP Packets: 7 packet(s)

表1-5 display link-aggregation member-port 命令显示信息描述表

字段	描述
Flags	LACP协议的状态标识，长度为1字节，该字节自低位至高位分别以英文字母A~H表示，某一位为1时打印出对应的英文字母，为0时不打印对应的英文字母。各标志位的含义如下： • A: LACP 是否开启标志。1 表示开启；0 表示关闭 • B: LACP 长/短超时标志。1 表示短超时；0 表示长超时 • C: 发送端认为本成员端口所在链路是否可聚合。1 表示是；0 表示否 • D: 发送端认为本成员端口所在链路是否处于同步状态。1 表示是；0 表示否 • E: 发送端认为本成员端口所在链路是否处于收集状态。1 表示是；0 表示否 • F: 发送端认为本成员端口所在链路是否处于分发状态。1 表示是；0 表示否 • G: 发送端的接收状态机是否处于默认状态。1 表示是；0 表示否 • H: 发送端的接收状态机是否处于超时状态。1 表示是；0 表示否
Aggregate Interface	本成员端口所属的聚合接口
Local	本端信息
Port Number	端口的编号
Port Priority	端口优先级
Oper-key	操作Key的值
Flag	LACP协议的状态标志值
Remote	对端信息
System ID	设备ID（由系统的LACP优先级和系统的MAC地址共同构成）
Received LACP Packets	收到的LACP报文总数
Illegal	非法报文的总数
Sent LACP Packets	发出的LACP报文总数

1.1.9 display link-aggregation summary

display link-aggregation summary 命令用来显示所有聚合组的摘要信息。

【命令】

display link-aggregation summary

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

由于静态聚合组无法获知对端信息，因此静态聚合组的对端信息无显示或显示为 **None**，并不代表对端系统的实际信息。

【举例】

```
# 显示所有聚合组的摘要信息。
<Sysname> display link-aggregation summary
Aggregate Interface Type:
BAGG -- Bridge-Aggregation, BLAGG -- Blade-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e267-6c6a
```

AGG Interface	AGG Mode	Partner ID	Selected Ports	Unselected Ports	Individual Ports	Share Type
RAGG1	S	None	1	0	0	NonS
BAGG2	D	0x8000, 00e0-fcfc-ff01	2	0	0	Shar

表1-6 display link-aggregation summary 命令显示信息描述表

字段	描述
Aggregate Interface Type	聚合接口类型： - BAGG：表示二层聚合接口 - RAGG：表示三层聚合接口
Aggregation Mode	聚合组类型： - S：表示静态聚合 - D：表示动态聚合
Loadsharing Type	负载分担类型： - Shar：表示负载分担类型 - NonS：表示非负载分担类型
Actor System ID	本端的设备ID（由系统的LACP优先级和系统的MAC地址共同构成）
AGG Interface	聚合接口的类型和编号
AGG Mode	聚合组的类型
Partner ID	对端的设备ID（由系统的LACP优先级和系统的MAC地址共同构成）
Selected Ports	处于选中状态的成员端口数量
Unselected Ports	处于非选中状态的成员端口数量
Individual Ports	处于独立状态的成员端口数量
Share Type	负载分担类型

1.1.10 display link-aggregation verbose

display link-aggregation verbose 命令用来显示已有聚合接口所对应聚合组的详细信息。

【命令】

```
display link-aggregation verbose [ { bridge-aggregation | route-aggregation }  
[ interface-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

bridge-aggregation: 显示二层聚合接口所对应聚合组的详细信息。

route-aggregation: 显示三层聚合接口所对应聚合组的详细信息。

interface-number: 聚合接口的编号。必须是当前已经创建的聚合接口编号。

【使用指导】

如果未指定聚合接口的类型，将显示设备支持的所有接口的相关信息。

如果仅指定了聚合接口的类型，将显示所有已创建的该类型聚合接口的相关信息。

只有在设备上创建了二层或三层聚合接口之后，才能指定 **bridge-aggregation** 或 **route-aggregation** 参数。

【举例】

二层聚合接口 1 所对应的聚合组是动态聚合组，显示该聚合组的详细信息。

```
<Sysname> display link-aggregation verbose bridge-aggregation 1  
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing  
Port Status: S -- Selected, U -- Unselected, I -- Individual  
Port: A -- Auto port  
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,  
        D -- Synchronization, E -- Collecting, F -- Distributing,  
        G -- Defaulted, H -- Expired
```

Aggregate Interface: Bridge-Aggregation1

Creation Mode: Manual

Aggregation Mode: Dynamic

Loadsharing Type: Shar

System ID: 0x8000, 000f-e267-6c6a

Local:

Port	Status	Priority	Oper-Key	Flag
GE1/0/1	S	32768	2	{ACDEF}

GE1/0/2	S	32768	2	{ACDEF}
GE1/0/3	S	32768	2	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
GE1/0/1	1	32768	2	0x8000, 000f-e267-57ad	{ACDEF}
GE1/0/2	1	32768	2	0x8000, 000f-e267-57ad	{ACDEF}
GE1/0/3	1	32768	2	0x8000, 000f-e267-57ad	{ACDEF}

三层聚合接口 1 所对应的聚合组是动态聚合组，显示该聚合组的详细信息。

```
<Sysname> display link-aggregation verbose route-aggregation 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

Aggregate Interface: Route-Aggregation1

Creation Mode: Manual

Aggregation Mode: Dynamic

Loadsharing Type: Shar

System ID: 0x8000, 000f-e267-6c6a

Local:

Port	Status	Priority	Oper-Key	Flag
GE1/0/1	S	32768	2	{ACDEF}
GE1/0/2	S	32768	2	{ACDEF}
GE1/0/3	S	32768	2	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
GE1/0/1	1	32768	2	0x8000, 000f-e267-57ad	{ACDEF}
GE1/0/2	1	32768	2	0x8000, 000f-e267-57ad	{ACDEF}
GE1/0/3	1	32768	2	0x8000, 000f-e267-57ad	{ACDEF}

二层聚合接口 2 所对应的聚合组是静态聚合组，显示该聚合组的详细信息。

```
<Sysname> display link-aggregation verbose bridge-aggregation 2
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

Aggregate Interface: Bridge-Aggregation2

Aggregation Mode: Static

Loadsharing Type: Shar

Port	Status	Priority	Oper-Key

```

GE1/0/1      S      32768    1
GE1/0/2      S      32768    1
GE1/0/3      S      32768    1
# 三层聚合接口 2 所对应的聚合组是静态聚合组，显示该聚合组的详细信息。
<Sysname> display link-aggregation verbose route-aggregation 2
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
      D -- Synchronization, E -- Collecting, F -- Distributing,
      G -- Defaulted, H -- Expired

```

```

Aggregate Interface: Route-Aggregation2
Aggregation Mode: Static
Loadsharing Type: Shar
  Port          Status  Priority Oper-Key
-----
GE1/0/1         S       32768    1
GE1/0/2         S       32768    1
GE1/0/3         S       32768    1

```

表1-7 display link-aggregation verbose 命令显示信息描述表

字段	描述
Loadsharing Type	负载分担类型： - Shar：表示负载分担类型 - NonS：表示非负载分担类型
Port Status	端口状态： - Selected：表示处于选中状态 - Unselected：表示处于非选中状态 - Individual：表示处于独立状态
Port	端口类型，Auto port表示为该端口为自动端口
Flags	LACP协议的状态标志，长度为1字节，该字节自低位至高位分别以字母A～H表示，取值为1的标志位显示为对应的字母，取值为0的标志为不显示。各标志位的含义如下： - A：LACP 是否开启标志。1表示开启；0表示关闭 - B：LACP 长/短超时标志。1表示短超时；0表示长超时 - C：发送端认为本成员端口所在链路是否可聚合。1表示是；0表示否 - D：发送端认为本成员端口所在链路是否处于同步状态。1表示是；0表示否 - E：发送端认为本成员端口所在链路是否处于收集状态。1表示是；0表示否 - F：发送端认为本成员端口所在链路是否处于分发状态。1表示是；0表示否 - G：发送端的接收状态机是否处于默认状态。1表示是；0表示否 - H：发送端的接收状态机是否处于超时状态。1表示是；0表示否
Aggregate Interface	聚合接口的名称

字段	描述
Creation Mode	动态聚合组的创建方式： • Auto: 表示自动创建 • Manual: 表示手工创建
Aggregation Mode	聚合组的工作模式： • Static: 表示静态聚合 • Dynamic: 表示动态聚合
System ID	设备ID（由系统的LACP优先级和系统的MAC地址共同构成）
Local	本端信息： • Port: 端口的类型和编号 • Status: 端口的选中/非选中/独立状态 • Priority: 端口优先级 • Oper-Key: 操作 Key 的值 • Flag: LACP 协议的状态标志值  说明 静态聚合组只显示本端信息，显示信息中不包括 Flag 字段
Remote	对端信息： • Actor: 本端的端口类型和编号，当对端端口是参考端口时，参考端口会显示在对应的本端端口上 • Partner: 对端端口的端口索引 • Priority: 对端端口的端口优先级 • Oper-Key: 对端端口的操作 Key 的值 • System ID: 对端的设备 ID • Flag: 对端的 LACP 协议的状态标志值

1.1.11 interface bridge-aggregation

interface bridge-aggregation 命令用来创建二层聚合接口，并进入二层聚合接口视图。如果指定的二层聚合接口已经存在，则直接进入该二层聚合接口视图。

undo interface bridge-aggregation 命令用来删除二层聚合接口。

【命令】

```
interface bridge-aggregation interface-number
undo interface bridge-aggregation interface-number
```

【缺省情况】

不存在二层聚合接口。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface-number: 指定二层聚合接口的编号。设备支持的取值范围为 1~64。

【使用指导】

创建二层聚合接口后，系统将自动生成同编号的二层聚合组，且该聚合组缺省工作在静态聚合模式下。

删除二层聚合接口的同时会删除其对应的二层聚合组，如果该聚合组内有成员端口，那么这些成员端口将自动从该聚合组中退出。

【举例】

创建二层聚合接口 1，并进入二层聚合接口 1 的视图。

```
<Sysname> system-view  
[Sysname] interface bridge-aggregation 1  
[Sysname-Bridge-Aggregation1]
```

1.1.12 interface route-aggregation

interface route-aggregation 命令用来创建三层聚合接口/子接口，并进入三层聚合接口/子接口视图。如果指定的三层聚合接口/子接口已经存在，则直接进入该三层聚合接口/子接口视图。

undo interface route-aggregation 命令用来删除三层聚合接口/子接口。

【命令】

```
interface          route-aggregation          { interface-number          |  
interface-number.subnumber }  
undo interface    route-aggregation          { interface-number          |  
interface-number.subnumber }
```

【缺省情况】

不存在三层聚合接口/子接口。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface-number: 指定三层聚合接口的编号，取值范围为 1~64。

interface-number.subnumber: 指定三层聚合子接口。其中 *interface-number* 为主接口编号；*subnumber* 为子接口编号，取值范围为 1~4094。

【使用指导】

创建三层聚合接口后，系统将自动生成同编号的三层聚合组，且该聚合组缺省工作在静态聚合模式下。

删除三层聚合接口的同时会删除其对应的三层聚合组以及该接口下的所有聚合子接口，如果该聚合组内有成员端口，那么这些成员端口将自动从该聚合组中退出。

如果删除三层聚合子接口，则不会影响其主接口以及主接口对应的聚合组状态。

【举例】

```
# 创建三层聚合接口 1，并进入三层聚合接口 1 的视图。  
<Sysname> system-view  
[Sysname] interface route-aggregation 1  
[Sysname-Route-Aggregation1]  
# 创建三层聚合子接口 1.1，并进入三层聚合子接口 1.1 的视图。  
<Sysname> system-view  
[Sysname] interface route-aggregation 1.1  
[Sysname-Route-Aggregation1.1]
```

1.1.13 jumboframe enable

jumboframe enable 命令用来允许超长帧通过。

undo jumboframe enable 命令用来禁止超长帧通过。

undo jumboframe enable size 命令用来恢复缺省情况。

【命令】

```
jumboframe enable [ size ]  
undo jumboframe enable [ size ]
```

【缺省情况】

设备允许最大长度的超长帧为 9216。

【视图】

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

size: 聚合接口上允许通过的超长帧的最大长度，单位为字节，取值为 9216。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 允许超长帧通过二层聚合接口 1。  
<Sysname> System-view
```

```
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] jumboframe enable
# 允许超长帧通过三层聚合接口 1。
<Sysname> System-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] jumboframe enable
```

1.1.14 lacp edge-port

lacp edge-port 命令用来配置聚合接口为聚合边缘接口。

undo lacp edge-port 命令用来恢复缺省情况。

【命令】

```
lacp edge-port
undo lacp edge-port
```

【缺省情况】

聚合接口不是聚合边缘接口。

【视图】

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

该命令主要用于在网络设备与服务器等终端设备相连的场景中。当网络设备配置了动态聚合模式，而终端设备未配置动态聚合模式时，网络设备的聚合成员端口都可以作为普通物理口转发报文，从而保证终端设备与网络设备间的多条链路可以相互备份，增加可靠性。

该配置仅在聚合接口对应的聚合组为动态聚合组时生效。

当聚合接口配置为聚合边缘接口后，聚合流量重定向功能将不能正常使用。

【举例】

```
# 配置二层聚合接口 1 为聚合边缘接口。
<Sysname> System-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] lacp edge-port
# 配置三层聚合接口 1 为聚合边缘接口。
<Sysname> System-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] lacp edge-port
```

1.1.15 lacp mode

lacp mode passive 命令用来配置端口的 LACP 工作模式为 PASSIVE。

undo lacp mode 命令用来恢复缺省情况。

【命令】

```
lacp mode passive
undo lacp mode
```

【缺省情况】

端口的 LACP 工作模式为 ACTIVE。

【视图】

二层以太网接口视图
三层以太网接口视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

执行本命令后，只有在当前端口为动态聚合组成员端口时，配置才生效。

如果动态聚合组内成员端口的 LACP 工作模式为 PASSIVE，且对端的 LACP 工作模式也为 PASSIVE 时，两端将不能发送 LACPDU。如果两端中任何一端的 LACP 工作模式为 ACTIVE 时，两端将可以发送 LACPDU。

【举例】

```
# 配置端口 GigabitEthernet1/0/1 的 LACP 工作模式为 PASSIVE。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp mode passive
```

1.1.16 lacp period short

lacp period short 命令用来配置端口的 LACP 超时时间为短超时（3 秒）。

undo lacp period 命令用来恢复缺省情况。

【命令】

```
lacp period short
undo lacp period
```

【缺省情况】

端口的 LACP 超时时间为长超时（90 秒）。

【视图】

二层以太网接口视图
三层以太网接口视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

请不要在 ISSU 升级前配置 LACP 超时时间为短超时, 否则在 ISSU 升级期间会出现网络流量中断, 导致流量转发不通。有关 ISSU 升级的详细介绍请参见“基础配置指导”中的“ISSU 配置”。

【举例】

```
# 配置端口 GigabitEthernet1/0/1 的 LACP 超时时间为短超时（3 秒）。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp period short
```

1.1.17 lacp system-priority

lacp system-priority 命令用来配置系统的 LACP 优先级。

undo lacp system-priority 命令用来恢复缺省情况。

【命令】

```
lacp system-priority priority
undo lacp system-priority
```

【缺省情况】

系统的 LACP 优先级为 32768。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

priority: 系统的 LACP 优先级, 取值范围为 0~65535。该数值越小, 优先级越高。

【举例】

```
# 配置系统的 LACP 优先级为 64。
<Sysname> system-view
[Sysname] lacp system-priority 64
```

【相关命令】

- **link-aggregation port-priority**

1.1.18 link-aggregation auto-aggregation enable

link-aggregation auto-aggregation enable 命令用来开启全自动聚合功能。

undo link-aggregation auto-aggregation enable 命令用来关闭全自动聚合功能。

【命令】

```
link-aggregation auto-aggregation enable
undo link-aggregation auto-aggregation enable
```

【缺省情况】

全自动聚合功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启 LLDP 功能和全自动聚合功能后，当本端端口收到对端发来的 LLDP 报文，根据报文信息，自动创建一个聚合组，同时将连接相同对端设备的端口加入该聚合组。若关闭 LLDP 功能或者关闭全自动聚合功能，端口将退出聚合组，但自动创建的聚合组不会被删除。

配置本命令后，开启了 LLDP 功能的三层以太网接口下可能无法创建子接口。

配置本命令后，对于自动加入聚合组的成员端口，建议不要修改其配置，以避免该成员端口退出聚合组。

当端口自动加入聚合组时，如果端口下存在 **port link-aggregation group** 配置，则以端口下配置为准。

【举例】

开启全自动聚合功能。

```
<Sysname> system
```

```
[Sysname] link-aggregation auto-aggregation enable
```

【相关命令】

- **lldp enable**（二层技术-以太网交换命令参考/LLDP）
- **lldp global enable**（二层技术-以太网交换命令参考/LLDP）
- **port link-aggregation group**

1.1.19 link-aggregation global load-sharing mode

link-aggregation global load-sharing mode 命令用来配置全局采用的聚合负载分担类型。

undo link-aggregation global load-sharing mode 命令用来恢复缺省情况。

【命令】

```
link-aggregation global load-sharing mode { destination-ip |  
destination-mac | destination-port | ingress-port | source-ip | source-mac |  
source-port } *
```

```
undo link-aggregation global load-sharing mode
```

【缺省情况】

设备按照源 IP 地址和目的 IP 地址进行负载分担。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

destination-ip: 表示按报文的目的 IP 地址进行聚合负载分担。

destination-mac: 表示按报文的目的 MAC 地址进行聚合负载分担。

destination-port: 表示按报文的目的服务端口进行聚合负载分担。

ingress-port: 表示按报文的入端口进行聚合负载分担。

source-ip: 表示按报文的源 IP 地址进行聚合负载分担。

source-mac: 表示按报文的源 MAC 地址进行聚合负载分担。

source-port: 表示按报文的源服务端口进行聚合负载分担。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

对于设备不支持的聚合负载分担类型，系统将提示用户不支持。

【举例】

配置全局按照报文目的 MAC 地址进行聚合负载分担。

```
<Sysname> system-view
```

```
[Sysname] link-aggregation global load-sharing mode destination-mac
```

【相关命令】

- **bandwidth**
- **link-aggregation load-sharing mode**

1.1.20 link-aggregation ignore vlan

link-aggregation ignore vlan 命令用来配置二层聚合接口的忽略 VLAN。

undo link-aggregation ignore vlan 命令用来取消二层聚合接口配置的忽略 VLAN。

【命令】

link-aggregation ignore vlan *vlan-id-list*

undo link-aggregation ignore vlan *vlan-id-list*

【缺省情况】

未配置二层聚合接口的忽略 VLAN。

【视图】

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

vlan-id-list: 忽略 VLAN 列表。表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] }&<1-10>**, **vlan-id1** 和 **vlan-id2** 取值范围为 1~4094, **vlan-id2** 的值要大于或等于 **vlan-id1** 的值, **&<1-10>**表示前面的参数最多可以重复输入 10 次。

【使用指导】

通过本命令配置二层聚合接口的忽略 VLAN 后, 二层聚合接口在确定其成员端口的选中状态时忽略这些 VLAN 允许通过的配置 (包括是否允许 VLAN 通过, 以及通过的方式), 也就是说即使二层聚合接口及其成员端口关于这些 VLAN 的允许通过的配置不一致, 也不影响成员端口的选中状态。

本命令仅对 Hybrid 或者 Trunk 类型的端口所允许通过的 VLAN 范围有效。

【举例】

在二层聚合接口 1 上配置忽略 VLAN 50, 这时该聚合接口在确定其成员端口的选中状态时, 不考虑 VLAN 50 允许通过的配置是否一致。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation ignore vlan 50
```

1.1.21 link-aggregation lacp traffic-redirect-notification enable

link-aggregation lacp traffic-redirect-notification enable 命令用来开启聚合流量重定向功能。

undo link-aggregation lacp traffic-redirect-notification enable 命令用来关闭聚合流量重定向功能。

【命令】

```
link-aggregation lacp traffic-redirect-notification enable
undo link-aggregation lacp traffic-redirect-notification enable
```

【缺省情况】

聚合流量重定向功能处于关闭状态。

【视图】

系统视图
二层聚合接口视图
三层聚合接口视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

在开启了聚合流量重定向功能后, 当手工关闭聚合组内某选中端口或重启聚合组内某选中端口所在的 slot 时, 系统可以将该端口上的流量重定向到其他选中端口上, 从而实现聚合链路上流量的不中

断。聚合流量重定向过程中，对于聚合组中新选中的端口，流量不会重定向到该端口上。其中，已知单播报文可以实现零丢包，非已知单播报文不保证不丢包。

只有动态聚合组支持聚合流量重定向功能。

必须在聚合链路两端都开启聚合流量重定向功能才能实现聚合链路上流量的不中断。

当聚合接口配置为聚合边缘接口后，聚合流量重定向功能将不能正常使用。

全局的配置对所有聚合组都有效，而聚合组内的配置只对当前聚合组有效。对于一个聚合组来说，优先采用该聚合组内的配置，只有该聚合组内未进行配置时，才采用全局的配置。

建议优先选择开启聚合接口的聚合流量重定向功能。开启全局的聚合流量重定向功能时，如果有连接其它厂商设备的聚合接口，可能影响该聚合组的正常通信。

【举例】

开启聚合流量重定向功能。

```
<Sysname> system-view
```

```
[Sysname] link-aggregation lacp traffic-redirect-notification enable
```

1.1.22 link-aggregation load-sharing mode

link-aggregation load-sharing mode 命令用来配置聚合组内采用的聚合负载分担类型。

undo link-aggregation load-sharing mode 命令用来恢复缺省情况。

【命令】

```
link-aggregation load-sharing mode { destination-ip | destination-mac |  
source-ip | source-mac } *
```

```
undo link-aggregation load-sharing mode
```

【缺省情况】

聚合组内采用的聚合负载分担类型与全局的配置相同。

【视图】

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

destination-ip: 表示按报文的目的 IP 地址进行聚合负载分担。

destination-mac: 表示按报文的目的 MAC 地址进行聚合负载分担。

source-ip: 表示按报文的源 IP 地址进行聚合负载分担。

source-mac: 表示按报文的源 MAC 地址进行聚合负载分担。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

对于设备不支持的聚合负载分担类型，系统将提示用户不支持。

【举例】

```
# 配置二层聚合接口 1 对应的聚合组内按照报文目的 MAC 地址进行聚合负载分担。
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation load-sharing mode destination-mac
# 配置三层聚合接口 1 对应的聚合组内按照报文目的 MAC 地址进行聚合负载分担。
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation load-sharing mode destination-mac
```

【相关命令】

- **bandwidth**
- **link-aggregation global load-sharing mode**

1.1.23 link-aggregation load-sharing mode local-first

link-aggregation load-sharing mode local-first 命令用来配置聚合负载分担采用本地转发优先。

undo link-aggregation load-sharing mode local-first 命令用来取消聚合负载分担采用本地转发优先。

【命令】

```
link-aggregation load-sharing mode local-first
undo link-aggregation load-sharing mode local-first
```

【缺省情况】

聚合负载分担采用本地转发优先。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

取消聚合负载分担采用本地转发优先后，从聚合接口转发的报文将在 IRF 所有成员设备的所有选中端口间进行负载分担。

【举例】

```
# 取消聚合负载分担采用本地转发优先。
<Sysname> system-view
[Sysname] undo link-aggregation load-sharing mode local-first
```

1.1.24 link-aggregation mode

link-aggregation mode dynamic 命令用来配置聚合组工作在动态聚合模式下，同时开启 LACP 协议。

undo link-aggregation mode 命令用来恢复缺省情况。

【命令】

link-aggregation mode dynamic

undo link-aggregation mode

【缺省情况】

聚合组工作在静态聚合模式下。

【视图】

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

当聚合组中存在成员端口时，如果修改聚合组的工作模式，则可能导致聚合组中选中端口变为非选中状态，影响流量转发，请用户根据实际情况修改聚合组的工作模式。

【举例】

配置二层聚合接口 1 对应的聚合组工作在动态聚合模式下。

```
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
```

配置三层聚合接口 1 对应的聚合组工作在动态聚合模式下。

```
<Sysname> system-view
```

```
[Sysname] interface route-aggregation 1
```

```
[Sysname-Route-Aggregation1] link-aggregation mode dynamic
```

1.1.25 link-aggregation port-priority

link-aggregation port-priority 命令用来配置端口优先级。

undo link-aggregation port-priority 命令用来恢复缺省情况。

【命令】

link-aggregation port-priority *priority*

undo link-aggregation port-priority

【缺省情况】

端口优先级为 32768。

【视图】

二层以太网接口视图
三层以太网接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

priority: 端口优先级，取值范围为 0~65535。该数值越小，优先级越高。

【举例】

```
# 配置二层以太网接口 GigabitEthernet1/0/1 的端口优先级为 64。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-aggregation port-priority 64
# 配置三层以太网接口 GigabitEthernet1/0/2 的端口优先级为 64。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] link-aggregation port-priority 64
```

【相关命令】

- **lacp system-priority**

1.1.26 link-aggregation selected-port maximum

link-aggregation selected-port maximum 命令用来配置聚合组中的最大选中端口数。
undo link-aggregation selected-port maximum 命令用来恢复缺省情况。

【命令】

```
link-aggregation selected-port maximum max-number  
undo link-aggregation selected-port maximum
```

【缺省情况】

聚合组中的最大选中端口数仅受设备硬件能力的限制。

【视图】

二层聚合接口视图
三层聚合接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

max-number: 聚合组中的最大选中端口数。取值范围为 1~16。

【使用指导】

执行本命令可能导致聚合组内部分成员端口变为非选中状态。

本端和对端配置的聚合组中的最大选中端口数必须一致。

同一聚合组内，最大选中端口数配置值不能小于最小选中端口数配置值。

当配置了聚合组中的最大选中端口数之后，最大选中端口数将同时受配置值和设备硬件能力的限制，即取二者的较小值作为限制值。

用户借此可实现两端口间的冗余备份：在一个聚合组中只添加两个成员端口，并配置该聚合组中的最大选中端口数为 1，这样这两个成员端口在同一时刻就只能有一个成为选中端口，而另一个将作为备份端口。

【举例】

配置二层聚合接口 1 对应的聚合组中的最大选中端口数为 5。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port maximum 5
```

配置三层聚合接口 1 对应的聚合组中的最大选中端口数为 5。

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation selected-port maximum 5
```

【相关命令】

- **link-aggregation selected-port minimum**

1.1.27 link-aggregation selected-port minimum

link-aggregation selected-port minimum 命令用来配置聚合组中的最小选中端口数。

undo link-aggregation selected-port minimum 命令用来恢复缺省情况。

【命令】

```
link-aggregation selected-port minimum min-number
undo link-aggregation selected-port minimum
```

【缺省情况】

聚合组中的最小选中端口数不受限制。

【视图】

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

min-number：聚合组中的最小选中端口数。设备支持的取值范围为 1~16。

【使用指导】

执行本命令可能导致聚合组内所有成员端口都变为非选中状态。

本端和对端配置的聚合组中的最小选中端口数必须一致。

同一聚合组内，最小选中端口数配置值不能大于最大选中端口数配置值。

【举例】

配置二层聚合接口 1 对应的聚合组中的最小选中端口数为 3。

```
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1
```

```
[Sysname-Bridge-Aggregation1] link-aggregation selected-port minimum 3
```

配置三层聚合接口 1 对应的聚合组中的最小选中端口数为 3。

```
<Sysname> system-view
```

```
[Sysname] interface route-aggregation 1
```

```
[Sysname-Route-Aggregation1] link-aggregation selected-port minimum 3
```

【相关命令】

- **link-aggregation selected-port maximum**

1.1.28 link-delay

link-delay 命令用来配置聚合接口物理连接状态抑制功能。

undo link-delay 命令用来恢复缺省情况。

【命令】

```
link-delay [ msec ] delay-time [ mode { up | updown } ]
```

```
undo link-delay [ msec ] delay-time [ mode { up | updown } ]
```

【缺省情况】

接口状态改变时，系统会将接口状态改变立即上报 CPU。

【视图】

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

msec: 表示配置的抑制时间为毫秒级。不指定该参数时，表示配置的抑制时间为秒级。

delay-time: 接口物理连接状态抑制时间值，0 表示不抑制，即接口状态改变时立即上报 CPU。

- 未指定 **msec** 参数时，取值范围为 0~30，单位为秒。
- 指定 **msec** 参数时，取值范围为 0~10000，且为 100 的倍数，单位为毫秒。

mode up: 设置聚合接口物理连接 up 状态抑制功能。

mode updown: 设置聚合接口物理连接 up 和 down 状态抑制功能。

【使用指导】

使用该命令时，选取的参数不同，抑制效果不同：

- 不指定 **mode** 参数：表示接口状态从 **up** 变成 **down** 时，不会立即上报 CPU。而是等待 *delay-time* 时间后，再检查接口状态，如果状态仍然是 **down**，再上报。接口状态从 **down** 变成 **up** 时，立即上报 CPU。
- **mode up**：表示接口状态从 **down** 变成 **up** 时，不会立即上报 CPU。而是等待 *delay-time* 时间后，再检查接口状态，如果状态仍然是 **up**，再上报。接口状态从 **up** 变成 **down** 时，立即上报 CPU。
- **mode updown**：表示接口状态从 **up** 变成 **down** 或者 **down** 变成 **up** 时，都不会立即上报 CPU。等待 *delay-time* 时间后，再检查接口状态，如果状态仍然是 **down** 或者 **up**，再上报。

同一接口下，接口状态从 **up** 变成 **down** 的抑制时间和接口状态从 **down** 变成 **up** 的抑制时间可以不同。如果在同一端口下，多次执行本命令配置了不同的抑制时间，则两个抑制时间会分别以最新配置为准。

【举例】

设置二层聚合接口 1 的物理连接 **down** 状态抑制时间为 8 秒。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-delay 8
```

设置三层聚合接口 1 的物理连接 **down** 状态抑制时间为 8 秒。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-delay 8
```

1.1.29 mtu

mtu 命令用来配置三层聚合接口/子接口的 MTU 值。

undo mtu 命令用来恢复缺省情况。

【命令】

mtu size
undo mtu

【缺省情况】

三层聚合接口/子接口的 MTU 值为 1500 字节。

【视图】

三层聚合接口视图

三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

size：MTU 值的大小，单位为字节。取值范围为 46～1560。

【举例】

```
# 配置三层聚合接口 1 的 MTU 值为 1430 字节。
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] mtu 1430
```

【相关命令】

- **display interface**

1.1.30 port link-aggregation group

port link-aggregation group 命令用来将接口加入指定的聚合组。

undo port link-aggregation group 命令用来将接口从已加入的聚合组中删除。

【命令】

```
port link-aggregation group group-id
undo port link-aggregation group
```

【缺省情况】

接口未加入任何聚合组。

【视图】

二层以太网接口视图

三层以太网接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-id: 指定聚合组所对应聚合接口的编号。设备支持的取值范围为 1~64。

【使用指导】

二层以太网接口只能加入二层聚合组，三层以太网接口只能加入三层聚合组。

一个接口只能加入一个聚合组。

以太网接口不能和以太网子接口加入同一个聚合组。

加入聚合组的以太网接口不能再创建子接口；已创建子接口的以太网接口不能加入聚合组。

成员端口为以太网子接口的聚合组对应的聚合接口不能再创建聚合子接口；以太网子接口不能加入已创建聚合子接口的聚合组。

以太网冗余接口的成员接口和冗余组节点的成员接口不能再加入聚合组。有关以太网冗余接口和冗余组节点的详细介绍，请参见“可靠性配置指导”中的“冗余备份”。

【举例】

```
# 将二层以太网接口 GigabitEthernet1/0/1 加入二层聚合组 1 中。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 1
# 将三层以太网接口 GigabitEthernet1/0/2 加入三层聚合组 2 中。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-aggregation group 2
```

1.1.31 reset counters interface

reset counters interface 命令用来清除聚合接口上的统计信息。

【命令】

```
reset counters interface [ { bridge-aggregation | route-aggregation }
[ interface-number ] ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

bridge-aggregation: 清除二层聚合接口上的统计信息。

route-aggregation: 清除三层聚合接口上的统计信息。

interface-number: 聚合接口的编号，取值范围为已创建的聚合接口的编号。

【使用指导】

在某些情况下，需要统计一定时间内某二层聚合接口的流量，这就需要在统计开始前清除该接口上原有的统计信息，以便重新进行统计。

如果未指定聚合接口的类型，将清除所有接口的统计信息。

如果仅指定了聚合接口的类型，将清除所有已创建的该类型聚合接口的相关信息。

只有在设备上创建了二层或三层聚合接口之后，才能指定 **bridge-aggregation** 或 **route-aggregation** 参数。

【举例】

清除二层聚合接口 1 上的统计信息。

```
<Sysname> reset counters interface bridge-aggregation 1
```

1.1.32 reset lacp statistics

reset lacp statistics 命令用来清除成员端口上的 LACP 统计信息。

【命令】

```
reset lacp statistics [ interface interface-list ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface interface-list: 表示清除指定成员端口上的 LACP 统计信息。*interface-list* 为成员端口列表，表示一个或多个成员端口。表示方式为 *interface-list* = *interface-type* *interface-number1* [**to** *interface-type* *interface-number2*]。其中，*interface-type* 为接口类型，*interface-number1* 和 *interface-number2* 为接口编号。*interface-number2* 的值要大于等于 *interface-number1* 的值。若未指定本参数，则清除所有成员端口上的 LACP 统计信息。

【举例】

```
# 清除所有成员端口上的 LACP 统计信息。  
<Sysname> reset lacp statistics
```

【相关命令】

- **display link-aggregation member-port**

1.1.33 shutdown

shutdown 命令用来关闭接口。

undo shutdown 命令用来打开接口。

【命令】

shutdown
undo shutdown

【缺省情况】

接口处于开启状态。

【视图】

二层聚合接口视图
三层聚合接口视图
三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

当打开/关闭三层聚合接口时，会同时打开/关闭其下的所有子接口，而打开/关闭三层聚合子接口则不会对其主接口有影响。

【举例】

```
# 开启二层聚合接口 1。  
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo shutdown
# 开启三层聚合接口 1。
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] undo shutdown
```


目 录

1 VLAN	1-1
1.1 VLAN配置命令	1-1
1.1.1 bandwidth	1-1
1.1.2 default	1-1
1.1.3 description	1-2
1.1.4 display interface vlan-interface	1-3
1.1.5 display vlan	1-6
1.1.6 display vlan brief	1-7
1.1.7 interface vlan-interface	1-8
1.1.8 mtu	1-9
1.1.9 name	1-10
1.1.10 reset counters interface vlan-interface	1-10
1.1.11 shutdown	1-11
1.1.12 vlan	1-12
1.2 基于端口的VLAN配置命令	1-13
1.2.1 display port	1-13
1.2.2 port	1-14
1.2.3 port access vlan	1-15
1.2.4 port hybrid pvid	1-16
1.2.5 port hybrid vlan	1-16
1.2.6 port link-type	1-17
1.2.7 port trunk permit vlan	1-18
1.2.8 port trunk pvid	1-19
1.3 VLAN组配置命令	1-20
1.3.1 display vlan-group	1-20
1.3.2 vlan-group	1-21
1.3.3 vlan-list	1-22

1 VLAN

1.1 VLAN配置命令

1.1.1 bandwidth

bandwidth 命令用来配置 VLAN 接口的期望带宽。

undo bandwidth 命令用来恢复缺省情况。

【命令】

bandwidth *bandwidth-value*

undo bandwidth

【缺省情况】

接口的期望带宽 = 接口的波特率 ÷ 1000 (kbps)。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

bandwidth-value: 表示接口的期望带宽，取值范围为 1~400000000，单位为 kbps。

【使用指导】

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

【举例】

配置 VLAN 接口 1 的期望带宽为 10000kbps。

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 1
```

```
[Sysname-Vlan-interface1] bandwidth 10000
```

1.1.2 default

default 命令用来恢复 VLAN 接口的缺省配置。

【命令】

default

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】



注意

接口下的某些配置取消后，会对现有功能产生影响，建议您在执行该命令前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

【举例】

将 VLAN 接口 1 恢复为缺省配置。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] default
```

1.1.3 description

description 命令用来配置 VLAN 或 VLAN 接口的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

VLAN 的描述信息为“VLAN *vlan-id*”，其中 *vlan-id* 为该 VLAN 的四位数编号，如果该 VLAN 的编号不足四位，则会在编号前增加 0，补齐四位。例如，VLAN 100 的描述信息为“VLAN 0100”；VLAN 接口的描述信息为该 VLAN 接口的接口名，如“Vlan-interface1 Interface”。

【视图】

VLAN 视图

VLAN 接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

text: VLAN 或 VLAN 接口的描述信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

用户可以根据功能或者连接情况为 VLAN 或 VLAN 接口配置特定的描述信息，以便记忆和管理 VLAN 或 VLAN 接口。

【举例】

```
# 将 VLAN 2 的描述信息配置为 sales-private。
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] description sales-private
# 将 VLAN 接口 2 的描述信息配置为 linktoPC56。
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] description linktoPC56
```

【相关命令】

- **display interface vlan-interface**
- **display vlan**

1.1.4 display interface vlan-interface

display interface vlan-interface 命令用来显示 VLAN 接口的相关信息。

【命令】

```
display interface [ vlan-interface [ interface-number ] ] [ brief  
[ description | down ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

vlan-interface interface-number: VLAN 接口的编号，显示指定 VLAN 接口的信息。如果不指定 **vlan-interface** 参数，将显示设备支持的所有接口的相关信息；如果指定 **vlan-interface** 参数，不指定 **interface-number** 参数，将显示已创建的所有 VLAN 接口的信息。

brief: 显示接口的概要信息。不指定该参数时，将显示接口的详细信息。

description: 用来显示用户配置的接口的全部描述信息。如果不指定该 **description** 参数，只显示描述信息中的前 27 个字符。

down: 显示当前物理状态为 down 的接口的信息以及 down 的原因。不指定该参数时，将不会根据接口物理状态来过滤显示信息。

【举例】

```
# 显示 VLAN-interface 2 的相关信息。
```

```

<Sysname> display interface vlan-interface 2
Vlan-interface2
Current state: DOWN
Line protocol state: DOWN
Description: Vlan-interface2 Interface
Bandwidth: 100000 kbps
Maximum transmission unit: 1500
Internet protocol processing : Disabled
IP packet frame type: Ethernet II, hardware address: 000f-e249-8050
IPv6 packet frame type: Ethernet II, hardware address: 000f-e249-8050
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
# 显示 VLAN-interface 2 的概要信息。
<Sysname> display interface vlan-interface 2 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
Vlan2              DOWN DOWN      --

```

表1-1 display interface vlan-interface 命令显示信息描述表

字段	描述
Vlan-interface2	VLAN接口名
Current state	VLAN接口的物理状态，状态可能为： - Administratively DOWN: 表示该 VLAN 接口已经通过 shutdown 命令被关闭，即管理状态为关闭 - DOWN: 表示该 VLAN 接口的管理状态为开启，但物理状态为关闭，即该接口对应的 VLAN 内没有处于 UP 状态的物理端口（可能因为没有物理连线或者线路故障） - UP: 该端口的管理状态和物理状态均为开启
Line protocol state	VLAN接口的链路层协议状态，状态可能为： - DOWN: 该 VLAN 接口的协议状态为关闭 - UP: 该 VLAN 接口的协议状态为开启
Description	VLAN接口的描述信息
Bandwidth	VLAN接口的期望带宽
Maximum transmission unit	VLAN接口允许通过的MTU
Internet protocol processing : Disabled	该接口还不具有处理IP报文的能力，当没有为该接口配置IP地址时会显示该信息
IP packet frame type	IPv4发送帧格式
hardware address	VLAN接口对应的MAC地址

字段	描述
IPv6 packet frame type	IPv6发送帧格式
Last clearing of counters	最近一次使用 reset counters interface vlan-interface 命令清除接口下的统计信息的时间。如果从设备启动一直没有执行 reset counters interface vlan-interface 命令清除过该接口下的统计信息，则显示Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	当前接口最近300秒内输入（input）和输出（output）报文的平均速率（单位分别为字节/秒、比特/秒和数据包/秒）。
Input: 0 packets, 0 bytes, 0 drops	接口输入的报文总数（分别以包和字节为单位进行了统计），输入报文中丢弃的报文数。
Output: 0 packets, 0 bytes, 0 drops	接口输出的报文总数（分别以包和字节为单位进行了统计），输出报文中丢弃的报文数。
Brief information on interfaces in route mode	三层模式下（route）的接口的概要信息，即三层接口的概要信息
Link: ADM - administratively down; Stby - standby	- 如果某接口的 Link 属性值为“ADM”，则表示该接口被管理员通过 shutdown 命令关闭，需要在该接口下执行 undo shutdown 命令才能恢复端口本身的物理状态 - 如果某接口的 Link 属性值为“Stby”，则表示该接口是一个处于 Standby 状态的备份接口，使用 display interface-backup state 命令可以查看该备份接口对应的主接口
Protocol: (s) - spoofing	如果某接口的Protocol属性值中带有“(s)”字符串，则表示该接口的数据链路层协议状态显示为UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的
Interface	接口名称缩写
Link	接口物理连接状态，取值为： - UP：表示接口物理上是连通的 - DOWN：表示接口物理上是不通的 - ADM：表示接口被管理员通过 shutdown 命令关闭，需要执行 undo shutdown 命令才能恢复接口本身的物理状态 - Stby：表示该接口是一个处于 Standby 状态的备份接口
Protocol	接口数据链路层协议状态，取值为： - UP：表示接口的数据链路层协议状态为开启 - DOWN：表示接口的数据链路层协议状态为关闭 - UP(s)：表示接口的数据链路层协议状态显示为UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的
Primary IP	接口主IP地址

【相关命令】

- reset counters interface vlan-interface**

1.1.5 display vlan

display vlan 命令用来显示 VLAN 的相关信息。

【命令】

display vlan [*vlan-id1* [*to vlan-id2*] | **all** | **dynamic** | **static**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vlan-id1: 显示指定 VLAN 的信息。*vlan-id1* 为 VLAN 的编号，取值范围为 1~4094。

vlan-id1 to vlan-id2: 显示 ID 在指定范围内的 VLAN 的信息。*vlan-id1* 和 *vlan-id2* 为指定 VLAN 的编号，取值范围为 1~4094。*vlan-id2* 的值要大于或等于 *vlan-id1* 的值。

all: 显示所有 VLAN 的信息。

dynamic: 显示系统动态创建的 VLAN 的数量和编号。动态 VLAN 是指通过 RADIUS 服务器下发的 VLAN。

static: 显示系统静态创建的 VLAN 的数量和 VLAN 编号。静态 VLAN 是指通过命令行手工创建的 VLAN。

【举例】

显示 VLAN 2 的信息。

```
<Sysname> display vlan 2
VLAN ID: 2
VLAN type: Static
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:   None
Untagged ports:
    GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

显示 VLAN 3 的信息。

```
<Sysname> display vlan 3
VLAN ID: 3
VLAN type: static
Route interface: Configured
IPv4 address: 1.1.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:   None
```

Untagged ports: None

表1-2 display vlan 命令显示信息描述表

字段	解释
VLAN ID	VLAN的编号
VLAN type	VLAN的类型： • Static: 静态 VLAN • Dynamic: 动态 VLAN
Route interface	设备上是否创建了对应的VLAN接口： • Not configured: 未创建 • Configured: 已创建
Description	VLAN的描述信息
Name	VLAN的名称
IP address	VLAN接口的主用IP地址，如果VLAN接口没有配置IP地址，则不显示该字段，如果VLAN接口上还配置了从IP地址，可以使用 display interface vlan-interface 或者在VLAN接口视图下使用 display this 命令查看
Subnet mask	VLAN接口的主用IP地址的子网掩码，如果VLAN接口没有配置IP地址，则不显示该字段
Tagged ports	该VLAN报文从哪些端口发送时需要携带Tag标记
Untagged ports	该VLAN报文从哪些端口发送时不需要携带Tag标记

【相关命令】

- **vlan**

1.1.6 display vlan brief

display vlan brief 命令用来显示设备上所有已创建 VLAN 的概要信息。

【命令】

display vlan brief

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示设备上所有已创建 VLAN 的概要信息。


```

<Sysname> display vlan brief
Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1
VLAN ID   Name                               Port
1          VLAN 0001                       GE1/0/1  GE1/0/2  GE1/0/3
2          VLAN 0002
3          VLAN 0003

```

表1-3 display vlan brief 命令显示信息描述表

字段	描述
Brief information about all VLANs:	所有VLAN的概要信息
Supported Minimum VLAN ID	系统支持的最小VLAN ID
Supported Maximum VLAN ID	系统支持的最大VLAN ID
Default VLAN ID	缺省VLAN ID
VLAN ID	VLAN的编号
Name	VLAN的名称
Port	允许该VLAN报文通过的端口

1.1.7 interface vlan-interface

interface vlan-interface 命令用来创建 VLAN 接口并进入 VLAN 接口视图。如果该 VLAN 接口已经存在，则直接进入 VLAN 接口视图。

undo interface vlan-interface 命令用来删除指定的 VLAN 接口。

【命令】

```

interface vlan-interface interface-number
undo interface vlan-interface interface-number

```

【缺省情况】

不存在 VLAN 接口。

【视图】

系统视图

【缺省用户角色】

```

network-admin
context-admin

```

【参数】

interface-number: VLAN 接口的编号，取值范围为 1~4094。

【使用指导】

在创建 VLAN 接口之前，对应的 VLAN 必须已经存在，否则将不能创建指定的 VLAN 接口。

【举例】

```
# 创建 VLAN 接口 2 并进入视图。  
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] quit  
[Sysname] interface vlan-interface 2  
[Sysname-Vlan-interface2]
```

【相关命令】

- **display interface vlan-interface**

1.1.8 mtu

mtu 命令用来配置 VLAN 接口的 MTU 值。

undo mtu 命令用来恢复缺省情况。

【命令】

```
mtu size  
undo mtu
```

【缺省情况】

VLAN 接口的 MTU 值为 1500。

【视图】

VLAN 接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

size: 表示接口允许通过的 MTU（Maximum Transmission Unit，最大传输单元）值的大小，单位为字节。取值范围 46~1500。

【使用指导】

如果当前接口同时配置 **mtu** 和 **ip mtu** 命令，则设备会以 **ip mtu** 命令配置的接口 MTU 值对报文进行分片，不会再按照 **mtu** 命令配置的 MTU 值对报文进行分片。有关 **ip mtu** 命令的详细介绍，请参见“三层技术-IP 业务命令参考”中的“IP 性能优化”。

【举例】

```
# 配置 VLAN 接口 1 的 MTU 值为 1492 字节。  
<Sysname> system-view  
[Sysname] interface vlan-interface 1  
[Sysname-Vlan-interface1] mtu 1492
```

【相关命令】

- **display interface vlan-interface**

1.1.9 name

name 命令用来指定当前 VLAN 的名称。

undo name 命令用来恢复缺省情况。

【命令】

name text

undo name

【缺省情况】

VLAN 的名称为“VLAN *vlan-id*”，其中 *vlan-id* 为该 VLAN 的四位数编号，如果该 VLAN 的编号不足四位，则会在编号前增加 0，补齐四位。例如，VLAN 100 的名称为“VLAN 0100”。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: VLAN 名称，为 1~32 个字符的描述信息，区分大小写。

【使用指导】

当设备上配置了 MAC 地址认证功能后，可以通过 RADIUS 服务器来对认证通过的端口下发 VLAN。某些 RADIUS 服务器可以向设备发送需要下发的 VLAN 编号或者 VLAN 名称，当 VLAN 数量很多的时候，使用名称可以更明确的定位 VLAN。

【举例】

指定 VLAN 2 的名称为“test vlan”。

```
<Sysname> system-view
```

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] name test vlan
```

【相关命令】

- **display vlan**

1.1.10 reset counters interface vlan-interface

reset counters interface vlan-interface 命令用来清除 VLAN 接口的统计信息。

【命令】

reset counters interface [vlan-interface [*interface-number*]]

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

vlan-interface interface-number: VLAN 接口的编号，清除指定 VLAN 接口的统计信息。
如果不指定 **vlan-interface** 参数，则清除所有接口的统计信息；如果指定 **vlan-interface** 参数，不指定 **interface-number** 参数，则清除所有 VLAN 接口的统计信息。

【使用指导】

在某些情况下，需要统计一定时间内某接口的流量，这就需要在统计开始前清除该接口原有的统计信息，重新进行统计。

【举例】

清除 VLAN 接口 2 的统计信息。
<Sysname> reset counters interface vlan-interface 2

【相关命令】

- **display interface vlan-interface**

1.1.11 shutdown

shutdown 命令用来手工关闭 VLAN 接口。
undo shutdown 命令用来手工开启 VLAN 接口。

【命令】

shutdown
undo shutdown

【缺省情况】

未手工关闭 VLAN 接口。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

如果未手工关闭 VLAN 接口，此时 VLAN 接口状态受 VLAN 中端口状态的影响，即：

- 当 VLAN 中所有以太网端口状态均为 down 时，VLAN 接口为 down 状态，即关闭状态。
- 当 VLAN 中有一个或一个以上的以太网端口处于 up 状态时，则 VLAN 接口处于 up 状态。

如果手工关闭 VLAN 接口，则 VLAN 接口的状态始终为 down (Administratively)，不受 VLAN 中端口状态的影响。

配置 VLAN 接口参数前，为了避免配置过程中对网络造成影响，建议先使用 **shutdown** 命令手工关闭接口，之后再配置参数。配置完成后，使用 **undo shutdown** 命令取消手工关闭接口，使配置的参数生效。

当 VLAN 接口出现故障时，可以使用 **shutdown** 命令手工关闭接口，然后再使用 **undo shutdown** 命令取消手工关闭接口，这样有可能使接口恢复正常。

关闭和打开 VLAN 接口对于属于这个 VLAN 的任何一个以太网端口本身都不起作用，以太网端口的状态不随 VLAN 接口状态的变化而改变。

【举例】

将 VLAN 接口 2 关闭后再重新打开。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] shutdown
[Sysname-Vlan-interface2] undo shutdown
```

1.1.12 vlan

vlan vlan-id 命令用来创建 VLAN，并进入 VLAN 视图。如果指定的 VLAN 已存在，则直接进入该 VLAN 的视图。

vlan vlan-id1 to vlan-id2 命令用来批量创建 *vlan-id1*~*vlan-id2* 之间的所有 VLAN，保留 VLAN 除外。

vlan all 命令用来批量创建 VLAN 1~4094。

undo vlan 命令用来删除 VLAN。

【命令】

```
vlan { vlan-id1 [ to vlan-id2 ] | all }
undo vlan { vlan-id1 [ to vlan-id2 ] | all }
```

【缺省情况】

系统只有一个缺省 VLAN（VLAN 1）。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

vlan-id1: VLAN 的编号，取值范围为 1~4094。

vlan-id1 to vlan-id2: 指定 VLAN 的编号范围。*vlan-id1* 和 *vlan-id2* 为 VLAN 的编号，取值范围为 1~4094。*vlan-id2* 的值要大于或等于 *vlan-id1* 的值。

all: 除保留 VLAN 外的其他 VLAN，当设备允许创建的最大 VLAN 数小于 4094 时，不支持该参数。

【使用指导】

用户不能创建和删除缺省 VLAN（VLAN 1）和保留 VLAN。

动态学习到的 VLAN，以及被其他应用锁定不让删除的 VLAN，都不能使用 **undo vlan** 命令直接删除。只有将相关配置删除之后，才能删除相应的 VLAN。

【举例】

创建 VLAN 2，并进入该 VLAN 视图。

```
<Sysname> system-view
```

```
[Sysname] vlan 2
```

```
[Sysname-vlan2]
```

批量创建 VLAN 4~100。

```
<Sysname> system-view
```

```
[Sysname] vlan 4 to 100
```

【相关命令】

- **display vlan**

1.2 基于端口的VLAN配置命令

1.2.1 display port

display port 命令用来显示设备上存在的 Hybrid 或 Trunk 端口。

【命令】

display port { hybrid | trunk }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

hybrid: 显示设备当前存在的 Hybrid 端口。

trunk: 显示设备当前存在的 Trunk 端口。

【举例】

显示当前设备存在的 Hybrid 端口。

```
<Sysname> display port hybrid
```

Interface	PVID	VLAN Passing
GE1/0/1	100	Tagged: 1000, 1002, 1500, 1600-1611, 2000, 2555-2558, 3000, 4000 Untagged: 1, 10, 15, 18, 20-30, 44, 55, 67, 100, 150-160, 200, 255, 286, 300-302

显示当前设备存在的 Trunk 端口。

```
<Sysname> display port trunk
```

Interface	PVID	VLAN Passing
GE1/0/2	2	1-4, 6-100, 145, 177, 189-200, 244, 289, 400, 555, 600-611, 1000, 2006-2008

表1-4 display port 命令显示信息描述表

字段	描述
Interface	接口名称
PVID	该端口的缺省VLAN ID
VLAN Passing	表示该端口实际通过的VLAN（该VLAN已经创建，并且接口允许其通过）
Tagged	表示哪些VLAN的报文通过该端口时必须携带VLAN Tag
Untagged	表示哪些VLAN的报文通过该端口时必须去掉VLAN Tag

1.2.2 port

port 命令用来向 VLAN 中添加一个或一组 Access 端口。

undo port 命令用来从 VLAN 中删除一个或一组 Access 端口。

【命令】

```
port interface-list
```

```
undo port interface-list
```

【缺省情况】

系统将所有端口都加入到 VLAN 1。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-list: 以太网接口列表。表示方式为 *interface-list* = { *interface-type interface-number1* [*to interface-type interface-number2*] }&<1-10>, 其中 *interface-type interface-number* 为端口类型和端口编号, *interface-number2* 的值要大于或等于 *interface-number1* 的值, &<1-10>表示前面的参数最多可以输入 10 次。

【使用指导】

通过本命令只能将 Access 端口加入到 VLAN 中, 不能将 Trunk 和 Hybrid 端口加入到 VLAN 中, 并且不能通过本命令向 VLAN 1 中添加或删除 Access 端口。

设备上的所有端口的缺省链路类型都是 Access 类型, 但用户可以自行切换端口类型, 具体配置可参考命令 **port link-type**。

【举例】

```
# 向 VLAN2 中添加端口 GigabitEthernet1/0/1~GigabitEthernet1/0/2。
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

【相关命令】

- **display vlan**

1.2.3 port access vlan

port access vlan 命令用来将 Access 端口加入到指定的 VLAN 中。

undo port access vlan 命令用来恢复缺省情况。

【命令】

```
port access vlan vlan-id
undo port access vlan
```

【缺省情况】

所有 Access 端口都属于 VLAN 1。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

vlan-id: 指定的 VLAN 编号，取值范围为 1~4094。

【使用指导】

缺省情况下所有的 Access 端口都属于 VLAN 1，因此不能通过本命令将 Access 端口加入 VLAN 1。

若需将 Access 端口所属的 VLAN 从其他 VLAN 变更为 VLAN 1，请执行 **undo port access vlan** 命令。

在将 Access 端口加入到指定 VLAN 之前，该 VLAN 必须已经存在。

【举例】

```
# 将 GigabitEthernet1/0/1 端口加入到 VLAN 3 中。
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 3
```


1.2.4 port hybrid pvid

port hybrid pvid 命令用来配置 Hybrid 端口的缺省 VLAN。

undo port hybrid pvid 命令用来配置 Hybrid 端口的缺省 VLAN 为 1。

【命令】

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

【缺省情况】

Hybrid 端口的缺省 VLAN 为该端口在链路类型为 Access 时的所属 VLAN。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

vlan-id: 指定接口的缺省的 VLAN ID，取值范围为 1~4094。

【使用指导】

对 Hybrid 端口，执行 **undo vlan** 命令删除端口的缺省 VLAN 后，端口的缺省 VLAN 配置不会改变，即可以使用已经不存在的 VLAN 作为缺省 VLAN。

建议本机 Hybrid 端口的缺省 VLAN 和相连的对端设备的 Hybrid 端口的缺省 VLAN 保持一致。

配置缺省 VLAN 后，必须使用 **port hybrid vlan** 命令配置端口允许缺省 VLAN 的报文通过，该端口才能转发缺省 VLAN 的报文。

【举例】

配置端口 GigabitEthernet1/0/1（Hybrid 类型）的缺省 VLAN 为 100，并允许 VLAN 100 通过。

```
<Sysname> system-view
```

```
[Sysname] vlan 100
```

```
[Sysname-vlan100] quit
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
```

```
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 100
```

```
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

【相关命令】

- **port hybrid vlan**
- **port link-type**

1.2.5 port hybrid vlan

port hybrid vlan 命令用来允许指定的 VLAN 通过当前 Hybrid 端口。

undo port hybrid vlan 命令用来禁止指定的 VLAN 通过当前 Hybrid 端口。

【命令】

```
port hybrid vlan vlan-id-list { tagged | untagged }  
undo port hybrid vlan vlan-id-list
```

【缺省情况】

Hybrid 端口只允许该端口在链路类型为 Access 时的所属 VLAN 的报文以 Untagged 方式通过。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

vlan-id-list: VLAN 列表, Hybrid 端口允许通过的 VLAN 范围。表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] }&<1-10>**, **vlan-id** 取值范围为 1~4094, **vlan-id2** 的值要大于或等于 **vlan-id1** 的值, **&<1-10>** 表示前面的参数最多可以重复输入 10 次。该 VLAN 必须是设备上已创建的 VLAN, 否则, 该命令执行失败。

tagged: 该端口在转发指定的 VLAN 报文时将携带 VLAN Tag。

untagged: 该端口在转发指定的 VLAN 报文时将去掉 VLAN Tag。

【使用指导】

Hybrid 端口允许多个 VLAN 通过。如果多次使用 **port hybrid vlan** 命令, 那么 Hybrid 端口上允许通过的 VLAN 是这些 **vlan-id-list** 的合集。

【举例】

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口, 允许 VLAN 2、4、50~VLAN 100 通过, 并且发送这些 VLAN 的报文时携带 VLAN Tag。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
```

```
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged
```

【相关命令】

- **port link-type**

1.2.6 port link-type

port link-type 命令用来配置端口的链路类型。

undo port link-type 命令用来恢复缺省情况。

【命令】

```
port link-type { access | hybrid | trunk }
```

undo port link-type

【缺省情况】

所有端口的链路类型均为 Access 类型。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

access: 配置端口的链路类型为 Access 类型。

hybrid: 配置端口的链路类型为 Hybrid 类型。

trunk: 配置端口的链路类型为 Trunk 类型。

【使用指导】

Trunk 端口和 Hybrid 端口之间不能直接切换，只能先设为 Access 端口，再配置为其他类型端口。

【举例】

配置端口 GigabitEthernet1/0/1 配置为 Trunk 端口。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

1.2.7 port trunk permit vlan

port trunk permit vlan 命令用来允许指定的 VLAN 通过当前 Trunk 端口。

undo port trunk permit vlan 命令用来禁止指定的 VLAN 通过当前 Trunk 端口。

【命令】

port trunk permit vlan { *vlan-id-list* | all }

undo port trunk permit vlan { *vlan-id-list* | all }

【缺省情况】

Trunk 端口只允许 VLAN 1 的报文通过。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

vlan-id-list: VLAN 列表, Trunk 端口允许通过的 VLAN 范围。表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] }&<1-10>**, **vlan-id** 取值范围为 1~4094, **vlan-id2** 的值要大于或等于 **vlan-id1** 的值, **&<1-10>** 表示前面的参数最多可以重复输入 10 次。

all: 表示允许所有 VLAN 通过该 Trunk 端口。建议用户谨慎使用 **port trunk permit vlan all** 命令, 以防止未授权 VLAN 的用户通过该端口访问受限资源。

【使用指导】

Trunk 端口可以允许多个 VLAN 通过。如果多次执行 **port trunk permit vlan** 命令, 那么 Trunk 端口上允许通过的 VLAN 是这些 **vlan-id-list** 的集合。

Trunk 端口发送出去的报文, 只有缺省 VLAN 的报文不带 VLAN Tag, 其他 VLAN 的报文均会保留 VLAN Tag。

【举例】

配置端口 GigabitEthernet1/0/1 为 Trunk 端口, 允许 VLAN 2、4、50~100 通过。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100
```

【相关命令】

- **port link-type**

1.2.8 port trunk pvid

port trunk pvid 命令用来配置 Trunk 端口的缺省 VLAN。

undo port trunk pvid 命令用来恢复缺省情况。

【命令】

```
port trunk pvid vlan vlan-id
undo port trunk pvid
```

【缺省情况】

Trunk 端口的缺省 VLAN 为 VLAN 1。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

vlan-id: 指定接口的缺省 VLAN ID, 取值范围为 1~4094。

【使用指导】

对 Trunk 端口, 执行 **undo vlan** 命令删除端口的缺省 VLAN 后, 端口的缺省 VLAN 配置不会改变, 即使用已经不存在的 VLAN 作为缺省 VLAN。

本端设备 Trunk 端口的缺省 VLAN ID 和相连的对端设备的 Trunk 端口的缺省 VLAN ID 必须一致, 否则报文将不能正确传输。

配置缺省 VLAN 后, 必须使用 **port trunk permit vlan** 命令配置端口允许缺省 VLAN 的报文通过, 该端口才能转发缺省 VLAN 的报文。

【举例】

配置端口 GigabitEthernet1/0/1 (Trunk 类型) 的缺省 VLAN 为 VLAN 100, 并允许 VLAN 100 通过。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 100
```

【相关命令】

- **port link-type**
- **port trunk permit vlan**

1.3 VLAN组配置命令

1.3.1 display vlan-group

display vlan-group 命令用来显示创建的 VLAN 组及其 VLAN 成员列表。

【命令】

display vlan-group [*group-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

group-name: VLAN 组的名称, 为 1~31 个字符的字符串, 区分大小写, 首字符必须为字母。若不指定该参数, 则表示显示所有 VLAN 组的信息。

【举例】

显示指定 VLAN 组 test001 的信息。

```
<Sysname> display vlan-group test001
VLAN group: test001
```

```

        VLAN list: 2-4 100 200
# 显示所有 VLAN 组的信息。
<Sysname> display vlan-group
VLAN group: rnd
        VLAN list: Null
VLAN group: test001
        VLAN list: 2-4 100 200

```

表1-5 display vlan-group 命令显示信息描述表

字段	描述
VLAN group	VLAN组名称
VLAN list	对应的该VLAN组内的VLAN列表

【相关命令】

- **vlan-group**
- **vlan-list**

1.3.2 vlan-group

vlan-group 命令用来创建一个 VLAN 组，并进入 VLAN 组视图。如果指定的 VLAN 组已经存在，则直接进入该 VLAN 组视图。

undo vlan-group 命令用来删除指定的 VLAN 组。

【命令】

```

vlan-group group-name
undo vlan-group group-name

```

【缺省情况】

不存在 VLAN 组。

【视图】

系统视图

【缺省用户角色】

```

network-admin
context-admin

```

【参数】

group-name: VLAN 组的名称，为 1~31 个字符的字符串，区分大小写，首字符必须为字母。

【使用指导】

VLAN 组是一组 VLAN 的集合。VLAN 组内可以添加多个 VLAN 列表。

【举例】

```

# 创建一个 VLAN 组，名称为 test001，并进入 VLAN 组视图。
<Sysname> system-view

```

```
[Sysname] vlan-group test001
[Sysname-vlan-group-test001]
```

【相关命令】

- **vlan-list**

1.3.3 vlan-list

vlan-list 命令用来在 VLAN 组内添加 VLAN 成员。

undo vlan-list 命令用来从 VLAN 组内删除 VLAN 成员。

【命令】

```
vlan-list vlan-id-list
undo vlan-list vlan-id-list
```

【缺省情况】

当前 VLAN 组中不存在 VLAN 列表。

【视图】

VLAN 组视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

vlan-id-list：VLAN 列表。表示方式为 *vlan-id-list* = { *vlan-id1* [**to** *vlan-id2*] }&<1-10>, *vlan-id* 取值范围为 1~4094, *vlan-id2* 的值要大于或等于 *vlan-id1* 的值, &<1-10>表示前面的参数最多可以重复输入 10 次。

【举例】

向 VLAN 组 test001 内添加 VLAN 成员：VLAN 2~VLAN 4、VLAN 100、VLAN 200。

```
<Sysname> system-view
[Sysname] vlan-group test001
[Sysname-vlan-group-test001] vlan-list 2 to 4 100 200
```

【相关命令】

- **vlan-group**

目 录

1 LLDP	1-1
1.1 LLDP配置命令	1-1
1.1.1 display lldp local-information	1-1
1.1.2 display lldp neighbor-information	1-5
1.1.3 display lldp statistics	1-12
1.1.4 display lldp status	1-15
1.1.5 display lldp tlv-config	1-17
1.1.6 lldp admin-status	1-21
1.1.7 lldp check-change-interval	1-22
1.1.8 lldp enable	1-23
1.1.9 lldp encapsulation snap	1-23
1.1.10 lldp fast-count	1-24
1.1.11 lldp global enable	1-25
1.1.12 lldp hold-multiplier	1-25
1.1.13 lldp ignore-pvid-inconsistency	1-26
1.1.14 lldp management-address	1-27
1.1.15 lldp management-address-format string	1-28
1.1.16 lldp max-credit	1-29
1.1.17 lldp mode	1-29
1.1.18 lldp notification med-topology-change enable	1-30
1.1.19 lldp notification remote-change enable	1-31
1.1.20 lldp source-mac vlan	1-32
1.1.21 lldp timer fast-interval	1-32
1.1.22 lldp timer notification-interval	1-33
1.1.23 lldp timer reinit-delay	1-33
1.1.24 lldp timer tx-interval	1-34
1.1.25 lldp tlv-enable	1-34

1 LLDP

1.1 LLDP配置命令

1.1.1 display lldp local-information

display lldp local-information 命令用来显示 LLDP 本地信息。

【命令】

```
display lldp local-information [ global | interface interface-type  
interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

global: 显示全局 LLDP 本地信息。

interface *interface-type interface-number*: 显示指定接口上的 LLDP 本地信息，*interface-type interface-number* 表示接口类型和接口编号。

【使用指导】

如果未指定任何参数，将显示所有 LLDP 本地信息，包括全局 LLDP 信息以及所有开启了 LLDP 功能且状态为 up 的接口上的 LLDP 信息。

【举例】

显示所有 LLDP 本地信息。

```
<Sysname> display lldp local-information  
Global LLDP local-information:  
Chassis ID           : 741f-4a28-b65e  
System name          : T1030-93  
System description   :  
    UNIS Uniware Software. Software Version 7.1.064, Ess 8536P03  
    UNIS T1000-G60  
    Copyright (c) 2004-2019 New UNIS Technologies Co., Ltd. All rights reserved.  
System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge  
System capabilities enabled   : Bridge, Router, Customer Bridge  
MED information:  
Device class           : Connectivity device  
MED inventory information of master board:  
HardwareRev            : Ver.A  
FirmwareRev            : Basic Version: 1.05  
Extend Version: 1.05
```

```

SoftwareRev          : Version 7.10
SerialNum            : 210235A1RMH155000065
Manufacturer name    : UNIS
Model name           : T1000-G60
Asset tracking identifier : Unknown
LLDP local-information of port 1[GigabitEthernet1/0/0]:
Port ID type         : Interface name
Port ID              : GigabitEthernet1/0/0
Port description     : GigabitEthernet1/0/0 Interface
LLDP agent nearest-bridge management address:
Management address type : IPv4
Management address     : 192.168.100.108
Management address interface type : IfIndex
Management address interface ID : 1
Management address OID : 0
LLDP agent nearest-nontpmr management address:
Management address type : IPv4
Management address     : 192.168.100.108
Management address interface type : IfIndex
Management address interface ID : 1
Management address OID : 0
LLDP agent nearest-customer management address:
Management address type : IPv4
Management address     : 192.168.100.108
Management address interface type : IfIndex
Management address interface ID : 1
Management address OID : 0
Link aggregation supported : Yes
Link aggregation enabled  : No
Aggregation port ID      : 0
Auto-negotiation supported : Yes
Auto-negotiation enabled  : No
OperMau                  : Speed(100)/Duplex(Full)
Power port class         : PD
PSE power supported      : No
PSE power enabled       : No
PSE pairs control ability : No
Power pairs              : Signal
Port power classification : Class 0
Maximum frame size       : 9216
Transmit Tw              : 0 us
Receive Tw               : 0 us
Fallback Tw              : 0 us
Echo Transmit Tw         : 0 us
Echo Receive Tw          : 0 us
PoE PSE power source     : Unknown
Port PSE priority        : Unknown
Port available power value : 0.0 w

```

表1-1 display lldp local-information 命令显示信息描述表

字段	描述
Global LLDP local-information	本设备的全局LLDP本地信息
Chassis ID	Chassis ID值，为本设备的桥MAC地址
System name	系统名称
System description	系统描述
System capabilities supported	系统所支持的功能： • Bridge：表示支持交换功能 • Router：表示支持路由功能 • Telephone：表示支持电话功能 • Customer Bridge：表示支持客户桥功能 • Service Bridge：表示支持服务桥功能
System capabilities enabled	系统已开启的功能： • Bridge：表示交换功能已开启 • Router：表示路由功能已开启 • Customer Bridge：表示客户桥功能已开启 • Service Bridge：表示服务桥功能已开启
MED information	MED设备相关信息
Device class	MED设备类型： • Connectivity device：表示网络设备 • Class I：表示一般终端设备，即所有需要 LLDP 发现服务的终端设备 • Class II：表示媒体终端设备，即具备媒体能力的终端设备，其能力包含了一般终端设备的能力。该类设备支持媒体流 • Class III：表示通讯终端设备，即直接支持目标用户 IP 通讯系统的终端设备，其能力包含了一般终端设备和媒体终端设备的所有能力。该类设备直接被目标用户所使用
MED inventory information of master board	主控板MED资产信息
HardwareRev	产品的硬件版本
FirmwareRev	产品的固件版本
SoftwareRev	产品的软件版本
SerialNum	序列号
Manufacturer name	制造厂商
Model name	模块名称
Asset tracking identifier	资产跟踪ID
LLDP local-information of port 1	端口1上LLDP本地信息

字段	描述
Port ID type	端口ID类型： - MAC address: 表示 MAC 地址 - Interface name: 表示接口名称
Port ID	端口ID值，根据本设备的Port ID type取相应类型的值
Port description	端口描述
LLDP agent nearest-bridge management address	LLDP最近桥代理的管理地址
LLDP agent nearest-customer management address	LLDP最近客户桥代理的管理地址
LLDP agent nearest-nontpmr management address	LLDP最近非TPMR桥代理的管理地址
Management address type	管理地址类型
Management address	管理地址
Management address interface type	管理地址所在接口的编码方式
Management address interface ID	管理地址接口索引
Management address OID	管理地址对象标识符
Link aggregation supported	端口是否支持链路聚合
Link aggregation enabled	端口是否已开启链路聚合
Aggregation port ID	聚合组中该成员端口的编号，未开启链路聚合功能时为0
Auto-negotiation supported	端口是否支持自协商
Auto-negotiation enabled	端口是否已开启自协商
OperMau	端口自适应的速率和双工状态
Power port class	PoE类型： - PSE (Power Sourcing Equipment, 供电设备) - PD (Powered Device, 受电设备)
PSE power supported	是否支持PSE供电
PSE power enabled	是否已开启PSE供电
PSE pairs control ability	供电方式是否可控
Power pairs	PoE端口的远程供电模式： - Signal: 表示信号线供电模式 - Spare: 表示空闲线供电模式

字段	描述
Port power classification	PD的端口控制级别： - Class 0: 表示级别 0 - Class 1: 表示级别 1 - Class 2: 表示级别 2 - Class 3: 表示级别 3 - Class 4: 表示级别 4
Maximum frame size	端口支持的最大帧长度
PoE PSE power source	PSE所采用的电源类型： - Unknown: 表示采用的电源类型未知 - Primary: 表示采用主用电源作为电源 - Backup: 表示采用备用电源作为电源
Port PSE priority	PSE上端口的供电优先级： - Unknown: 表示优先级未知 - Critical: 表示优先级为 1 级 - High: 表示优先级为 2 级 - Low: 表示优先级为 3 级
Port available power value	PSE上端口可提供的功率，或PD上端口所需的功率，单位为瓦特
Transmit Tw	本端发送的等待时间，单位为微秒
Receive Tw	本端向对端请求的等待时间，单位为微秒
Fallback Tw	本端向对端请求的候选等待时间，单位为微秒
Echo Transmit Tw	收到的对端发送的等待时间，单位为微秒
Echo Receive Tw	收到的对端请求的等待时间，单位为微秒

1.1.2 display lldp neighbor-information

display lldp neighbor-information 命令用来显示由邻居设备发来的 LLDP 信息。

【命令】

```
display lldp neighbor-information [ [ [ interface interface-type
interface-number ] [ agent { nearest-bridge | nearest-customer |
nearest-nontpmr } ] [ verbose ] ] | list [ system-name system-name ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口收到的由邻居设备发来的 LLDP 信息, *interface-type interface-number* 表示接口类型和接口编号。如果未指定该参数, 将显示所有接口收到的由邻居设备发来的 LLDP 信息。

agent: 显示指定类型 LLDP 代理收到的由邻居设备发来的 LLDP 信息。如果未指定该参数, 将显示所有类型 LLDP 代理收到的由邻居设备发来的 LLDP 信息。

nearest-bridge: 表示最近桥代理。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

verbose: 显示由邻居设备发来的 LLDP 详细信息。如果未指定该参数, 将显示由邻居设备发来的 LLDP 概要信息。

list: 按列表显示由邻居设备发来的 LLDP 信息。

system-name *system-name*: 按列表显示由指定邻居设备发来的 LLDP 信息。*system-name* 表示邻居设备的系统名称, 为 1~255 个字符的字符串。如果未指定该参数, 将按列表显示由所有邻居设备发来的 LLDP 信息。

【举例】

显示所有接口最近桥代理收到的由邻居设备发来的 LLDP 详细信息。

```
<Sysname> display lldp neighbor-information agent nearest-bridge verbose
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
  LLDP Neighbor index : 1
  Update time         : 0 days, 0 hours, 1 minutes, 1 seconds
  Chassis type        : MAC address
  Chassis ID          : 000f-0055-0002
  Port ID type        : Interface name
  Port ID             : GigabitEthernet1/0/1
  Time to live        : 121
  Port description    : GigabitEthernet1/0/1 Interface
  System name         : Sysname
  System description  : UNIS Uniware Platform Software, Software Version 7.1.064,
                        Alpha 7164
                        UNIS Simware32
                        Copyright (c) 2004-2019 New UNIS Technologies Co., Ltd. All rights reserved.
  System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
  System capabilities enabled   : Bridge, Router, Customer Bridge
  Management address type      : IPv4
  Management address          : 192.168.1.55
  Management address interface type : IfIndex
  Management address interface ID  : Unknown
  Management address OID        : 0
  Port VLAN ID(PVID): 1
  Link aggregation supported    : Yes
  Link aggregation enabled     : Yes
```

```

Aggregation port ID      : 52
Management VLAN ID      : 5
Auto-negotiation supported : Yes
Auto-negotiation enabled  : Yes
OperMau                  : Speed(1000)/Duplex(Full)
Power port class          : PD
PSE power supported       : Yes
PSE power enabled         : Yes
PSE pairs control ability : Yes
Power pairs               : Signal
Port power classification : Class 0
Maximum frame size        : 1500
Transmit Tw               : 100 us
Receive Tw                : 90 us
Fallback Tw               : 90 us
Echo Transmit Tw          : 0 us
Echo Receive Tw           : 0 us
PoE PSE power source      : Primary
Port PSE priority         : Low
Port available power value : 2.2 w

```

显示所有接口所有类型 LLDP 代理收到的由邻居设备发来的 LLDP 概要信息。

```

<Sysname> display lldp neighbor-information
LLDP neighbor-information of port 52[GigabitEthernet1/0/3]:
LLDP agent nearest-bridge:
  LLDP neighbor index : 3
  ChassisID/subtype    : 0011-2233-4400/MAC address
  PortID/subtype       : 000c-29f5-c71f/MAC address
  Capabilities         : Bridge, Router, Customer Bridge

  LLDP neighbor index : 6
  ChassisID/subtype    : 0011-2233-4400/MAC address
  PortID/subtype       : 000c-29f5-c715/MAC address
  Capabilities         : None

```

```

LLDP neighbor-information of port 52[GigabitEthernet1/0/3]:
LLDP agent nearest-nontpmr:
  LLDP neighbor index : 6
  ChassisID/subtype    : 0011-2233-4400/MAC address
  PortID/subtype       : 000c-29f5-c715/MAC address
  Capabilities         : None

```

按列表显示类型 LLDP 代理所有邻居设备发来的 LLDP 信息。

```

<Sysname> display lldp neighbor-information list
Chassis ID : * -- --Nearest nontpmr bridge neighbor
             # -- --Nearest customer bridge neighbor
             Default -- -- Nearest bridge neighbor
Local Interface Chassis ID      Port ID      System Name
GE1/0/1          000f-e25d-ee91 GigabitEthernet1/0/1      System1

```

表1-2 display lldp neighbor-information 命令显示信息描述表

字段	描述
LLDP agent nearest-bridge	LLDP缺省代理，即最近桥代理
LLDP agent nearest-customer	LLDP最近客户桥代理
LLDP agent nearest-nontpmr	LLDP最近非TPMR桥代理
LLDP neighbor-information of port 1	端口1上收到的LLDP邻居信息
LLDP Neighbor index	邻居索引
Update time	邻居信息最新更新时间
Chassis type	Chassis ID类型： - Chassis component: 表示底架组件 - Interface alias: 表示接口别名 - Port component: 表示端口组件 - MAC address: 表示 MAC 地址 - Network address(ipv4): 表示网络地址（括号里表示地址类型） - Interface name: 表示接口名称 - Locally assigned: 表示邻居自定义
Chassis ID	Chassis ID值，根据邻居设备的Chassis type取相应类型的值
Port ID type	端口ID类型： - Interface alias: 表示接口别名 - Port component: 表示端口组件 - MAC address: 表示 MAC 地址 - Network Address(ipv4): 表示网络地址（括号里表示地址类型） - Interface name: 表示接口名称 - Agent circuit ID: 表示代理巡回标识 - Locally assigned: 表示邻居自定义
Port ID	端口ID值，根据邻居设备的Port ID type取相应类型的值
Time to live	邻居信息在本地的存活时间
Port description	端口描述
System name	系统名称
System description	系统描述
System capabilities supported	系统所支持的功能： - Bridge: 表示支持交换功能 - Router: 表示支持路由功能 - Customer Bridge: 表示支持客户桥功能 - Service Bridge: 表示支持服务桥功能

字段	描述
System capabilities enabled	系统已开启的功能： • Bridge：表示交换功能已开启 • Router：表示路由功能已开启 • Customer Bridge：表示支持客户桥功能 • Service Bridge：表示支持服务桥功能
Management address type	管理地址类型
Management address	管理地址
Management address interface type	管理地址接口类型
Management address interface ID	管理地址接口索引
Management address OID	管理地址对象标识符
Port VLAN ID	端口VLAN ID
Link aggregation supported	端口是否支持链路聚合
Link aggregation enabled	端口是否已开启链路聚合
Aggregation port ID	聚合组中该成员端口的编号，未开启链路聚合功能时为0
Management VLAN ID	管理VLAN ID
Auto-negotiation supported	端口是否支持自协商
Auto-negotiation enabled	端口是否已开启自协商
OperMau	端口自适应的速率和双工状态
Power port class	PoE类型： • PSE：表示供电设备 • PD：表示受电设备
PSE power supported	是否支持PSE供电
PSE power enabled	是否已开启PSE供电
PSE pairs control ability	供电方式是否可控
Power pairs	PoE端口的远程供电模式： • Signal：表示信号线供电模式 • Spare：表示空闲线供电模式
Port power classification	PD的端口控制级别： • Class 0：表示级别 0 • Class 1：表示级别 1 • Class 2：表示级别 2 • Class 3：表示级别 3 • Class 4：表示级别 4

字段	描述
Power type	供电类型： • Type 1 PD: 表示类型 1 PD • Type 2 PD: 表示类型 2 PD • Type 1 PSE: 表示类型 1 PSE • Type 2 PSE: 表示类型 2 PSE
Power source	功率来源（功率来源根据供电类型为PD类型或PSE类型，取值不同）： PSE • Unknown: 表示采用的电源类型未知 • Primary: 表示采用主用电源作为电源 • Backup: 表示采用备用电源作为电源 • Reserved: 保留 PD • Unknown: 表示采用的电源类型未知 • PSE: 表示采用 PSE 作为电源 • Local: 表示采用本地电源作为电源 • PSE and local: 表示采用 PSE 和本地电源作为电源
Power priority	功率优先级： • Unknown: 表示优先级未知 • Critical: 表示优先级为 1 级 • High: 表示优先级为 2 级 • Low: 表示优先级为 3 级
PD requested power value	PD请求功率值，单位为瓦特
PSE allocated power value	PSE分配功率值，单位为瓦特
Maximum frame size	端口支持的最大帧长度
PoE PSE power source	PSE所采用的电源类型： • Unknown: 表示采用的电源类型未知 • Primary: 表示采用主用电源作为电源 • Backup: 表示采用备用电源作为电源
PoE PD power source	PD所采用的电源类型： • Unknown: 表示采用的电源类型未知 • PSE: 表示采用 PSE 作为电源 • Local: 表示采用本地电源作为电源 • PSE and local: 表示采用 PSE 和本地电源作为电源
PoE service type	PoE服务类型

字段	描述
Port PSE priority	PSE上端口的供电优先级： - Unknown: 表示优先级未知 - Critical: 表示优先级为 1 级 - High: 表示优先级为 2 级 - Low: 表示优先级为 3 级
Port PD priority	PD上端口的受电优先级： - Unknown: 表示优先级未知 - Critical: 表示优先级为 1 级 - High: 表示优先级为 2 级 - Low: 表示优先级为 3 级
Port available power value	PSE上端口可提供的功率，或PD上端口所需的功率，单位为瓦特
HardwareRev	产品的硬件版本
FirmwareRev	产品的固件版本
SoftwareRev	产品的软件版本
SerialNum	序列号
Manufacturer name	制造厂商
Model name	模块名称
Asset tracking identifier	资产跟踪ID
Unknown basic TLV	未知的基本TLV
TLV type	未知的基本TLV类型
TLV information	未知的基本TLV的具体信息
Unknown organizationally-defined TLV	未知组织定义TLV
TLV OUI	未知组织定义TLV的对象唯一标识
TLV subtype	未知的组织定义TLV类型
Index	未知组织的索引
Chassis ID/subtype	Chassis ID值及Chassis ID类型
Port ID/subtype	Port ID值及PortID类型
Software version	邻居软件版本
Platform version	邻居平台版本
Duplex	双工状态
Capabilities	系统已开启的功能： - Bridge: 表示开启交换功能 - Router: 表示开启路由功能 - None: 表示该邻居未发布该 TLV

字段	描述
Local Interface	接收LLDP信息的本端端口
Chassis ID : * -- -- Nearest nontpmr bridge neighbor #-- -- Nearest customer bridge neighbor	*符号：表示该邻居是最近非TPMR桥代理类型邻居 #符号：表示该邻居是最近客户桥代理类型邻居
Transmit Tw	本端发送的等待时间，单位为微秒
Receive Tw	本端向对端请求的等待时间，单位为微秒
Fallback Tw	本端向对端请求的候选等待时间，单位为微秒
Echo Transmit Tw	收到的对端发送的等待时间，单位为微秒
Echo Receive Tw	收到的对端请求的等待时间，单位为微秒

1.1.3 display lldp statistics

display lldp statistics 命令用来显示 LLDP 的统计信息。

【命令】

```
display lldp statistics [ global | [ interface interface-type  
interface-number ] [ agent { nearest-bridge | nearest-customer |  
nearest-nontpmr } ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

global：显示全局 LLDP 统计信息。

interface interface-type interface-number：显示指定接口上的 LLDP 统计信息，*interface-type interface-number* 表示接口类型和接口编号。

agent：显示指定类型 LLDP 代理的统计信息。如果未指定该参数，将显示所有类型 LLDP 代理的统计信息。

nearest-bridge：表示最近桥代理。

nearest-customer：表示最近客户桥代理。

nearest-nontpmr：表示最近非 TPMR 桥代理。

【使用指导】

如果未指定任何参数，将同时显示全局和接口上的 LLDP 统计信息。

【举例】

显示全局和接口上的 LLDP 统计信息。

```

<Sysname> display lldp statistics
LLDP statistics global information:
LLDP neighbor information last change time:0 days, 0 hours, 4 minutes, 40 seconds
The number of LLDP neighbor information inserted : 1
The number of LLDP neighbor information deleted : 1
The number of LLDP neighbor information dropped : 0
The number of LLDP neighbor information aged out : 1

LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
The number of LLDP frames transmitted : 0
The number of LLDP frames received : 0
The number of LLDP frames discarded : 0
The number of LLDP error frames : 0
The number of LLDP TLVs discarded : 0
The number of LLDP TLVs unrecognized : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted : 0
The number of CDP frames received : 0
The number of CDP frames discarded : 0
The number of CDP error frames : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted : 0
The number of LLDP frames received : 0
The number of LLDP frames discarded : 0
The number of LLDP error frames : 0
The number of LLDP TLVs discarded : 0
The number of LLDP TLVs unrecognized : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted : 0
The number of CDP frames received : 0
The number of CDP frames discarded : 0
The number of CDP error frames : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted : 0
The number of LLDP frames received : 0
The number of LLDP frames discarded : 0
The number of LLDP error frames : 0
The number of LLDP TLVs discarded : 0
The number of LLDP TLVs unrecognized : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted : 0
The number of CDP frames received : 0
The number of CDP frames discarded : 0
The number of CDP error frames : 0
# 显示接口 GigabitEthernet1/0/1 的最近客户桥代理上的 LLDP 统计信息。

```

```

<Sysname> display lldp statistics interface gigabitethernet 1/0/1 agent nearest-customer
LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-customer:
The number of LLDP frames transmitted           : 0
The number of LLDP frames received               : 0
The number of LLDP frames discarded              : 0
The number of LLDP error frames                  : 0
The number of LLDP TLVs discarded                : 0
The number of LLDP TLVs unrecognized            : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted             : 0
The number of CDP frames received               : 0
The number of CDP frames discarded              : 0
The number of CDP error frames                   : 0

```

表1-3 display lldp statistics 命令显示信息描述表

字段	描述
LLDP agent nearest-bridge	LLDP缺省代理，即最近桥代理
LLDP agent nearest-customer	LLDP最近客户桥代理
LLDP agent nearest-nontpmr	LLDP最近非TPMR桥代理
LLDP statistics global information	全局LLDP统计信息
LLDP neighbor information last change time	邻居信息的最后更新时间
The number of LLDP neighbor information inserted	邻居信息的增加次数
The number of LLDP neighbor information deleted	邻居信息的删除次数
The number of LLDP neighbor information dropped	由于空间不足而导致丢弃邻居信息的次数
The number of LLDP neighbor information aged out	邻居信息的老化数量
LLDP statistics Information of port 1	端口1上的LLDP统计信息
The number of LLDP frames transmitted	发送的LLDP帧总数
The number of LLDP frames received	收到的LLDP帧总数
The number of LLDP frames discarded	丢弃的LLDP帧总数
The number of LLDP error frames	收到的错误LLDP帧总数
The number of LLDP TLVs discarded	丢弃的LLDP TLV总数
The number of LLDP TLVs unrecognized	不可识别的LLDP TLV总数
The number of LLDP neighbor information aged out	老化的LLDP邻居信息总数
The number of CDP frames transmitted	（暂不支持）发送的CDP帧总数
The number of CDP frames received	（暂不支持）收到的CDP帧总数
The number of CDP frames discarded	（暂不支持）丢弃的CDP帧总数
The number of CDP error frames	（暂不支持）收到的错误CDP帧总数

1.1.4 display lldp status

display lldp status 命令用来显示 LLDP 的状态信息。

【命令】

display lldp status [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上的 LLDP 状态信息，*interface-type interface-number* 表示接口类型和接口编号。如果未指定该参数，将显示所有开启了 LLDP 功能的接口上的 LLDP 状态信息。

agent: 显示指定类型 LLDP 代理的状态信息。如果未指定该参数，将显示所有类型 LLDP 代理的状态信息。

nearest-bridge: 表示最近桥代理。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

【举例】

显示全局和所有接口上的 LLDP 状态信息。

```
<Sysname> display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 5
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval           : 30s
Fast transmit interval      : 1s
Transmit max credit         : 5
Hold multiplier             : 4
Reinit delay                : 2s
Trap interval               : 5s
Fast start times            : 3

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP        : Enable
Admin status                : TX_RX
Trap flag                   : No
MED trap flag               : No
```

```

Polling interval           : 0s
Number of LLDP neighbors   : 5
Number of MED neighbors    : 2
Number of CDP neighbors    : 0
Number of sent optional TLV : 12
Number of received unknown TLV : 5

LLDP agent nearest-nontpmr:
Port status of LLDP       : Enable
Admin status              : TX_RX
Trap flag                 : No
MED trap flag             : No
Polling interval         : 0s
Number of LLDP neighbors   : 5
Number of MED neighbors    : 2
Number of CDP neighbors    : 0
Number of sent optional TLV : 12
Number of received unknown TLV : 5

LLDP agent nearest-customer:
Port status of LLDP       : Enable
Admin status              : TX_RX
Trap flag                 : No
MED trap flag             : No
Polling interval         : 0s
Number of LLDP neighbors   : 5
Number of MED neighbors    : 2
Number of CDP neighbors    : 0
Number of sent optional TLV : 12
Number of received unknown TLV : 5

```

表1-4 display lldp status 命令显示信息描述表

字段	描述
Bridge mode of LLDP	LLDP桥模式: • service-bridge: 表示服务桥模式 • customer-bridge: 表示客户桥模式
LLDP agent nearest-bridge	LLDP缺省代理，即最近桥代理
LLDP agent nearest-customer	LLDP最近客户桥代理
LLDP agent nearest-nontpmr	LLDP最近非TPMR桥代理
Global status of LLDP	LLDP功能是否已全局开启
The current number of LLDP neighbors	当前设备的LLDP邻居总数
The current number of CDP neighbors	（暂不支持）当前设备的CDP邻居总数
LLDP neighbor information last changed time	邻居信息的最后更新时间
Transmit interval	LLDP报文的发送间隔

字段	描述
Hold multiplier	TTL乘数
Reinit delay	端口初始化延迟时间
Transmit max credit	LLDP报文发包限速令牌桶的最大值
Trap interval	Trap信息的发送间隔
Fast start times	快速发送LLDP报文的个数
LLDP status information of port 1	端口1上的LLDP状态信息
Port status of LLDP	LLDP功能是否已在端口上开启
Admin status	端口LLDP工作模式： • TX_RX: 表示既发送也接收 LLDP 报文 • Rx_Only: 表示只接收不发送 LLDP 报文 • Tx_Only: 表示只发送不接收 LLDP 报文 • Disable: 表示既不发送也不接收 LLDP 报文
Trap Flag	LLDP Trap功能是否已开启
MED trap flag	LLDP-MED Trap功能是否已开启
Polling interval	轮询间隔，0表示轮询功能处于关闭状态
Number of neighbors	端口LLDP邻居数量
Number of MED neighbors	端口MED邻居设备的数量
Number of CDP neighbors	（暂不支持）端口CDP邻居设备的数量
Number of sent optional TLV	端口在一个LLDP报文中发送的可选TLV总数
Number of received unknown TLV	端口在所有LLDP报文中收到的不能识别的TLV总数

1.1.5 display lldp tlv-config

display lldp tlv-config 命令用来显示接口上可发送的可选 TLV 信息。

【命令】

```
display lldp tlv-config [ interface interface-type interface-number ]
[ agent { nearest-bridge | nearest-customer | nearest-nontpmr } ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口上可发送的可选 TLV 信息，*interface-type interface-number* 表示接口类型和接口编号。如果未指定该参数，将显示所有接口上可发送的可选 TLV 信息。

agent: 显示指定类型 LLDP 代理的可选 TLV 信息。如果未指定该参数，将显示所有类型 LLDP 代理的可选 TLV 信息。

nearest-bridge: 表示最近桥代理。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

【举例】

显示接口 GigabitEthernet1/0/1 上可发送的可选 TLV 信息。

```
<Sysname> display lldp tlv-config interface gigabitethernet 1/0/1
```

```
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
```

```
LLDP agent nearest-bridge:
```

NAME	STATUS	DEFAULT

Basic optional TLV:

Port Description TLV	YES	YES
System Name TLV	YES	YES
System Description TLV	YES	YES
System Capabilities TLV	YES	YES
Management Address TLV	YES	YES

IEEE 802.1 extend TLV:

Port VLAN ID TLV	NO	NO
Port And Protocol VLAN ID TLV	NO	NO
VLAN Name TLV	NO	NO
DCBX TLV	NO	NO
EVB TLV	NO	NO
Link Aggregation TLV	YES	YES
Management VID TLV	NO	NO

IEEE 802.3 extend TLV:

MAC-Physic TLV	YES	YES
Power via MDI TLV	YES	YES
Maximum Frame Size TLV	YES	YES

LLDP-MED extend TLV:

Capabilities TLV	YES	YES
Network Policy TLV	NO	NO
Location Identification TLV	NO	NO
Extended Power via MDI TLV	YES	YES
Inventory TLV	YES	YES

```
LLDP agent nearest-nontpmr:
```

NAME	STATUS	DEFAULT

Basic optional TLV:

Port Description TLV	NO	NO
System Name TLV	NO	NO

System Description TLV	NO	NO
System Capabilities TLV	NO	NO
Management Address TLV	NO	NO
IEEE 802.1 extend TLV:		
Port VLAN ID TLV	NO	NO
Port And Protocol VLAN ID TLV	NO	NO
VLAN Name TLV	NO	NO
DCBX TLV	NO	NO
EVB TLV	NO	NO
Link Aggregation TLV	NO	NO
Management VID TLV	NO	NO
IEEE 802.3 extend TLV:		
MAC-Physic TLV	NO	NO
Power via MDI TLV	NO	NO
Maximum Frame Size TLV	NO	NO
LLDP-MED extend TLV:		
Capabilities TLV	NO	NO
Network Policy TLV	NO	NO
Location Identification TLV	NO	NO
Extended Power via MDI TLV	NO	NO
Inventory TLV	NO	NO
LLDP agent nearest-customer:		
NAME	STATUS	DEFAULT
Basic optional TLV:		
Port Description TLV	YES	YES
System Name TLV	YES	YES
System Description TLV	YES	YES
System Capabilities TLV	YES	YES
Management Address TLV	YES	YES
IEEE 802.1 extend TLV:		
Port VLAN ID TLV	NO	NO
Port And Protocol VLAN ID TLV	NO	NO
VLAN Name TLV	NO	NO
DCBX TLV	NO	NO
EVB TLV	NO	NO
Link Aggregation TLV	YES	YES
Management VID TLV	NO	NO
IEEE 802.3 extend TLV:		
MAC-Physic TLV	NO	NO
Power via MDI TLV	NO	NO
Maximum Frame Size TLV	NO	NO
LLDP-MED extend TLV:		
Capabilities TLV	NO	NO
Network Policy TLV	NO	NO
Location Identification TLV	NO	NO
Extended Power via MDI TLV	NO	NO
Inventory TLV	NO	NO

表1-5 display lldp tlv-config 命令显示信息描述表

字段	描述
LLDP agent nearest-bridge	LLDP 缺省代理，即最近桥代理
LLDP agent nearest-customer	LLDP最近客户桥代理
LLDP agent nearest-nontpmr	LLDP最近非TPMR桥代理
LLDP tlv-config of port 1	端口1上可发送的可选TLV类型
NAME	TLV类型
STATUS	端口是否配置发布指定类型TLV
DEFAULT	端口发布指定类型TLV的缺省情况
Basic optional TLV	端口可以发送的基本TLV类型
Port Description TLV	端口描述TLV
System Name TLV	系统名称TLV
System Description TLV	系统描述TLV
System Capabilities TLV	系统能力集TLV
Management Address TLV	管理地址TLV
IEEE 802.1 extended TLV	端口可发送的IEEE 802.1组织定义的TLV类型
Port VLAN ID TLV	端口VLAN ID TLV
Port And Protocol VLAN ID TLV	协议VLAN ID TLV
VLAN Name TLV	VLAN名称TLV
DCBX TLV	（暂不支持）DCBX（Data Center Bridging Exchange Protocol，数据中心桥能力交换协议）TLV
EVB TLV	（暂不支持）EVB（Edge Virtual Bridging，边缘虚拟桥接）模块TLV
Management VID TLV	管理VLAN TLV
IEEE 802.3 extended TLV	端口可发送的IEEE 802.3组织定义的TLV类型
MAC-Physic TLV	端口物理属性TLV
Power via MDI TLV	供电能力TLV
Link Aggregation TLV	链路聚合TLV
Maximum Frame Size TLV	最大帧长度TLV
LLDP-MED extend TLV	LLDP-MED TLV
Capabilities TLV	MED能力集TLV
Network Policy TLV	网络策略TLV
Location Identification TLV	位置标识TLV
Extended Power via MDI TLV	扩展供电能力TLV

字段	描述
Inventory TLV	资产信息TLV，包括以下几种： • Hardware Revision TLV：终端设备硬件版本 • Firmware Revision TLV：终端设备固件版本 • Software Revision TLV：终端设备软件版本 • Serial Number TLV：终端设备序列号 • Manufacturer Name TLV：终端设备的制造厂商名称 • Model name TLV：终端设备的模块名称 • Asset ID TLV：终端设备的资产标识符，以便目录管理和资产跟踪

1.1.6 lldp admin-status

lldp admin-status 命令用来配置 LLDP 的工作模式。

undo lldp admin-status 命令用来恢复缺省情况。

【命令】

在二层以太网接口视图/三层以太网接口视图下：

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] admin-status { disable
| rx | tx | txrx }
```

```
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] admin-status
```

在二层聚合接口视图/三层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } admin-status { disable |
rx | tx | txrx }
```

```
undo lldp agent { nearest-customer | nearest-nontpmr } admin-status
```

【缺省情况】

LLDP 最近桥代理的工作模式为 TxRx，既发送也接收 LLDP 报文。其他类型的 LLDP 代理的工作模式为 Disable，即不发送也不接收 LLDP 报文。

【视图】

二层以太网接口视图

三层以太网接口视图

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent：配置指定类型 LLDP 代理的工作模式。在以太网接口视图下，未指定时表示配置最近桥代理的工作模式。

nearest-customer：表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

disable: 表示工作模式为 Disable，既不发送也不接收 LLDP 报文。

rx: 表示工作模式为 Rx，只接收不发送 LLDP 报文。

tx: 表示工作模式为 Tx，只发送不接收 LLDP 报文。

txrx: 表示工作模式为 TxRx，既发送也接收 LLDP 报文。

【举例】

配置接口 GigabitEthernet1/0/1 上最近客户桥代理 LLDP 的工作模式为 Rx。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx
```

1.1.7 lldp check-change-interval

lldp check-change-interval 命令用来开启轮询功能并配置轮询间隔。

undo lldp check-change-interval 命令用来关闭轮询功能。

【命令】

在二层以太网接口视图/三层以太网接口视图下：

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] check-change-interval
interval
```

```
undo lldp [ agent { nearest-customer | nearest-nontpmr } ]
check-change-interval
```

在二层聚合接口视图/三层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } check-change-interval
interval
```

```
undo lldp agent { nearest-customer | nearest-nontpmr }
check-change-interval
```

【缺省情况】

轮询功能处于关闭状态。

【视图】

二层以太网接口视图

三层以太网接口视图

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent: 配置指定类型 LLDP 代理的轮询功能。在以太网接口视图下，未指定时表示配置最近桥代理的轮询功能。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

interval: 表示轮询间隔，取值范围为 1~30，单位为秒。

【举例】

在接口 GigabitEthernet1/0/1 的最近客户桥代理上开启轮询功能，并配置轮询间隔为 30 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30
```

1.1.8 lldp enable

lldp enable 命令用来在接口上开启 LLDP 功能。

undo lldp enable 命令用来在接口上关闭 LLDP 功能。

【命令】

```
lldp enable
undo lldp enable
```

【缺省情况】

接口上的 LLDP 功能处于开启状态。

【视图】

二层以太网接口视图
三层以太网接口视图
二层聚合接口视图
三层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

只有当全局和接口上都开启了 LLDP 功能后，该功能才会生效。

【举例】

在接口 GigabitEthernet1/0/1 上关闭 LLDP 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo lldp enable
```

【相关命令】

- **lldp global enable**

1.1.9 lldp encapsulation snap

lldp encapsulation snap 命令用来配置 LLDP 报文的封装格式为 SNAP 格式。

undo lldp encapsulation 命令用来恢复缺省情况。

【命令】

在二层以太网接口视图/三层以太网接口视图下：

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] encapsulation snap  
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] encapsulation
```

在二层聚合接口视图/三层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } encapsulation snap  
undo lldp agent { nearest-customer | nearest-nontpmr } encapsulation
```

【缺省情况】

LLDP 报文的封装格式为 Ethernet II 格式。

【视图】

二层以太网接口视图

三层以太网接口视图

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent：配置指定类型 LLDP 代理的封装格式。在以太网接口视图下，未指定时表示配置最近桥代理的封装格式。

nearest-customer：表示最近客户桥代理。

nearest-nontpmr：表示最近非 TPMR 桥代理。

【使用指导】

LLDP CDP 报文的封装格式只能为 SNAP 格式，不能为 Ethernet II 格式。

【举例】

配置接口 GigabitEthernet1/0/1 上发送的 LLDP 报文的封装格式为 SNAP 格式。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] lldp encapsulation snap
```

1.1.10 lldp fast-count

lldp fast-count 命令用来配置快速发送 LLDP 报文的个数。

undo lldp fast-count 命令用来恢复缺省情况。

【命令】

```
lldp fast-count count
```

```
undo lldp fast-count
```

【缺省情况】

快速发送 LLDP 报文的个数为 4 个。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

count: 表示快速发送 LLDP 报文的个数，取值范围为 1~8。

【举例】

配置快速发送 LLDP 报文的个数为 5 个。

```
<Sysname> system-view
```

```
[Sysname] lldp fast-count 5
```

1.1.11 lldp global enable

lldp global enable 命令用来全局开启 LLDP 功能。

undo lldp global enable 命令用来全局关闭 LLDP 功能。

【命令】

lldp global enable

undo lldp global enable

【缺省情况】

设备未全局开启 LLDP 功能。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

只有当全局和接口上都开启了 LLDP 功能后，该功能才会生效。

【举例】

全局关闭 LLDP 功能。

```
<Sysname> system-view
```

```
[Sysname] undo lldp global enable
```

【相关命令】

- **lldp enable**

1.1.12 lldp hold-multiplier

lldp hold-multiplier 命令用来配置 TTL 乘数。

undo lldp hold-multiplier 命令用来恢复缺省情况。

【命令】

```
lldp hold-multiplier value
undo lldp hold-multiplier
```

【缺省情况】

TTL 乘数为 4。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

value: 表示 TTL 乘数，取值范围为 2~10。

【使用指导】

LLDP 报文所携 Time To Live TLV 中 TTL 的值用来设置邻居信息在本地设备上的老化时间，由于 $TTL = \text{Min}(65535, (TTL \text{ 乘数} \times \text{LLDP 报文的发送间隔} + 1))$ ，即取 65535 与 $(TTL \text{ 乘数} \times \text{LLDP 报文的发送间隔} + 1)$ 中的最小值，因此通过调整 TTL 乘数可以控制本设备信息在邻居设备上的老化时间。

【举例】

```
# 配置 TTL 乘数为 6。
<Sysname> system-view
[Sysname] lldp hold-multiplier 6
```

【相关命令】

- `lldp timer tx-interval`

1.1.13 lldp ignore-pvid-inconsistency

`lldp ignore-pvid-inconsistency` 命令用来关闭 LLDP 的 PVID 不一致检查功能。

`undo lldp ignore-pvid-inconsistency` 命令用来开启 LLDP 的 PVID 不一致检查功能。

【命令】

```
lldp ignore-pvid-inconsistency
undo lldp ignore-pvid-inconsistency
```

【缺省情况】

LLDP 的 PVID 不一致检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

缺省情况下，LLDP 会对接口接收报文中的 PVID TLV 进行检查，如果发现报文中 PVID 与本端不一致，LLDP 会打印日志信息，提示用户。但在一些特殊情况下，可以允许链路两端的 PVID 配置不一致，此时可以关闭 LLDP 的 PVID 不一致性检查功能。

【举例】

```
# 关闭 LLDP 的 PVID 不一致检查功能。
<Sysname> system-view
[Sysname] lldp ignore-pvid-inconsistency
```

1.1.14 lldp management-address

lldp management-address 命令用来配置接口收到携带 Management Address TLV 的 LLDP 报文后生成 ARP 表项或 ND 表项。

undo lldp management-address 命令用来恢复缺省情况。

【命令】

```
lldp management-address { arp-learning | nd-learning } [ vlan vlan-id ]
undo lldp management-address { arp-learning | nd-learning }
```

【缺省情况】

接口收到携带 Management Address TLV 的 LLDP 报文后不生成 ARP 表项和 ND 表项。

【视图】

三层以太网接口视图

【缺省用户角色】

network-admin

【参数】

arp-learning: 表示接口收到携带 IPv4 格式 Management Address TLV 的 LLDP 报文后，会生成该报文携带的管理地址与报文源 MAC 地址组成的 ARP 表项。

nd-learning: 表示接口收到携带 IPv6 格式 Management Address TLV 的 LLDP 报文后，会生成该报文携带的管理地址与报文源 MAC 地址组成的 ND 表项。

vlan vlan-id: 指定的 VLAN ID 为三层以太网子接口编号，取值范围为 1~4094。指定该参数后，生成的 ARP 表项或 ND 表项中的接口为到该 VLAN ID 对应的三层以太网子接口；如果该 VLAN ID 对应的三层以太网子接口不存在，则生成的表项中的接口为主接口。不指定该参数时表示生成的表项中的接口为主接口。

【使用指导】

ARP 表项和 ND 表项的生成互不影响，可同时配置。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 收到携带 IPv4 格式 Management Address TLV 的 LLDP 报文后，生成 ARP 表项。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] lldp management-address arp-learning
```

【相关命令】

- **lldp source-mac vlan**

1.1.15 lldp management-address-format string

lldp management-address-format string 命令用来配置管理地址在 TLV 中的封装格式为字符串格式。

undo lldp management-address-format 命令用来恢复缺省情况。

【命令】

在二层以太网接口视图/三层以太网接口视图下：

```
lldp [ agent { nearest-customer | nearest-nontpmr } ]  
management-address-format string  
undo lldp [ agent { nearest-customer | nearest-nontpmr } ]  
management-address-format
```

在二层聚合接口视图/三层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } management-address-format  
string  
undo lldp agent { nearest-customer | nearest-nontpmr }  
management-address-format
```

【缺省情况】

管理地址在 TLV 中的封装格式为数字格式。

【视图】

二层以太网接口视图

三层以太网接口视图

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent：配置指定 LLDP 代理类型管理地址在 TLV 中的封装格式。在以太网接口视图下，未指定时表示配置最近桥代理的管理地址在 TLV 中的封装格式。

nearest-customer：表示最近客户桥代理。

nearest-nontpmr：表示最近非 TPMR 桥代理。

【使用指导】

如果邻居将管理地址以字符串格式封装在 TLV 中，用户可在本地设备上也将封装格式改为字符串，以保证与邻居设备的正常通信。

【举例】

在接口 GigabitEthernet1/0/1 的最近客户桥代理上配置管理地址在 TLV 中的封装格式为字符串格式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format string
```

1.1.16 lldp max-credit

lldp max-credit 命令用来配置限制发送报文速率的令牌桶大小。

undo lldp max-credit 命令用来恢复缺省情况。

【命令】

```
lldp max-credit credit-value
undo lldp max-credit
```

【缺省情况】

限制发送报文速率的令牌桶大小为 5。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

credit-value: 表示 LLDP 发包限速的令牌桶大小，取值范围 1~100。

【举例】

配置 LLDP 发包限速的令牌桶大小为 10。

```
<Sysname> system-view
[Sysname] lldp max-credit 10
```

1.1.17 lldp mode

lldp mode 命令用来配置 LLDP 桥模式。

undo lldp mode 命令用来恢复缺省情况。

【命令】

```
lldp mode service-bridge
undo lldp mode
```

【缺省情况】

LLDP 桥模式为客户桥模式。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

service-bridge: 表示服务桥模式。

【使用指导】

LLDP 桥模式命令用于控制设备支持不同的 LLDP 代理。

- 工作于服务桥模式时，设备可支持最近桥代理和最近非 TPMR 桥代理，即对上述类型的代理 MAC 的 LLDP 报文进行处理，其他目的 MAC 的 LLDP 报文进行 VLAN 内透传。
- 工作于客户桥模式时，设备可支持最近桥代理、最近非 TPMR 桥代理及最近客户桥代理，即对上述类型的代理 MAC 的 LLDP 报文进行处理，其他目的 MAC 的 LLDP 报文进行 VLAN 内透传。



说明

桥模式配置只在 LLDP 全局开启后才能生效，LLDP 全局关闭时，只能作为客户桥对三种类型代理 MAC 的 LLDP 报文进行拦截。

【举例】

配置 LLDP 桥模式为服务桥模式。

```
<Sysname> system-view
```

```
[Sysname] lldp mode service-bridge
```

【相关命令】

- **lldp global enable**

1.1.18 lldp notification med-topology-change enable

lldp notification med-topology-change enable 命令用来开启 LLDP-MED Trap 功能。

undo lldp notification med-topology-change enable 命令用来关闭 LLDP-MED Trap 功能。

【命令】

lldp notification med-topology-change enable

undo lldp notification med-topology-change enable

【缺省情况】

LLDP-MED Trap 功能处于关闭状态。

【视图】

二层以太网接口视图

三层以太网接口视图

【缺省用户角色】

network-admin

【举例】

在接口 GigabitEthernet1/0/1 上开启 LLDP-MED Trap 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp notification med-topology-change enable
```

1.1.19 lldp notification remote-change enable

lldp notification remote-change enable 命令用来开启 LLDP Trap 功能。

undo lldp notification remote-change enable 命令用来关闭 LLDP Trap 功能。

【命令】

在二层以太网接口视图/三层以太网接口视图下：

```
lldp [ agent { nearest-customer | nearest-nontpmr } ] notification
remote-change enable
undo lldp [ agent { nearest-customer | nearest-nontpmr } ] notification
remote-change enable
```

在二层聚合接口视图/三层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } notification
remote-change enable
undo lldp agent { nearest-customer | nearest-nontpmr } notification
remote-change enable
```

【缺省情况】

LLDP Trap 功能处于关闭状态。

【视图】

二层以太网接口视图

三层以太网接口视图

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent：开启指定类型 LLDP 代理的 LLDP Trap 功能。在以太网接口视图下，未指定时表示开启最近桥代理类型 LLDP 代理的 LLDP Trap 功能。

nearest-customer：表示最近客户桥代理。

nearest-nontpmr：表示最近非 TPMR 桥代理。

【举例】

在接口 GigabitEthernet1/0/1 最近客户桥代理上开启 LLDP Trap 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer notification remote-change enable
```

1.1.20 lldp source-mac vlan

lldp source-mac vlan 命令用来配置 LLDP 报文源 MAC 地址为指定三层以太网子接口的 MAC 地址。

undo lldp source-mac vlan 命令用来恢复缺省情况。

【命令】

```
lldp source-mac vlan vlan-id  
undo lldp source-mac vlan
```

【缺省情况】

LLDP 报文源 MAC 地址为主接口的 MAC 地址。

【视图】

三层以太网接口视图

【缺省用户角色】

network-admin

【参数】

vlan-id: 指定的 VLAN ID 为三层以太网子接口编号, 取值范围为 1~4094。指定该参数后, LLDP 报文源 MAC 地址为该 VLAN ID 对应的三层以太网子接口的 MAC 地址; 如果该 VLAN ID 对应的三层以太网子接口不存在, 则 LLDP 报文源 MAC 地址为主接口的 MAC 地址。

【举例】

配置 LLDP 报文源 MAC 地址为指定三层以太网子接口的 MAC 地址。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] lldp source-mac vlan 4094
```

【相关命令】

- **lldp management-address arp-learning**

1.1.21 lldp timer fast-interval

lldp timer fast-interval 命令用来配置 LLDP 快速发送报文的时间间隔。

undo lldp timer fast-interval 命令用来恢复缺省情况。

【命令】

```
lldp timer fast-interval interval  
undo lldp timer fast-interval
```

【缺省情况】

LLDP 快速发送报文的时间间隔为 1 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 表示 LLDP 快速发送报文的时间间隔，取值范围为 1~3600，单位为秒。

【举例】

配置 LLDP 快速发送报文的时间间隔为 2 秒。

```
<Sysname> system-view
```

```
[Sysname] lldp timer fast-interval 2
```

1.1.22 lldp timer notification-interval

lldp timer notification-interval 命令用来配置 LLDP Trap 和 LLDP-MED Trap 信息的发送间隔。

undo lldp timer notification-interval 命令用来恢复缺省情况。

【命令】

```
lldp timer notification-interval interval
```

```
undo lldp timer notification-interval
```

【缺省情况】

LLDP Trap 和 LLDP-MED Trap 信息的发送间隔均为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 表示 LLDP Trap 和 LLDP-MED Trap 信息的发送间隔，取值范围为 5~3600，单位为秒。

【举例】

配置 LLDP Trap 和 LLDP-MED Trap 信息的发送间隔为 8 秒。

```
<Sysname> system-view
```

```
[Sysname] lldp timer notification-interval 8
```

1.1.23 lldp timer reinit-delay

lldp timer reinit-delay 命令用来配置接口初始化的延迟时间。

undo lldp timer reinit-delay 命令用来恢复缺省情况。

【命令】

```
lldp timer reinit-delay delay
```

undo lldp timer reinit-delay

【缺省情况】

接口初始化的延迟时间为 2 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

delay: 接口初始化的延迟时间，取值范围为 1~10，单位为秒。

【举例】

```
# 配置接口初始化的延迟时间为 4 秒。
<Sysname> system-view
[Sysname] lldp timer reinit-delay 4
```

1.1.24 lldp timer tx-interval

lldp timer tx-interval 命令用来配置 LLDP 报文的发送间隔。

undo lldp timer tx-interval 命令用来恢复缺省情况。

【命令】

```
lldp timer tx-interval interval
undo lldp timer tx-interval
```

【缺省情况】

LLDP 报文的发送间隔为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 表示 LLDP 报文的发送间隔，取值范围为 5~32768，单位为秒。

【举例】

```
# 配置 LLDP 报文的发送间隔为 20 秒。
<Sysname> system-view
[Sysname] lldp timer tx-interval 20
```

1.1.25 lldp tlv-enable

lldp tlv-enable 命令用来配置接口上允许发布的 TLV 类型。

undo lldp tlv-enable 命令用来配置接口上禁止发布的 TLV 类型。

【命令】

在二层以太网接口视图下：

- 配置最近桥代理 LLDP 接口上允许发布的 TLV 类型

```
lldp tlv-enable { basic-tlv { all | port-description | system-capability |  
system-description | system-name | management-address-tlv [ ipv6 ]  
[ ip-address ] } | dot1-tlv { all | port-vlan-id | link-aggregation |  
protocol-vlan-id [ vlan-id ] | vlan-name [ vlan-id ] | management-vid  
[ mvlan-id ] } | dot3-tlv { all | mac-physic | max-frame-size | power } | med-tlv  
{ all | capability | inventory | network-policy [ vlan-id ] |  
power-over-ethernet | location-id { civic-address device-type country-code  
{ ca-type ca-value } &<1-10> | elin-address tel-number } } }
```

```
undo lldp tlv-enable { basic-tlv { all | port-description | system-capability  
| system-description | system-name | management-address-tlv [ ipv6 ]  
[ ip-address ] } | dot1-tlv { all | port-vlan-id | link-aggregation |  
protocol-vlan-id | vlan-name | management-vid } | dot3-tlv { all | mac-physic  
| max-frame-size | power } | med-tlv { all | capability | inventory |  
network-policy [ vlan-id ] | power-over-ethernet | location-id } }
```

- 配置最近非 TPMR 代理 LLDP 接口上允许发布的 TLV 类型

```
lldp agent nearest-nontpmr tlv-enable { basic-tlv { all | port-description |  
system-capability | system-description | system-name |  
management-address-tlv [ ipv6 ] [ ip-address ] } | dot1-tlv { all |  
port-vlan-id | link-aggregation } }
```

```
lldp tlv-enable dot1-tlv { protocol-vlan-id [ vlan-id ] | vlan-name [ vlan-id ]  
| management-vid [ mvlan-id ] }
```

```
undo lldp agent nearest-nontpmr tlv-enable { basic-tlv { all |  
port-description | system-capability | system-description | system-name |  
management-address-tlv [ ipv6 ] [ ip-address ] } | dot1-tlv { all |  
port-vlan-id | link-aggregation } }
```

```
undo lldp tlv-enable dot1-tlv { protocol-vlan-id | vlan-name |  
management-vid }
```

- 配置最近客户桥代理 LLDP 接口上允许发布的 TLV 类型

```
lldp agent nearest-customer tlv-enable { basic-tlv { all | port-description  
| system-capability | system-description | system-name |  
management-address-tlv [ ipv6 ] [ ip-address ] } | dot1-tlv { all |  
port-vlan-id | link-aggregation } }
```

```
lldp tlv-enable dot1-tlv { protocol-vlan-id [ vlan-id ] | vlan-name [ vlan-id ]  
| management-vid [ mvlan-id ] }
```

```
undo lldp agent nearest-customer tlv-enable { basic-tlv { all |  
port-description | system-capability | system-description | system-name |  
management-address-tlv [ ipv6 ] [ ip-address ] } | dot1-tlv { all |  
port-vlan-id | link-aggregation } }
```

```
undo lldp tlv-enable dot1-tlv { protocol-vlan-id | vlan-name |  
management-vid }
```

在三层以太网接口视图下：

```
lldp tlv-enable { basic-tlv { all | port-description | system-capability |  
system-description | system-name | management-address-tlv [ ipv6 ]  
[ ip-address | interface loopback interface-number ] } | dot1-tlv { all |  
link-aggregation } | dot3-tlv { all | mac-physic | max-frame-size | power } |  
med-tlv { all | capability | inventory | power-over-ethernet | location-id  
{ civic-address device-type country-code { ca-type ca-value }&<1-10> |  
elin-address tel-number } } }
```

```
lldp agent { nearest-nontpmr | nearest-customer } tlv-enable { basic-tlv { all  
| port-description | system-capability | system-description | system-name |  
management-address-tlv [ ipv6 ] [ ip-address ] } | dot1-tlv { all |  
link-aggregation } }
```

```
undo lldp tlv-enable { basic-tlv { all | port-description | system-capability  
| system-description | system-name | management-address-tlv [ ipv6 ]  
[ ip-address | interface loopback interface-number ] } | dot1-tlv { all |  
link-aggregation } | dot3-tlv { all | mac-physic | max-frame-size | power } |  
med-tlv { all | capability | inventory | power-over-ethernet | location-id } }
```

```
undo lldp agent { nearest-nontpmr | nearest-customer } tlv-enable { basic-tlv  
{ all | port-description | system-capability | system-description |  
system-name | management-address-tlv [ ipv6 ] [ ip-address ] } | dot1-tlv { all  
| link-aggregation } }
```

在二层聚合接口视图下：

```
lldp agent nearest-nontpmr tlv-enable { basic-tlv { all |  
management-address-tlv [ ipv6 ] [ ip-address ] | port-description |  
system-capability | system-description | system-name } | dot1-tlv { all |  
port-vlan-id } }
```

```
lldp agent nearest-customer tlv-enable { basic-tlv { all |  
management-address-tlv [ ipv6 ] [ ip-address ] | port-description |  
system-capability | system-description | system-name } | dot1-tlv { all |  
port-vlan-id } }
```

```
lldp tlv-enable dot1-tlv { protocol-vlan-id [ vlan-id ] | vlan-name [ vlan-id ]  
| management-vid [ mvlan-id ] }
```

```
undo lldp agent nearest-nontpmr tlv-enable { basic-tlv { all |  
management-address-tlv [ ipv6 ] [ ip-address ] | port-description |  
system-capability | system-description | system-name } | dot1-tlv { all |  
port-vlan-id } }
```

```
undo lldp agent nearest-customer tlv-enable { basic-tlv { all |  
management-address-tlv [ ipv6 ] [ ip-address ] | port-description |
```

```
system-capability | system-description | system-name } | dot1-tlv { all |  
port-vlan-id } }
```

```
undo lldp tlv-enable dot1-tlv { protocol-vlan-id | vlan-name |  
management-vid }
```

在三层聚合接口视图下：

```
lldp agent { nearest-customer | nearest-nontpmr } tlv-enable basic-tlv { all  
| management-address-tlv [ ipv6 ] [ ip-address ] | port-description |  
system-capability | system-description | system-name }
```

```
undo lldp agent { nearest-customer | nearest-nontpmr } tlv-enable basic-tlv  
{ all | management-address-tlv [ ipv6 ] [ ip-address ] | port-description |  
system-capability | system-description | system-name }
```

【缺省情况】

二层以太网接口上：

- 最近桥代理允许发布除 Location-id TLV、Port And Protocol VLAN ID TLV、VLAN Name TLV 和 Management VLAN ID TLV 之外所有类型的 TLV；
- 最近客户桥代理允许发布基本 TLV 和 IEEE 802.1 组织定义 TLV。

三层以太网接口上：

- 最近桥代理允许发布除 Network Policy TLV 之外所有类型的 TLV，其中 IEEE 802.1 组织定义的 TLV 只支持 Link Aggregation TLV；
- 最近非 TPMR 桥代理不发布任何 TLV；
- 最近客户桥代理允许发布基本 TLV 和 IEEE 802.1 组织定义 TLV，其中 IEEE 802.1 组织定义的 TLV 只支持 Link Aggregation TLV。

二层聚合接口上：

- 最近非 TPMR 桥代理不发布任何 TLV；
- 最近客户桥代理允许发布基本 TLV 和 IEEE 802.1 组织定义 TLV，其中 IEEE 802.1 组织定义的 TLV 只支持 Port And Protocol VLAN ID TLV、VLAN Name TLV 及 Management VLAN ID TLV。

三层聚合接口上：

- 最近非 TPMR 桥代理不发布任何 TLV；
- 最近客户桥代理只允许发布基本 TLV。

【视图】

二层以太网接口视图

三层以太网接口视图

二层聚合接口视图

三层聚合接口视图

【缺省用户角色】

network-admin

【参数】

agent: 配置指定类型 LLDP 代理允许发布的 TLV 类型。在以太网接口视图下，未指定时表示配置最近桥代理允许发布的 TLV 类型。

nearest-customer: 表示最近客户桥代理。

nearest-nontpmr: 表示最近非 TPMR 桥代理。

all: 发布指定类型的所有可选 TLV:

- 如果为 **basic-tlv** 参数指定 **all**，则允许发布所有基本 TLV。
- 如果为 **dot1-tlv** 参数指定 **all**，则允许发布所有 802.1 组织定义 TLV。
- 如果为 **dot3-tlv** 参数指定 **all**，则允许发布所有 802.3 组织定义 TLV。
- 如果为 **med-tlv** 参数指定 **all**，则允许发布除 **location-id** 以外所有的可选 LLDP-MED TLV。

basic-tlv: 表示基本类型 TLV。

management-address-tlv [ipv6] [ip-address | interface loopback interface-number]: 表示 Management Address TLV。其中，**ipv6** 表示 LLDP 报文中所要发布的管理地址为 IPv6 格式的地址。**ip-address** 表示在 LLDP 报文中发布的管理地址为指定的 IP 地址，**interface loopback interface-number** 表示在 LLDP 报文中发布的管理地址为指定的 LoopBack 接口的 IP 地址。其缺省值如下:

- 执行 **lldp tlv-enable** 命令时:

- 在二层以太网接口视图/二层聚合接口视图下，如果 **ip-address** 参数未指定，则发布的管理地址为当前接口允许通过的、对应 VLAN 接口上配置有 IPv4/IPv6 地址且处于 up 状态的最小 VLAN 的 IPv4/IPv6 地址。

如果指定了 **ipv6** 参数，则发布的管理地址为 IPv6 地址。如果未指定 **ipv6** 参数，则发布的管理地址为对应 VLAN 接口的 IP 地址。

如果当前接口允许通过的所有 VLAN 所对应的 VLAN 接口上都未配置 IPv4/IPv6 地址或均处于 down 状态，则发布当前接口的 MAC 地址。

- 在三层以太网接口视图下，如果 **ip-address** 参数未指定，或指定的 LoopBack 接口不存在或 LoopBack 接口没有配置 IPv4/IPv6 地址，发布的管理地址为当前发送 LLDP 报文接口的 IPv4/IPv6 地址。

如果指定了 **ipv6** 参数，则发布的管理地址为 IPv6 地址。如果未指定 **ipv6** 参数，则发布的管理地址为对应接口的 IP 地址。

如果当前接口未配置 IPv4/IPv6 地址，则发布当前接口的 MAC 地址。

- 在三层聚合接口视图下，如果 **ip-address** 参数未指定，发布的管理地址为当前发送 LLDP 报文接口的 IPv4/IPv6 地址。

如果指定了 **ipv6** 参数，则发布的管理地址为 IPv6 地址。如果未指定 **ipv6** 参数，则发布的管理地址为对应接口的 IP 地址。

如果当前接口未配置 IPv4/IPv6 地址，则发布当前接口的 MAC 地址。

- 执行 **undo lldp tlv-enable** 命令时:

- 在二层以太网接口视图/二层聚合接口视图/三层以太网接口视图/三层聚合接口视图下:

如果不带 **ipv6**、**ip-address** 和 **interface loopback interface-number** 参数表示不发布该 TLV;

如果带 **ipv6**、**ip-address** 和 **interface loopback interface-number** 参数表示按缺省值发布该 TLV。

port-description: 表示 Port Description TLV。

system-capability: 表示 System Capabilities TLV。

system-description: 表示 System Description TLV。

system-name: 表示 System Name TLV。

dot1-tlv: 表示 IEEE 802.1 组织定义的 TLV。

port-vlan-id: 表示 Port VLAN ID TLV。

protocol-vlan-id [*vlan-id*]: 表示 Port And Protocol VLAN ID TLV, *vlan-id* 为所要发布 VLAN 的 VLAN ID, 取值范围为 1~4094, 缺省值为该端口所属 VLAN 中最小的 VLAN ID。

vlan-name [*vlan-id*]: 表示 VLAN Name TLV, *vlan-id* 为所要发布 VLAN 的 VLAN ID, 取值范围为 1~4094, 缺省值为该端口所属 VLAN 中最小的 VLAN ID。如果未指定 *vlan-id*, 且端口未加入任何 VLAN, 所要发布的 VLAN 为该端口 PVID。

management-vid [*mvlan-id*]: 表示 Management VLAN ID TLV。 *mvlan-id* 指定要发布管理 VLAN 的 VLAN ID, 取值范围为 1~4094。如果未指定该参数, 则表示发布 0, 表示当前 LLDP agent 未配置管理 VLAN。

link-aggregation: 表示 Link Aggregation TLV。

dot3-tlv: 表示 IEEE 802.3 组织定义的 TLV。

mac-physic: 表示 MAC/PHY Configuration/Status TLV。

max-frame-size: 表示 Maximum Frame Size TLV。

power: 表示 Power Via MDI TLV 和 Power Stateful Control TLV。

med-tlv: 表示 LLDP-MED TLV。

capability: 表示 LLDP-MED Capabilities TLV。

inventory: 表示 Hardware Revision TLV、Firmware Revision TLV、Software Revision TLV、Serial Number TLV、Manufacturer Name TLV、Model Name TLV 和 Asset ID TLV。

location-id: 表示 Location Identification TLV。

civic-address: 表示 Location Identification TLV 封装网络设备的普通地址信息。

device-type: 表示设备类型, 取值范围为 0~2。0 表示设备类型为 DHCP server, 1 表示设备类型为 Network device, 2 表示设备类型为 LLDP-MED Endpoint。

country-code: 表示国家编码, 取值范围请参考 ISO 3166。

{ *ca-type ca-value* }&<1-10>: 地址信息。*ca-type* 表示地址信息类型, 取值范围为 0~255; *ca-value* 表示地址信息, 为 1~250 个字符的字符串。&<1-10>表示前面的参数最多可以输入 10 次。

elin-address: Location Identification TLV 封装紧急电话号码。

tel-number: 表示紧急电话号码, 为 10~25 个字符的字符串, 只能包含数字。

network-policy [*vlan-id*]: 表示 Network Policy TLV, *vlan-id* 为要发布的 Voice VLAN ID, 取值范围为 1~4094。

power-over-ethernet: 表示 Extended Power-via-MDI TLV。

【使用指导】

聚合接口不支持最近桥代理。

在使用本命令时若不指定 **all** 参数，每次只能配置某类型下的一种可选 TLV，此时可通过多次使用该命令来配置各类型下的多种可选 TLV。

如果禁止发布 802.3 的组织定义的 MAC/PHY Configuration/Status TLV，则 LLDP-MED TLV 将不会被发布，不论其是否被允许发布；如果禁止发布 LLDP-MED Capabilities TLV，则其它 LLDP-MED TLV 将不会被发布，不论其是否被允许发布。

IEEE 802.1 组织定义的 TLV 的 Port And Protocol VLAN ID TLV、VLAN Name TLV 及 Management VLAN ID TLV 只能基于最近桥代理配置，但是其配置会被最近非 TPMR 桥代理和最近客户桥代理继承。

【举例】

配置接口 GigabitEthernet1/0/1 上最近客户桥代理允许发布 IEEE 802.1 组织定义的 Link Aggregation 可选 TLV。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv
link-aggregation
```


目 录

1 二层转发.....	1-1
1.1 普通二层转发配置命令.....	1-1
1.1.1 display mac-forwarding statistics.....	1-1
1.1.2 reset mac-forwarding statistics.....	1-2
1.2 快速二层转发配置命令.....	1-3
1.2.1 display mac-forwarding cache ip	1-3
1.2.2 display mac-forwarding cache ip fragment.....	1-4
1.2.3 display mac-forwarding cache ipv6	1-5
1.2.4 mac fast-forwarding check-vlan-id	1-6
1.3 Bridge转发配置命令.....	1-7
1.3.1 add interface	1-7
1.3.2 add vlan	1-8
1.3.3 bridge	1-8
1.3.4 bridge tunnel-encapsulation skip	1-10
1.3.5 bypass enable.....	1-10
1.3.6 bypass enable external	1-11
1.3.7 display bridge bypass status	1-12
1.3.8 mac-address max-mac-count	1-13
1.4 快速Bridge转发配置命令.....	1-14
1.4.1 bridge fast-forwarding check-vlan-id.....	1-14
1.4.2 display bridge cache ip	1-14
1.4.3 display bridge cache ip fragment.....	1-15
1.4.4 display bridge cache ipv6	1-16

1 二层转发

1.1 普通二层转发配置命令

1.1.1 display mac-forwarding statistics

display mac-forwarding statistics 命令用来显示二层转发统计信息。

【命令】

```
display mac-forwarding statistics [ interface interface-type interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface interface-type interface-number: 显示指定接口的二层转发统计信息。其中，*interface-type interface-number* 为指定接口类型和接口编号。如果未指定该参数，将显示二层转发全局统计信息。

【举例】

显示二层转发全局统计信息。

```
<Sysname> display mac-forwarding statistics
Input:
  Sum:                888          Unknown Unicast:    0
  Broadcast:          0           Multicast:          0
  Filtered:           0           STP discarded:     0
  Service dropped:    0           Source dropped:    0
  Unknown dropped:    0           Learning dropped:  0
  Blackhole dropped:  0           Suppress dropped:  0
  Source MAC dropped: 0
Deliver:
  Sum:                111          L2 protocol:       11
  Local MAC address: 100
Output:
  Sum:                666          Filtered:          0
  Blackhole dropped:  0           STP discarded:     0
  Service dropped:    0           Dest MAC dropped:  0
```

显示接口 GigabitEthernet1/0/1 的二层转发统计信息。

```
<Sysname> display mac-forwarding statistics interface gigabitethernet 1/0/1
GigabitEthernet1/0/1:
Input frames: 100      Output frames:100
Filtered:      0
```

表1-1 display mac-forwarding statistics 命令显示信息描述表

字段	描述
Input	接收报文的统计信息，包括： • Sum: 接收的以太帧总数 • Filtered: 按照 802.1Q Tagged VLAN 入接口过滤规则过滤掉的以太帧数量 • Service dropped: 入方向业务丢弃的以太帧数量 • Source dropped: 因源 MAC 地址为零、组播或广播而丢弃的以太帧数量 • Unknown dropped: 因设置源未知丢弃而丢弃的以太帧数量 • Learning dropped: 因设置学习禁止转发而丢弃的以太帧数量 • Suppress dropped: 未知单播、广播或组播报文抑制丢弃的以太帧数量 • Broadcast: 接收到的广播目的 MAC 地址以太帧数量 • Multicast: 接收到的组播目的 MAC 地址以太帧数量 • Unknown unicast: 接收到的未知单播 MAC 地址以太帧数量 • Blackhole dropped: 源 MAC 地址为黑洞 MAC 地址时丢弃的以太帧数量 • Source MAC dropped: 源 MAC 地址为丢弃类型 MAC 地址时丢弃的以太帧数量
Deliver	发送报文的统计信息，包括： • Sum: 上送 CPU 处理的以太帧总数 • L2 protocol: 上送 CPU 的二层协议以太帧数量 • Local MAC address: 目的地址为本地三层 VLAN 虚接口 MAC 地址的以太帧数量
Output	丢弃报文的统计信息，包括： • Sum: 发出的以太帧总数 • Filtered: 按照 802.1Q Tagged VLAN 出接口过滤规则过滤掉的以太帧数量 • Blackhole dropped: 目的 MAC 地址为黑洞 MAC 地址时丢弃的以太帧数量 • Service dropped: 出方向业务丢弃的以太帧数量 • Dest MAC dropped: 因设置目的 MAC 地址丢弃而丢弃的以太帧数量
GigabitEthernet1/0/1	接口GigabitEthernet1/0/1的二层转发统计信息： • Input frames: 接口接收以太帧数量 • Output frames: 接口发送以太帧数量 • Filtered: 接口过滤掉的其他 VLAN 的以太帧数量

1.1.2 reset mac-forwarding statistics

reset mac-forwarding statistics 命令用来清除二层转发统计信息。

【命令】

reset mac-forwarding statistics

【视图】

用户视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

清除二层转发统计信息。
<Sysname> reset mac-forwarding statistics

1.2 快速二层转发配置命令

1.2.1 display mac-forwarding cache ip

display mac-forwarding cache ip 命令用来显示 IP 快速转发表信息。

【命令】

display mac-forwarding cache ip [*ip-address*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ip-address: 显示指定 IP 地址的快速转发表信息。如果不指定 **ip-address**，将显示所有快速转发表信息。

slot slot-number: 显示指定成员设备的快速转发表信息。**slot-number** 表示设备在 IRF 中的成员编号。如果不指定 **slot slot-number**，将显示所有成员设备的快速转发表信息。

【举例】

显示 IP 快速转发表信息。
<Sysname> display mac-forwarding cache ip
Total number of mac-forwarding entries: 2

SIP	SPort	DIP	DPort	Pro	Input_If	Output_If	VLAN
1.1.1.2	99	1.1.1.1	2048	1	GE1/0/1	GE1/0/2	2
1.1.1.1	98	1.1.1.2	2012	1	GE1/0/2	GE1/0/1	2

表1-2 display mac-forwarding cache ip 命令显示信息描述表

字段	描述
Total number of mac-forwarding entries	快速转发表项数目
SIP	源IP地址
SPort	源端口号
DIP	目的IP地址
DPort	目的端口号
Pro	协议号
Input_If	报文入接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及入接口，“-”表示接口不存在）
Output_If	报文出接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及出接口，“-”表示接口不存在）
VLAN	VLAN ID

1.2.2 display mac-forwarding cache ip fragment

display mac-forwarding cache ip fragment 命令用来显示分片报文快速转发表信息。

【命令】

display mac-forwarding cache ip fragment [*ip-address*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ip-address: 显示指定 IP 地址的分片报文快速转发表信息。如果不指定 *ip-address*，将显示所有分片报文快速转发表信息。

slot slot-number: 显示指定成员设备的分片报文快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果不指定本参数，将显示所有成员设备的分片报文快速转发表信息。

【举例】

显示分片报文快速转发表信息。

```
<Sysname> display mac-forwarding cache ip fragment
Total number of fragment mac-forwarding entries: 2
SIP          SPort  DIP          DPort  Pro  Input_If  ID    VLAN
1.1.1.1      117    1.1.1.2      0       1    GE1/0/1   2828  1
```

1.1.1.2 110 1.1.1.1 67 17 GE1/0/2 2322 1

表1-3 display mac-forwarding cache ip fragment 命令显示信息描述表

字段	描述
Total number of fragment mac-forwarding entries	分片报文快速转发表项数目
SIP	源IP地址
SPort	源端口号
DIP	目的IP地址
DPort	目的端口号
Pro	协议号
Input_if	报文入接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及入接口，“-”表示接口不存在）
ID	分片IP报文ID
VLAN	VLAN ID

1.2.3 display mac-forwarding cache ipv6

display mac-forwarding cache ipv6 命令用来显示 IPv6 快速转发表信息。

【命令】

display mac-forwarding cache ipv6 [*ipv6-address*] [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ipv6-address: 显示指定 IPv6 地址的 IPv6 快速转发表信息。如果不指定 *ipv6-address*，将显示所有 IPv6 地址的 IPv6 快速转发表信息。

slot slot-number: 显示指定成员设备的 IPv6 快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果不指定本参数，将显示所有成员设备的 IPv6 快速转发表信息。

【举例】

显示 IPv6 快速转发表信息。

```
<Sysname> display mac-forwarding cache ipv6
Total number of IPv6 mac-forwarding items: 1
Src IP: 2002::1                               Src port: 129
Dst IP: 2001::1                               Dst port: 65535
```

VLAN ID: 2
Protocol: 2
Input interface: GE1/0/2
Output interface: GE1/0/1

表1-4 display mac-forwarding cache ipv6 命令显示信息描述表

字段	描述
Total number of IPv6 mac-forwarding items	IPv6快速转发表项数目
Src IP	源IPv6地址
Src port	源端口号
Dst IP	目的IPv6地址
Dst Port	目的端口号
VLAN ID	VLAN ID
Protocol	协议号
Input interface	报文入接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及入接口，“-”表示接口不存在）
Output interface	报文出接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及出接口，“-”表示接口不存在）

1.2.4 mac fast-forwarding check-vlan-id

mac fast-forwarding check-vlan-id 命令用来开启快速二层转发时对 VLAN ID 字段的检查功能。

undo mac fast-forwarding check-vlan-id 命令用来关闭快速二层转发时对 VLAN ID 字段的检查功能。

【命令】

mac fast-forwarding check-vlan-id
undo mac fast-forwarding check-vlan-id

【缺省情况】

快速二层转发时对 VLAN ID 字段的检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

本功能处于开启状态时，二层转发在查找快速转发表时将检查 VLAN ID 是否匹配，数据流的 VLAN ID 与快速转发表中不一致时则判定为与表项不匹配。

配置本功能后，设备在判断报文所属的 TCP 会话时忽略对 VLAN ID 的检查。

【举例】

开启快速二层转发时对 VLAN ID 字段的检查功能。

```
<Sysname> system-view  
[Sysname] mac fast-forwarding check-vlan-id
```

1.3 Bridge转发配置命令

1.3.1 add interface

add interface 命令用来向反射/透传/黑洞模式 Bridge 转发实例添加接口。

undo add interface 命令用来删除反射/透传/黑洞模式 Bridge 转发实例中的接口。

【命令】

```
add interface interface-type interface-number  
undo add interface interface-type interface-number
```

【缺省情况】

手工创建的反射/透传/黑洞模式 Bridge 转发实例中没有添加任何接口。

【视图】

反射模式 Bridge 视图

透传模式 Bridge 视图

黑洞模式 Bridge 视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type interface-number：表示接口类型和编号。

【使用指导】

仅支持添加二层或者三层物理接口以及二层聚合接口到反射/透传/黑洞模式 Bridge 转发实例。

每个反射/黑洞模式 Bridge 转发实例只能添加一个接口。

每个手工创建的透传模式 Bridge 转发实例只能添加两个接口，且这两个接口的类型必须保持一致。

同一个接口不能添加到不同的 Bridge 转发实例。对于自动创建的透传模式 Bridge 转发实例，设备在自动创建 Bridge 转发实例后，会自动将子卡上的一对接口添加到此 Bridge 转发实例中，且自动创建的透传模式 Bridge 转发实例不支持手工添加或删除接口。

若在反射/黑洞模式 Bridge 视图下多次配置本命令，则最后一次执行的命令生效；若在手工创建的透传模式 Bridge 转发实例对应的 Bridge 视图下多次配置本命令，则最近两次执行的命令生效。

【举例】

配置接口 GigabitEthernet1/0/1 加入 Bridge 1。

```
<Sysname> system-view  
[Sysname] bridge 1 reflect
```



```
[Sysname-bridge1-reflect] add interface gigabitethernet 1/0/1
```

1.3.2 add vlan

add vlan 命令用来向跨 VLAN 模式 Bridge 转发实例中添加 VLAN。

undo add vlan 命令用来删除跨 VLAN 模式 Bridge 转发实例中添加的 VLAN。

【命令】

```
add vlan vlan-id-list  
undo add vlan [vlan-id-list ]
```

【缺省情况】

跨 VLAN 模式 Bridge 转发实例下不存在 VLAN。

【视图】

跨 VLAN 模式 Bridge 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

vlan-id-list：VLAN 列表。表示方式为 *vlan-id-list* = { *vlan-id1* [*to* *vlan-id2*] }&<1-10>, *vlan-id* 取值范围为 1~4094, *vlan-id2* 的值要大于或等于 *vlan-id1* 的值, &<1-10>表示前面的参数最多可以重复输入 10 次。

【使用指导】

不论 VLAN 是否被创建，都可以加入到 Bridge 转发实例中。

如果多次配置 **add vlan** 命令，那么加入到 Bridge 转发实例中的 VLAN 是多次配置的合集。

同一个 VLAN 不能加入到不同 Bridge 转发实例中。

执行 **undo add vlan** 命令的时候，如果没有指定 *vlan-id-list* 参数，则表示删除跨 VLAN 模式 Bridge 转发实例中的所有 VLAN。

【举例】

```
# 向 Bridge 2 添加 VLAN 2、3、5、50~70。  
<Sysname> system-view  
[Sysname] bridge 2 inter-vlan  
[Sysname-bridge2-inter-vlan] add vlan 2 3 5 50 to 70
```

1.3.3 bridge

bridge 命令用来手工创建指定转发模式的 Bridge 转发实例，并进入 Bridge 视图。如果指定的 Bridge 转发实例已通过手工或自动方式创建，则直接进入该 Bridge 转发实例对应的视图。

undo bridge 命令用来删除手工创建的 Bridge 转发实例的配置。

【命令】

```
bridge bridge-index [ blackhole | forward | inter-vlan | reflect ]  
undo bridge { bridge-index | all }
```

【缺省情况】

不存在 Bridge 转发实例。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

bridge-index: Bridge 转发实例索引信息。手工创建的 Bridge 转发实例中 bridge-index 的取值范围为 1~128；自动创建的透传模式 Bridge 转发实例中 bridge-index 的取值范围为 32768~1082400。

blackhole: 指定 Bridge 转发实例的转发模式为黑洞模式。

forward: 指定 Bridge 转发实例的转发模式为透传模式。

inter-vlan: 指定 Bridge 转发实例的转发模式为跨 VLAN 模式。

reflect: 指定 Bridge 转发实例的转发模式为反射模式。

all: 删除全部 Bridge 转发实例。

【使用指导】

本命令用来手工创建 Bridge 转发实例。创建时，必须指定其工作模式，且一个 Bridge 转发实例只能配置一种工作模式。

透传模式的 Bridge 转发实例既可以通过本命令手工创建，也可以通过插入硬件 Bypass 子卡后由设备自动生成。设备在自动创建透传模式 Bridge 转发实例后，会自动将子卡上的一对接口添加到此 Bridge 转发实例中。自动创建的透传模式 Bridge 转发实例及其包含的接口不支持手工删除。

【举例】

创建 Bridge 1，配置其转发模式为黑洞模式。

```
<Sysname> system-view
[Sysname] bridge 1 blackhole
[Sysname-bridge1-blackhole]
```

创建 Bridge 2，配置其转发模式为透传模式。

```
<Sysname> system-view
[Sysname] bridge 2 forward
[Sysname-bridge2-forward]
```

创建 Bridge 3，配置其转发模式为跨 VLAN 模式。

```
<Sysname> system-view
[Sysname] bridge 3 inter-vlan
[Sysname-bridge3-inter-vlan]
```

创建 Bridge 4，配置其转发模式为反射模式。

```
<Sysname> system-view
[Sysname] bridge 4 reflect
[Sysname-bridge4-reflect]
```

1.3.4 bridge tunnel-encapsulation skip

bridge tunnel-encapsulation skip 命令用来在 Inline 转发时忽略报文的隧道封装。

undo bridge tunnel-encapsulation skip 命令用来恢复缺省情况。

【命令】

```
bridge tunnel-encapsulation skip
undo bridge tunnel-encapsulation skip
```

【缺省情况】

Inline 转发时未忽略报文的隧道封装。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

缺省情况下，设备对隧道报文进行 Inline 转发时，根据封装后的报文头信息进行转发。开启 Inline 转发时报文的隧道封装忽略功能后，则根据封装前的原始报文信息进行转发。

本命令仅在 Inline 透传模式下生效。

【举例】

```
# 配置 Inline 转发时忽略报文的隧道封装。
<Sysname> system-view
[Sysname] bridge tunnel-encapsulation skip
```

1.3.5 bypass enable

bypass enable 命令用来开启内部 Bypass 功能。

undo bypass enable 命令用来关闭 Bypass 功能。

【命令】

```
bypass enable
undo bypass enable
```

【缺省情况】

Bypass 功能处于关闭状态。

【视图】

反射模式 Bridge 视图/透传模式 Bridge 视图/黑洞模式 Bridge 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

Inline 转发可以根据接口指导报文的转发,开启 Bypass 功能后,设备会根据配置的 Inline 转发模式,选择对应的接口将报文直接转发或者丢弃,不再进行安全业务处理。

多次执行 **bypass enable** 命令和 **bypass enable external** 命令,最后一次执行的命令生效。

【举例】

开启内部 Bypass 功能。

```
<Sysname> system-view
[Sysname] bridge 1 forward
[Sysname-bridge-1-forward] bypass enable
```

1.3.6 bypass enable external

bypass enable external 命令用来开启外部 Bypass 功能。

undo bypass enable 命令用来关闭 Bypass 功能。

【命令】

```
bypass enable external [ auto [ check-interval interval ] ]
undo bypass enable
```

【缺省情况】

Bypass 功能处于关闭状态。

【视图】

透传模式 Bridge 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

auto: 开启自动外部 Bypass 功能。

check-interval interval: 接口状态检查定时器。*interval* 表示检查时间间隔,取值范围为 1~3600,单位为秒,缺省值为 15 秒。

【使用指导】

多次执行本命令,最后一次执行的命令生效。

多次执行 **bypass enable** 命令和 **bypass enable external** 命令,最后一次执行的命令生效。

开启外部 Bypass 功能后,用户流量不再经过安全设备处理,直接通过 PFC 设备转发。

开启外部 Bypass 功能时:

- 如果不指定 **auto** 参数,则表示开启静态外部 Bypass 功能,用户流量直接通过 PFC 转发,不经过安全设备处理。
- 如果指定 **auto** 参数,则表示开启动态外部 Bypass 功能。在安全设备上将与 PFC 相连的两个接口加入 Bridge 转发实例。安全设备通过检查这两个接口的状态,决定自动启用外部 Bypass 功能。当透传模式 Bridge 实例中的某一接口状态变为 DOWN 时,开启外部 Bypass 功能,用户流量不经过安全设备,直接通过 PFC 转发。同时,设备会按周期 *interval* 检查接

口状态，如果检查到两个接口都变为 UP 状态，则自动关闭外部 Bypass 功能，恢复由安全设备处理用户流量。

多台设备组成 IRF 时不支持外部 Bypass 功能。

配置外部 Bypass 功能时，有如下限制：

- 仅管理 Context 支持配置。对于以共享方式分配的二层以太网接口，在管理 Context 内配置外部 bypass 功能时：
 - 如果外部 Bypass 功能生效，用户流量通过 PFC 转发，用户 Context 中该二层以太网接口上存在影响流量转发的配置，则该配置不生效，流量仍会通过 PFC 转发。
 - 如果外部 Bypass 功能不生效，用户流量不通过 PFC 转发，用户 Context 中该二层以太网接口上存在影响流量转发的配置，则该配置生效，流量按照配置的转发规则转发。
- 仅支持在手工创建的透传模式 Bridge 转发实例中配置，对于插入硬件 Bypass 子卡后设备自动创建的透传模式 Bridge 转发实例，仅支持内部 Bypass 功能。
- 仅支持在一个手工创建的透传模式 Bridge 视图下配置。加入透传模式 Bridge 实例的两个接口，必须在同一 slot 上。

【举例】

开启外部 Bypass 功能。

```
<Sysname> system-view
[Sysname] bridge 1 forward
[Sysname-bridge-1-forward] bypass enable external
```

1.3.7 display bridge bypass status

display bridge bypass status 命令用来显示 Bypass 功能状态。

【命令】

display bridge *bridge-index* bypass status

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

bridge-index：显示指定 Bridge 转发实例的 Bypass 功能状态。

【使用指导】

只在缺省 Context 内支持本命令。

【举例】

显示 Bridge 1 的 Bypass 功能状态。

```
<Sysname> display bridge 1 bypass status
```

Current external bypass status: Disable

The bypass device is faulty.

表1-5 display bridge bypass status 命令显示信息描述表

字段	描述
Current external bypass status	外部Bypass功能当前工作状态： • Enable: 外部 Bypass 功能处于开启状态 • Disable: 外部 Bypass 功能处于关闭状态
The bypass device is faulty	Bypass设备故障

1.3.8 mac-address max-mac-count

mac-address max-mac-count 命令用来配置 Bridge 实例下 MAC 地址最大学习数。

undo mac-address max-mac-count 命令用来恢复缺省情况。

【命令】

mac-address max-mac-count *count*

undo mac-address max-mac-count

【缺省情况】

Bridge 转发实例的 MAC 地址最大学习数为 4096。

【视图】

跨 VLAN 模式 Bridge 视图

【缺省用户角色】

network-admin

context-admin

【参数】

count: Bridge 转发实例的 MAC 地址数学习上限，取值范围为 0~4096，0 即表示不允许该 Bridge 转发实例学习 MAC 地址。

【使用指导】

通过配置 Bridge 转发实例的 MAC 地址数学习上限，用户可以控制设备维护的 Bridge 的 MAC 地址表的表项数量。当 Bridge 实例学习到的 MAC 地址数达到上限时，该 Bridge 转发实例将不再对 MAC 地址进行学习。

【举例】

配置 Bridge 2 的最大 MAC 学习数

```
<Sysname> system-view
```

```
[Sysname] bridge 2 inter-vlan
```

```
[Sysname-bridge2-inter-vlan] mac-address max-mac-count 10
```

1.4 快速Bridge转发配置命令

1.4.1 bridge fast-forwarding check-vlan-id

bridge fast-forwarding check-vlan-id 命令用来开启 Bridge 转发时对 VLAN ID 字段的检查功能。

undo bridge fast-forwarding check-vlan-id 命令关闭 Bridge 转发时对 VLAN ID 字段的检查功能。

【命令】

```
bridge fast-forwarding check-vlan-id
undo bridge fast-forwarding check-vlan-id
```

【缺省情况】

Bridge 转发时对 VLAN ID 字段的检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

本功能处于开启状态时, Bridge 转发在查找快速转发表时将检查 VLAN ID 是否匹配, 数据流的 VLAN ID 与快速转发表中不一致时则判定为与表项不匹配。

配置本功能后, 设备在判断报文所属的 TCP 会话时忽略对 VLAN ID 的检查。

【举例】

```
# 开启 Bridge 转发时对 VLAN ID 字段的检查功能。
<Sysname> system-view
[Sysname] bridge fast-forwarding check-vlan-id
```

1.4.2 display bridge cache ip

display bridge cache ip 命令用来显示 Bridge 转发创建的 IP 快速转发表信息。

【命令】

```
display bridge cache ip { inline | inter-vlan } [ ip-address ] [ slot
slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin

context-operator

【参数】

- inline:** 显示 Inline 转发的快速转发表信息。
- inter-vlan:** 显示跨 VLAN 转发的快速转发表信息。
- ip-address:** 显示指定 IP 地址的快速转发表信息。如果不指定 *ip-address*，将显示所有快速转发表信息。
- slot slot-number:** 显示指定成员设备的快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果不指定本参数，将显示所有成员设备的快速转发表信息。

【举例】

```
# 显示 Bridge 转发创建的 IP 快速转发表信息。
<Sysname> display bridge cache ip inline
Total number of bridge-forwarding entries: 2
SIP          SPort DIP          DPort Pro InVLAN OutVLAN Output_If
1.1.1.3      470  1.1.1.2      0     1   3     2     GE1/0/1
1.1.1.2      470  1.1.1.3      2048  1   2     3     GE1/0/2
```

表1-6 display bridge cache ip 命令显示信息描述表

字段	描述
Total number of bridge-forwarding entries	快速转发表项数目
SIP	源IP地址
SPort	源端口号
DIP	目的IP地址
DPort	目的端口号
Pro	协议号
InVLAN	报文入VLAN
OutVLAN	报文出VLAN
Output_If	报文出接口

1.4.3 display bridge cache ip fragment

display bridge cache ip fragment 命令用来显示 Bridge 转发创建的分片报文快速转发表信息。

【命令】

```
display bridge cache ip fragment { inline | inter-vlan } [ ip-address ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

inline: 显示 Inline 转发的分片报文快速转发表信息。

inter-vlan: 显示跨 VLAN 转发的分片报文快速转发表信息。

ip-address: 显示指定 IP 地址的分片报文快速转发表信息。如果不指定 *ip-address*，将显示所有分片报文快速转发表信息。

slot slot-number: 显示指定成员设备的分片报文快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果不指定本参数，将显示所有成员设备的分片报文快速转发表信息。

【举例】

显示 Bridge 转发创建的分片报文快速转发表信息。

```
<Sysname> display bridge cache ip fragment inline
Total number of fragment bridge-forwarding entries: 2
SIP          SPort DIP          DPort Pro InVLAN ID
2.1.1.2      2320 2.1.1.1      2048  1   2       7298
2.1.1.1      2048 2.1.1.2      2320  1   3       6826
```

表1-7 display bridge cache ip fragment 命令显示信息描述表

字段	描述
Total number of fragment bridge-forwarding entries	分片报文快速转发表项数目
SIP	源IP地址
SPort	源端口号
DIP	目的IP地址
DPort	目的端口号
Pro	协议号
InVLAN	报文入VLAN
ID	分片IP报文ID

1.4.4 display bridge cache ipv6

display bridge cache ipv6 命令用来显示 Bridge 转发创建的 IPv6 快速转发表信息。

【命令】

display bridge cache ipv6 { inline | inter-vlan } [ipv6-address] [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

inline: 显示 Inline 转发的 IPv6 快速转发表信息。
inter-vlan: 显示跨 VLAN 转发的 IPv6 快速转发表信息。
ipv6-address: 显示指定 IPv6 地址的 IPv6 快速转发表信息。如果不指定 *ipv6-address*，将显示所有 IPv6 地址的 IPv6 快速转发表信息。
slot slot-number: 显示指定成员设备的 IPv6 快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果不指定本参数，将显示所有成员设备的 IPv6 快速转发表信息。

【举例】

显示 Bridge 转发创建的 IPv6 快速转发表信息。

```
<Sysname> display bridge cache ipv6 inline
Total number of IPv6 bridge-forwarding items: 1
Src IP: 10::12                               Src Port: 427
Dst IP: 10::11                               Dst Port: 32768
InVLAN: 2                                    OutVLAN: 3
Protocol: 58
Context ID: 257
Bridge ID: 10
Output interface: GE1/0/1
```

表1-8 display bridge cache ipv6 命令显示信息描述表

字段	描述
Total number of IPv6 bridge-forwarding items	IPv6快速转发表项数目
Src IP	源IPv6地址
Src port	源端口号
Dst IP	目的IPv6地址
Dst Port	目的端口号
InVLAN	报文入VLAN
OutVLAN	报文出VLAN
Protocol	协议号
Context ID	CONTEXT ID
Bridge ID	Bridge转发实例ID

字段	描述
Output interface	报文出接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及出接口，“-”表示接口不存在）

目 录

1 环路检测.....	1-1
1.1 环路检测配置命令.....	1-1
1.1.1 display loopback-detection.....	1-1
1.1.2 loopback-detection action	1-2
1.1.3 loopback-detection enable	1-3
1.1.4 loopback-detection global action	1-4
1.1.5 loopback-detection global enable	1-5
1.1.6 loopback-detection interval-time.....	1-6

1 环路检测

1.1 环路检测配置命令

1.1.1 display loopback-detection

display loopback-detection 命令用来显示环路检测的配置和运行情况。

【命令】

display loopback-detection

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示环路检测的配置和运行情况。
<Sysname> display loopback-detection
Loopback detection is enabled.
Loopback detection interval is 30 second(s).
Loopback is detected on following interfaces:
Interface Action mode VLANs
GigabitEthernet1/0/3 None 10

表1-1 display loopback-detection 命令显示信息描述表

字段	描述
Loopback detection is enabled	环路检测功能已开启
Loopback detection is disabled	环路检测功能已关闭
Loopback detection interval is 30 second(s)	环路检测的时间间隔为30秒
Loopback is detected on following interfaces	下列端口被检测到存在环路
Interface	端口名称

字段	描述
Action mode	环路检测的处理模式： • Block: 当系统检测到端口出现环路时，除了生成日志信息外，还会禁止端口学习 MAC 地址并将端口阻塞 • None: 当系统检测到端口出现环路时，除了生成日志信息外不对该端口进行任何处理 • No-learning: 当系统检测到端口出现环路时，除了生成日志信息外，还会禁止端口学习 MAC 地址 • Shutdown: 当系统检测到端口出现环路时，除了生成日志信息外，还会自动关闭该端口，使其不能收发任何报文。端口被关闭后能够自动恢复，恢复时间由 shutdown-interval 命令（请参考“基础配置命令参考”中的“设备管理”）决定
VLANs	接口下检测到的产生环路的VLAN
No loopback is detected	未检测到环路

1.1.2 loopback-detection action

loopback-detection action 命令用来在端口上配置环路检测的处理模式。

undo loopback-detection action 命令用来恢复缺省情况。

【命令】

在二层以太网接口视图下：

```
loopback-detection action { block | no-learning | shutdown }
```

```
undo loopback-detection action
```

在二层聚合接口视图下：

```
loopback-detection action shutdown
```

```
undo loopback-detection action
```

【缺省情况】

当系统检测到端口出现环路时不对该端口进行任何处理，仅生成日志信息。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

block: 表示 Block 模式，即当系统检测到端口出现环路时，除了生成日志信息外，还会禁止端口学习 MAC 地址并将端口阻塞。二层聚合接口不支持本模式。

no-learning: 表示 No-learning 模式，即当系统检测到端口出现环路时，除了生成日志信息外，还会禁止端口学习 MAC 地址。二层聚合接口不支持本模式。

shutdown: 表示 Shutdown 模式，即当系统检测到端口出现环路时，除了生成日志信息外，还会自动关闭该端口，使其不能收发任何报文。被关闭的端口将在 **shutdown-interval** 命令（请参考“基础配置命令参考”中的“设备管理”）所配置的时间之后自动恢复。

【使用指导】

用户可以使用 **loopback-detection global action** 命令在系统视图下全局配置环路检测的处理模式。

系统视图下的配置对所有端口都有效，接口视图下的配置则只对当前端口有效，且接口视图下的配置优先级较高。

【举例】

在端口 GigabitEthernet1/0/1 上配置环路检测的处理模式为 Shutdown 模式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection action shutdown
```

【相关命令】

- **display loopback-detection**
- **loopback-detection global action**

1.1.3 loopback-detection enable

loopback-detection enable 命令用来在端口上开启环路检测功能。

undo loopback-detection enable 用来在端口上关闭环路检测功能。

【命令】

```
loopback-detection enable vlan { vlan-id-list | all }
undo loopback-detection enable vlan { vlan-id-list | all }
```

【缺省情况】

端口上的环路检测功能处于关闭状态。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

vlan-id-list: VLAN 列表，表示多个 VLAN 的编号。表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] } <1-10>**。其中，**vlan-id** 为指定 VLAN 的编号，取值范围为 1~4094。**<1-10>** 表示前面的参数最多可以输入 10 次。且 **vlan-id2** 的值大于等于 **vlan-id1** 的值。

all: 表示所有已创建的 VLAN。

【使用指导】

用户可以使用 **loopback-detection global enable** 命令在系统视图下全局开启环路检测功能。

设备全局或者端口开启环路检测功能，当设备上任一端口收到设备发送的任一 VLAN 的环路检测报文时，会触发该端口的环路保护动作。

【举例】

```
# 在端口 GigabitEthernet1/0/1 上开启 VLAN 10~20 内的环路检测功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection enable vlan 10 to 20
```

【相关命令】

- **display loopback-detection**
- **loopback-detection global enable**

1.1.1.4 loopback-detection global action

loopback-detection global action 命令用来全局配置环路检测的处理模式。

undo loopback-detection global action 命令用来恢复缺省情况。

【命令】

```
loopback-detection global action shutdown
undo loopback-detection global action
```

【缺省情况】

当系统检测到端口出现环路时不对该端口进行任何处理，仅生成日志信息。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

shutdown：表示 Shutdown 模式，即当系统检测到端口出现环路时，除了生成日志信息外，还会自动关闭该端口，使其不能收发任何报文。被关闭的端口将在 **shutdown-interval** 命令（请参考“基础配置命令参考”中的“设备管理”）所配置的时间之后自动恢复。

【使用指导】

可以使用 **loopback-detection action** 命令在接口视图下配置当前端口的环路检测处理模式。系统视图下的配置对所有端口都有效，接口视图下的配置则只对当前端口有效，且接口视图下的配置优先级较高。

【举例】

```
# 全局配置环路检测的处理模式为 Shutdown 模式。
```



```
<Sysname> system-view
[Sysname] loopback-detection global action shutdown
```

【相关命令】

- **display loopback-detection**
- **loopback-detection action**

1.1.5 loopback-detection global enable

loopback-detection global enable 命令用来全局开启环路检测功能。

undo loopback-detection global enable 用来全局关闭环路检测功能。

【命令】

```
loopback-detection global enable vlan { vlan-id-list | all }
undo loopback-detection global enable vlan { vlan-id-list | all }
```

【缺省情况】

环路检测功能处于全局关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

vlan-id-list: VLAN 列表, 表示多个 VLAN 的编号。表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] }** &<1-10>。其中, **vlan-id** 为指定 VLAN 的编号, 取值范围为 1~4094。&<1-10> 表示前面的参数最多可以输入 10 次。且 **vlan-id2** 的值大于等于 **vlan-id1** 的值。

all: 表示所有已创建的 VLAN。

【使用指导】

可以使用 **loopback-detection enable** 命令在接口视图下开启当前端口的环路检测功能。

设备全局或者端口开启环路检测功能, 当设备上任一端口收到设备发送的任一 VLAN 的环路检测报文时, 会触发该端口的环路保护动作。

【举例】

全局开启 VLAN 10~20 内的环路检测功能。

```
<Sysname> system-view
[Sysname] loopback-detection global enable vlan 10 to 20
```

【相关命令】

- **display loopback-detection**
- **loopback-detection enable**

1.1.6 loopback-detection interval-time

loopback-detection interval-time 命令用来配置环路检测的时间间隔。

undo loopback-detection interval-time 命令用来恢复缺省情况。

【命令】

```
loopback-detection interval-time interval
undo loopback-detection interval-time
```

【缺省情况】

环路检测的时间间隔为 30 秒。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interval: 环路检测的时间间隔，取值范围为 1~300，单位为秒。

【使用指导】

当开启了环路检测功能后，系统开始以一定的时间间隔发送环路检测报文，该间隔越长耗费的系统性能越少，该间隔越短环路检测的灵敏度越高。用户可以通过本命令调整发送环路检测报文的时间间隔，以在系统性能和环路检测的灵敏度之间进行平衡。

【举例】

```
# 配置环路检测的时间间隔为 10 秒。
<Sysname> system-view
[Sysname] loopback-detection interval-time 10
```

【相关命令】

- **display loopback-detection**



UNIS 入侵检测系统

三层技术-IP 业务命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《三层技术-IP 业务命令参考》主要介绍 IP 地址、IP 转发基础、快速转发、ARP、域名解析、IP 性能优化、邻接表、IPv6 基础、IPv6 快速转发和多 CPU 报文负载分担的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用 “[]” 括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由 “#” 号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号 “< >” 表示按钮名，如 “单击<确定>按钮”。
[]	带方括号 “[]” 表示窗口名、菜单名和数据表，如 “弹出[新建用户]窗口”。

格 式	意 义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 ARP.....	1-1
1.1 ARP配置命令	1-1
1.1.1 arp check enable	1-1
1.1.2 arp check log enable	1-1
1.1.3 arp ip-unnumbered learning enable	1-2
1.1.4 arp max-learning-num.....	1-3
1.1.5 arp max-learning-number	1-4
1.1.6 arp static.....	1-5
1.1.7 arp timer aging	1-6
1.1.8 display arp	1-7
1.1.9 display arp <i>ip-address</i>	1-10
1.1.10 display arp timer aging	1-10
1.1.11 display arp vpn-instance	1-11
1.1.12 reset arp	1-12
2 免费ARP.....	2-1
2.1 免费ARP配置命令	2-1
2.1.1 arp ip-conflict log prompt	2-1
2.1.2 arp send-gratuitous-arp.....	2-1
2.1.3 gratuitous-arp mac-change retransmit	2-2
2.1.4 gratuitous-arp-learning enable	2-3
2.1.5 gratuitous-arp-sending enable	2-4
3 代理ARP.....	3-1
3.1 代理ARP配置命令	3-1
3.1.1 display local-proxy-arp	3-1
3.1.2 display proxy-arp	3-1
3.1.3 local-proxy-arp enable	3-2
3.1.4 proxy-arp enable	3-3
4 ARP Snooping	4-1
4.1 ARP Snooping配置命令	4-1
4.1.1 arp snooping enable.....	4-1
4.1.2 display arp snooping	4-1
4.1.3 reset arp snooping	4-2

5 ARP快速应答 5-1

5.1 ARP快速应答配置命令 5-1

5.1.1 arp fast-reply enable..... 5-1

1 ARP

1.1 ARP配置命令

1.1.1 arp check enable

arp check enable 命令用来开启动态 ARP 表项的检查功能。

undo arp check enable 命令用来关闭动态 ARP 表项的检查功能。

【命令】

arp check enable

undo arp check enable

【缺省情况】

动态 ARP 表项的检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

动态 ARP 表项检查功能可以控制设备上是否可以学习 ARP 报文中的发送端 MAC 地址为组播 MAC 的动态 ARP 表项。

开启 ARP 表项的检查功能后，设备上不能学习 ARP 报文中发送端 MAC 地址为组播 MAC 的动态 ARP 表项，也不能手工添加 MAC 地址为组播 MAC 的静态 ARP 表项。

关闭 ARP 表项的检查功能后，设备可以学习以太网源 MAC 地址为单播 MAC 且 ARP 报文中发送端 MAC 地址为组播 MAC 的动态 ARP 表项，也可以手工添加 MAC 地址为组播 MAC 的静态 ARP 表项。

【举例】

开启动态 ARP 表项的检查功能。

```
<Sysname> system-view
```

```
[Sysname] arp check enable
```

1.1.2 arp check log enable

arp check log enable 命令开启 ARP 日志信息功能。

undo arp check log enable 命令关闭 ARP 日志信息功能。

【命令】

arp check log enable

undo arp check log enable

【缺省情况】

设备 ARP 日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

ARP 日志可以方便管理员定位问题和解决问题，对处理 ARP 报文的信息进行的记录，

设备生成的 ARP 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

为了防止设备输出过多的 ARP 日志信息而影响设备性能，除了审计或定位问题，一般情况下建议不要打开此功能。

【举例】

开启 ARP 日志信息功能。

```
<Sysname> system-view
```

```
[Sysname] arp check log enable
```

1.1.3 arp ip-unnumbered learning enable

arp ip-unnumbered learning enable 命令用来开启在地址借用的接口学习不同网段 ARP 表项的功能。

undo arp ip-unnumbered learning enable 命令用来关闭借在地址借用的接口学习不同网段 ARP 表项的功能。

【命令】

arp ip-unnumbered learning enable

undo arp ip-unnumbered learning enable

【缺省情况】

在地址借用的接口学习不同网段 ARP 表项的功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

在某些组网环境中，当配置某个接口借用指定接口 IP 地址后，由于借用到的地址所在的网段和对端接口的地址可能处于不同网段，导致接口收到不同网段的 ARP 报文时无法学习到 ARP 表项。配置

本功能后，可以使接口收到不在同一网段的 ARP 报文后学习对应的 ARP 表项，保证该接口和对端可以通信。

关闭本功能后，配置了地址借用功能的接口不再学习不同网段的 ARP 表项，已经学到的 ARP 表项老化后删除。

只有在接口上通过 **ip address unnumbered** 命令开启 IP 地址借用功能后，本功能才生效。

【举例】

配置接口 GigabitEthernet1/0/1 借用接口 GigabitEthernet1/0/2 的 IP 地址，在接口 GigabitEthernet1/0/1 上开启在地址借用的接口学习不同网段 ARP 表项的功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address unnumbered interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/1] arp ip-unnumbered learning enable
```

【相关命令】

- **ip address unnumbered**（三层技术—IP 业务命令参考/IP 地址）

1.1.4 arp max-learning-num

arp max-learning-num 命令用来配置接口允许学习动态 ARP 表项的最大数目。

undo arp max-learning-num 命令用来恢复缺省情况。

【命令】

```
arp max-learning-num max-number
undo arp max-learning-num
```

【缺省情况】

接口允许学习动态 ARP 表项的最大数目为 16384。

【视图】

二层以太网接口视图
二层聚合接口视图
三层以太网接口视图
三层以太网子接口视图
三层聚合接口视图
三层聚合子接口视图
以太网冗余接口
以太网冗余子接口
VLAN 接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

max-number：接口允许学习动态 ARP 表项的最大数目。取值范围为 0~16384。

【使用指导】

设备可以通过 ARP 协议自动生成动态 ARP 表项。为了防止部分接口下的用户占用过多的 ARP 资源，可以通过设置接口学习动态 ARP 表项的最大数目来进行限制。当接口学习动态 ARP 表项的数目达到所设置的值时，该接口将不再学习动态 ARP 表项。

当配置接口允许学习动态 ARP 表项的最大数目为 0 时，表示禁止接口学习动态 ARP 表项。

【举例】

```
# 配置 VLAN 接口 40 上可以学习动态 ARP 表项的最大数目为 10。
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 10
# 配置接口 GigabitEthernet1/0/1 上可以学习动态 ARP 表项的最大数目为 10。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp max-learning-num 10
# 配置二层聚合接口 1 上可以学习动态 ARP 表项的最大数目为 10。
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] arp max-learning-num 10
# 配置三层聚合接口 1 上可以学习动态 ARP 表项的最大数目为 10。
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] arp max-learning-num 10
```

1.1.5 arp max-learning-number

arp max-learning-number 命令用来配置设备允许学习动态 ARP 表项的最大数目。

undo arp max-learning-number 命令用来恢复缺省情况。

【命令】

```
arp max-learning-number max-number slot slot-number
undo arp max-learning-number slot slot-number
```

【缺省情况】

设备允许学习动态 ARP 表项的最大数目为 16384。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

max-number：设备允许学习动态 ARP 表项的最大数目，取值范围为 0~16384。

slot slot-number: 设置指定成员设备上学习动态 ARP 表项的最大数目, *slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

设备可以通过 ARP 协议自动生成动态 ARP 表项。为了防止用户占用过多的 ARP 资源, 可以通过设置设备学习动态 ARP 表项的最大数目来进行限制。当设备学习动态 ARP 表项的数目达到所设置的值时, 该设备将不再学习动态 ARP 表项。

当配置设备允许学习动态 ARP 表项的最大数目为 0 时, 表示禁止该设备学习动态 ARP 表项。

【举例】

限制 Slot1 上学习的 ARP 表项的最大数目为 64。

```
<Sysname> system-view  
[Sysname] arp max-learning-number 64 slot 1
```

1.1.6 arp static

arp static 命令用来配置静态 ARP 表项。

undo arp 命令用来删除 ARP 表项。

【命令】

```
arp static ip-address mac-address [ vlan-id interface-type interface-number ]  
[ vpn-instance vpn-instance-name ]  
undo arp ip-address [ vpn-instance-name ]
```

【缺省情况】

不存在静态 ARP 表项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: ARP 表项的 IP 地址部分。

mac-address: ARP 表项的 MAC 地址部分, 格式为 H-H-H。

vlan-id: 静态 ARP 表项所属的 VLAN, 取值范围为 1~4094。

interface-type interface-number: 指定接口类型和接口编号。

vpn-instance vpn-instance-name: 指定静态 ARP 表项所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。该 VPN 实例必须已经存在。如果未指定本参数, 则表示静态 ARP 表项位于公网中。

【使用指导】

静态 ARP 表项通过手工配置和维护, 不会被老化, 不会被动态 ARP 表项覆盖, 可以增加通信的安全性。

静态 ARP 表项分为短静态 ARP 表项和长静态 ARP 表项：

- 对于已经解析的短静态 ARP 表项，会由于外部事件，比如解析到的出接口状态 **down** 或者 *vlan-id* 所对应的 VLAN 和 VLAN 接口被删除等原因，恢复到未解析状态。
- 对于长静态 ARP 表项，根据设备的当前状态可能处于有效或无效两种状态。处于无效状态的原因可能是该 ARP 表项中的 IP 地址与本地 IP 地址冲突或设备上没有与该 ARP 表项中的 IP 地址在同一网段的接口地址等原因。处于无效状态的长静态 ARP 表项不能指导报文转发。

指定 *vlan-id interface-type interface-number* 参数时，需要注意：

- *interface-type interface-number* 可以为以太网接口或聚合接口。
- *vlan-id* 所对应的 VLAN 和 VLAN 接口必须存在，接口 *interface-type interface-number* 必须属于此 VLAN。
- *vlan-id* 对应的 VLAN 接口的 IP 地址必须和 *ip-address* 属于同一网段。
- *vlan-id* 所对应的 VLAN 和 VLAN 接口被删除时，如果是长静态 ARP 表项则被删除，如果是已经解析的短静态 ARP 表项则重新变为未解析状态。

【举例】

配置一条长静态 ARP 表项，IP 地址为 202.38.10.2，对应的 MAC 地址为 00e0-fc01-0000，此条 ARP 表项对应的出接口为属于 VLAN 10 的接口 GigabitEthernet1/0/1。

```
<Sysname> system-view
```

```
[Sysname] arp static 202.38.10.2 00e0-fc01-0000 10 gigabitethernet 1/0/1
```

【相关命令】

- **display arp**
- **reset arp**

1.1.7 arp timer aging

arp timer aging 命令用来配置动态 ARP 表项的老化时间。

undo arp timer aging 命令用来恢复缺省情况。

【命令】

arp timer aging *aging-time*

undo arp timer aging

【缺省情况】

动态 ARP 表项的老化时间为 20 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

aging-time：动态 ARP 表项的老化时间，取值范围为 1~1440，单位为分钟。

【使用指导】

为适应网络的变化，ARP 表需要不断更新。ARP 表中的动态 ARP 表项并非永远有效，每一条记录都有一个生存周期，到达生存周期仍得不到刷新的记录将被从 ARP 表中删除，这个生存周期被称作老化时间。如果在到达老化时间前记录被刷新，则重新计算老化时间。

配置代理 ARP 功能后，应该减小动态 ARP 表项的老化时间，以尽快使无效动态 ARP 表项失效，减少发给设备而设备却不能转发的报文，以尽快删除无效的动态 ARP 表项。

【举例】

```
# 配置动态 ARP 表项的老化时间为 10 分钟。  
<Sysname> system-view  
[Sysname] arp timer aging 10
```

【相关命令】

- **display arp timer aging**

1.1.8 display arp

display arp 命令用来显示 ARP 表项。

【命令】

```
display arp [ [ all | dynamic | static ] [ slot slot-number ] | vlan vlan-id |  
interface interface-type interface-number ] [ count | verbose ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin  
network-operator  
context-admin  
context-operator
```

【参数】

all: 显示所有的 ARP 表项。

dynamic: 显示动态 ARP 表项。

static: 显示静态 ARP 表项。

slot *slot-number*: 显示指定成员设备的 ARP 表项。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的 ARP 表项。

vlan *vlan-id*: 显示指定 VLAN 的 ARP 表项，*vlan-id* 的取值范围为 1~4094。

interface *interface-type interface-number*: 显示指定接口的 ARP 表项。*interface-type interface-number* 用来指定接口类型和接口编号。如果未指定本参数，则显示所有接口的 ARP 表项。

count: 显示 ARP 表项的数目。

verbose: 显示 ARP 表项的详细信息。

【使用指导】

使用本命令可以查看静态和动态 ARP 表项的具体内容，包括 IP 地址、MAC 地址、VLAN ID、出口、表项类型以及老化时间等信息。

【举例】

显示所有 ARP 表项的信息。

```
<Sysname> display arp all
```

Type:	S-Static	D-Dynamic	O-Openflow	R-Rule	I-Invalid		
IP address	MAC address	SVLAN/VSI	Interface/Link ID	Aging	Type		
1.1.1.1	02e0-f102-0023	1	GE1/0/1	--	S		
1.1.1.2	00e0-fc00-0001	12	GE1/0/2	16	D		
1.1.1.3	00e0-fe50-6503	12	Tunnel1	16	D		

显示所有 ARP 表项的详细信息。

```
<Sysname> display arp all verbose
```

Type:	S-Static	D-Dynamic	O-Openflow	R-Rule	I-Invalid		
IP address	: 1.1.1.1			MAC address	: 02e0-f102-0023		
Type	: Static			Aging	: --		
Interface	: GE1/0/1			SVLAN/CVLAN	: 1/--		
VPN instance	: --						
Link ID	: --						
VXLAN ID	: --						
VSI name	: --						
VSI interface	: --						
MPLS PW ID	: --						
MPLS peer PE address:	--						
Nickname	: 0x0000						
IP address	: 1.1.1.2			MAC address	: 00e0-fc00-0001		
Type	: Dynamic			Aging	: 16 min		
Interface	: GE1/0/2			SVLAN/CVLAN	: 12/--		
VPN instance	: --						
Link ID	: --						
VXLAN ID	: --						
VSI name	: --						
VSI interface	: --						
MPLS PW ID	: --						
MPLS peer PE address:	--						
Nickname	: 0x0000						
IP address	: 1.1.1.3			MAC address	: 00e0-fe50-6503		
Type	: Dynamic			Aging	: 16 min		
Interface	: Tunnel1			SVLAN/CVLAN	: 12/--		
VPN instance	: --						
Link ID	: --						
VXLAN ID	: --						
VSI name	: --						
VSI interface	: --						
MPLS PW ID	: --						

MPLS peer PE address: --

Nickname : 0x0000

显示所有 ARP 表项的数目。

<Sysname> display arp all count

Total number of entries : 3

表1-1 display arp 命令显示信息描述表

字段	描述
IP address	ARP表项的IP地址
MAC address	ARP表项的MAC地址
SVLAN/VSI	ARP表项所属的VLAN ID（当表项类型为静态表项时，“--”表示未解析的短静态ARP表项；如果ARP表项中的接口不属于某个VLAN，也显示“--”）
Interface	ARP表项所对应的出接口（当表项类型为静态表项时，“--”表示未解析的短静态ARP表项）
Link ID	出链路标识符，如果ARP表项不属于VSI，则显示为“--”
Aging	ARP表项的老化时间，对于静态ARP表项，本字段取值为“--”，表示没有老化时间；对于动态ARP表项，取值包括： • 具体老化时间值，单位为分钟 • “--”表示老化时间不可知
Type	ARP表项类型：动态，用D表示；静态，用S表示；OpenFlow，用O表示；Rule，用R表示；多端口，用M表示；无效，用I表示
SVLAN/CVLAN	ARP表项所属的外层VLAN ID/内层VLAN ID（当表项类型为静态表项时，“--”表示未解析的短静态ARP表项；如果ARP表项中的接口不属于某个VLAN，也显示“--”）
VPN instance	VPN实例名称，“--”表示未配置相应ARP的VPN实例
VXLAN ID	（暂不支持）ARP表项对应的VXLAN ID，又称VNI（VXLAN网络标识符）。“--”表示该表项不属于任何VXLAN
VSI name	ARP表项的VSI的名称，“--”表示该表项不属于VSI
VSI interface	与VSI关联的VSI虚接口，如果未指定VSI关联的VSI虚接口，则显示“--”
MPLS PW ID	ARP表项的PW编号，如果未指定PW连接，则显示“--”
MPLS peer PE address	PW连接中远端PE设备的IP地址，如果不存在远端PE，则显示“--”
Nickname	（暂不支持）ARP表项的Nickname（长度为4的十六进制数字，例如0x012a），
Total number of entries	ARP表项数目

【相关命令】

- **arp static**
- **reset arp**

1.1.9 display arp ip-address

display arp ip-address 命令用来显示指定 IP 地址的 ARP 表项。

【命令】

display arp ip-address [slot slot-number] [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ip-address: 显示指定 IP 地址的 ARP 表项。

slot slot-number: 显示指定成员设备的 ARP 表项。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的 ARP 表项。

verbose: 显示 ARP 表项的详细信息。

【使用指导】

用户可以通过本命令查看指定 IP 地址的 ARP 表项的具体内容,包括 IP 地址、MAC 地址、VLAN ID、出接口、表项类型以及老化时间等信息。

【举例】

显示 IP 地址为 20.1.1.1 的 ARP 表项的信息。

```
<Sysname> display arp 20.1.1.1
Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IP address      MAC address      SVLAN/VSI   Interface/Link ID      Aging Type
20.1.1.1        00e0-fc00-0001   --          --                      --      S
```

【相关命令】

- **arp static**
- **reset arp**

1.1.10 display arp timer aging

display arp timer aging 命令用来显示动态 ARP 表项的老化时间。

【命令】

display arp timer aging

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示动态 ARP 表项的老化时间。
<Sysname> display arp timer aging
Current ARP aging time is 20 minute(s)(default)
以上显示信息表示动态 ARP 表项的缺省老化时间为 20 分钟。

【相关命令】

- **arp timer aging**

1.1.11 display arp vpn-instance

display arp vpn-instance 命令用来显示指定 VPN 实例的 ARP 表项。

【命令】

display arp vpn-instance *vpn-instance-name* [**count** | **verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance-name: 显示指定 VPN 实例的 ARP 表项。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，不可以包含空格，区分大小写。

count: 显示 ARP 表项的数目。

verbose: 显示 ARP 表项的详细信息。

【使用指导】

用户可以通过本命令查看指定 VPN 实例的 ARP 表项的具体内容，包括 IP 地址、MAC 地址、VLAN ID、出接口、表项类型以及老化时间等信息。

【举例】

显示 VPN 实例名为 test 的 ARP 表项。
<Sysname> display arp vpn-instance test
Type: S-Static D-Dynamic O-Openflow R-Rule I-Invalid
IP address MAC address SVLAN/VSI Interface/Link ID Aging Type

20.1.1.1 00e0-fc00-0001 -- -- S

【相关命令】

- **arp static**
- **reset arp**

1.1.12 reset arp

reset arp 命令用来清除 ARP 表项。

【命令】

reset arp { all | dynamic | interface *interface-type interface-number* | slot *slot-number* | static }

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

all: 表示清除所有的 ARP 表项。

dynamic: 表示清除动态 ARP 表项。

static: 表示清除静态 ARP 表项。

slot *slot-number*: 表示清除指定成员设备的 ARP 表项。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除主设备上的 ARP 表项。

interface *interface-type interface-number*: 表示清除指定接口的 ARP 表项。*interface-type interface-number* 用来指定接口的类型和编号。如果未指定本参数，则清除所有接口的 ARP 表项。

【举例】

清除静态 ARP 表项。
<Sysname> reset arp static

【相关命令】

- **arp static**
- **display arp**

2 免费ARP

2.1 免费ARP配置命令

2.1.1 arp ip-conflict log prompt

arp ip-conflict log prompt 命令用来开启源 IP 地址冲突提示功能。

undo arp ip-conflict log prompt 命令用来关闭源 IP 地址冲突提示功能。

【命令】

arp ip-conflict log prompt

undo arp ip-conflict log prompt

【缺省情况】

设备采用出厂配置启动时，源 IP 地址冲突提示功能处于开启状态。

设备采用空配置启动时，源 IP 地址冲突提示功能处于关闭状态。

关于出厂配置和空配置的详细介绍，请参见“基础配置指导”中的“配置文件管理”。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【举例】

在设备上开启源 IP 地址冲突提示功能。

```
<Sysname> system-view
```

```
[Sysname] arp ip-conflict log prompt
```

2.1.2 arp send-gratuitous-arp

arp send-gratuitous-arp 命令用来在接口上开启定时发送免费 ARP 功能，并设置发送免费 ARP 报文的时间间隔。

undo arp send-gratuitous-arp 命令用来关闭定时发送免费 ARP 功能。

【命令】

arp send-gratuitous-arp [interval interval]

undo arp send-gratuitous-arp

【缺省情况】

定时发送免费 ARP 功能处于关闭状态。

【视图】

三层以太网接口视图

三层以太网子接口视图
三层聚合接口视图
三层聚合子接口视图
VLAN 接口视图
以太网冗余接口视图
以太网冗余子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval interval: 发送免费 ARP 报文的时间间隔，取值范围为 200~200000，单位为毫秒，缺省值为 2000。

【使用指导】

配置本命令后，只有当接口链路状态 up 并且配置 IP 地址后，此功能才真正生效。

只能为接口主 IP 地址和手工配置的从 IP 地址发送免费 ARP。主 IP 地址可以是手工配置或者通过其他方式获取的，但是从 IP 地址必须是手工配置的。

如果修改了免费 ARP 报文的发送时间间隔，则在下一个发送时间间隔才能生效。

如果同时在很多接口下开启本功能，或者每个接口有大量的从 IP 地址，或者两种情况共存的同时又配置很小的发送时间间隔，那么免费 ARP 报文的实际发送时间间隔可能会远远高于用户设定的时间间隔。

【举例】

在接口 GigabitEthernet1/0/1 上开启定时发送免费 ARP 功能，发送免费 ARP 报文的时间间隔为 300 毫秒。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] arp send-gratuitous-arp interval 300
```

2.1.3 gratuitous-arp mac-change retransmit

gratuitous-arp mac-change retransmit 命令用来配置当接口 MAC 地址变化时，重新发送免费 ARP 报文的次数和时间间隔。

undo gratuitous-arp mac-change retransmit 命令用来恢复缺省情况。

【命令】

gratuitous-arp mac-change retransmit *times interval seconds*
undo gratuitous-arp mac-change retransmit

【缺省情况】

当设备的接口 MAC 地址变化时，该接口只会发送一次免费 ARP 报文。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

times: 重发免费 ARP 报文的次数，取值范围为 1~10。

interval seconds: 重发免费 ARP 报文的时间间隔，**seconds** 取值范围为 1~10，单位为秒。

【使用指导】

当设备的 MAC 地址发生变化后，设备会通过免费 ARP 报文将修改后的 MAC 地址通告给其他设备。由于目前免费 ARP 报文没有重传机制，其他设备可能无法收到免费 ARP 报文。为了解决这个问题，用户可以配置当接口 MAC 地址变化时，该接口重新发送免费 ARP 报文的次数和时间间隔，保证其他设备可以收到该免费 ARP 报文。

执行本命令后，设备会按照指定的时间间隔重发免费 ARP 报文，直到到达配置的发送次数为止。

【举例】

配置当接口 MAC 地址变化时，该接口重新发送 3 次免费 ARP 报文，重新发送免费 ARP 报文时间间隔为 5 秒。

```
<Sysname> system-view
```

```
[Sysname] gratuitous-arp mac-change retransmit 3 interval 5
```

2.1.4 gratuitous-arp-learning enable

gratuitous-arp-learning enable 命令用来开启免费 ARP 报文的学习功能。

undo gratuitous-arp-learning enable 命令用来关闭免费 ARP 报文学习功能。

【命令】

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

【缺省情况】

免费 ARP 报文的学习功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

开启免费 ARP 报文学习功能后，设备会根据收到的免费 ARP 报文中携带的信息对自身维护的 ARP 表进行修改（新建或者更新 ARP 表项）。

关闭免费 ARP 报文学习功能后，设备不会根据收到的免费 ARP 报文来新建 ARP 表项，但是会更新已存在的对应 ARP 表项。如果用户不希望通过免费 ARP 报文来新建 ARP 表项，可以关闭免费 ARP 报文学习功能，以节省 ARP 表项资源。

【举例】

```
# 开启免费 ARP 报文的学习功能。  
<Sysname> system-view  
[Sysname] gratuitous-arp-learning enable
```

2.1.5 gratuitous-arp-sending enable

gratuitous-arp-sending enable 命令用来开启设备收到非同一网段的 ARP 请求时发送免费 ARP 报文功能。

undo gratuitous-arp-sending enable 命令用来关闭设备收到非同一网段的 ARP 请求时发送免费 ARP 报文功能。

【命令】

```
gratuitous-arp-sending enable  
undo gratuitous-arp-sending enable
```

【缺省情况】

设备收到非同一网段的 ARP 请求时发送免费 ARP 报文功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【举例】

```
# 关闭设备收到非同一网段的 ARP 请求时发送免费 ARP 报文功能。  
<Sysname> system-view  
[Sysname] undo gratuitous-arp-sending enable
```

3 代理ARP

3.1 代理ARP配置命令

3.1.1 display local-proxy-arp

display local-proxy-arp 命令用来显示本地代理 ARP 的状态。

【命令】

display local-proxy-arp [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface *interface-type interface-number*: 显示指定接口的本地代理 ARP 的状态。
interface-type interface-number 指定接口类型和接口编号。如果未指定本参数，则显示所有接口的本地代理 ARP 的状态。

【使用指导】

使用本命令可以查看本地代理 ARP 是处于开启（enabled）状态还是关闭（disabled）状态。

【举例】

```
# 显示接口 GigabitEthernet1/0/1 的本地代理 ARP 状态。  
<Sysname> display local-proxy-arp interface gigabitethernet 1/0/1  
Interface GigabitEthernet1/0/1  
Local Proxy ARP status: enabled
```

【相关命令】

- **local-proxy-arp enable**

3.1.2 display proxy-arp

display proxy-arp 命令用来显示代理 ARP 的状态。

【命令】

display proxy-arp [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface interface-type Interface-number: 显示指定接口的代理 ARP 的状态。
interface-type interface-number 用来指定接口类型和接口编号。如果未指定本参数，则显示所有接口的代理 ARP 的状态。

【使用指导】

使用本命令可以查看代理 ARP 是处于开启（enabled）状态还是关闭（disabled）状态。

【举例】

```
# 显示接口 GigabitEthernet1/0/1 的代理 ARP 状态。
<Sysname> display proxy-arp interface gigabitethernet 1/0/1
Interface GigabitEthernet1/0/1
Proxy ARP status: disabled
```

【相关命令】

- **proxy-arp enable**

3.1.3 local-proxy-arp enable

local-proxy-arp enable 命令用来开启本地代理 ARP 功能。

undo local-proxy-arp enable 命令用来关闭本地代理 ARP 功能。

【命令】

local-proxy-arp enable [*ip-range start-ip-address to end-ip-address*]
undo local-proxy-arp enable

【缺省情况】

本地代理 ARP 功能处于关闭状态。

【视图】

三层以太网接口视图
三层以太网子接口视图
三层聚合接口视图
三层聚合子接口视图
VLAN 接口视图
以太网冗余接口视图
以太网冗余子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-range start-ip-address to end-ip-address: 配置对指定 IP 地址范围进行本地代理 ARP。*start-ip-address* 表示起始 IP 地址。*end-ip-address* 表示结束 IP 地址。*start-ip-address* 必须小于等于 *end-ip-address*。

【使用指导】

如果 ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理 ARP 功能的设备就可以回答该请求，这个过程称作代理 ARP（Proxy ARP）。

代理 ARP 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

代理 ARP 分为普通代理 ARP 和本地代理 ARP，二者的应用场景有所区别：

- 普通代理 ARP 的应用场景为：想要互通的主机分别连接到设备的不同三层接口上，且这些主机不在同一个广播域中。
- 本地代理 ARP 的应用场景为：想要互通的主机连接到设备的同一个三层接口上，且这些主机不在同一个广播域中。

需要注意的是，多次执行本命令配置不同的 IP 地址范围进行本地代理 ARP 时，最后一次执行的命令生效。

【举例】

在接口 GigabitEthernet1/0/1 上开启本地代理 ARP 功能。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] local-proxy-arp enable
```

在接口 GigabitEthernet1/0/1 上开启本地代理 ARP 功能，并指定进行 ARP 代理的 IP 地址范围。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20
```

【相关命令】

- **display local-proxy-arp**

3.1.4 proxy-arp enable

proxy-arp enable 命令用来开启代理 ARP 功能。

undo proxy-arp enable 命令用来关闭代理 ARP 功能。

【命令】

proxy-arp enable

undo proxy-arp enable

【缺省情况】

代理 ARP 功能处于关闭状态。

【视图】

三层以太网接口视图

三层以太网子接口视图
三层聚合接口视图
三层聚合子接口视图
VLAN 接口视图
以太网冗余接口视图
以太网冗余子接口视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

如果 ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理 ARP 功能的设备就可以回答该请求，这个过程称作代理 ARP（Proxy ARP）。

代理 ARP 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

代理 ARP 分为普通代理 ARP 和本地代理 ARP，二者的应用场景有所区别：

- 普通代理 ARP 的应用场景为：想要互通的主机分别连接到设备的不同三层接口上，且这些主机不在同一个广播域中。
- 本地代理 ARP 的应用场景为：想要互通的主机连接到设备的同一个三层接口上，且这些主机不在同一个广播域中。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上开启代理 ARP。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] proxy-arp enable
```

【相关命令】

- **display proxy-arp**

4 ARP Snooping

4.1 ARP Snooping配置命令

4.1.1 arp snooping enable

arp snooping enable 命令用来开启 ARP Snooping 功能。

undo arp snooping enable 命令用来关闭 ARP Snooping 功能。

【命令】

arp snooping enable
undo arp snooping enable

【缺省情况】

ARP Snooping 功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 开启 VLAN 2 下的 ARP Snooping 功能。  
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] arp snooping enable
```

4.1.2 display arp snooping

display arp snooping 命令用来显示 ARP Snooping 表项。

【命令】

display arp snooping [vlan *vlan-id*] [slot *slot-number*] [count]
display arp snooping ip *ip-address* [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vlan *vlan-id*: 显示指定 VLAN 的 ARP Snooping 表项。*vlan-id* 的取值范围为 1~4094。

count: 显示当前 ARP Snooping 表项的计数。

ip *ip-address*: 显示指定 IP 地址的 ARP Snooping 表项。

slot *slot-number*: 显示指定成员设备上的所有 ARP Snooping 表项。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的 ARP Snooping 表项。

【举例】

显示 VLAN 2 下的 ARP Snooping 表项。

```
<Sysname> display arp snooping vlan 2
```

IP Address	MAC Address	VLAN ID	Interface	Aging	Status
3.3.3.3	0003-0003-0003	2	GE1/0/1	20	Valid
3.3.3.4	0004-0004-0004	2	GE1/0/2	5	Invalid

显示当前 ARP Snooping 表项的计数。

```
<Sysname> display arp snooping count
Total entries: 2
```

表4-1 display arp snooping 命令显示信息描述表

字段	描述
IP Address	ARP Snooping表项的IP地址
MAC Address	ARP Snooping表项的MAC地址
VLAN ID	ARP Snooping表项所属的VLAN ID
Interface	ARP Snooping表项所对应的入接口
Aging	ARP Snooping表项的老化时间，单位为分钟。
Status	ARP Snooping表项的状态，分为以下三种： - Valid: 有效 - Invalid: 无效 - Collision: 冲突
Total entries	ARP Snooping表项数目

【相关命令】

- **reset arp snooping**

4.1.3 reset arp snooping

reset arp snooping 命令用来清除 ARP Snooping 表项。

【命令】

reset arp snooping [**ip** *ip-address* | **vlan** *vlan-id*]

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip *ip-address*: 清除指定 IP 地址的 ARP Snooping 表项。

vlan *vlan-id*: 清除指定 VLAN 的 ARP Snooping 表项。*vlan-id* 的取值范围为 1~4094。

【使用指导】

如果未指定参数，则清除所有的 ARP Snooping 表项。

【举例】

清除 VLAN 2 下的 ARP Snooping 表项。

```
<Sysname> reset arp snooping vlan 2
```

【相关命令】

- **display arp snooping**

5 ARP快速应答

5.1 ARP快速应答配置命令

5.1.1 arp fast-reply enable

arp fast-reply enable 命令用来开启 ARP 快速应答功能。

undo arp fast-reply enable 命令用来关闭 ARP 快速应答功能。

【命令】

arp fast-reply enable

undo arp fast-reply enable

【缺省情况】

ARP 快速应答功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

context-admin

【举例】

开启 VLAN 2 下的 ARP 快速应答功能。

```
<Sysname> system-view
```

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] arp fast-reply enable
```

目 录

1 IP地址	1-1
1.1 IP地址配置命令	1-1
1.1.1 display ip interface	1-1
1.1.2 display ip interface brief	1-3
1.1.3 ip address	1-5
1.1.4 ip address unnumbered	1-6

1 IP地址

1.1 IP地址配置命令

1.1.1 display ip interface

display ip interface 命令用来显示三层接口与 IP 相关的配置和统计信息。

【命令】

display ip interface [*interface-type* [*interface-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-type: 指定接口类型。

interface-number: 指定接口编号。

【使用指导】

display ip interface 命令用来查看三层接口与 IP 相关的配置和统计信息，包括接口上接收和发送的单播报文数、字节数和组播报文数，以及接口上收到的 TTL 无效报文数和 ICMP 报文数等。通过对显示信息中报文收发情况的分析，可以初步判断网络是否遭到攻击和攻击的可能来源。如果仅指定接口类型，则显示所有该类型接口的信息。如果未指定任何参数，则显示所有三层接口的 IP 相关的配置和统计信息。

【举例】

显示接口 GigabitEthernet1/0/1 与 IP 相关的配置和统计信息。

```
<Sysname> display ip interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: DOWN
Line protocol current state: DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address: 1.255.255.255
The Maximum Transmit Unit: 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
TTL invalid packet number:          0
ICMP packet input number:           0
    Echo reply:                      0
    Unreachable:                     0
```

```

Source quench:          0
Routing redirect:       0
Echo request:           0
Router advert:          0
Router solicit:         0
Time exceed:            0
IP header bad:          0
Timestamp request:      0
Timestamp reply:        0
Information request:    0
Information reply:      0
Netmask request:        0
Netmask reply:          0
Unknown type:           0

```

表1-1 display ip interface 命令显示信息描述表

字段	描述
current state	接口当前的物理状态，可能的状态及含义如下： - Administratively DOWN: 表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 - DOWN: 该接口的管理状态为开启，但物理状态为关闭（可能因为未连接好或者线路故障） - UP: 该接口的管理状态和物理状态均为开启
Line protocol current state	接口数据链路层协议状态，可能的状态及含义如下： - DOWN: 表示接口的数据链路层协议状态为关闭 - UP: 表示接口的数据链路层协议状态为开启 - UP (spoofing): 该接口的协议状态为欺骗性开启，即虽然接口的链路层协议状态显示是开启的，但实际可能没有对应的链路，或者所对应的链路不是永久存在而是按需建立的
Internet Address is <i>ip-address/mask-length (Type)</i>	接口的IP地址，IP地址后可携带如下参数： - Primary: 表示手动配置的主 IP 地址 - Sub: 表示手动配置的从 IP 地址 - Unnumbered: 表示借用 IP 地址  说明 <i>Type</i> 的取值情况与接口类型有关，请以实际情况为准。
Broadcast address	接口所在网段的广播地址
The Maximum Transmit Unit	接口的最大传输单元，单位为字节
input packets, bytes, multicasts output packets, bytes, multicasts	接口上接收和发送的所有报文数、字节数以及组播报文数（设备启动后就开始统计此信息）
TTL invalid packet number	接口上收到的TTL无效的报文个数（设备启动后就开始统计此信息）

字段	描述
ICMP packet input number:	接口上收到的ICMP报文的总数（设备启动后就开始统计此信息），包括如下报文：
Echo reply:	• Echo 应答报文
Unreachable:	• 不可达报文
Source quench:	• 源站抑制报文
Routing redirect:	• 路由重定向报文
Echo request:	• Echo 请求报文
Router advert:	• 路由器通告报文
Router solicit:	• 路由器请求报文
Time exceed:	• 超时报文
IP header bad:	• IP 报文头错误报文
Timestamp request:	• 时间戳请求报文
Timestamp reply:	• 时间戳响应报文
Information request:	• 信息请求报文
Information reply:	• 信息响应报文
Netmask request:	• 掩码请求报文
Netmask reply:	• 掩码响应报文
Unknown type:	• 未知类型报文

【相关命令】

- **display ip interface brief**
- **ip address**

1.1.2 display ip interface brief

display ip interface brief 命令用来显示三层接口与 IP 相关的简要信息。

【命令】

```
display ip interface [ interface-type [ interface-number ] ] brief
[ description ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-type: 显示指定类型接口的 IP 基本配置信息。如果未指定本参数，则显示所有三层接口与 IP 相关的简要信息。

interface-number: 显示指定接口的 IP 基本配置信息。如果未指定本参数，则显示该类型所有三层接口的与 IP 相关的简要信息。

description: 显示接口完整的描述信息。如果未指定本参数，则最多可以显示 16 个字符，如果超过 16 个字符，那么则显示前 14 个字符和 “...”。

【使用指导】

display ip interface brief 命令用来查看三层接口与 IP 相关的简要信息，包括接口的物理和链路层协议状态、IP 地址、描述信息等。

【举例】

```
# 显示 GigabitEthernet 接口的基本配置信息。
<Sysname> display ip interface gigabitethernet brief
*down: administratively down
(s): spoofing (l): loopback
Interface                Physical Protocol IP Address      Description
GE1/0/1                   up          up          5.5.5.1        Link to CoreRo...
<Sysname> display ip interface gigabitethernet brief description
*down: administratively down
(s): spoofing (l): loopback
Interface                Physical Protocol IP Address      Description
GE1/0/1                   up          up          5.5.5.1        Link to CoreRouter
```

表1-2 display ip interface brief 命令显示信息描述表

字段	描述
*down: administratively down	接口处于管理down状态，即采用 shutdown 命令关闭了该接口
(s) : spoofing	接口的欺骗属性，即接口的链路层协议状态显示是up的，但实际可能没有对应的链路，或者所对应的链路不是永久存在而是按需建立的
Interface	接口的名称
Physical	接口的物理状态，可能的状态及含义如下： • *down: 表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 • down: 该接口的管理状态为开启，但物理状态为关闭（可能因为未连接好或者线路故障） • up: 该接口的管理状态和物理状态均为开启
Protocol	接口的链路层协议状态，可能的状态及含义如下： • down: 该接口的协议状态为关闭 • down(l): 该接口的协议状态为 loopback down • up: 该接口的协议状态为开启 • up(l): 该接口的协议状态为 loopback up • up(s): 该接口的协议状态为 spoofing up

字段	描述
IP Address	接口的IP地址（如果未配置则显示“--”）
Description	接口的描述信息（如果未配置则显示“--”）

【相关命令】

- **display ip interface**
- **ip address**

1.1.3 ip address

ip address 命令用来配置接口的 IP 地址。

undo ip address 命令用来删除接口的 IP 地址。

【命令】

【缺省情况】

未配置接口 IP 地址。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: 接口的 IP 地址，为点分十进制格式。

mask-length: 子网掩码长度，即掩码中连续“1”的个数，取值范围为 1~31，当接口为 LoopBack 接口时，取值范围为 1~32。

mask: 接口 IP 地址相应的子网掩码，为点分十进制格式。

sub: 表示该地址为接口的从 IP 地址。

【使用指导】

ip address 命令用来配置接口的 IP 地址。设备的每个接口可以配置多个 IP 地址，其中一个为主 IP 地址，其余为从 IP 地址。一般情况下，一个接口只需配置一个主 IP 地址，有时为了实现一个接口下的多个子网之间能够通信，需要在接口上配置从 IP 地址。

一个接口只能有一个主 IP 地址，在同一个接口上多次执行本命令，最后一次执行的命令生效。

undo ip address 命令中不指定任何参数表示删除该接口的所有 IP 地址。**undo ip address ip-address { mask | mask-length }**表示删除主 IP 地址。**undo ip address ip-address { mask | mask-length } sub**表示删除指定的从 IP 地址。

同一接口的主、从 IP 地址可以在同一网段，但不同接口之间、主接口及其子接口之间、同一主接口下不同子接口之间的 IP 地址不可以在同一网段。

【举例】

为接口 GigabitEthernet1/0/1 配置主 IP 地址为 129.102.0.1，从 IP 地址为 202.38.160.1，子网掩码都为 255.255.255.0。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address 129.102.0.1 255.255.255.0
[Sysname-GigabitEthernet1/0/1] ip address 202.38.160.1 255.255.255.0 sub
```

【相关命令】

- **display ip interface**
- **display ip interface brief**

1.1.4 ip address unnumbered

ip address unnumbered 命令用来配置本接口借用指定接口的 IP 地址。

undo ip address unnumbered 命令用来恢复缺省情况。

【命令】

```
ip address unnumbered interface interface-type interface-number
undo ip address unnumbered
```

【缺省情况】

本接口未借用其它接口的 IP 地址。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interface interface-type interface-number: 被借用接口的接口类型及接口编号。

【使用指导】

所谓“IP 地址借用”，是指一个接口上未配置 IP 地址，但为了使该接口能正常使用，就向同一设备上其它有 IP 地址的接口借用一个 IP 地址。

IP 地址借用的使用场景如下：

- 在 IP 地址资源比较匮乏的环境下，为了节约 IP 地址资源，可以配置某个接口借用其他接口的 IP 地址。
- 如果某个接口只是偶尔使用，可以配置该接口借用其他接口的 IP 地址，而不必让其一直占用一个单独的 IP 地址。

Loopback 接口的 IP 地址可被其它接口借用，但本身不能借用其它接口的地址。

一个接口的地址可以借给多个接口。如果被借用接口有多个手动配置的 IP 地址，则只有手动配置的主 IP 地址能被借用。

由于借用方接口本身没有 IP 地址，无法在此接口上启用动态路由协议。所以必须手动配置一条到对端网段的静态路由，才能实现设备间的连通。

【举例】

配置接口 GigabitEthernet1/0/2 借用接口 GigabitEthernet1/0/1 的 IP 地址。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/2
```

```
[Sysname-GigabitEthernet1/0/2] ip address unnumbered interface gigabitethernet 1/0/1
```

目 录

1 域名解析	1-1
1.1 域名解析配置命令	1-1
1.1.1 display dns domain	1-1
1.1.2 display dns host	1-2
1.1.3 display dns server	1-3
1.1.4 display ipv6 dns server	1-4
1.1.5 dns domain	1-5
1.1.6 dns dscp	1-6
1.1.7 dns proxy enable	1-6
1.1.8 dns server	1-7
1.1.9 dns source-interface	1-8
1.1.10 dns spoofing	1-9
1.1.11 ip host	1-10
1.1.12 ipv6 dns dscp	1-11
1.1.13 ipv6 dns server	1-12
1.1.14 ipv6 dns spoofing	1-13
1.1.15 ipv6 host	1-14
1.1.16 reset dns host	1-15
2 DDNS	2-1
2.1 DDNS配置命令	2-1
2.1.1 ddns apply policy	2-1
2.1.2 ddns dscp	2-2
2.1.3 ddns policy	2-2
2.1.4 display ddns policy	2-3
2.1.5 interval	2-5
2.1.6 method	2-6
2.1.7 password	2-7
2.1.8 ssl-client-policy	2-7
2.1.9 url	2-8
2.1.10 username	2-10

1 域名解析

1.1 域名解析配置命令

1.1.1 display dns domain

display dns domain 命令用来显示域名后缀信息。

【命令】

display dns domain [**vpn-instance** *vpn-instance-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance *vpn-instance-name*：显示指定 VPN 实例内的域名后缀信息。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的域名后缀信息。

【举例】

显示公网静态配置和动态获得的域名后缀信息。

```
<Sysname> display dns domain
```

Type:

D: Dynamic S: Static

No.	Type	Domain suffix
1	S	com
2	D	net

表1-1 display dns domain 命令显示信息描述表

字段	描述
No.	序号
Type	域名后缀类型： - S：表示静态配置的域名后缀 (暂不支持)D：表示通过 DHCP 等协议动态获得的域名后缀
Domain suffix	域名后缀

【相关命令】

- **dns domain**

1.1.2 display dns host

display dns host 命令用来显示域名解析信息。

【命令】

display dns host [**ip** | **ipv6**] [**vpn-instance** *vpn-instance-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ip: 显示 A 类查询的信息。A 类查询用来解析域名对应的 IPv4 地址。
ipv6: 显示 AAAA 类查询的信息。AAAA 类查询用来解析域名对应的 IPv6 地址。
vpn-instance *vpn-instance-name*: 显示指定 VPN 实例的域名解析信息。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的域名解析信息。

【使用指导】

如果未指定 **ip** 和 **ipv6** 参数，则显示所有查询类型的域名解析信息。

【举例】

```
# 显示所有查询类型的域名解析信息。
<Sysname> display dns host
Type:
  D: Dynamic    S: Static

Total number: 3
No.  Host name      Type  TTL      Query type  IP addresses
1    sample.com      D     3132     A           192.168.10.1
                                           192.168.10.2
                                           192.168.10.3
2    zig.sample.com  S     -        A           192.168.1.1
3    sample.net      S     -        AAAA        FE80::4904:4448
```

表1-2 display dns host 命令显示信息描述表

字段	描述
No.	序号

字段	描述
Host name	查询名称
Type	域名解析信息的类型： • S: 表示静态配置的域名解析信息，即通过 ip host 或 ipv6 host 命令配置的主机名及其对应的主机 IPv4/IPv6 地址 • D: 表示通过动态域名解析获得的域名解析信息
TTL	域名解析信息的剩余有效时间，单位为秒 静态信息的TTL值显示为“-”
Query type	查询类型，取值包括A和AAAA
IP addresses	主机名对应的IP地址 • 对于 A 类查询类型，为 IPv4 地址 • 对于 AAAA 类查询类型，为 IPv6 地址

【相关命令】

- **reset dns host**
- **ip host**
- **ipv6 host**

1.1.1.3 display dns server

display dns server 命令用来显示域名服务器的 IPv4 地址信息。

【命令】

display dns server [*vpn-instance vpn-instance-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
 network-operator
 context-admin
 context-operator

【参数】

vpn-instance vpn-instance-name: 显示指定 VPN 实例内的域名服务器 IPv4 地址信息。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的域名服务器 IPv4 地址信息。

【举例】

显示公网的域名服务器 IPv4 地址信息。
 <Sysname> display dns server
 Type:

D: Dynamic S: Static

No.	Type	IP address
1	S	202.114.0.124
2	S	169.254.65.125

表1-3 display dns server 命令显示信息描述表

字段	描述
No.	域名服务器的序号
Type	域名服务器类型 - S 表示静态指定的域名服务器信息 (暂不支持)D 表示通过 DHCP 等协议动态获得的域名服务器信息
IP address	域名服务器的IPv4地址

【相关命令】

- **dns server**

1.1.4 display ipv6 dns server

display ipv6 dns server 命令用来显示域名服务器的 IPv6 地址信息。

【命令】

display ipv6 dns server [vpn-instance vpn-instance-name]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance vpn-instance-name: 显示指定 VPN 实例内的域名服务器 IPv6 地址信息。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的域名服务器 IPv6 地址信息。

【举例】

显示公网域名服务器的 IPv6 地址信息。

<Sysname> display ipv6 dns server

Type:

D: Dynamic S: Static

No.	Type	IPv6 address	Outgoing Interface

1 S 2::2

表1-4 display ipv6 dns server 命令显示信息描述表

字段	描述
No.	域名服务器的序号
Type	域名服务器类型 - S 表示静态指定的域名服务器信息 (暂不支持)D 表示通过 DHCP 等协议动态获得的域名服务器信息
IPv6 address	域名服务器的IPv6地址
Outgoing Interface	出接口名

【相关命令】

- **ipv6 dns server**

1.1.5 dns domain

dns domain 命令用来添加域名后缀。

undo dns domain 命令用来删除指定的域名后缀。

【命令】

dns domain *domain-name* [**vpn-instance** *vpn-instance-name*]

undo dns domain *domain-name* [**vpn-instance** *vpn-instance-name*]

【缺省情况】

未配置域名后缀，即只根据用户输入的域名信息进行解析。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

domain-name: 域名后缀，由“.”分隔的字符串组成（如 aabbcc.com），每个字符串的长度不超过 63 个字符，包括“.”在内的总长度不超过 253 个字符。不区分大小写，字符串中可以包含字母、数字、“-”、“_”或“.”。

vpn-instance vpn-instance-name: 为指定 VPN 实例添加域名后缀。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网添加域名后缀。

【使用指导】

域名解析时，用户只需要输入域名的部分字段，系统会按照域名后缀配置的先后顺序，依次将输入的域名加上不同的域名后缀进行解析。

本命令配置的域名后缀同时用于 IPv4 域名解析和 IPv6 域名解析。

公网或每个 VPN 实例内最多可以配置 16 个域名后缀。可同时在公网和 VPN 实例内配置域名后缀。

【举例】

为公网添加一个域名后缀 com。

```
<Sysname> system-view  
[Sysname] dns domain com
```

【相关命令】

- **display dns domain**

1.1.6 dns dscp

dns dscp 命令用来指定 DNS 客户端或 DNS proxy 发送 DNS 报文的 DSCP 优先级。

undo dns dscp 命令用来恢复缺省情况。

【命令】

```
dns dscp dscp-value  
undo dns dscp
```

【缺省情况】

DNS 客户端或 DNS proxy 发送 DNS 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

dscp-value: DNS 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

【举例】

配置发送的 DNS 报文的 DSCP 优先级为 30。

```
<Sysname> system-view  
[Sysname] dns dscp 30
```

1.1.7 dns proxy enable

dns proxy enable 命令用来开启 DNS proxy 功能。

undo dns proxy enable 命令用来关闭 DNS proxy 功能。

【命令】

```
dns proxy enable
```


undo dns proxy enable

本命令的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	支持
T5000-G30	支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	不支持
T1000-CN60/T1000-CN80	不支持

【缺省情况】

DNS proxy 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

本命令的配置同时用于 IPv4 域名解析和 IPv6 域名解析。

【举例】

```
# 开启 DNS proxy 功能。
<Sysname> system-view
[Sysname] dns proxy enable
```

1.1.8 dns server

dns server 命令用来配置域名服务器的 IPv4 地址。

undo dns server 命令用来删除域名服务器的 IPv4 地址。

【命令】

```
dns server ip-address [ vpn-instance vpn-instance-name ]
undo dns server [ ip-address ] [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未配置域名服务器的 IPv4 地址。

【视图】

系统视图

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: 域名服务器的 IPv4 地址。在接口视图下执行 **undo** 命令时需要指定本参数。

vpn-instance vpn-instance-name: 为指定 VPN 实例配置域名服务器的 IPv4 地址。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置域名服务器的 IPv4 地址。

【使用指导】

在进行服务器域名解析时，系统按照域名服务器 IPv4 地址配置的先后顺序，依次向各个域名服务器发送查询请求。

公网或单个 VPN 实例内最多可以配置 6 个域名服务器的 IPv4 地址。可同时在公网和 VPN 实例内配置域名服务器的 IPv4 地址。

执行 **undo dns server** 命令时如果未指定 **ip-address** 参数，则删除公网或指定 VPN 实例中的所有域名服务器 IPv4 地址。

【举例】

```
# 配置域名服务器的 IPv4 地址为 172.16.1.1。
<Sysname> system-view
[Sysname] dns server 172.16.1.1
# 在接口 GigabitEthernet1/0/1 配置域名服务器的 IPv4 地址为 172.16.1.1。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dns server 172.16.1.1
```

【相关命令】

- **display dns server**

1.1.9 dns source-interface

dns source-interface 命令用来指定 DNS 报文的源接口。

undo dns source-interface 命令用来恢复缺省情况。

【命令】

```
dns source-interface interface-type interface-number [ vpn-instance  
vpn-instance-name ]  
undo dns source-interface interface-type interface-number [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

设备根据 DNS server 的地址，通过路由表查找报文的出接口，并将该出接口的主 IP 地址作为发送到该服务器的 DNS 查询报文的源地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type interface-number: 源接口的接口类型和接口编号。

vpn-instance vpn-instance-name: 为指定 VPN 实例配置 DNS 报文的源接口。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置 DNS 报文的源接口。

【使用指导】

通过本命令指定 DNS 报文的源接口后，系统将选择指定接口的主 IPv4 地址或根据 RFC 3484 中定义的规则选择指定接口的某个 IPv6 地址，作为 DNS 查询报文的源地址。

本命令的配置同时用于 IPv4 域名解析和 IPv6 域名解析。

公网或每个 VPN 实例内只能配置 1 个源接口。多次执行本命令，最后一次执行的命令生效。可同时在公网和 VPN 实例内配置源接口。

无论配置的源接口是否属于指定的 VPN 实例，该配置都会生效。不建议将不属于 VPN 实例的接口配置为该 VPN 实例的源接口。

【举例】

```
# 指定公网 DNS 报文的源接口为 GigabitEthernet1/0/1。  
<Sysname> system-view  
[Sysname] dns source-interface gigabitethernet 1/0/1
```

1.1.10 dns spoofing

dns spoofing 命令用来开启 DNS spoofing 功能，并指定应答的 IPv4 地址。

undo dns spoofing 命令关闭 DNS spoofing 功能。

【命令】

dns spoofing ip-address [vpn-instance vpn-instance-name]
undo dns spoofing ip-address [vpn-instance vpn-instance-name]

本命令的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	支持
T5000-G30	支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	不支持
T1000-CN60/T1000-CN80	不支持

【缺省情况】

DNS spoofing 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: 用来欺骗性应答域名解析请求的 IPv4 地址。

vpn-instance vpn-instance-name: 为指定 VPN 实例配置 DNS spoofing 功能。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示为公网配置 DNS spoofing 功能。

【使用指导】

配置 DNS spoofing 前, 需要先开启 DNS proxy 功能。

开启 DNS spoofing 功能后, 如果设备上未配置域名服务器地址或不存在到达域名服务器的路由, 则会利用配置的应答 IP 地址作为域名解析结果, 欺骗性地应答 A 类域名解析请求。

公网或每个 VPN 实例内只能配置 1 个 DNS spoofing 应答的 IPv4 地址。多次执行本命令, 最后一次执行的命令生效。可同时在公网和 VPN 实例内配置 DNS spoofing 功能。

【举例】

开启公网的 DNS spoofing 功能, 并指定应答的 IPv4 地址为 1.1.1.1。

```
<Sysname> system-view  
[Sysname] dns proxy enable  
[Sysname] dns spoofing 1.1.1.1
```

【相关命令】

- **dns proxy enable**

1.1.11 ip host

ip host 命令用来配置主机名及其对应的主机 IPv4 地址。

undo ip host 命令用来删除主机名及其对应的主机 IPv4 地址。

【命令】

```
ip host host-name ip-address [ vpn-instance vpn-instance-name ]  
undo ip host host-name ip-address [ vpn-instance vpn-instance-name ]
```

【缺省情况】

不存在主机名及 IPv4 地址的对应关系。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

host-name: 主机名, 为 1~253 个字符的字符串, 不区分大小写, 字符串中可以包含字母、数字、“-”、“_”和“.”。

ip-address: 与主机名对应的 IPv4 地址。

vpn-instance vpn-instance-name: 为指定 VPN 实例配置主机名和 IPv4 地址的对应关系。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示为公网配置主机名和 IPv4 地址的对应关系。

【使用指导】

公网或单个 VPN 实例内最多可以配置 1024 个主机名和 IPv4 地址的对应关系。可同时在公网和 VPN 实例内配置主机名和 IPv4 地址的对应关系。

在公网或单个 VPN 实例内, 一个主机名只能对应一个 IPv4 地址。多次执行本命令, 最后一次执行的命令生效。

ip、**-a**、**-c**、**-f**、**-h**、**-i**、**-m**、**-n**、**-p**、**-q**、**-r**、**-s**、**-t**、**-tos**、**-v** 和 **-vpn-instance** 已被系统用作 **ping** 命令的参数关键字, 在配置主机名时, 请避免使用相同的字符串作为主机名。
ping 命令支持的参数形式, 请参考“网络管理和监控”中的“**ping**”命令。

【举例】

配置公网内主机名 aaa 对应的 IPv4 地址为 10.110.0.1。

```
<Sysname> system-view
```

```
[Sysname] ip host aaa 10.110.0.1
```

【相关命令】

- **display dns host**

1.1.12 ipv6 dns dscp

ipv6 dns dscp 命令用来指定 IPv6 DNS 客户端或 IPv6 DNS proxy 发出的 IPv6 DNS 报文的 DSCP 优先级。

undo ipv6 dns dscp 命令用来恢复缺省情况。

【命令】

```
ipv6 dns dscp dscp-value
```

```
undo ipv6 dns dscp
```

【缺省情况】

IPv6 DNS 客户端或 IPv6 DNS proxy 发出的 IPv6 DNS 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value: IPv6 DNS 报文的 DSCP 优先级, 取值范围为 0~63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级, 决定报文传输的优先程度。配置的 DSCP 优先级的取值越大, 报文的优先级越高。

【举例】

配置发送的 IPv6 DNS 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ipv6 dns dscp 30
```

1.1.13 ipv6 dns server

ipv6 dns server 命令用来配置域名服务器的 IPv6 地址。

undo ipv6 dns server 命令用来删除域名服务器的 IPv6 地址。

【命令】

```
ipv6 dns server ipv6-address [ interface-type interface-number ]
[ vpn-instance vpn-instance-name ]
undo ipv6 dns server [ ipv6-address [ interface-type interface-number ] ]
[ vpn-instance vpn-instance-name ]
```

【缺省情况】

未配置域名服务器的 IPv6 地址。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address: 域名服务器的 IPv6 地址。

interface-type interface-number: 指定报文的出接口的接口类型和接口编号。如果未指定本参数, 则根据路由表查找报文的出接口。域名服务器的 IPv6 地址为链路本地地址时, 必须指定本参数。域名服务器的 IPv6 地址为全球单播地址时, 无法指定本参数。

vpn-instance *vpn-instance-name*: 为指定 VPN 实例配置域名服务器的 IPv6 地址。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示为公网配置域名服务器的 IPv6 地址。

【使用指导】

在进行服务器域名解析时, 系统按照域名服务器 IPv6 地址配置的先后顺序, 依次向各个域名服务器发送查询请求。

公网或单个 VPN 实例内最多可以配置 6 个域名服务器的 IPv6 地址。可同时在公网和 VPN 实例内配置域名服务器的 IPv6 地址。

执行 **undo ipv6 dns server** 命令时如果未指定 *ipv6-address* 参数，则删除公网或指定 VPN 实例中的所有域名服务器 IPv6 地址。

【举例】

配置公网内域名服务器的 IPv6 地址为 2002::1。

```
<Sysname> system-view
```

```
[Sysname] ipv6 dns server 2002::1
```

【相关命令】

- **display ipv6 dns server**

1.1.14 ipv6 dns spoofing

ipv6 dns spoofing 命令用来开启 DNS spoofing 功能，并指定应答的 IPv6 地址。

undo ipv6 dns spoofing 命令用来关闭 DNS spoofing 功能。

【命令】

```
ipv6 dns spoofing ipv6-address [ vpn-instance vpn-instance-name ]
```

```
undo ipv6 dns spoofing ipv6-address [ vpn-instance vpn-instance-name ]
```

【缺省情况】

DNS spoofing 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address：用来欺骗性应答域名解析请求的 IPv6 地址。

vpn-instance *vpn-instance-name*：为指定 VPN 实例配置 DNS spoofing 功能。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置 DNS spoofing 功能。

【使用指导】

本命令必须和 **dns proxy enable** 命令一起使用。

开启 DNS spoofing 功能后，如果设备上未配置域名服务器地址或不存在到达域名服务器的路由，则会利用配置的应答 IPv6 地址作为域名解析结果，欺骗性地应答 AAAA 类域名解析请求。

公网或每个 VPN 实例内只能配置 1 个 DNS spoofing 应答的 IPv6 地址。多次执行本命令，最后一次执行的命令生效。可同时在公网和 VPN 实例内配置 DNS spoofing 功能。

【举例】

为公网开启 DNS spoofing 功能，并指定应答的 IPv6 地址为 2001::1。

```
<Sysname> system-view
[Sysname] dns proxy enable
[Sysname] ipv6 dns spoofing 2001::1
```

【相关命令】

- **dns proxy enable**

1.1.15 ipv6 host

ipv6 host 命令用来配置主机名及其对应的主机 IPv6 地址。

undo ipv6 host 命令用来删除主机名及其对应的主机 IPv6 地址。

【命令】

```
ipv6 host host-name ipv6-address [ vpn-instance vpn-instance-name ]
undo ipv6 host host-name ipv6-address [ vpn-instance vpn-instance-name ]
```

【缺省情况】

不存在主机名及 IPv6 地址的对应关系。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

host-name: 主机名，为 1~253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”和“.”。

ipv6-address: 与主机名对应的 IPv6 地址。

vpn-instance *vpn-instance-name*: 为指定 VPN 实例配置主机名和 IPv6 地址的对应关系。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示为公网配置主机名和 IPv6 地址的对应关系。

【使用指导】

公网或每个 VPN 实例内最多可以配置 1024 个主机名和 IPv6 地址的对应关系。可同时在公网和 VPN 实例内配置主机名和 IPv6 地址的对应关系。

在公网或同一个 VPN 实例内，一个主机名只能对应一个 IPv6 地址。多次执行本命令，最后一次执行的命令生效。

-a、**-c**、**-i**、**-m**、**-q**、**-s**、**-t**、**-tc**、**-v** 和 **-vpn-instance** 已被系统用作 **ping ipv6** 命令的参数关键字，在配置主机名时，请避免使用相同的字符串作为主机名。**ping ipv6** 命令支持的参数形式，请参考“网络管理和监控”中的“**ping ipv6**”命令。

【举例】

配置公网内主机名 aaa 对应的 IPv6 地址为 2001::1。

```
<Sysname> system-view
[Sysname] ipv6 host aaa 2001::1
```


【相关命令】

- **ip host**

1.1.16 reset dns host

reset dns host 命令用来清除动态域名解析缓存信息。

【命令】

reset dns host [**ip** | **ipv6**] [**vpn-instance** *vpn-instance-name*]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip: 清除 A 类查询的动态缓存信息。A 类查询用来解析域名对应的 IPv4 地址。

ipv6: 清除 AAAA 类查询的动态缓存信息。AAAA 类查询用来解析域名对应的 IPv6 地址。

vpn-instance *vpn-instance-name*: 清除指定 VPN 实例的动态域名解析缓存信息。

vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则清除公网的动态域名解析缓存信息。

【使用指导】

如果未指定 **ip** 和 **ipv6** 参数，则清除所有查询类型的动态域名解析缓存信息。

【举例】

清除公网所有查询类型的动态域名解析缓存信息。

```
<Sysname> reset dns host
```

【相关命令】

- **display dns host**

2 DDNS

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
T5000-G20	支持
T5000-G30	不支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	不支持
T1000-CN60/T1000-CN80	不支持

2.1 DDNS配置命令

2.1.1 ddns apply policy

ddns apply policy 命令用来在接口上应用指定的 DDNS 策略来更新指定的 FQDN 与接口主 IP 地址的对应关系，并启动 DDNS 更新。

undo ddns apply policy 命令用来在接口上取消应用 DDNS 策略，停止 DDNS 更新。

【命令】

ddns apply policy *policy-name* [**fqdn** *domain-name*]

undo ddns apply policy *policy-name*

【缺省情况】

没有为接口指定任何 DDNS 策略和需要更新的 FQDN，且未启动 DDNS 更新。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: DDNS 策略名称，为 1~32 个字符的字符串，不区分大小写。

fqdn domain-name: 指定需要更新该 FQDN 与 IP 地址的对应关系，用于替换 DDNS 更新请求 URL 中的<h>。**domain-name** 为主机名，主机名，为 1~253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”和“.”。

【使用指导】

一个接口上最多可以应用 4 个 DDNS 策略。

重复应用名称相同的 DDNS 策略，并指定不同的 FQDN 时，最后一次执行的命令生效，同时发起一次 DDNS 更新。

【举例】

在接口 GigabitEthernet1/0/1 下指定应用 DDNS 策略 steven_policy 来更新合格域名 www.whatever.com 与 IP 地址的对应关系，并启动 DDNS 更新功能。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ddns apply policy steven_policy fqdn www.whatever.com
```

【相关命令】

- **ddns policy**
- **display ddns policy**

2.1.2 ddns dscp

ddns dscp 命令用来配置发送 DDNS 报文的 DSCP 优先级。

undo ddns dscp 命令用来恢复缺省情况。

【命令】

```
ddns dscp dscp-value
```

```
undo ddns dscp
```

【缺省情况】

配置发送 DDNS 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value: DDNS 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 优先级用来体现报文自身的优先等级，决定报文传输的优先程度。配置的 DSCP 优先级的取值越大，报文的优先级越高。

【举例】

配置发送的 DDNS 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
```

```
[Sysname] ddns dscp 30
```

2.1.3 ddns policy

ddns policy 命令用来创建 DDNS 策略，并进入 DDNS 策略视图。如果指定的 DDNS 策略视图已存在，则直接进入 DDNS 策略视图。

undo ddns policy 命令用来删除 DDNS 策略。

【命令】

```
ddns policy policy-name  
undo ddns policy policy-name
```

【缺省情况】

设备上不存在 DDNS 策略。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

policy-name: DDNS 策略名称，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

设备上最多可以创建 16 个 DDNS 策略。

【举例】

```
# 创建名称为 steven_policy 的 DDNS 策略，并进入 DDNS 策略视图。  
<Sysname> system-view  
[Sysname] ddns policy steven_policy
```

【相关命令】

- **display ddns policy**
- **ddns apply policy**

2.1.4 display ddns policy

display ddns policy 命令用来显示 DDNS 策略的信息。

【命令】

```
display ddns policy [ policy-name ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin  
network-operator  
context-admin  
context-operator
```

【参数】

policy-name: DDNS 策略名称，为 1~32 个字符的字符串，不区分大小写。如果未指定本参数，则显示所有 DDNS 策略的信息。

【举例】

显示名称为 steven_policy 的 DDNS 策略的信息。

```
<Sysname> display ddns policy steven_policy
DDNS policy: steven_policy
  URL          : http://members.3322.org/dyndns/update?
                  system=dyndns&hostname=<h> &myip=<a>
  Username     : steven
  Password     : *****
  Method       : GET
  SSL client policy:
  Interval     : 1 days 0 hours 1 minutes
```

显示所有 DDNS 策略的信息。

```
<Sysname> display ddns policy
DDNS policy: steven_policy
  URL          : http://members.3322.org/dyndns/update?system=
                  dyndns&hostname=<h> &myip=<a>
  Username     : steven
  Password     : *****
  Method       : GET
  SSL client policy:
  Interval     : 0 days 0 hours 30 minutes
```

```
DDNS policy: tom-policy
  URL          : http://members.3322.org/dyndns/update?system=
                  dyndns&hostname=<h> &myip=<a>
  Username     :
  Password     :
  Method       : GET
  SSL client policy:
  Interval     : 0 days 0 hours 15 minutes
```

```
DDNS policy: u-policy
  URL          : oray://phservice2.oray.net
  Username     : username
  Password     :
  Method       : -
  SSL client policy:
  Interval     : 0 days 0 hours 15 minutes
```

表2-1 display ddns policy 命令显示信息描述表

字段	描述
DDNS policy	DDNS策略名称
URL	DDNS更新请求的URL地址。未配置时显示为空
Username	登录DDNS服务器的用户名。未配置时显示为空
Password	登录DDNS服务器的密码。未配置时显示为空，有配置时显示为 “*****”

字段	描述
Method	采用HTTP或HTTPS报文发送DDNS更新请求时，使用的参数传输方式取值包括： - GET：表示参数传输方式为 GET 方式 - POST：表示参数传输方式为 POST 方式
SSL client policy	关联的SSL客户端策略名称。未配置时显示为空
Interval	定时发起DDNS更新请求的时间间隔

【相关命令】

- ddns policy**

2.1.5 interval

interval 命令用来指定定时发起更新请求的时间间隔。

undo interval 命令用来恢复缺省情况。

【命令】

interval days [hours [minutes]]

undo interval

【缺省情况】

定时发起 DDNS 更新请求的时间间隔是 1 小时。

【视图】

DDNS 策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

days：天，取值范围为 0~365。

hours：小时，取值范围为 0~23。

minutes：分钟，取值范围为 0~59。

【使用指导】

不论是否到达定时发起更新请求的时间，只要对应接口的主 IP 地址发生改变或接口的链路状态由 down 变为 up，都会立即发起更新请求。

如果配置时间间隔为 0，则不会定时发起更新，除非对应接口的 IP 地址发生改变或接口的链路状态由 down 变为 up。

多次执行本命令，最后一次执行的命令生效。如果 DDNS 策略已经应用到接口上，则立即触发一次 DDNS 更新，并以最后一次配置的时间间隔为更新周期。

【举例】

```
# 为 DDNS 策略 steven_policy 指定定时发起更新请求的时间间隔为 1 天零 1 分。  
<Sysname> system-view  
[Sysname] ddns policy steven_policy  
[Sysname-ddns-policy-steven_policy] interval 1 0 1
```

【相关命令】

- **display ddns policy**
- **ddns policy**

2.1.6 method

method 命令用来配置采用 HTTP 或 HTTPS 报文发送 DDNS 更新请求时使用的参数传输方式。

undo method 命令用来恢复缺省情况。

【命令】

```
method { http-get | http-post }  
undo method
```

【缺省情况】

采用 HTTP 或 HTTPS 报文发送 DDNS 更新请求时使用的参数的传输方式为 http-get。

【视图】

DDNS 策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

http-get: 参数的传输方式为 http-get。

http-post: 参数的传输方式为 http-post。

【使用指导】

采用 HTTP 或 HTTPS 报文发送 DDNS 更新请求时，不同的 DDNS 服务器要求使用的参数传输方式可能不同。例如 DNS 服务器，需要使用 http-post 参数传输方式。通过本配置可以修改参数传输方式，以满足 DDNS 服务器的要求。

本命令仅在基于 HTTP 或 HTTPS 与 DDNS 服务器通信时生效。基于其他协议与 DDNS 服务器通信时，本命令不生效。

通过本命令修改 DDNS 策略的参数传输方式时，如果该 DDNS 策略已经应用到接口上，则立即触发一次 DDNS 更新。

【举例】

```
# 配置 DDNS 策略 steven_policy 采用 HTTP 或 HTTPS 报文发送 DDNS 更新请求时使用的参数传输方式为 http-post 方式。  
<Sysname> system-view  
[Sysname] ddns policy steven_policy
```

```
[Sysname-ddns-policy-steven_policy] method http-post
```

【相关命令】

- **display ddns policy**
- **ddns policy**

2.1.7 password

password 命令用来指定登录 DDNS 服务器的密码。

undo password 命令用来恢复缺省情况。

【命令】

```
password { cipher | simple } string  
undo password
```

【缺省情况】

未指定登录 DDNS 服务器的密码。

【视图】

DDNS 策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

cipher: 表示以密文方式设置密码。

simple: 表示以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~32 个字符的字符串，密文密码为 1~73 个字符的字符串。

【举例】

为 DDNS 策略 steven_policy 指定登录 DDNS 服务器的密码为 nevets。

```
<Sysname> system-view  
[Sysname] ddns policy steven_policy  
[Sysname-ddns-policy-steven_policy] password simple nevets
```

【相关命令】

- **display ddns policy**
- **ddns policy**
- **url**
- **username**

2.1.8 ssl-client-policy

ssl-client-policy 命令用来指定与 DDNS 策略关联的 SSL 客户端策略。

undo ssl-client-policy 命令用来恢复缺省情况。

【命令】

```
ssl-client-policy policy-name  
undo ssl-client-policy
```

【缺省情况】

未指定与 DDNS 策略关联的 SSL 客户端策略。

【视图】

DDNS 策略视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

policy-name: SSL 客户端策略名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

SSL 客户端策略只对 URL 为 HTTPS 地址的 DDNS 更新请求有效。

多次执行本命令，为同一个 DDNS 策略关联不同的 SSL 客户端策略时，DDNS 策略将只与最后配置的 SSL 客户端策略关联。

【举例】

```
# 将 SSL 客户端策略 ssl_policy 与 DDNS 策略 steven_policy 关联。  
<Sysname> system-view  
[Sysname] ddns policy steven_policy  
[Sysname-ddns-policy-steven_policy] ssl-client-policy ssl_policy
```

【相关命令】

- **ddns policy**
- **display ddns policy**
- **ssl-client-policy**（安全命令参考/SSL）

2.1.9 url

url 命令用来指定 DDNS 更新请求的 URL 地址。

undo url 命令用来恢复缺省情况。

【命令】

```
url request-url  
undo url
```

【缺省情况】

未指定 DDNS 更新请求的 URL 地址。

【视图】

DDNS 策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

request-url: DDNS 更新请求的 URL 地址，为 1~240 个字符的字符串，区分大小写。

【使用指导】

不同DDNS服务器的请求更新URL地址有所不同。常见的DDNS服务器URL地址格式如 [表 2-2](#) 所示。

表2-2 常见的 DDNS 更新请求 URL 地址格式列表

DDNS 服务器	DDNS 更新请求的 URL 地址格式
www.3322.org	http://members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
DYNDNS	http://members.dyndns.org/nic/update?system=dyndns&hostname=<h>&myip=<a>
DYNS	http://www.dyns.cx/postscript.php?host=<h>&ip=<a>
ZONEEDIT	http://dynamic.zoneedit.com/auth/dynamic.html?host=<h>&dnsto=<a>
TZO	http://cgi.tzo.com/webclient/signedon.html?TZOName=<h>IPAddress=<a>
EASYDNS	http://members.easydns.com/dyn/ez-ipupdate.php?action=edit&myip=<a>&host_id=<h>
HEIPV6TB	http://dyn.dns.he.net/nic/update?hostname=<h>&myip=<a>
CHANGE-IP	http://nic.changeip.com/nic/update?hostname=<h>&offline=1
NO-IP	http://dynupdate.no-ip.com/nic/update?hostname=<h>&myip=<a>
DHS	http://members.dhs.org/nic/hosts?domain=dyn.dhs.org&hostname=<h>&hostscmd=edit&hostscmdstage=2&type=1&ip=<a>
HP	https://server-name/nic/update?group=group-name&myip=<a>
ODS	ods://update.ods.org
GNUDIP	gnudip://server-name
花生壳	oray://phservice2.oray.net

URL 地址中不支持携带用户名和密码，配置用户名和密码请配合 **username** 和 **password** 命令使用，请根据实际情况修改。

HP 和 GNUDIP 是通用的 DDNS 更新协议，*server-name* 是使用对应 DDNS 更新协议的服务提供商的服务器域名或地址。

DDNS 更新请求的 URL 地址可以以“http://”开头，表示基于 HTTP 与 DDNS 服务器通信；以“https://”开头，表示基于 HTTPS 与 DDNS 服务器通信；以“ods://”开头，表示基于 TCP 与 ODS 服务器通信；以“gnudip://”开头，表示基于 TCP 与 GNUDIP 服务器通信；以“oray://”开头，表示基于 TCP 与花生壳 DDNS 服务器通信。

members.3322.org 和 phservice2.oray.net 是服务提供商提供 DDNS 服务的域名。花生壳提供 DDNS 服务的域名可能是 phservice2.oray.net、phddns60.oray.net、client.oray.net 和 ph031.oray.net 等，请根据实际情况修改域名。

URL 地址中的端口号是可选项,如果不包含端口号则使用缺省端口号:HTTP 是 80,HTTPS 是 443,花生壳 DDNS 服务器是 6060。

<h>由系统根据接口上应用 DDNS 策略时指定的 FQDN 自动填写,<a>由系统根据应用 DDNS 策略的接口的主 IP 地址自动填写,用户可以不更改 URL 中的<h>和<a>。用户也可以手工输入需要更新的 FQDN 和 IP 地址,代替 URL 中的<h>和<a>,此时,应用 DDNS 策略时指定的 FQDN 将不会生效。为了避免配置错误,建议用户不要修改 URL 中的<h>和<a>。

花生壳 DDNS 服务器的 URL 地址中不能指定用于更新的 FQDN 和 IP 地址。用户可在接口上应用 DDNS 策略时指定 FQDN;用于更新的 IP 地址是应用 DDNS 策略的接口的主 IP 地址。

为避免歧义,请尽量不要在 DDNS 服务器上申请含有“:”、“@”或“?”字符的用户名和密码。多次执行本命令,最后一次执行的命令生效。

【举例】

为 DDNS 策略 steven_policy 指定 DDNS 更新请求的 URL 地址。DDNS 服务提供商为 www.3322.org。

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] url
http://members.3322.org/dyndns/update?system=dyndns&hostname=<h> &myip=<a>
```

【相关命令】

- **display ddns policy**
- **ddns policy**
- **password**
- **username**

2.1.10 username

username 命令用来指定登录 DDNS 服务器的用户名。

undo username 命令用来恢复缺省情况。

【命令】

```
username username
undo username
```

【缺省情况】

未指定登录 DDNS 服务器的用户名。

【视图】

DDNS 策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

username: 登录 DDNS 服务器的用户名,为 1~32 个字符的字符串,区分大小写。

【举例】

为 DDNS 策略 `steven_policy` 指定登录 DDNS 服务器的用户名为 `steven`。

```
<Sysname> system-view
[Sysname] ddns policy steven_policy
[Sysname-ddns-policy-steven_policy] username steven
```

【相关命令】

- **display ddns policy**
- **ddns policy**
- **password**
- **url**

目 录

1 IP转发基础	1-1
1.1 IP转发基础配置命令	1-1
1.1.1 display fib	1-1
2 负载分担	2-1
2.1 负载分担配置命令	2-1
2.1.1 ip load-sharing local-first enable	2-1
2.1.2 ip load-sharing mode	2-1

1 IP转发基础

1.1 IP转发基础配置命令

1.1.1 display fib

display fib 命令用来显示 FIB 表项的信息。

【命令】

```
display fib [ vpn-instance vpn-instance-name ] [ ip-address [ mask |  
mask-length ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance *vpn-instance-name*：显示指定 VPN 实例的 FIB 表项的信息。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果不指定 VPN 实例，则显示公网的 FIB 表项的信息。

ip-address：显示与指定目的 IP 地址匹配的 FIB 表项的信息。

mask：IP 地址掩码。

mask-length：IP 地址掩码长度，取值范围为 0~32。

【使用指导】

如果配置 *ip-address* 时不指定掩码和掩码长度，则显示与指定目的 IP 地址最长匹配的 FIB 表项的信息；如果配置 *ip-address* 时指定了掩码或掩码长度，则显示与指定目的 IP 地址和掩码精确匹配的 FIB 表项的信息。

【举例】

显示公网的所有 FIB 表项的信息。

```
<Sysname> display fib
```

```
Destination count: 5 FIB entry count: 5
```

```
Flag:
```

```
U:Useable    G:Gateway    H:Host      B:Blackhole  D:Dynamic    S:Static  
R:Relay      F:FRR
```

Destination/Mask	Nexthop	Flag	OutInterface/Token	Label
0.0.0.0/32	127.0.0.1	UH	InLoop0	Null
192.168.100.0/24	192.168.100.96	U	GE1/0/0	Null
127.0.0.0/8	127.0.0.1	U	InLoop0	Null
127.0.0.0/32	127.0.0.1	UH	InLoop0	Null
127.0.0.1/32	127.0.0.1	UH	InLoop0	Null

显示私网的 FIB 表项的信息。

```
<Sysname> display fib vpn-instance vpn1
Destination count: 6 FIB entry count: 6
```

Flag:

U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static
R:Relay F:FRR

Destination/Mask	Nexthop	Flag	OutInterface/Token	Label
0.0.0.0/32	127.0.0.1	UH	InLoop0	Null
20.20.20.0/24	20.20.20.25	U	GE1/0/0	Null
20.20.20.0/32	20.20.20.25	UBH	GE1/0/0	Null
20.20.20.25/32	127.0.0.1	UH	InLoop0	Null
20.20.20.25/32	20.20.20.25	H	GE1/0/0	Null
20.20.20.255/32	20.20.20.25	UBH	GE1/0/0	Null

显示目的地址为 10.2.1.1 的 FIB 表项的信息。

```
<Sysname> display fib 10.2.1.1
```

Destination count: 1 FIB entry count: 1

Flag:

U:Useable G:Gateway H:Host B:Blackhole D:Dynamic S:Static
R:Relay F:FRR

Destination/Mask	Nexthop	Flag	OutInterface/Token	Label
10.2.1.1/32	127.0.0.1	UH	InLoop0	Null

表1-1 display fib 命令显示信息描述表

字段	描述
Destination count	目的地址的个数
FIB entry count	FIB表项数目
Destination/Mask	目的地址/掩码长度
Nexthop	转发的下一跳地址

字段	描述
Flag	路由的标志： • U：表示可用路由 • G：表示网关路由 • H：表示主机路由 • B：表示黑洞路由 • D：表示动态路由 • S：表示静态路由 • R：表示迭代路由 • F：表示快速重路由
OutInterface/Token	转发接口/LSP索引号
Label	内层标签值

2 负载分担

2.1 负载分担配置命令

2.1.1 ip load-sharing local-first enable

ip load-sharing local-first enable 命令用来开启等价路由负载分担本地优先功能。

undo ip load-sharing local-first enable 命令用来关闭等价路由负载分担本地优先功能。

【命令】

```
ip load-sharing local-first enable
undo ip load-sharing local-first enable
```

【缺省情况】

等价路由负载分担本地优先功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

等价路由负载分担本地优先功能仅在 IRF 模式下生效。

【举例】

```
# 开启等价路由负载分担本地优先功能。
<Sysname> system-view
[Sysname] ip load-sharing local-first enable
```

2.1.2 ip load-sharing mode

ip load-sharing mode 命令用来配置负载分担方式。

undo ip load-sharing mode 命令用来恢复缺省情况。

【命令】

```
ip load-sharing mode { per-flow [ dest-ip | dest-port | ip-pro | src-ip |
src-port ] * | per-packet } { global | slot slot-number }
undo ip load-sharing mode { global | slot slot-number }
```

【缺省情况】

设备基于报文逐流进行负载分担。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

per-flow: 基于报文逐流进行负载分担。

dest-ip: 基于报文的目的 IP 地址逐流进行负载分担。

dest-port: 基于报文的目的端口逐流进行负载分担。

ip-pro: 基于报文的 IP 协议号逐流进行负载分担。

src-ip: 基于报文的源 IP 地址逐流进行负载分担。

src-port: 基于报文的源端口逐流进行负载分担。

global: 表示全局配置。

per-packet: 基于报文逐包进行负载分担。

slot slot-number: 在指定成员设备上配置负载分担方式。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则在所有成员设备上配置负载分担方式。

【使用指导】

配置基于报文逐包进行负载分担方式在快速转发情况下不生效。

【举例】

配置指定 slot 基于报文逐流进行负载分担。

```
<Sysname> system-view
```

```
[Sysname] ip load-sharing mode per-flow slot 1
```

目 录

1 快速转发	1-1
1.1 快速转发配置命令	1-1
1.1.1 display ip fast-forwarding aging-time	1-1
1.1.2 display ip fast-forwarding cache	1-1
1.1.3 display ip fast-forwarding fragcache	1-2
1.1.4 ip fast-forwarding aging-time	1-3
1.1.5 ip fast-forwarding load-sharing	1-4
1.1.6 reset ip fast-forwarding cache	1-5

1 快速转发

1.1 快速转发配置命令

1.1.1 display ip fast-forwarding aging-time

display ip fast-forwarding aging-time 命令用来显示快速转发表项的老化时间。

【命令】

display ip fast-forwarding aging-time

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示快速转发表项的老化时间。

```
<Sysname> display ip fast-forwarding aging-time  
Aging time: 30s
```

表1-1 display ip fast-forwarding aging-time 命令显示信息描述表

字段	描述
Aging time	快转表项的老化时间

【相关命令】

- **ip fast-forwarding aging-time**

1.1.2 display ip fast-forwarding cache

display ip fast-forwarding cache 命令用来显示快速转发表信息。

【命令】

display ip fast-forwarding cache [*ip-address*] [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

ip-address: 显示指定 IP 地址的快速转发表信息。如果不指定 **ip-address**，将显示所有快速转发表信息。

slot slot-number: 显示指定成员设备的快速转发表信息。**slot-number** 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备的快速转发表信息。

【举例】

显示所有快速转发表的信息。

```
<Sysname> display ip fast-forwarding cache
Total number of fast-forwarding entries: 1
SIP          SPort DIP          DPort Pro Input_If  Output_If  Flg
7.0.0.13     68    8.0.0.1      67    17  GE1/0/3   GE1/0/1    5
```

表1-2 display ip fast-forwarding cache 命令显示信息描述表

字段	描述
Total number of fast-forwarding entries	快速转发表项数目
SIP	源IP地址
SPort	源端口号
DIP	目的IP地址
DPort	目的端口号
Pro	协议号
Input_If	报文入接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及入接口，“-”表示接口不存在）
Output_If	报文出接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及出接口，“-”表示接口不存在）
Flg	内部标记，主要是标记分片等内部操作信息

【相关命令】

- **reset ip fast-forwarding cache**

1.1.3 display ip fast-forwarding fragcache

display ip fast-forwarding fragcache 命令用来显示分片报文快速转发表信息。

【命令】

display ip fast-forwarding fragcache [*ip-address*] [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ip-address: 显示指定 IP 地址的分片报文快速转发表信息。如果不指定 **ip-address**，将显示所有分片报文快速转发表信息。

slot slot-number: 显示指定成员设备的分片报文快速转发表信息。**slot-number** 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备的分片报文快速转发表信息。

【举例】

```
# 显示所有分片报文快速转发表信息。
<Sysname> display ip fast-forwarding fragcache
Total number of fragment fast-forwarding entries: 1
SIP          SPort DIP          DPort Pro Input_If  ID
7.0.0.13     68   8.0.0.1     67    17  GE1/0/3    2
```

表1-3 display ip fast-forwarding fragcache 命令显示信息描述表

字段	描述
Total number of fragment fast-forwarding entries	分片报文快速转发表项数目
SIP	源IP地址
SPort	源端口号
DIP	目的IP地址
DPort	目的端口号
Pro	协议号
Input_If	报文入接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及入接口，“-”表示接口不存在）
ID	分片IP报文ID

【相关命令】

- **reset ip fast-forwarding cache**

1.1.4 ip fast-forwarding aging-time

ip fast-forwarding aging-time 命令用来配置快速转发表项的老化时间。
undo ip fast-forwarding aging-time 命令用来恢复缺省情况。

【命令】

ip fast-forwarding aging-time aging-time
undo ip fast-forwarding aging-time

【缺省情况】

快速转发表项的老化时间为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

aging-time: 快速转发表项的老化时间，取值范围为 10～300，单位为秒。

【举例】

```
# 配置快速转发表项的老化时间为 20 秒。
<Sysname> system-view
[Sysname] ip fast-forwarding aging-time 20
```

【相关命令】

- **display ip fast-forwarding aging-time**

1.1.5 ip fast-forwarding load-sharing

ip fast-forwarding load-sharing 命令用来开启快转负载分担功能。

undo ip fast-forwarding load-sharing 命令用来关闭快转负载分担功能。

【命令】

```
ip fast-forwarding load-sharing
undo ip fast-forwarding load-sharing
```

【缺省情况】

快转负载分担功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启快速转发负载分担功能后，当一条数据流从不同入接口上来进行转发时，不再根据入接口不同区分数据流，根据报文中的信息标识一条数据流。

关闭快速转发负载分担功能后，将会根据入接口的不同对已标识的数据流再次做出区分，即将入接口作为区分数据流的另一特征标识。

【举例】

```
# 开启快转负载分担功能。
```

```
<Sysname> system-view
[Sysname] ip fast-forwarding load-sharing
```

1.1.6 reset ip fast-forwarding cache

reset ip fast-forwarding cache 命令用来清除快速转发表中的信息。

【命令】

```
reset ip fast-forwarding cache [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

slot slot-number: 清除指定成员设备的快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除所有成员设备的快速转发表信息。

【举例】

```
# 清除快速转发表信息。
<Sysname> reset ip fast-forwarding cache
```

【相关命令】

- **display ip fast-forwarding cache**
- **display ip fast-forwarding fragcache**

目 录

1 多CPU报文负载分担	1-1
1.1.1 forwarding policy	1-1

1 多CPU报文负载分担

1.1.1 forwarding policy

forwarding policy 命令用来配置报文负载分担策略。

undo forwarding policy 命令用来恢复缺省情况。

【命令】

```
forwarding policy { per-flow [ three-tuple ] | per-packet }  
undo forwarding policy
```

【缺省情况】

采用基于五元组的报文负载分担策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

per-flow: 基于流处理，设备可以基于三元组和五元组划分流，将三元组或五元组相同的一条流分配到同一个或多个 CPU 进行处理，处理过程保证先进先出。

enhance: 增强模式的流处理。配置本参数后，同一条流的入方向、转发和出方向分担到不同的 CPU 进行处理，从而提升单条流的处理性能。

three-tuple: 采用基于三元组的报文负载分担策略。如果不指定本参数，则表示采用基于五元组的报文负载分担策略。

设备各款型对于 **three-tuple** 参数支持情况有所不同，详细差异信息如下：

型号	说明
T5000-G20	不支持
T5000-G30	支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	不支持
T1000-CN60/T1000-CN80	不支持

per-packet: 基于报文处理，将报文依次发送到不同的 CPU 进行处理，不保证报文的处理顺序。

【举例】

配置基于五元组的报文负载分担策略。

```
<Sysname> system-view
```

```
[Sysname] forwarding policy per-flow
```

目 录

1 邻接表	1-1
1.1 IPv4 邻接表配置命令	1-1
1.1.1 display adjacent-table	1-1
1.2 IPv6 邻接表配置命令	1-3
1.2.1 display ipv6 adjacent-table	1-3

1 邻接表

1.1 IPv4邻接表配置命令

1.1.1 display adjacent-table

display adjacent-table 命令用来显示 IPv4 邻接表项的信息。

【命令】

```
display adjacent-table { all | physical-interface interface-type interface-number | routing-interface interface-type interface-number | slot slot-number } [ count | verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

all: 显示所有的 IPv4 邻接表项的信息。

physical-interface *interface-type interface-number*: 显示指定物理接口上的 IPv4 邻接表项的信息。

routing-interface *interface-type interface-number*: 显示指定路由接口上的 IPv4 邻接表项的信息。

slot *slot-number*: 显示指定成员设备的 IPv4 邻接表项的信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv4 邻接表项的信息。

count: 显示 IPv4 邻接表项的数目。

verbose: 显示 IPv4 邻接表项的详细信息。

【举例】

显示所有 IPv4 邻接表项的详细信息。

```
<Sysname> display adjacent-table all verbose
  IP address           : 0.0.0.0
  Routing interface    : GE1/0/1
  Physical interface   : GE1/0/1
  Logical interface    : N/A
  Service type         : ETH
  Action type          : Forwarding
  Link media type      : P2P
```

```

Slot                : 0
Cpu                 : 0
VPN index           : 0
Virtual circuit information : N/A
Link head information(IP) : 4500000000000000ff2f0000002020201020202020000
                                0800
Link head information(MPLS) : 4500000000000000ff2f0000002020201020202020000
                                0800

```

显示指定 slot 的 IPv4 邻接表项的信息。

```
<Sysname> display adjacent-table slot 1
```

IP address	Routing interface	Physical interface	Type
0.0.0.0	GE1/0/1	GE1/0/1	ETH

显示指定 slot 的 IPv4 邻接表项的数目。

```
<Sysname> display adjacent-table slot 1 count
```

```
Total entries on slot 1: 1
```

表1-1 display adjacent-table 命令显示信息描述表

字段	描述
IP address	报文转发下一跳的IP地址（对于P2P链路，不需要下一跳IP地址信息，本字段的值填为0.0.0.0；对于NBMA链路，取值0.0.0.0表示缺省邻接表，从缺省虚链路转发）
Routing interface	路由出接口
Physical interface	路由出接口对应的实际发送报文的物理接口
Logical interface	发送报文的逻辑接口（如果没有此信息，则显示为N/A）
Service type/Type	链路层协议类型
Action type	报文处理类型： - Forwarding：表示转发 - Drop：表示丢弃
Link media type	链路介质类型： - P2P：表示点到点链路 - NBMA：表示点对多点链路
Cpu	（暂不支持）CPU编号
VPN index	VPN索引
Virtual circuit information	虚链路信息，如PVC、DLCI等（如果没有此信息，则显示为N/A）
Link head information(IP)	IPv4协议对应的链路层头信息
Link head information(MPLS)	MPLS协议对应的链路层头信息

1.2 IPv6邻接表配置命令

1.2.1 display ipv6 adjacent-table

display ipv6 adjacent-table 命令用来显示 IPv6 邻接表项的信息。

【命令】

```
display ipv6 adjacent-table { all | physical-interface interface-type interface-number | routing-interface interface-type interface-number | slot slot-number } [ count | verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

all: 显示所有的 IPv6 邻接表项的信息。

physical-interface *interface-type interface-number*: 显示指定物理接口上的 IPv6 邻接表项的信息。

routing-interface *interface-type interface-number*: 显示指定路由接口上的 IPv6 邻接表项的信息。

slot *slot-number*: 显示指定成员设备的 IPv6 邻接表项的信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 邻接表项的信息。

count: 显示 IPv6 邻接表项的数目。

verbose: 显示 IPv6 邻接表项的详细信息。

【举例】

显示所有 IPv6 邻接表项的详细信息。

```
<Sysname> display ipv6 adjacent-table all verbose
```

```
IPv6 address           : N/A
Routing interface       : GE1/0/1
Physical interface      : GE1/0/1
Logical interface       : N/A
Service type            : ETH
Action type             : Forwarding
Link media type         : P2P
Slot                   : 1
Cpu                     : 0
VPN index               : 0
Virtual circuit information : N/A
Link head information(IPv6) : 4500000000000000ff2f0000002020201020202020000
```

```

86dd
Link head information(MPLS) : 4500000000000000ff2f000002020201020202020000
86dd
# 显示指定 slot 的 IPv6 邻接表项的信息。
<Sysname> display ipv6 adjacent-table slot 1
IPv6 address      Routing interface  Physical interface  Type
N/A              GE1/0/1          GE1/0/1            ETH
# 显示指定 slot 的 IPv6 邻接表项的数目。
<Sysname> display ipv6 adjacent-table slot 1 count
Total entries on slot 1: 1

```

表1-2 display ipv6 adjacent-table 命令显示信息描述表

字段	描述
IPv6 address	报文转发下一跳的IPv6地址（对于P2P链路，不需要下一跳IPv6地址信息，本字段的值填为0::0，显示为N/A；对于NBMA链路，取值0::0表示缺省邻接表，从缺省虚链路转发）
Routing interface	路由出接口
Physical interface	路由出接口对应的实际发送报文的物理接口
Logical interface	发送报文的逻辑接口（如果没有此信息，则显示为N/A）
Service type/Type	链路层协议类型
Action type	报文处理类型： - Forwarding：表示转发 - Drop：表示丢弃
Link media type	链路介质类型： - P2P：表示点到点链路 - NBMA：表示点对多点链路
Cpu	（暂不支持）CPU编号
VPN index	VPN索引
Virtual circuit information	虚链路信息，如PVC、DLCI等（如果没有此信息，则显示为N/A）
Link head information(IPv6)	IPv6协议对应的链路层头信息
Link head information(MPLS)	MPLS协议对应的链路层头信息

目 录

1 IP性能优化	1-1
1.1 IP性能优化配置命令	1-1
1.1.1 display icmp statistics	1-1
1.1.2 display ip statistics	1-2
1.1.3 display rawip	1-4
1.1.4 display rawip verbose	1-5
1.1.5 display tcp	1-9
1.1.6 display tcp statistics	1-10
1.1.7 display tcp verbose	1-14
1.1.8 display udp	1-19
1.1.9 display udp statistics	1-20
1.1.10 display udp verbose	1-21
1.1.11 ip forward-broadcast	1-24
1.1.12 ip icmp error-interval	1-25
1.1.13 ip icmp source	1-26
1.1.14 ip mtu	1-27
1.1.15 ip reassemble local enable	1-28
1.1.16 ip redirects enable	1-28
1.1.17 ip ttl-expires enable	1-29
1.1.18 ip unreachable enable	1-30
1.1.19 reset ip statistics	1-31
1.1.20 reset tcp statistics	1-31
1.1.21 reset udp statistics	1-32
1.1.22 tcp mss	1-32
1.1.23 tcp path-mtu-discovery	1-33
1.1.24 tcp syn-cookie enable	1-34
1.1.25 tcp timer fin-timeout	1-34
1.1.26 tcp timer syn-timeout	1-35
1.1.27 tcp timestamps enable	1-36
1.1.28 tcp window	1-36

1 IP性能优化

1.1 IP性能优化配置命令

1.1.1 display icmp statistics

display icmp statistics 命令用来显示 ICMP 流量统计信息。

【命令】

display icmp statistics [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备的 ICMP 流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 ICMP 流量统计信息。

【使用指导】

display icmp statistics 命令用来显示设备接收和发送的各类 ICMP 流量的统计信息。

【举例】

显示 ICMP 流量统计信息。

```
<Sysname> display icmp statistics
  Input: bad formats      0          bad checksum          0
         echo            175        destination unreachable 0
         source quench    0          redirects            0
         echo replies     201        parameter problem     0
         timestamp        0          information requests  0
         mask requests    0          mask replies          0
         time exceeded    0          invalid type          0
         router advert    0          router solicit        0
         broadcast/multicast echo requests ignored 0
         broadcast/multicast timestamp requests ignored 0
  Output: echo            0          destination unreachable 0
         source quench    0          redirects            0
         echo replies     175        parameter problem     0
         timestamp        0          information replies   0
         mask requests    0          mask replies          0
```

```

time exceeded 0          bad address          0
packet error  1442       router advert        3

```

表1-1 display icmp statistics 命令显示信息描述表

字段	描述
bad formats	输入的格式错误报文数
bad checksum	输入的校验和错误报文数
echo	输入/输出的响应请求报文数
destination unreachable	输入/输出的目的不可达报文数
source quench	输入/输出的源站抑制报文数
redirects	输入/输出的重定向报文数
echo replies	输入/输出的响应应答报文数
parameter problem	输入/输出的参数错误报文数
timestamp	输入/输出的时间戳报文数
information requests	输入的信息请求报文数
mask requests	输入/输出的掩码请求报文数
mask replies	输入/输出的掩码应答报文数
invalid type	输入的非法类型报文数
router advert	输入的路由器公告报文数
router solicit	输入的路由器请求报文数
broadcast/multicast echo requests ignored	输入的广播/组播响应请求丢弃报文数
broadcast/multicast timestamp requests ignored	输入的广播/组播时间戳请求丢弃报文数
information replies	输出的信息应答报文数
time exceeded	输入/输出的超时报文数
bad address	输出的目的地址非法报文数
packet error	输出的错误报文数
router advert	输入/输出的路由器公告报文数

1.1.2 display ip statistics

display ip statistics 命令用来显示 IP 报文统计信息。

【命令】

display ip statistics [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number：显示指定成员设备的 IP 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IP 报文统计信息。

【使用指导】

display ip statistics 命令用来显示 IP 报文统计信息，包括接收报文、发送报文、分片、重组的统计信息。

【举例】

```
# 显示 IP 报文统计信息。
<Sysname> display ip statistics
  Input:          sum          7120          local          112
                 bad protocol  0           bad format      0
                 bad checksum  0           bad options     0
                 dropped       0
  Output:         forwarding   0           local          27
                 dropped       0           no route       2
                 compress fails 0
  Reassembling:   fragments    0           reassembled     0
                 dropped       0           timeouts       0
  Fragment:       fragmented   0           couldn't fragment 0
                 output frags  0
  Forwarded Frags: sum          0
```

表1-2 display ip statistics 命令显示信息描述表

字段		描述
Input:	sum	接收报文总数
	local	接收的目的地址是本地的报文数
	bad protocol	未知协议的报文数
	bad format	格式错误的报文数
	bad checksum	校验和错误的报文数
	bad options	选项错误的报文数
	dropped	接收时丢弃的报文数
Output:	forwarding	转发的报文数
	local	本地发送报文数
	dropped	发送时丢弃的报文数

字段		描述
	no route	查不到路由的报文数
	compress fails	压缩失败的报文数
Reassembling:	fragments	收到需要重组的分片报文数
	reassembled	重组成功的报文数
	dropped	重组失败后丢弃的分片报文数
	timeouts	重组超时的次数
Fragment:	fragmented	分片成功的报文数
	couldn't fragment	分片失败的报文数
	output frags	分片成功并发送的分片报文数
Forwarded Frags:	sum	直接转发的分片报文数

【相关命令】

- **display ip interface**（三层技术-IP 业务命令参考/IP 地址）
- **reset ip statistics**

1.1.3 display rawip

display rawip 命令用来显示 RawIP 连接摘要信息。

【命令】

display rawip [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备的 RawIP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 RawIP 连接摘要信息。

【使用指导】

display rawip 命令用来显示 RawIP 连接摘要信息，包括本端 IP 地址、对端 IP 地址、使用 RawIP socket 的协议号等信息。

【举例】

显示 RawIP 连接摘要信息。

```
<Sysname> display rawip
Local Addr      Foreign Addr      Protocol  Slot  PCB
0.0.0.0         0.0.0.0           1         1     0x0000000000000009
0.0.0.0         0.0.0.0           1         1     0x0000000000000008
0.0.0.0         0.0.0.0           1         5     0x0000000000000002
```

表1-3 display rawip 命令显示信息描述表

字段	描述
Local Addr	本端IP地址
Foreign Addr	对端IP地址
Protocol	使用RawIP socket的协议号
PCB	协议控制块索引

1.1.4 display rawip verbose

display rawip verbose 命令用来显示 RawIP 连接详细信息。

【命令】

```
display rawip verbose [ slot slot-number [ pcb pcb-index ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

pcb pcb-index: 显示指定协议控制块索引的 RawIP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

slot slot-number: 显示指定成员设备的 RawIP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 RawIP 连接详细信息。

【使用指导】

display rawip verbose 命令用来显示 RawIP 连接详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号、以及 RawIP 连接的源 IP 地址和目的 IP 地址等信息。

【举例】

```
# 显示 RawIP 连接详细信息。
<Sysname> display rawip verbose
Total RawIP socket number: 1

Connection info: src = 0.0.0.0, dst = 0.0.0.0
```

Location: slot 6
 Creator: ping[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 1
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xfffff
 Receive VRF: 0xfffff

表1-4 display rawip verbose 命令显示信息描述表

字段	描述
Total RawIP socket number	RawIP socket总数
Connection info	连接信息，分别为源IP地址、目的IP地址
Location	socket所在位置，在非集中式设备上执行本命令时，才显示此字段
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，包括： • NOFDREF：用户已经关闭 • ISCONNECTED：连接已经建立 • ISCONNECTING：正在建立连接 • ISDISCONNECTING：正在断开连接 • ASYNC：异步方式 • ISDISCONNECTED：连接已经断开 • PROTOREF：协议强关联 • N/A：不处于上述状态

字段	描述
Options	socket的选项，包括： • SO_DEBUG：记录套接字的调试信息 • SO_ACCEPTCONN：server 端监听连接请求 • SO_REUSEADDR：允许本地地址重复使用 • SO_KEEPALIVE：协议需要查询空闲的连接 • SO_DONTROUTE：设置不查路由表（用于目的地址是直连网络的情况） • SO_BROADCAST：套接字支持广播报文 • SO_LINGER：套接字关闭但仍发送剩余数据 • SO_OOBINLINE：带外数据采用内联方式存储 • SO_REUSEPORT：允许本地端口重复使用 • SO_TIMESTAMP：记录入报文时间戳，只对非连接的协议有效，时间精确到毫秒 • SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建 SIGPIPE • SO_FILTER：设置报文过滤条件，对接收报文有效 • SO_TIMESTAMPNS：和时间戳选项功能类似，时间可以精确到纳秒 • N/A：未设置选项
Error	影响socket连接的错误码
Receiving buffer (cc/hiwat/lowat/drop/state)	接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、丢包数和状态，包括： • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Sending buffer (cc/hiwat/lowat/state)	发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，包括： • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Type	使用的socket类型，包括： • 1: SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 • 2: SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 • 3: SOCK_RAW，RAW 模式的通信方式 • N/A：不是上述类型
Protocol	使用socket的协议号

字段	描述
Inpcb flags	Internet协议控制块中的标记，包括： • INP_RECVOPTS: 接收传入的 IP 选项 • INP_RECVRETOPTS: 接收回应的 IP 选项 • INP_RECVDSTADDR: 接收目的 IP 地址 • INP_HDRINCL: 用户提供整个 IP 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_RECVIF: 接收报文时记录报文的入接口 • INP_RECVTTL: 携带报文的 TTL，仅 UDP 和 RawIP 支持 • INP_DONTFRAG: 设置不可分片标志 • INP_ROUTER_ALERT: 接收携带路由器告警选项的报文，仅 RawIP 支持 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • INP_RCVMACADDR: 接收报文的 MAC • INP_RECVTOS: 携带报文的 TOS，仅 UDP 和 RawIP 支持 • INP_USEICMPSRC: 使用配置的 ICMP 地址作为源地址 • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb extflag	Internet协议控制块中的扩展标记，包括： • INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 • INP_RCVPWID: 接收报文时记录报文的 PW ID • INP_EXTRCVICMPERR: 接收 ICMP 差错报文 • INP_EXTFILTER: 接收报文时对报文内容进行过滤 • N/A: 不是上述标记
Inpcb vflag	Internet协议控制块中的IP版本标记，包括： • INP_IPV4: 运用与 IPv4 通信 • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
TTL(minimum TTL)	Internet协议控制块中的生存周期，括号中为最小生存周期
Send VRF	发送实例
Receive VRF	接收实例

1.1.5 display tcp

display tcp 命令用来显示 TCP 连接摘要信息。

【命令】

display tcp [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number：显示指定成员设备的 TCP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 TCP 连接摘要信息。

【使用指导】

display tcp 命令用来显示 TCP 连接摘要信息，包括本端 IP 地址及端口号、对端 IP 地址及端口号、TCP 连接的状态等信息。

【举例】

```
# 显示 TCP 连接摘要信息。
<Sysname> display tcp
*: TCP MD5 Connection
Local Addr:port      Foreign Addr:port    State      Slot  PCB
*0.0.0.0:21          0.0.0.0:0            LISTEN     1     0x00000000000000c387
192.168.20.200:23    192.168.20.14:1284   ESTABLISHED 1     0x0000000000000009
192.168.20.200:23    192.168.20.14:1283   ESTABLISHED 1     0x0000000000000002
```

表1-5 display tcp 命令显示信息描述表

字段	描述
*	如果某个连接前有此标识，则表示该TCP连接是采用MD5加密算法认证的连接
Local Addr:port	本端IP地址及端口号
Foreign Addr:port	对端IP地址及端口号

字段	描述
State	TCP连接状态，包括： • CLOSED：服务器收到客户端的关闭连接请求回应后所处的状态 • LISTEN：服务器在等待连接请求时所处的状态 • SYN_SENT：客户端发出连接请求等待服务器回应时所处的状态 • SYN_RCVD：服务器收到客户端连接请求时所处的状态 • ESTABLISHED：服务器和客户端双方建立连接并能进行双向数据传递的状态 • CLOSE_WAIT：服务器收到客户端关闭连接请求时所处的状态 • FIN_WAIT_1：客户端发出关闭连接请求等待服务器回应时所处的状态 • CLOSING：连接双方在向对端发出关闭连接请求后等待对端回应过程中收到对端发出的关闭连接请求时所处的状态 • LAST_ACK：服务器向客户端发出关闭连接请求等待回应时所处的状态 • FIN_WAIT_2：客户端收到服务器关闭连接回应后所处的状态 • TIME_WAIT：客户端收到服务器的关闭连接请求后所处的状态
PCB	协议控制块索引

1.1.6 display tcp statistics

display tcp statistics 命令用来显示 TCP 连接的流量统计信息。

【命令】

display tcp statistics [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number：显示指定成员设备的 TCP 连接流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 TCP 连接流量统计信息。

【使用指导】

display tcp statistics 命令用来显示 TCP 连接的流量统计信息，包括接收报文、发送报文以及 Syncookie/syncookie 等相关统计信息。

【举例】

```
# 显示 TCP 连接的流量统计信息。
<Sysname> display tcp statistics
Received packets:
```

Total: 4150
packets in sequence: 1366 (134675 bytes)
window probe packets: 0, window update packets: 0
checksum error: 0, offset error: 0, short error: 0
packets dropped for lack of memory: 0
packets dropped due to PAWS: 0
duplicate packets: 12 (36 bytes), partially duplicate packets: 0 (0 bytes)
out-of-order packets: 0 (0 bytes)
packets with data after window: 0 (0 bytes)
packets after close: 0
ACK packets: 3531 (795048 bytes)
duplicate ACK packets: 33, ACK packets for unsent data: 0

Sent packets:

Total: 4058
urgent packets: 0
control packets: 50
window probe packets: 3, window update packets: 11
data packets: 3862 (795012 bytes), data packets retransmitted: 0 (0 bytes)
ACK-only packets: 150 (52 delayed)
unnecessary packet retransmissions: 0

Syncache/syncookie related statistics:

entries added to syncache: 12
syncache entries retransmitted: 0
duplicate SYN packets: 0
reply failures: 0
successfully build new socket: 12
bucket overflows: 0
zone failures: 0
syncache entries removed due to RST: 0
syncache entries removed due to timed out: 0
ACK checked by syncache or syncookie failures: 0
syncache entries aborted: 0
syncache entries removed due to bad ACK: 0
syncache entries removed due to ICMP unreachable: 0
SYN cookies sent: 0
SYN cookies received: 0

SACK related statistics:

SACK recoveries: 1
SACK retransmitted segments: 0 (0 bytes)
SACK blocks (options) received: 0
SACK blocks (options) sent: 0
SACK scoreboard overflows: 0

Other statistics:

retransmitted timeout: 0, connections dropped in retransmitted timeout: 0

```

persist timeout: 0
keepalive timeout: 21, keepalive probe: 0
keepalive timeout, so connections disconnected: 0
fin_wait_2 timeout, so connections disconnected: 0
initiated connections: 29, accepted connections: 12, established connections:
23
closed connections: 50051 (dropped: 0, initiated dropped: 0)
bad connection attempt: 0
ignored RSTs in the window: 0
listen queue overflows: 0
RTT updates: 3518(attempt segment: 3537)
correct ACK header predictions: 0
correct data packet header predictions: 568
resends due to MTU discovery: 0
packets dropped with MD5 authentication: 0
packets permitted with MD5 authentication: 0

```

表1-6 display tcp statistics 命令显示信息描述表

字段		描述
Received packets:	Total	接收的报文总数
	packets in sequence	按顺序到达的报文数，括号中为字节数
	window probe packets	接收的窗口探测报文数
	window update packets	接收的窗口更新报文数
	checksum error	接收的校验和错误报文数
	offset error	接收的偏移量错误报文数
	short error	接收的报文长度太短的报文数
	packets dropped for lack of memory	由于内存不足而被丢弃的报文数
	packets dropped due to PAWS	由于PAWS（防止序号回绕）而被丢弃的报文数
	duplicate packets	接收的完全重复报文数，括号中为字节数
	partially duplicate packets	接收的部分重复报文数，括号中为字节数
	out-of-order packets	接收的顺序错乱的报文数，括号中为字节数
	packets with data after window	落在接收窗口外的报文数，括号中为字节数
	packets after close	在连接关闭后到达的报文数
	ACK packets	接收的ACK确认报文数，括号中为字节数
	duplicate ACK packets	接收的重复的ACK确认报文数
	ACK packets for unsent data	接收的确认未发送数据的ACK报文数
Sent packets:	Total	发送的报文总数
	urgent packets	发送的紧急数据报文数

字段		描述
	control packets	发送的控制报文数，括号中为包含的重传数据报文数
	window probe packets	发送的窗口探测报文数
	window update packets	发送的窗口更新报文数
	data packets	发送的数据报文数，括号中为字节数
	data packets retransmitted	重发的数据报文数，括号中为字节数
	ACK-only packets	发送的ACK报文数，括号中为延迟ACK报文数
	unnecessary packet retransmissions	报文非必要重传次数
Syncache/syncookie related statistics:	entries added to syncache	添加的syncache对象数
	syncache entries retransmitted	重传的syncache对象数
	duplicate SYN packets	重复的SYN报文数
	reply failures	回复失败的报文数
	successfully build new socket	创建子socket成功数
	bucket overflows	bucket溢出次数
	zone failures	内存分配失败次数
	syncache entries removed due to RST	由于收到RST（复位连接）报文段而删除的syncache对象个数
	syncache entries removed due to timed out	定时器超时且重传次数超过限制时syncache对象删除数
	ACK checked by syncache or syncookie failures	接收到ACK报文时查找syncache处理失败数
	syncache entries aborted	创建子socket失败数
	syncache entries removed due to bad ACK	由于bad ACK而删除的syncache对象数
	syncache entries removed due to ICMP unreachable	由于接收到ICMP差错报文导致删除的syncache对象数
	SYN cookies sent	SYN cookie发送数
	SYN cookies received	SYN cookie接收数
SACK related statistics	SACK recoveries	通过SACK进行恢复的次数
	SACK retransmitted segments	通过SACK进行重传的报文段个数，括号中为字节数
	SACK blocks (options) received	接收到的带选择性ACK选项的报文数
	SACK blocks (options) sent	发送的带选择性ACK选项的报文数
	SACK scoreboard overflows	本地维护的对端缺失报文段记录队列溢出次数
Other statistics	retransmitted timeout	重传定时器超时次数

字段	描述
connections dropped in retransmitted timeout	重传次数超过限制而丢弃的连接数
persist timeout	持续定时器超时次数
keepalive timeout	存活定时器超时次数
keepalive probe	发送的存活探测报文数
keepalive timeout, so connections disconnected	存活定时器超时而中断的连接数
fin_wait_2 timeout, so connections disconnected	Fin wait 2定时器超时而中断的连接数
initiated connections	发起连接次数
accepted connections	接受连接次数
established connections	已建立连接数
closed connections(dropped: 0, initiated dropped: 0)	已关闭连接数目，括号中为意外丢弃连接数（收到对端SYN之后）、主动连接失败数（收到对端SYN之前）
bad connection attempt	接收到的错误连接报文数
ignored RSTs in the window	窗口中忽略的RST报文数
listen queue overflows	监听队列溢出次数
RTT updates(attempt segment)	RTT更新次数，括号中为发送的报文数
correct ACK header predictions	ACK通过首部预测算法的次数
correct data packet header predictions	数据报文通过首部预测算法的次数
resends due to MTU discovery	由于MTU发现而重传的报文数
packets dropped with MD5 authentication	MD5验证丢弃报文数
packets permitted with MD5 authentication	MD5验证通过报文数

【相关命令】

- **reset tcp statistics**

1.1.7 display tcp verbose

display tcp verbose 命令用来显示 TCP 连接详细信息。

【命令】

display tcp verbose [slot slot-number [pcb pcb-index]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

pcb pcb-index: 显示指定协议控制块索引的 TCP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

slot slot-number: 显示指定成员设备的 TCP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 TCP 连接详细信息。

【使用指导】

display tcp verbose 命令用来显示 TCP 连接的详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号、以及 TCP 连接的源 IP 地址及端口号、目的 IP 地址及端口号、状态等信息。

【举例】

显示 TCP 连接详细信息。

```
<Sysname> display tcp verbose
```

```
TCP inpcb number: 1(tcpcb number: 1)
```

```
Connection info: src = 192.168.20.200:179 , dst = 192.168.20.14:4181
Location: slot 6
NSR standby: N/A
Creator: bgpd[199]
State: ISCONNECTED
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 65700 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat /state): 0 / 65700 / 512 / N/A
Type: 1
Protocol: 6
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Connection state: ESTABLISHED
TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
NSR state: READY(M)
Send VRF: 0x0
Receive VRF: 0x0
```

表1-7 display tcp verbose 命令显示信息描述表

字段	描述
TCP inpcb number	TCP类型internet协议控制块个数
tcpcb number	TCP控制块个数（处于TIME_WAIT状态的TCP则没有此计数）
Connection info	连接信息，分别为源IP地址及端口号、目的IP地址及端口号
Location	socket所在位置，在非集中式设备上执行本命令时，才显示此字段
NSR standby	NSR备所在IRF中的成员编号和槽位号，如果不存在NSR备，则显示“N/A”
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，包括： • NOFDREF：用户已经关闭 • ISCONNECTED：连接已经建立 • ISCONNECTING：正在建立连接 • ISDISCONNECTING：正在断开连接 • ASYNC：异步方式 • ISDISCONNECTED：连接已经断开 • PROTOREF：协议强关联 • N/A：不处于上述状态
Options	socket的选项，包括： • SO_DEBUG：记录套接字的调试信息 • SO_ACCEPTCONN：server 端监听连接请求 • SO_REUSEADDR：允许本地地址重复使用 • SO_KEEPALIVE：协议需要查询空闲的连接 • SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况 • SO_BROADCAST：套接字支持广播报文 • SO_LINGER：套接字关闭但仍发送剩余数据 • SO_OOBINLINE：带外数据采用内联方式存储 • SO_REUSEPORT：允许本地端口重复使用 • SO_TIMESTAMP：入报文记录时间戳，只对非连接的协议有效，时间精确到毫秒 • SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建SIGPIPE • SO_TIMESTAMPNS：和时间戳选项功能类似，时间可以精确到纳秒 • SO_KEEPAIVETIME：设置空闲探测时间 • N/A：未设置选项
Error	影响socket连接的错误码

字段	描述
Receiving buffer(cc/hiwat/lowat/drop/state)	接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、丢包数和状态，状态的取值包括： • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Sending buffer(cc/hiwat/lowat/state)	发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值包括： • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Type	使用的socket类型，类型的取值包括： • 1: SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 • 2: SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 • 3: SOCK_RAW，RAW 模式的通信方式 • N/A：不是上述类型
Protocol	使用socket的协议号
Inpcb flags	Internet协议控制块中的标记，标记的取值包括： • INP_RECVOPTS：接收传入的 IP 选项 • INP_RECVRETOPTS：接收回应的 IP 选项 • INP_RECVDSTADDR：接收目的 IP 地址 • INP_HDRINCL：用户提供整个 IP 头 • INP_REUSEADDR：重复使用地址 • INP_REUSEPORT：重复使用端口号 • INP_ANONPORT：用户未指定端口 • INP_RECVIF：接收报文时记录报文的入接口 • INP_RECVTTL：携带报文的 TTL，仅 UDP 和 RawIP 支持 • INP_DONTFRAG：设置不可分片标志 • INP_ROUTER_ALERT：接收携带路由器告警选项的报文，仅 RawIP 支持 • INP_PROTOCOL_PACKET：标识报文为协议报文 • INP_RCVVLANID：接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • INP_RCVMACADDR：接收报文的 MAC • INP_RECVTOS：携带报文的 TOS，仅 UDP 和 RawIP 支持 • INP_SYNCPCB：阻塞等待 inpcb 同步 • N/A：不是上述标记

字段	描述
Inpcb extflag	Internet协议控制块中的扩展标记，标记的取值包括： - INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 - INP_RCVPWID: 接收报文时记录报文的 PW ID - N/A: 不是上述标记
Inpcb vflag	Internet协议控制块中的IP版本标记，标记的取值包括： - INP_IPV4: 运用与 IPv4 通信 - INP_TIMEWAIT: 处于等待状态 - INP_ONESBCAST: 发送广播报文 - INP_DROPPED: 协议丢弃标志 - INP_SOCKREF: socket 强关联 - INP_DONTBLOCK: inpcb 同步时不能被阻塞 - N/A: 不是上述标记
TTL	Internet协议控制块中的生存周期，括号中为最小生存周期
Connection state	TCP连接状态，包括： - CLOSED: 服务器收到客户端的关闭连接请求回应后所处的状态 - LISTEN: 服务器在等待连接请求时所处的状态 - SYN_SENT: 客户端发出连接请求等待服务器回应时所处的状态 - SYN_RCVD: 服务器收到客户端连接请求时所处的状态 - ESTABLISHED: 服务器和客户端双方建立连接并能进行双向数据传递的状态 - CLOSE_WAIT: 服务器收到客户端关闭连接请求时所处的状态 - FIN_WAIT_1: 客户端发出关闭连接请求等待服务器回应时所处的状态 - CLOSING: 连接双方在向对端发出关闭连接请求后等待对端回应过程中收到对端发出的关闭连接请求时所处的状态 - LAST_ACK: 服务器向客户端发出关闭连接请求等待回应时所处的状态 - FIN_WAIT_2: 客户端收到服务器关闭连接回应后所处的状态 - TIME_WAIT: 客户端收到服务器的关闭连接请求后所处的状态
TCP options	TCP的选项类型，包括： - TF_MD5SIG: 使能密钥 - TF_PASSWORD: 已经设置密钥 - TF_NODELAY: 关闭延时 ACK - TF_NOOPT: TCP 不使用选项 - TF_NOPUSH: 对写入的最后部分不进行 PUSH 操作 - TF_BINDFOREIGNADDR: 绑定对端 IP 地址 - TF_NSR: 使能 TCP NSR - TF_REQ_SCALE: 使能窗口缩放因子选项 - TF_REQ_TSTMP: 使能时间戳选项 - TF_SACK_PERMIT: 使能选择性 ACK 选项

字段	描述
NSR state	TCP连接NSR状态，可能的状态如下： • CLOSED：关闭（初始）状态 • CLOSING：连接待关闭状态 • ENABLED：使能备份功能状态 • OPEN：连接开始同步状态 • PENDING：连接判定状态 • READY：连接备份就绪状态 • SMOOTH：连接平滑状态 角色：M表示主连接、S表示备份连接
Send VRF	发送实例
Receive VRF	接收实例

1.1.8 display udp

display udp 命令用来显示 UDP 连接摘要信息。

【命令】

display udp [slot *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number：显示指定成员设备的 UDP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 UDP 连接摘要信息。

【使用指导】

display udp 命令用来显示 UDP 连接摘要信息，包括本端 IP 地址及端口号、对端 IP 地址及端口号等信息。

【举例】

显示 UDP 连接摘要信息。

```
<Sysname> display udp
Local Addr:port      Foreign Addr:port    Slot  PCB
0.0.0.0:69           0.0.0.0:0            1     0x0000000000000003
192.168.20.200:1024  192.168.20.14:69    5     0x0000000000000002
```

表1-8 display udp 命令显示信息描述表

字段	描述
Local Addr:port	本端IP地址及端口号
Foreign Addr:port	对端IP地址及端口号
PCB	协议控制块索引

1.1.9 display udp statistics

display udp statistics 命令用来显示 UDP 流量统计信息。

【命令】

display udp statistics [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备的 UDP 流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 UDP 流量统计信息。

【使用指导】

display udp statistics 命令用来显示 UDP 流量统计信息，包括接收和发送的各类 UDP 报文信息。

【举例】

显示 UDP 流量统计信息。

```
<Sysname> display udp statistics
```

```
Received packets:
```

```
Total: 240
```

```
checksum error: 0, no checksum: 0
```

```
shorter than header: 0, data length larger than packet: 0
```

```
no socket on port(unicast): 0
```

```
no socket on port(broadcast/multicast): 240
```

```
not delivered, input socket full: 0
```

```
Sent packets:
```

```
Total: 0
```

表1-9 display udp statistics 命令显示信息描述表

字段		描述
Received packets:	Total	接收的UDP报文总数
	checksum error	校验和出错的报文数
	no checksum	没有校验和的报文数
	shorter than header	报文长度比报文头部短的报文数
	data length larger than packet	报文数据长度超过报文长度的报文数
	no socket on port(unicast)	端口上无socket的单播报文数
	no socket on port(broadcast/multicast)	端口上无socket的广播和组播报文数
	not delivered, input socket full	因为socket缓冲区已满而未向上层传送的报文数
Sent packets:	Total	发送的UDP报文总数

【相关命令】

- **reset udp statistics**

1.1.10 display udp verbose

display udp verbose 命令用来显示 UDP 连接详细信息。

【命令】

display udp verbose [slot slot-number [pcb pcb-index]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

pcb pcb-index: 显示指定协议控制块索引的 UDP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

slot slot-number: 显示指定成员设备的 UDP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 UDP 连接详细信息。

【使用指导】

display udp verbose 命令用来显示 UDP 连接的详细信息，包括 socket 的创建者、状态、选项、类型、使用的协议号、以及 UDP 连接的源 IP 地址及端口号、目的 IP 地址及端口号等信息。

【举例】

```
# 显示 UDP 连接详细信息。
<Sysname> display udp verbose
Total UDP socket number: 1

Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
Location: slot 6
Creator: sock_test_mips[250]
State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 2
Protocol: 17
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV4
TTL: 255(minimum TTL: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

表1-10 display udp verbose 命令显示信息描述表

字段	描述
Total UDP socket number	UDP socket总数
Connection info	连接信息，分别为源IP地址及端口号、目的IP地址及端口号
Location	socket所在位置，在非集中式设备上执行本命令时，才显示此字段
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，可能的状态如下： • NOFDREF：用户已经关闭 • ISCONNECTED：连接已经建立 • ISCONNECTING：正在建立连接 • ISDISCONNECTING：正在断开连接 • ASYNC：异步方式 • ISDISCONNECTED：连接已经断开 • PROTOREF：协议强关联 • N/A：不处于上述状态

字段	描述
Options	socket的选项，有以下几种： - SO_DEBUG：记录套接字的调试信息 - SO_ACCEPTCONN：server 端监听连接请求 - SO_REUSEADDR：允许本地地址重复使用 - SO_KEEPALIVE：协议需要查询空闲的连接 - SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况 - SO_BROADCAST：套接字支持广播报文 - SO_LINGER：套接字关闭但仍发送剩余数据 - SO_OOBINLINE：带外数据采用内联方式存储 - SO_REUSEPORT：允许本地端口重复使用 - SO_TIMESTAMP：入报文记录时间戳，只对非连接的协议有效，时间精确到毫秒 - SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建SIGPIPE - SO_TIMESTAMPNS：和时戳选项功能类似，时间可以精确到纳秒 - N/A：未设置选项
Error	影响socket连接的错误码
Receiving buffer(cc/hiwat/lowat/drop/state)	接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、丢包数和状态，状态的取值有： - CANTSENDMORE：不能发送数据到对端 - CANTRCVMORE：不能从对端接收数据 - RCVATMARK：接收标记 - N/A：不处于上述状态
Sending buffer(cc/hiwat/lowat/state)	发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态，状态的取值有： - CANTSENDMORE：不能发送数据到对端 - CANTRCVMORE：不能从对端接收数据 - RCVATMARK：接收标记 - N/A：不处于上述状态
Type	使用的socket类型，类型的取值有： 1: SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 2: SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 3: SOCK_RAW，RAW 模式的通信方式 - N/A：不是上述类型
Protocol	使用socket的协议号
Connection info	连接信息，分别为源IP地址及端口号、目的IP地址及端口号
Connection info	连接信息，分别为源IP地址及端口号、目的IP地址及端口号

字段	描述
Inpcb flags	Internet协议控制块中的标记，标记的取值有： • INP_RECVOPTS: 接收传入的 IP 选项 • INP_RECVRETOPTS: 接收回应的 IP 选项 • INP_RECVDSTADDR: 接收目的 IP 地址 • INP_HDRINCL: 用户提供整个 IP 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_RECVIF: 接收报文时记录报文的入接口 • INP_RECVTTL: 携带报文的 TTL，仅 UDP 和 RawIP 支持 • INP_DONTFRAG: 设置不可分片标志 • INP_ROUTER_ALERT: 接收携带路由器告警选项的报文，仅 RawIP 支持 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • INP_RCVMACADDR: 接收报文的 MAC • INP_RECVTOS: 携带报文的 TOS，仅 UDP 和 RawIP 支持 • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb extflag	Internet协议控制块中的扩展标记，标记的取值有： • INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 • INP_RCVPWID: 接收报文时记录报文的 PW ID • N/A: 不是上述标记
Inpcb vflag	Internet协议控制块中的IP版本标记，标记的取值有： • INP_IPV4: 运用与 IPv4 通信 • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
TTL	Internet协议控制块中的生存周期，括号中为最小生存周期
Send VRF	发送实例
Receive VRF	接收实例

1.1.11 ip forward-broadcast

ip forward-broadcast 命令用来配置允许接口接收和转发直连网段的定向广播报文。

undo ip forward-broadcast 命令用来禁止接口接收和转发直连网段的定向广播报文。

【命令】

```
ip forward-broadcast
undo ip forward-broadcast
```

【缺省情况】

设备禁止转发直连网段的定向广播报文；设备允许接收直连网段的定向广播报文。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

定向广播报文是指发送给特定网络的广播报文。该报文的 **目的 IP 地址** 中网络号码字段为特定网络的网络号，主机号码字段为全 1。

接口接收和转发直连网段的定向广播报文包括以下几种情况：

- 在接收定向广播报文的情况下，如果在接口上配置了此命令，设备允许接收此接口直连网段的定向广播报文。
- 在转发定向广播报文的情况下，如果在接口上配置了此命令，设备从其他接口接收到目的地为此接口直连网段的定向广播报文时，会从此接口转发此类报文。

在上述情况下，用户可以通过命令配置接口允许接收和转发直连网段的定向广播报文。

【举例】

配置允许接口 GigabitEthernet1/0/1 接收和转发直连网段的定向广播报文。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip forward-broadcast
```

1.1.12 ip icmp error-interval

ip icmp error-interval 用来配置发送 ICMP 差错报文对应的令牌刷新周期和令牌桶容量。

undo ip icmp error-interval 用来恢复缺省情况

【命令】

```
ip icmp error-interval interval [ bucketsize ]
undo ip icmp error-interval
```

【缺省情况】

令牌刷新周期为 100 毫秒，令牌桶容量为 10。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval: 令牌刷新周期, 取值范围 0~2147483647, 单位为毫秒。取值为 0 时, 表示不限制 ICMP 差错报文的发送。

bucketsize: 令牌桶中容纳的令牌数, 取值范围 1~200。

【使用指导】

如果网络中短时间内发送的 ICMP 差错报文过多, 将可能导致网络拥塞。为了避免这种情况, 用户可以控制设备在指定时间内发送 ICMP 差错报文的最大数目, 目前采用令牌桶算法来实现。

用户可以设置令牌桶的容量, 即令牌桶中可以同时容纳的令牌数; 同时可以设置令牌桶的刷新周期, 即每隔多长时间发放一个令牌到令牌桶中, 直到令牌桶中的令牌数达到配置的容量。一个令牌表示允许发送一个 ICMP 差错报文, 每当发送一个 ICMP 差错报文, 则令牌桶中减少一个令牌。如果连续发送的 ICMP 差错报文超过了令牌桶的容量, 则后续的 ICMP 差错报文将不能被发送出去, 直到按照所设置的刷新频率将新的令牌放入令牌桶中。

【举例】

配置设备发送 ICMP 差错报文对应的令牌刷新周期为 200 毫秒, 令牌桶容量为 40。

```
<Sysname> system-view  
[Sysname] ip icmp error-interval 200 40
```

1.1.13 ip icmp source

ip icmp source 命令用来指定 ICMP 报文源地址。

undo ip icmp source 命令用来删除指定的 ICMP 报文源地址。

【命令】

```
ip icmp source [ vpn-instance vpn-instance-name ] ip-address  
undo ip icmp source [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未指定 ICMP 报文源地址。设备使用出接口 IP 地址作为 ICMP 报文源地址。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

vpn-instance vpn-instance-name: 指定地址所在的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。指定的 VPN 实例必须已经存在。如果未指定本参数, 则表示公网内的 IP 地址。

ip-address: 表示设备发送 ICMP 报文时指定的源地址。

【使用指导】

在网络中 IP 地址配置较多的情况下，收到 ICMP 报文时，用户很难根据报文的源 IP 地址判断报文来自哪台设备。为了简化这一判断过程，可以配置 ICMP 报文指定源地址功能。用户配置特定地址（如环回口地址）为 ICMP 报文的源地址，可以简化判断。

设备发送 ICMP 差错报文（TTL 超时、端口不可达和参数错误等）和 ping echo request 报文时，都可以通过上述命令指定报文的源地址。

【举例】

配置设备发送 ICMP 报文时指定的源地址为 1.1.1.1。

```
<Sysname> system-view  
[Sysname] ip icmp source 1.1.1.1
```

1.1.14 ip mtu

ip mtu 命令用来配置接口上发送 IPv4 报文的 MTU。

undo ip mtu 命令用来恢复缺省情况。

【命令】

```
ip mtu mtu-size  
undo ip mtu
```

【缺省情况】

未配置接口上发送 IPv4 报文的 MTU。

【视图】

接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

mtu-size: MTU 的大小，单位为字节，取值范围为 128～1560。

【使用指导】

当设备使用某个接口发送报文时，发现报文长度大于该接口的发送 IPv4 报文的 MTU 值，则进行下列处理：

- 如果报文不允许分片，则将报文丢弃；
- 如果报文允许分片，则将报文进行分片转发。

为了减轻转发设备在传输过程中的分片和重组数据包的压力，更高效的利用网络资源，请根据实际组网环境设置合适的接口发送 IPv4 报文的 MTU 值，以减少分片的发生。

如果当前接口同时支持 **mtu** 和 **ip mtu** 命令，则设备会以 **ip mtu** 命令配置的接口发送 IPv4 报文的 MTU 值对报文进行分片，不会再按照 **mtu** 命令配置的 MTU 值对报文进行分片。

【举例】

```
# 配置 GigabitEthernet1/0/1 接口上发送 IPv4 报文的 MTU 值为 1280 字节。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip mtu 1280
```

1.1.15 ip reassemble local enable

ip reassemble local enable 命令用来开启 IP 分片报文本地重组功能。

undo ip reassemble local enable 命令用来关闭 IP 分片报文本地重组功能。

【命令】

```
ip reassemble local enable
undo ip reassemble local enable
```

【缺省情况】

IP 分片报文本地重组功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

多台设备组成的 IRF 环境下，当某成员设备收到目的为本 IRF 设备的 IP 分片报文时，需要把分片报文送到主设备进行重组，这样会导致报文重组性能较低的问题。当开启 IP 分片报文本地重组功能后，分片报文会在该成员设备上直接进行报文重组，这样就能提高分片报文的重组性能。开启 IP 分片报文本地重组功能后，如果分片报文是从设备上不同的成员设备进入的，会导致 IP 分片报文本地无法重组成功。

【举例】

```
# 开启 IP 分片报文本地重组功能。
<Sysname> system-view
[Sysname] ip reassemble local enable
```

1.1.16 ip redirects enable

ip redirects enable 命令用来开启设备的 ICMP 重定向报文的发送功能。

undo ip redirects enable 命令用来关闭设备的 ICMP 重定向报文的发送功能。

【命令】

```
ip redirects enable
undo ip redirects enable
```

【缺省情况】

ICMP 重定向报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

ICMP 重定向报文发送功能可以简化主机的管理，使具有很少选路信息的主机逐渐建立较完善的路由表，从而找到最佳路由。

主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时，缺省网关会向源主机发送 ICMP 重定向报文，通知主机重新选择正确的下一跳进行后续报文的发送。

满足下列条件时，设备会发送 ICMP 重定向报文：

- 接收和转发数据报文的接口是同一接口；
- 被选择的路由本身没有被 ICMP 重定向报文创建或修改过；
- 被选择的路由不是设备的默认路由；
- 数据报文中没有源路由选项。

【举例】

开启设备的 ICMP 重定向报文发送功能。

```
<Sysname> system-view
```

```
[Sysname] ip redirects enable
```

1.1.17 ip ttl-expires enable

ip ttl-expires enable 命令用来开启设备的 ICMP 超时报文的发送功能。

undo ip ttl-expires enable 命令用来关闭设备的 ICMP 超时报文的发送功能。

【命令】

ip ttl-expires enable

undo ip ttl-expires enable

【缺省情况】

ICMP 超时报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

ICMP 超时报文发送功能是在设备收到 IP 数据报文后，如果发生超时差错，则将报文丢弃并给源端发送 ICMP 超时差错报文。

设备在满足下列条件时会发送 ICMP 超时报文：

- 设备收到 IP 数据报文后，如果报文的目的地不是本地且报文的 TTL 字段是 1，则发送“TTL 超时” ICMP 差错报文；
- 设备收到目的地址为本地的 IP 数据报文的第一个分片后，启动定时器，如果所有分片报文到达之前定时器超时，则会发送“重组超时” ICMP 差错报文。

需要注意的是，关闭 ICMP 超时报文发送功能后，设备不会再发送“TTL 超时” ICMP 差错报文，但“重组超时” ICMP 差错报文仍会正常发送。

【举例】

开启设备的 ICMP 超时报文发送功能。

```
<Sysname> system-view
[Sysname] ip ttl-expires enable
```

1.1.18 ip unreachable enable

ip unreachable enable 命令用来开启设备的 ICMP 目的不可达报文的发送功能。

undo ip unreachable enable 命令用来关闭设备的 ICMP 目的不可达报文的发送功能。

【命令】

```
ip unreachable enable
undo ip unreachable enable
```

【缺省情况】

ICMP 目的不可达报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

ICMP 目的不可达报文发送功能是在设备收到 IP 数据报文后，如果发生目的不可达的差错，则将报文丢弃并给源端发送 ICMP 目的不可达差错报文。

设备在满足下列条件时会发送目的不可达报文：

- 设备在转发报文时，如果在路由表中未找到对应的转发路由，且路由表中没有缺省路由，则给源端发送“网络不可达” ICMP 差错报文；
- 设备收到目的地址为本地的数据报文时，如果设备不支持数据报文采用的传输层协议，则给源端发送“协议不可达” ICMP 差错报文；
- 设备收到目的地址为本地、传输层协议为 UDP 的数据报文时，如果报文的端口号与正在使用的进程不匹配，则给源端发送“端口不可达” ICMP 差错报文；
- 源端如果采用“严格的源路由选择”发送报文，当中间设备发现源路由所指定的下一个设备不在其直接连接的网络上，则给源端发送“源站路由失败”的 ICMP 差错报文；
- 设备在转发报文时，如果转发接口的 MTU 小于报文的长度，但报文被设置了不可分片，则给源端发送“需要进行分片但设置了不分片比特” ICMP 差错报文。

【举例】

```
# 开启设备的 ICMP 目的不可达报文发送功能。
<Sysname> system-view
[Sysname] ip unreachable enable
```

1.1.19 reset ip statistics

reset ip statistics 命令用来清除 IP 报文统计信息。

【命令】

```
reset ip statistics [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

slot slot-number: 清除指定成员设备的 IP 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除所有成员设备上的 IP 报文统计信息。

【使用指导】

在某些情况下，需要统计一定时间内接口的 IP 报文统计信息，这时必须在统计开始前清除原有的统计信息，重新进行统计。

【举例】

```
# 清除 IP 报文统计信息。
<Sysname> reset ip statistics
```

【相关命令】

- **display ip interface**（三层技术-IP 业务命令参考/IP 地址）
- **display ip statistics**

1.1.20 reset tcp statistics

reset tcp statistics 命令用来清除 TCP 连接的流量统计信息。

【命令】

```
reset tcp statistics
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 清除 TCP 连接的流量统计信息。  
<Sysname> reset tcp statistics
```

【相关命令】

- **display tcp statistics**

1.1.21 reset udp statistics

reset udp statistics 命令用来清除 UDP 流量统计信息。

【命令】

```
reset udp statistics
```

【视图】

用户视图

【缺省用户角色】

```
network-admin  
context-admin
```

【举例】

```
# 清除 UDP 流量统计信息。  
<Sysname> reset udp statistics
```

【相关命令】

- **display udp statistics**

1.1.22 tcp mss

tcp mss 命令用来配置接口的 TCP 最大报文段长度。

undo tcp mss 命令用来恢复缺省情况。

【命令】

```
tcp mss value  
undo tcp mss
```

【缺省情况】

未配置接口的 TCP 最大报文段长度。

【视图】

接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

value: TCP 最大报文段长度，取值范围为 128～（接口的最大 MTU 值－40），单位为字节。

【使用指导】

TCP 最大报文段长度（Max Segment Size, MSS）表示 TCP 连接的对端发往本端的最大 TCP 报文段的长度，目前作为 TCP 连接建立时的一个选项来协商：当一个 TCP 连接建立时，连接的双方要将 MSS 作为 TCP 报文的一个选项通告给对端，对端会记录下这个 MSS 值，后续在发送 TCP 报文时，会限制 TCP 报文的大小不超过该 MSS 值。当对端发送的 TCP 报文的长度小于本端的 TCP 最大报文段长度时，TCP 报文不需要分段；否则，对端需要对 TCP 报文按照最大报文段长度进行分段处理后再发给本端。

该配置仅对新建的 TCP 连接生效，对于配置前已建立的 TCP 连接不生效。

该配置仅对 IP 报文生效。

【举例】

配置接口 GigabitEthernet1/0/1 上 TCP 最大报文段长度为 300 字节。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] tcp mss 300
```

1.1.23 tcp path-mtu-discovery

tcp path-mtu-discovery 命令用来开启 TCP 连接的 Path MTU 探测功能。

undo tcp path-mtu-discovery 命令用来关闭 TCP 连接的 Path MTU 探测功能。

【命令】

```
tcp path-mtu-discovery [ aging age-time | no-aging ]
undo tcp path-mtu-discovery
```

【缺省情况】

TCP 连接的 Path MTU 探测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

aging *age-time*: Path MTU 的老化时间，*age-time* 的取值范围为 10～30，单位为分钟，缺省值为 10。

no-aging: Path MTU 不老化。

【使用指导】

开启 TCP 连接的 Path MTU 探测功能后，新建的 TCP 连接均会携带 Path MTU 探测属性，可以通过探测机制确定 Path MTU，按照数据路径上的最小 MTU 组织 TCP 分段长度，最大限度利用网络资源，避免 IP 分片的发生。

关闭 TCP 连接的 Path MTU 探测功能后，系统将停止所有正在运行的 Path MTU 定时器，此后创建的 TCP 连接均无 Path MTU 探测功能，但是对于此前已经建立的 TCP 连接，其 Path MTU 探测功能不会被关闭。

【举例】

开启 TCP 连接的 Path MTU 探测功能，Path MTU 的老化时间为 20 分钟。

```
<Sysname> system-view
```

```
[Sysname] tcp path-mtu-discovery aging 20
```

1.1.24 tcp syn-cookie enable

tcp syn-cookie enable 命令用来开启 SYN Cookie 功能，防止设备受到 SYN Flood 攻击。

undo tcp syn-cookie enable 命令用来关闭 SYN Cookie 功能。

【命令】

tcp syn-cookie enable

undo tcp syn-cookie enable

【缺省情况】

SYN Cookie 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

一般情况下，TCP 连接的建立需要经过三次握手，一些恶意的攻击者利用 TCP 连接的建立过程进行 SYN Flood 攻击：攻击者向服务器发送大量请求建立 TCP 连接的 SYN 报文，而不回应服务器的 SYN ACK 报文，导致服务器上建立了大量的 TCP 半连接。从而，达到耗费服务器资源，使服务器无法处理正常业务的目的。

SYN Cookie 功能用来防止 SYN Flood 攻击。当服务器收到 TCP 连接请求时，不建立 TCP 半连接，而直接向发起者回复 SYN ACK 报文。服务器接收到发起者回应的 ACK 报文后，才建立连接。通过这种方式，可以避免在服务器上建立大量的 TCP 半连接，防止服务器受到 SYN Flood 攻击。

【举例】

开启 SYN Cookie 功能。

```
<Sysname> system-view
```

```
[Sysname] tcp syn-cookie enable
```

1.1.25 tcp timer fin-timeout

tcp timer fin-timeout 命令用来配置 TCP 的 finwait 定时器超时时间。

undo tcp timer fin-timeout 命令用来恢复缺省情况。

【命令】

```
tcp timer fin-timeout time-value  
undo tcp timer fin-timeout
```

【缺省情况】

TCP finwait 定时器的超时时间为 675 秒。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

time-value: TCP finwait 定时器的超时时间，取值范围为 76～3600，单位为秒。

【使用指导】

当 TCP 的连接状态为 FIN_WAIT_2 时，启动 finwait 定时器，如果在定时器超时前未收到报文，则 TCP 连接终止；如果收到 FIN 报文，则 TCP 连接状态变为 TIME_WAIT 状态；如果收到非 FIN 报文，则从收到的最后一个非 FIN 报文开始重新计时，在超时后中止连接。

【举例】

```
# 配置 TCP finwait 定时器的超时时间为 800 秒。  
<Sysname> system-view  
[Sysname] tcp timer fin-timeout 800
```

1.1.26 tcp timer syn-timeout

tcp timer syn-timeout 命令用来配置 TCP 的 synwait 定时器超时时间。

undo tcp timer syn-timeout 命令用来恢复缺省情况。

【命令】

```
tcp timer syn-timeout time-value  
undo tcp timer syn-timeout
```

【缺省情况】

TCP synwait 定时器的超时时间为 75 秒。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

time-value: TCP synwait 定时器的超时时间，取值范围为 2～600，单位为秒。

【使用指导】

当发送 SYN 报文时，TCP 启动 synwait 定时器和重传 SYN 报文定时器，当 synwait 定时器超时且 SYN 报文重传未达到最大次数时，如果设备未收到回应报文，则 TCP 连接建立不成功；当 synwait 定时器未超时但是 SYN 报文重传达到最大次数时，如果设备未收到回应报文，则 TCP 连接建立不成功。

【举例】

```
# 配置 TCP synwait 定时器的超时时间为 80 秒。  
<Sysname> system-view  
[Sysname] tcp timer syn-timeout 80
```

1.1.27 tcp timestamps enable

tcp timestamps enable 命令用来配置发送 TCP 报文时添加 TCP 时间戳选项信息。

undo tcp timestamps enable 命令用来配置发送 TCP 报文时不添加 TCP 时间戳选项信息。

【命令】

```
tcp timestamps enable  
undo tcp timestamps enable
```

【缺省情况】

发送 TCP 报文时会添加 TCP 时间戳选项信息。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

TCP 报文中携带 TCP 时间戳选项信息时，建立 TCP 连接的两台设备通过 TCP 报文中的时间戳字段就可计算出 RTT（Round Trip Time，往返时间）值。在某些组网中，由于安全隐患，需要防止 TCP 连接上的中间设备获取到 TCP 时间戳信息，可以在建立 TCP 连接任意一端关闭发送 TCP 报文时添加时间戳选项信息功能。

开启或关闭本功能仅对新建的 TCP 连接生效，对于配置前已建立的 TCP 连接不生效。

【举例】

```
# 配置发送 TCP 报文时不添加 TCP 时间戳选项信息。  
<Sysname> system-view  
[Sysname] undo tcp timestamps enable
```

1.1.28 tcp window

tcp window 命令用来设置 TCP 连接的收发缓冲区大小。

undo tcp window 命令用来恢复缺省情况。

【命令】

```
tcp window window-size  
undo tcp window
```

【缺省情况】

TCP 连接的收发缓冲区大小为 63KB。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

window-size: TCP 连接的收发缓冲区大小，取值范围为 1~64，单位为 KB（千字节）。

【举例】

```
# 设置 TCP 连接的收发缓冲区大小为 3KB。  
<Sysname> system-view  
[Sysname] tcp window 3
```

目 录

1 IPv6 基础	1-1
1.1 IPv6 基础配置命令	1-1
1.1.1 display ipv6 fib	1-1
1.1.2 display ipv6 icmp statistics	1-2
1.1.3 display ipv6 interface	1-4
1.1.4 display ipv6 interface prefix	1-9
1.1.5 display ipv6 neighbors	1-11
1.1.6 display ipv6 neighbors count	1-12
1.1.7 display ipv6 neighbors vpn-instance	1-13
1.1.8 display ipv6 pathmtu	1-14
1.1.9 display ipv6 prefix	1-16
1.1.10 display ipv6 rawip	1-17
1.1.11 display ipv6 rawip verbose	1-17
1.1.12 display ipv6 statistics	1-21
1.1.13 display ipv6 tcp	1-25
1.1.14 display ipv6 tcp verbose	1-27
1.1.15 display ipv6 udp	1-32
1.1.16 display ipv6 udp verbose	1-33
1.1.17 ipv6 address	1-38
1.1.18 ipv6 address anycast	1-39
1.1.19 ipv6 address auto	1-40
1.1.20 ipv6 address auto link-local	1-40
1.1.21 ipv6 address eui-64	1-41
1.1.22 ipv6 address link-local	1-42
1.1.23 ipv6 address <i>prefix-number</i>	1-43
1.1.24 ipv6 extension-header drop enable	1-44
1.1.25 ipv6 hop-limit	1-44
1.1.26 ipv6 hoplimit-expires enable	1-45
1.1.27 ipv6 icmpv6 error-interval	1-46
1.1.28 ipv6 icmpv6 multicast-echo-reply enable	1-47
1.1.29 ipv6 icmpv6 source	1-47
1.1.30 ipv6 mtu	1-48
1.1.31 ipv6 nd dad attempts	1-49

1.1.32 ipv6 nd ns retrans-timer	1-50
1.1.33 ipv6 nd nud reachable-time	1-51
1.1.34 ipv6 nd ra halt	1-51
1.1.35 ipv6 nd ra hop-limit unspecified	1-52
1.1.36 ipv6 nd ra interval	1-53
1.1.37 ipv6 nd ra no-advlinkmtu	1-53
1.1.38 ipv6 nd ra prefix	1-54
1.1.39 ipv6 nd ra prefix default	1-55
1.1.40 ipv6 nd ra router-lifetime	1-56
1.1.41 ipv6 nd router-preference	1-57
1.1.42 ipv6 neighbor	1-58
1.1.43 ipv6 neighbor link-local minimize	1-59
1.1.44 ipv6 neighbor stale-aging	1-60
1.1.45 ipv6 neighbors max-learning-num	1-61
1.1.46 ipv6 pathmtu	1-61
1.1.47 ipv6 pathmtu age	1-62
1.1.48 ipv6 prefer temporary-address	1-63
1.1.49 ipv6 prefix	1-64
1.1.50 ipv6 reassemble local enable	1-64
1.1.51 ipv6 redirects enable	1-65
1.1.52 ipv6 temporary-address	1-66
1.1.53 ipv6 unreachable enable	1-67
1.1.54 local-proxy-nd enable	1-68
1.1.55 proxy-nd enable	1-68
1.1.56 reset ipv6 neighbors	1-69
1.1.57 reset ipv6 pathmtu	1-70
1.1.58 reset ipv6 statistics	1-71

1 IPv6 基础

1.1 IPv6基础配置命令

1.1.1 display ipv6 fib

display ipv6 fib 命令用来显示 IPv6 FIB 信息。

【命令】

```
display ipv6 fib [ vpn-instance vpn-instance-name ] [ ipv6-address  
[ prefix-length ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance *vpn-instance-name*：显示指定 VPN 实例的 IPv6 FIB 信息。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果不指定 **vpn-instance** 参数，则显示公网的 IPv6 FIB 信息。

ipv6-address：显示目的地址为指定 IPv6 地址的 IPv6 FIB 信息。如果不指定目的地址，则显示所有的 IPv6 FIB 信息。

prefix-length：目的地址的前缀长度，取值范围为 0~128。如果不指定前缀长度，则显示与指定目的 IPv6 地址最长匹配的 IPv6 FIB 信息

【举例】

显示公网所有的 IPv6 FIB 信息。

```
<Sysname> display ipv6 fib
```

```
Destination count: 1 FIB entry count: 1
```

```
Flag:
```

```
U:Useable  G:Gateway  H:Host  B:Blackhole  D:Dynamic  S:Static  
R:Relay    F:FRR
```

```
Destination: ::1
```

```
Prefix length: 128
```

```
Nexthop    : ::1
```

```
Flags: UH
```

```
Time stamp : 0x1
```

```
Label: Null
```

```
Interface  : InLoop0
```

```
Token: Invalid
```


表1-1 display ipv6 fib 命令显示信息描述表

字段	描述
Destination count	目的地址的个数
FIB entry count	IPv6 FIB表项数目
Destination	转发的目的地址
Prefix length	转发的目的地址的前缀长度
Nexthop	向目的地址转发报文的下一跳地址
Flags	路由的标志： • U：表示路由可用 • G：表示网关路由 • H：表示主机路由 • B：表示黑洞路由 • D：表示动态路由 • S：表示静态路由 • R：表示迭代路由 • F：表示快速重路由
Time stamp	IPv6 FIB表项的生成时间
Label	（暂不支持）MPLS内层标签，公网的IPv6 FIB信息中显示为Null
Interface	转发报文的出接口
Token	LSP索引号

1.1.2 display ipv6 icmp statistics

display ipv6 icmp statistics 命令用来显示 ICMPv6 流量统计信息。

【命令】

display ipv6 icmp statistics [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin

context-operator

【参数】

slot slot-number: 显示指定成员设备的 ICMPv6 流量统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 ICMPv6 流量统计信息。

【举例】

显示 ICMPv6 流量统计信息。

```
<Sysname> display ipv6 icmp statistics
  Input: bad code          0          too short          0
         checksum error    0          bad length         0
         path MTU changed  0          destination unreachable 0
         too big           0          parameter problem    0
         echo request      0          echo reply           0
         neighbor solicit  0          neighbor advertisement 0
         router solicit    0          router advertisement 0
         redirect          0          router renumbering   0
output: parameter problem  0          echo request         0
         echo reply        0          unreachable no route  0
         unreachable admin 0          unreachable beyond scope 0
         unreachable address 0        unreachable no port   0
         too big           0          time exceed transit   0
         time exceed reassembly 0      redirect             0
         ratelimited       0          other errors         0
```

表1-2 display ipv6 icmp statistics 命令显示信息描述表

字段	描述
bad code	接收的代码错误的报文数
too short	接收的长度过小的报文数
checksum error	接收的校验和错误的报文数
bad length	接收的长度错误的报文数
path MTU changed	接收的路径MTU改变报文数
destination unreachable	接收的目标不可达报文数
too big	接收/发送的数据包超长报文数
parameter problem	接收/发送的参数错误报文数
echo request	接收/发送的回显请求报文数
echo reply	接收/发送的回应响应报文数
neighbor solicit	接收的邻居请求报文数
neighbor advertisement	接收的邻居通告报文数

字段	描述
router solicit	接收的路由请求报文数
router advertisement	接收的路由通告报文数
redirect	接收/发送的重定向报文数
router renumbering	接收的路由器重计数报文数
unreachable no route	发送的路由不可达报文数
unreachable admin	发送的与目标的通信被管理策略禁止的报文数
unreachable beyondscope	发送的源地址超出范围的报文数
unreachable address	发送的地址不可达报文数
unreachable no port	发送的端口不可达报文数
time exceed transit	发送的传输超时报文数
time exceed reassembly	发送的重组超时报文数
ratelimited	因速率超过限制而未发送的报文数
other errors	发送的其他的错误报文数

1.1.3 display ipv6 interface

display ipv6 interface 命令用来显示接口的 IPv6 信息。

【命令】

display ipv6 interface [*interface-type* [*interface-number*]] [**brief**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-type: 显示指定类型接口的 IPv6 信息。

interface-number: 显示指定接口的 IPv6 信息。

brief: 显示接口摘要信息，包括接口的物理状态、链路层协议状态以及 IPv6 地址信息。如果不指定该参数，则显示接口的详细信息，包括接口上和 IPv6 相关的配置以及运行信息，以及 IPv6 报文统计信息。

【使用指导】

如果只指定接口类型，不指定接口编号，则显示所有指定类型接口的 IPv6 信息；

如果同时指定接口类型和接口编号，则显示指定接口的 IPv6 信息。

【举例】

查看接口 GigabitEthernet1/0/1 上的 IPv6 信息。

```
<Sysname> display ipv6 interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: UP
Line protocol current state: UP
IPv6 is enabled, link-local address is FE80::200:1FF:FE04:5D00 [TENTATIVE]
Global unicast address(es):
  10::1234:56FF:FE65:4322, subnet is 10::/64 [TENTATIVE] [AUTOCFG]
    [valid lifetime 4641s/preferred lifetime 4637s]
  20::1234:56ff:fe65:4322, subnet is 20::/64 [TENTATIVE] [EUI-64]
  30::1, subnet is 30::/64 [TENTATIVE] [ANYCAST]
  50::3, subnet is 50::/64 [TENTATIVE]
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:1
  FF02::1:FF04:5D00
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
InReceives:                0
InTooShorts:                0
InTruncatedPkts:           0
InHopLimitExceeds:         0
InBadHeaders:               0
InBadOptions:               0
ReasmReqds:                 0
ReasmOKs:                   0
InFragDrops:                0
InFragTimeouts:             0
OutFragFails:               0
InUnknownProtos:           0
InDelivers:                 0
OutRequests:                0
OutForwDatagrams:           0
InNoRoutes:                 0
InTooBigErrors:             0
```

```

OutFragOKs:          0
OutFragCreates:      0
InMcastPkts:         0
InMcastNotMembers:   0
OutMcastPkts:        0
InAddrErrors:        0
InDiscards:          0
OutDiscards:         0

```

表1-3 display ipv6 interface 命令显示信息描述表

字段	描述
GigabitEthernet1/0/1 current state	接口的物理状态，可能的状态及含义如下： - Administratively DOWN：表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 - DOWN：该接口的管理状态为开启，但物理状态为关闭（可能因为没有连接好或者线路故障） - UP：该接口的管理状态和物理状态均为开启
Line protocol current state	接口的链路层协议状态，可能的状态及含义如下： - DOWN：该接口的协议状态为关闭 - UP：该接口的协议状态为开启
IPv6 is enabled	接口的IPv6转发功能状态（为某接口配置任一IPv6地址后系统将自动使能该接口的IPv6功能，此例中处于使能状态）
link-local address	接口上配置的链路本地地址

字段	描述
Global unicast address(es)	接口上配置的全球单播地址 可能的IPv6地址状态及含义如下： ● TENTATIVE: 该状态为地址初始化状态，此时该地址可能正在进行 DAD 检测或准备进行 DAD 检测，处于该状态的地址不能作为报文的源地址或者目的地址 ● DUPLICATE: 该状态表明地址 DAD 检测已经结束，由于该地址在链路上不唯一，因此不能使用 ● PREFERRED: 该状态表明地址处于首选生命期以内。该状态的地址可以作为报文的源地址或者目的地址。为该状态时，不显示地址的状态标识 ● DEPRECATED: 该状态表明地址超过首选生命期，但是在有效生命期以内。该状态地址有效，但不应作为新建连接报文的源地址，目的地址是该地址的报文还可以被正常处理 如果地址来源不为手工配置的全球单播地址，则会标记地址来源。可能的地址来源及含义如下： ● AUTOCFG: 表示无状态自动配置的全球单播地址 ● EUI-64: 表示手工配置的 EUI-64 格式全球单播地址 ● RANDOM: 表示自动生成的临时地址 如果地址为手工配置的任播地址，则会标记ANYCAST
valid lifetime	接口上无状态自动配置的全球单播地址的有效生命期
preferred lifetime	接口上无状态自动配置的全球单播地址的首选生命期
Joined group address(es)	接口加入的组播组地址
MTU	接口的最大传输单元
ND DAD is enabled, number of DAD attempts	重复地址检测功能是否使能（该例中使能） 若处于使能状态则同时显示重复地址检测时发送邻居请求消息的次数（可通过ipv6 nd dad attempts命令进行配置） 若处于关闭状态则显示“ND DAD is disabled”（可通过配置重复地址检测时发送邻居请求消息的次数为0关闭该功能）
ND reachable time	保持邻居可达的时间
ND retransmit interval	邻居请求消息重传时间间隔
Hosts use stateless autoconfig for addresses	主机采用无状态自动配置的方式获取IPv6地址
InReceives	接口接收到的所有IPv6报文，包括各种错误的报文

字段	描述
InTooShorts	接口接收到的太短的IPv6报文，譬如报文长度不足40字节
InTruncatedPkts	接口接收到的IPv6报文，其实际长度小于报文内容中所指出的报文长度
InHopLimitExceeds	接口接收到的IPv6报文，其跳数超出限制
InBadHeaders	接口接收到的IPv6报文，其基本报文头错误
InBadOptions	接口接收到的IPv6报文，其扩展报文头错误
ReasmReqds	接口接收到的IPv6分片报文
ReasmOKs	接口接收到的IPv6分片，被组装好的报文，这里指的不是分片个数，是组装好的报文数
InFragDrops	接口接收到的IPv6分片报文，该分片报文由于错误被丢弃
InFragTimeouts	接口接收到的IPv6分片报文，该分片停留在系统缓冲中时间超过指定时间，被丢弃
OutFragFails	出接口上分片失败的报文
InUnknownProtos	接口接收到的IPv6报文，其协议类型不能被识别或不能被支持
InDelivers	接口接收到的IPv6报文，该报文被上送到IPv6的用户协议处（如ICMPv6、TCP、UDP等）
OutRequests	IPv6本地出报文，即各IPv6的用户协议层要求IPv6发送出去的报文
OutForwDatagrams	出接口上被转发的报文
InNoRoutes	接口接收到的IPv6报文，找不到匹配的路由被丢弃
InTooBigErrors	接口接收到的IPv6报文，转发时，由于超过链路MTU被丢弃
OutFragOKs	出接口上分片成功的报文
OutFragCreates	出接口上成功分片后的分片报文，指分片数
InMcastPkts	接口接收到的IPv6组播报文
InMcastNotMembers	接口接收到的IPv6组播报文，但该接口却没有加入对应组播组，报文被丢弃
OutMcastPkts	接口发送的IPv6组播报文
InAddrErrors	接口接收到的IPv6报文，其目的地址不合法，报文被丢弃
InDiscards	接口接收到的IPv6报文，由于资源问题被丢弃的报文，而不是由于报文内容等被丢弃的报文

字段	描述
OutDiscards	接口需要发送的报文，由于资源问题被丢弃的报文，而不是由于报文内容等被丢弃的报文

查看所有接口的 IPv6 摘要信息。

```
<Sysname> display ipv6 interface brief
```

```
*down: administratively down
```

```
(s): spoofing
```

Interface	Physical	Protocol	IPv6 Address
GigabitEthernet1/0/1	up	up	2001::1
GigabitEthernet1/0/2	up	up	Unassigned
GigabitEthernet1/0/3	down	down	Unassigned

表1-4 display ipv6 interface brief 命令显示信息描述表

字段	描述
*down: administratively down	接口处于管理down状态，即采用 shutdown 命令关闭了该接口
(s): spoofing	接口的欺骗属性，即接口的链路协议状态显示是 up 的，但实际可能没有对应的链路，或者所对应的链路不是永久存在而是按需建立的
Interface	接口的名称
Physical	接口的物理状态，可能的状态及含义如下： • *down：表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭 • down：该接口的管理状态为开启，但物理状态为关闭（可能因为没有连接好或者线路故障） • up：该接口的管理状态和物理状态均为开启
Protocol	接口的链路层协议状态，可能的状态及含义如下： • down：该接口的协议状态为关闭 • up：该接口的协议状态为开启
IPv6 Address	接口的IPv6地址，接口上有全球单播地址时，显示地址最小的全球单播地址，没有全球单播地址则显示链路本地地址，没有链路本地地址则显示“Unassigned”

1.1.4 display ipv6 interface prefix

display ipv6 interface prefix 命令用来显示接口的 IPv6 前缀信息。

【命令】

```
display ipv6 interface interface-type interface-number prefix
```


【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-type interface-number: 指定接口类型和接口编号。

【举例】

```
# 查看接口 GigabitEthernet1/0/1 的 IPv6 前缀信息。
<Sysname> display ipv6 interface gigabitethernet 1/0/1 prefix
Prefix: 1001::/65                                Origin: ADDRESS
Age:      -                                       Flag:    AL
Lifetime(Valid/Preferred): 2592000/604800

Prefix: 2001::/64                                Origin: STATIC
Age:      -                                       Flag:    L
Lifetime(Valid/Preferred): 3000/2000

Prefix: 3001::/64                                Origin: RA
Age:      600                                    Flag:    A
Lifetime(Valid/Preferred): -
```

表1-5 display ipv6 interface prefix 命令显示信息描述表

字段	描述
Prefix	IPv6地址前缀
Origin	前缀来源，包括： • STATIC: 手工配置前缀（命令 ipv6 nd ra prefix） • RA: 使能无状态地址自动配置功能后根据 RA 报文生成的前缀 • ADDRESS: 由手工配置的地址产生的前缀
Age	老化时间（单位为秒），“-”表示前缀不会老化
Flag	前缀随RA报文公告时携带的标记，“-”表示没有标记 • L: 表示前缀是直接可达的。没有此标记，则表示前缀不是该链路上直连可达的 • A: 表示前缀用于无状态自动配置。没有此标记，则表示前缀不用于无状态自动配置

字段	描述
Lifetime	前缀随RA报文公告时携带的生存时间（单位为秒），“-”表示前缀不需要公告 - Valid: 前缀的有效生命期 - Preferred: 前缀的首选生命期

【相关命令】

- ipv6 nd ra prefix**

1.1.5 display ipv6 neighbors

display ipv6 neighbors 命令用来显示邻居信息。

【命令】

```
display ipv6 neighbors { { ipv6-address | all | dynamic | static } [ slot
slot-number ] | interface interface-type interface-number | vlan vlan-id }
[ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ipv6-address: 显示指定 IPv6 地址的邻居信息。

all: 显示所有邻居的信息，包括公网和所有私网下动态获取的和静态配置的邻居信息。

dynamic: 显示所有动态获取的邻居信息。

static: 显示所有静态配置的邻居信息。

slot slot-number: 显示指定成员设备的邻居信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的邻居信息。

interface interface-type interface-number: 显示指定接口的邻居信息。*interface-type interface-number* 为接口类型和接口编号。

vlan vlan-id: 显示指定 VLAN 的邻居信息。*vlan-id* 表示 VLAN ID，取值范围为 1~4094。

verbose: 显示邻居的详细信息。

【举例】

查看所有的邻居信息。

```
<Sysname> display ipv6 neighbors all
```

```
Type: S-Static   D-Dynamic   O-Openflow   R-Rule   IS-Invalid-static
IPv6 address           MAC address   VID   Interface   State T   Age
```

```
FE80::200:5EFF:FE32:B800    0000-5e32-b800  N/A  GE1/0/1          REACH D  10
# 查看所有邻居的详细信息。
<Sysname> display ipv6 neighbors all verbose
IPv6 address  : FE80::200:5EFF:FE32:B800
MAC address   : 0000-5e32-b800          Type  : Static
State        : INCMP                   Aging  : --
Interface     : --                     VID    : 1
VPN instance  : --
Nickname      : 0x0
```

表1-6 display ipv6 neighbors 命令显示信息描述表

字段	描述
IPv6 Address	邻居的IPv6地址
Link Layer	邻居的链路层地址（MAC地址）
VID	与邻居相连的接口所属的VLAN
Interface	与邻居相连的接口
State	邻居的状态，包括： • INCMP：正在解析地址，邻居的链路层地址尚未确定 • REACH：邻居可达 • STALE：未确定邻居是否可达，设备不会再验证邻居的可达性，除非有数据发送给该邻居 • DELAY：未确定邻居是否可达，延迟一段时间发送邻居请求报文 • PROBE：未确定邻居是否可达，发送邻居请求报文来验证邻居的可达性
Type	邻居信息的类型，S表示静态配置，D表示动态获取，O表示从OpenFlow特性获取，特性获取，I表示无效
Age	静态项显示“-”，动态项显示上次可达以来经过的时间（单位为秒），如果始终不可达则显示“#”（只适用于动态项）
Vpn-instance	VPN实例名称，[No Vrf]表示没有配置相应表项的VPN实例
Nickname	（暂不支持）邻居表项的Nickname（长度为4的十六进制数字，例如0x012a）

【相关命令】

- **ipv6 neighbor**
- **reset ipv6 neighbors**

1.1.6 display ipv6 neighbors count

display ipv6 neighbors count 命令用来显示邻居表项的个数。

【命令】

```
display ipv6 neighbors { { all | dynamic | static } [ slot slot-number ] |  
interface interface-type interface-number | vlan vlan-id } count
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

all: 显示所有邻居表项的总个数，包括动态获取的和静态配置的邻居信息。

dynamic: 显示所有动态获取的邻居表项的总个数。

static: 显示所有静态配置的邻居表项的总个数。

slot *slot-number*: 显示指定成员设备的邻居表项的总个数。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的邻居表项的总个数。

interface *interface-type interface-number*: 显示指定接口的邻居表项的总个数。*interface-type interface-number* 为接口类型和接口编号。

vlan *vlan-id*: 显示指定 VLAN 的邻居表项的总个数。*vlan-id* 表示 VLAN ID，取值范围为 1～4094。

【举例】

显示动态获取的邻居表项的总个数。

```
<Sysname> display ipv6 neighbors dynamic count  
Total number of dynamic entries: 2
```

1.1.7 display ipv6 neighbors vpn-instance

display ipv6 neighbors vpn-instance 命令用来显示指定 VPN 实例的邻居信息。

【命令】

```
display ipv6 neighbors vpn-instance vpn-instance-name [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance-name:指定 ND 表项所属的 VPN 实例。**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。该 VPN 实例必须已经存在。

count: 显示指定 VPN 实例中的邻居表项的总数。

【举例】

```
# 显示名为 vpn1 的 VPN 实例中的邻居信息。
<Sysname> display ipv6 neighbors vpn-instance vpn1
Type: S-Static   D-Dynamic   O-Openflow   R-Rule   IS-Invalid-static
IPv6 address      MAC address      VID Interface   State T Age
FE80::200:5EFF:FE32:B800  0000-5e32-b800  N/A  GE1/0/1       REACH IS -
```

表1-7 display ipv6 neighbors vpn-instance 命令显示信息描述表

字段	描述
IPv6 address	邻居的IPv6地址
Link-layer	邻居的链路层地址（MAC地址）
VID	与邻居相连的接口所属的VLAN
Interface	与邻居相连的接口
State	邻居的状态，包括： • INCMP：正在解析地址，邻居的链路层地址尚未确定； • REACH：邻居可达； • STALE：未确定邻居是否可达，设备不会再验证邻居的可达性，除非有数据发送给该邻居； • DELAY：未确定邻居是否可达，延迟一段时间发送邻居请求报文； • PROBE：未确定邻居是否可达，发送邻居请求报文来验证邻居的可达性。
T	邻居信息的类型，S表示静态配置，D表示动态获取，I表示无效
Age	静态项显示“-”，动态项显示上次可达以来经过的时间（单位为秒），如果始终不可达则显示“#”（只适用于动态项）

1.1.8 display ipv6 pathmtu

display ipv6 pathmtu 命令用来显示 IPv6 的 PMTU 信息。

【命令】

```
display ipv6 pathmtu [ vpn-instance vpn-instance-name ] { ipv6-address |
{ all | dynamic | static } [ count ] }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance *vpn-instance-name*：显示指定 VPN 实例的 IPv6 PMTU 信息。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的 IPv6 PMTU 信息。

ipv6-address：显示到达指定 IPv6 地址的 PMTU 信息。

all：显示所有公网的 PMTU 信息。

dynamic：显示所有动态 PMTU 信息。

static：显示所有静态 PMTU 信息。

count：显示 PMTU 表项数目。

【举例】

显示所有 PMTU 信息。

```
<Sysname> display ipv6 pathmtu all
```

IPv6 destination address	PathMTU	Age	Type
1:2::3:2	1800	-	Static
1:2::4:2	1400	10	Dynamic
1:2::5:2	1280	10	Dynamic

显示所有 PMTU 表项数目。

```
<Sysname> display ipv6 pathmtu all count
```

Total number of entries: 3

表1-8 display ipv6 pathmtu 命令显示信息描述表

字段	描述
IPv6 destination address	IPv6目的地址
PathMTU	对应IPv6地址的PMTU值
Age	PMTU老化时间（单位为分钟），如果是静态表项则显示为“-”
Type	PMTU类型，Dynamic表示动态协商的PMTU，Static表示静态配置的PMTU
Total number of entries	PMTU表项数目

【相关命令】

- **ipv6 pathmtu**
- **reset ipv6 pathmtu**

1.1.9 display ipv6 prefix

display ipv6 prefix 命令用来显示静态 IPv6 前缀信息。

【命令】

display ipv6 prefix [*prefix-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

prefix-number：显示指定的 IPv6 前缀信息。*prefix-number* 表示 IPv6 前缀编号，取值范围为 1~1024。如果不指定本参数，则显示所有 IPv6 前缀的信息。

【使用指导】

静态 IPv6 前缀指的是通过 **ipv6 prefix** 命令创建的前缀。

【举例】

显示所有 IPv6 前缀的信息。
<Sysname> display ipv6 prefix
Number Prefix Type
1 1::/16 Static
显示 IPv6 前缀编号 1 的信息。
<Sysname> display ipv6 prefix 1
Number: 1
Type : Static
Prefix: ABCD:77D8::/32
Preferred lifetime 90 sec, valid lifetime 120 sec

表1-9 display ipv6 prefix 命令显示信息描述表

字段	描述
Number	前缀编号
Type	前缀的类型，取值为Static，表示静态IPv6前缀
Prefix	前缀及其长度。“Not-available”表示目前尚未获取到前缀
Preferred lifetime 90 sec	首选生命期，单位为秒。如果是静态IPv6前缀，则不显示该字段
valid lifetime 120 sec	有效生命期，单位为秒。如果是静态IPv6前缀，则不显示该字段

【相关命令】

- `ipv6 prefix`

1.1.10 `display ipv6 rawip`

`display ipv6 rawip` 命令用来显示 IPv6 RawIP 连接摘要信息。

【命令】

`display ipv6 rawip [ slot slot-number ]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备的 IPv6 RawIP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 RawIP 连接摘要信息。

【举例】

```
# 显示 IPv6 RawIP 连接摘要信息。
<Sysname> display ipv6 rawip
Local Addr      Foreign Addr      Protocol Slot  PCB
2001:2002:2003:2 3001:3002:3003:3 58      1    0x0000000000000009
004:2005:2006:20 004:3005:3006:30
07:2008         07:3008
2002::100       2002::138        58      2    0x0000000000000008
::              ::               58      5    0x0000000000000002
```

表1-10 `display ipv6 rawip` 命令显示信息描述表

字段	描述
Local Addr	本端IPv6地址
Foreign Addr	对端IPv6地址
Protocol	使用IPv6 RawIP socket的协议号
PCB	协议控制块索引

1.1.11 `display ipv6 rawip verbose`

`display ipv6 rawip verbose` 命令用来显示 IPv6 RawIP 连接详细信息。

【命令】

display ipv6 rawip verbose [slot slot-number [pcb pcb-index]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备的 IPv6 RawIP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 RawIP 连接详细信息。
pcb pcb-index: 显示指定协议控制块索引的 IPv6 RawIP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

【举例】

```
# 显示 Ipv6 RawIP 连接详细信息。
<Sysname> display ipv6 rawip verbose
Total RawIP socket number: 1

Connection info: src = ::, dst = ::
Location: slot: 2
Creator: ping ipv6[320]
State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 3
Protocol: 58
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

表1-11 display ipv6 rawip verbose 命令显示信息描述表

字段	描述
Total RawIP socket number	IPv6 RawIP socket总数
Connection info	连接信息，分别为源IPv6地址、目的IPv6地址

Location	socket所在位置
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，可能的状态如下： • NOFDREF：用户已经关闭 • ISCONNECTED：连接已经建立 • ISCONNECTING：正在建立连接 • ISDISCONNECTING：正在断开连接 • ASYNC：异步方式 • ISDISCONNECTED：连接已经断开 • PROTOREF：协议强关联 • N/A：不处于上述状态
Options	socket的选项，有以下几种： • SO_DEBUG：记录套接字的调试信息 • SO_ACCEPTCONN：server 端监听连接请求 • SO_REUSEADDR：允许本地地址重复使用 • SO_KEEPALIVE：协议需要查询空闲的连接 • SO_DONTROUTE：设置不查路由表，由于目的地址是直连网络的情况 • SO_BROADCAST：套接字支持广播报文 • SO_LINGER：套接字关闭但仍发送剩余数据 • SO_OOBINLINE：带外数据采用内联方式存储 • SO_REUSEPORT：允许本地端口重复使用 • SO_TIMESTAMP：记录入报文时间戳，只对非连接的协议有效，时间精确到毫秒 • SO_NOSIGPIPE：socket 不能发送数据导致返回失败时不创建 SIGPIPE • SO_TIMESTAMPNS：和时戳选项功能类似，时间可以精确到纳秒 • SO_KEEPALIVETIME：设置空闲探测时间，TCP 支持此选项 • SO_FILTER：设置报文过滤条件，OSI Socket 和 RawIP 支持此选项 • SO_USCBINDEX：获取接收报文里的 User Profile 索引 • N/A：没有设置选项
Error	影响socket连接的错误码
Receiving buffer (cc/hiwat/lowat/drop/state)	接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、丢包数和状态 状态的取值有：

	• CANTSENDMORE: 不能发送数据到对端 • CANTRCVMORE: 不能从对端接收数据 • RCVATMARK: 接收标记 • N/A: 不处于上述状态
Sending buffer (cc/hiwat/lowat/state)	发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间和状态状态的取值有： • CANTSENDMORE: 不能发送数据到对端 • CANTRCVMORE: 不能从对端接收数据 • RCVATMARK: 接收标记 • N/A: 不处于上述状态
Type	使用的socket类型，类型的取值有： • 1: SOCK_STREAM, 流模式，提供可靠的字节流。TCP 协议使用此类型 • 2: SOCK_DGRAM, 数据报模式的通信。UDP 协议使用此类型 • 3: SOCK_RAW, RAW 模式的通信方式 • N/A: 不是上述类型
Protocol	使用IPv6 RawIP socket的协议号，58表示ICMP协议
Inpcb flags	Internet协议控制块中的标记，标记的取值有： • INP_RECVOPTS: 接收传入的 IPv6 选项 • INP_RECVRETOPTS: 接收回应的 IPv6 选项 • INP_RECVDSTADDR: 接收目的 IPv6 地址 • INP_HDRINCL: 用户提供整个 IPv6 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • IN6P_IPV6_V6ONLY: 仅支持 IPv6 协议栈 • IN6P_PKTINFO: 接收报文的源地址和入接口 • IN6P_HOPLIMIT: 接收报文 hoplimit • IN6P_HOPOPTS: 接收报文的逐跳扩展头信息 • IN6P_DSTOPTS: 接收报文的扩展头信息 • IN6P_RTHDR: 接收报文的的路由扩展头信息 • IN6P_RTHDRDSTOPTS: 接收报文的的路由头前的目的扩展头信息

	• IN6P_TCLASS: 接收报文的优先级信息 • IN6P_AUTOFLOWLABEL: 使用随机流标签 • IN6P_RFC2292: 使用 RFC2292 API • IN6P_MTU: 感知路径 MTU 的变化, TCP 不支持 • INP_RCVMACADDR: 接收报文的 MAC • INP_USEICMPSRC: 使用配置的 ICMPv6 地址作为源地址 • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb extflag	Internet协议控制块中的扩展标记, 标记的取值有: • INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 • INP_RCVPWID: 接收报文时记录报文的 PW ID • N/A: 不是上述标记
Inpcb vflag	Internet协议控制块中的IP版本标记, 标记的取值有: • INP_IPV4: 运用与 IPv4 通信 • INP_IPV6: 运用与 IPv6 通信 • INP_IPV6PROTO: 运用 IPv6 协议创建的 inpcb • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
Hop limit(minimum hop limit)	Internet协议控制块中的跳数限制, 括号中为最小跳数限制
Send VRF	发送实例
Receive VRF	接收实例

1.1.12 display ipv6 statistics

display ipv6 statistics 命令用来显示 IPv6 报文及 ICMPv6 报文的统计信息。

【命令】

display ipv6 statistics [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备的 IPv6 报文及 ICMPv6 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 报文及 ICMPv6 报文统计信息。

【举例】

查看 IPv6 报文及 ICMPv6 报文的统计信息。

<Sysname> display ipv6 statistics

IPv6 statistics:

Sent packets:

Total: 0

Sent locally: 0 Forwarded: 0

Raw packets: 0 Discarded: 0

Fragments: 0 Fragments failed: 0

Routing failed: 0

Received packets:

Total: 0

Received locally: 0 Hop limit exceeded: 0

Fragments: 0 Reassembled: 0

Reassembly failures: 0 Reassembly timeout: 0

Format errors: 0 Option errors: 0

Protocol errors: 0

ICMPv6 statistics:

Sent packets:

Total: 0

Unreachable: 0 Too big: 0

Hop limit exceeded: 0 Reassembly timeouts: 0

Parameter problems: 0

Echo requests: 0 Echo replies: 0

Neighbor solicits: 0 Neighbor adverts: 0

Router solicits: 0 Router adverts: 0

Redirects: 0 Router renumbering: 0

Send failed:

Rate limitation: 0 Other errors: 0

Received packets:

Total: 0

```

Checksum errors:      0          Too short:      0
Bad codes:           0
Unreachable:         0          Too big:      0
Hop limit exceeded:  0          Reassembly timeouts: 0
Parameter problems: 0          Unknown error types: 0
Echo requests:       0          Echo replies:  0
Neighbor solicits:   0          Neighbor adverts: 0
Router solicits:     0          Router adverts: 0
Redirects:           0          Router renumbering: 0
Unknown info types:  0
Deliver failed:
Bad length:          0

```

表1-12 display ipv6 statistics 命令显示信息描述表

字段	描述
IPv6 statistics:	IPv6报文统计信息
Sent packets:	发送IPv6报文的统计信息，包括：
Total:	本地发送报文和转发报文的总数
Sent locally:	本地发送报文数
Forwarded:	转发报文数
Raw packets:	使用 raw socket 发送的报文数
Discarded:	丢弃报文数
Fragments:	发送分片报文数
Fragments failed:	分片报文发送失败的个数
Routing failed:	路由失败报文数
Received packets:	接收IPv6报文的统计信息，包括：
Total:	接收报文总数
Received locally:	本地接收报文数，即目的地是本机的报文数
Hop limit exceeded:	超出跳数范围的报文数
Fragments:	接收的分片报文数
Reassembled:	重组报文数
Reassembly failures:	重组失败的报文数
Reassembly timeout:	重组超时的报文数
Format errors:	格式错误的报文数
Option errors:	选项错误的报文数
Protocol errors:	协议错误的报文数
ICMPv6 statistics:	ICMPv6报文的统计信息

字段	描述
Sent packets:	发送ICMPv6报文的统计信息，包括：
Total:	• 发送报文总数
Unreached:	• 目的不可达报文数
Too big:	• 报文太长的报文数
Hop limit exceeded:	• 超出跳数限制的报文数
Reassembly timeouts:	• 分片重组超时报文数
Parameter problems:	• 参数错误报文数
Echo requests:	• 回应请求报文数
Echo replies:	• 回应响应报文数
Neighbor solicits:	• 邻居请求报文数
Neighbor adverts:	• 邻居通告报文数
Router solicits:	• 路由器请求报文数
Router adverts:	• 路由器通告报文数
Redirects:	• 重定向报文数
Router renumbering	• 路由器重编号报文数
Sent failed:	• 本机发送失败的报文数
Rate limitation:	• 因速率超过限制而未发送的报文数
Other errors:	• 其他错误的报文数

字段	描述
Received packets:	接收ICMPv6报文的统计信息，包括：
Total:	接收报文总数
Checksum errors:	校验和错误的报文数
Too short:	报文太短的报文数
Bad codes:	错误代码的报文数
Unreachable:	不可达报文数
Too big:	报文太长的报文数
Hop limit exceeded:	超出跳数限制的报文数
Reassembly timeouts:	分片重组超时的报文数
Parameter problems:	参数错误报文数
Unknown error types:	未知错误报文数
Echo requests:	回应请求报文数
Echo replies:	回应响应报文数
Neighbor solicits:	邻居请求报文数
Neighbor adverts:	邻居通告报文数
Router solicits:	路由器请求报文数
Router adverts:	路由器通告报文数
Redirects:	重定向报文数
Router renumbering:	路由器重编号报文数
Unknown info types:	未知信息报文数
Deliver failed:	上送本机失败的报文数
Bad length:	长度错误的报文数

【相关命令】

- reset ipv6 statistics**

1.1.13 display ipv6 tcp

display ipv6 tcp 命令用来显示 IPv6 TCP 连接摘要信息。

【命令】

display ipv6 tcp [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number：显示指定成员设备的 IPv6 TCP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 TCP 连接摘要信息。

【举例】

```
# 显示 IPv6 TCP 连接摘要信息。
<Sysname> display ipv6 tcp
*: TCP MD5 Connection
  LAddr->port      FAddr->port      State      Slot  PCB
*2001:2002:2003:2  3001:3002:3003:3 ESTABLISHED 1      0x0000000000000c387
004:2005:2006:20   004:3005:3006:30
07:2008->1200      07:3008->1200
2001::1->23         2001::5->1284    ESTABLISHED 2      0x0000000000000008
2003::1->25         2001::2->1283    LISTEN      3      0x0000000000000009
```

表1-13 display ipv6 tcp 命令显示信息描述表

字段	描述
*	如果某个连接前有此标识，则表示该TCP连接是采用MD5加密算法认证的连接
LAddr->port	本端IPv6地址及端口号
FAddr->port	对端IPv6地址及端口号
State	TCP连接状态，可能的状态如下： • CLOSED：服务器收到客户端的关闭连接请求回应后所处的状态 • LISTEN：服务器在等待连接请求时所处的状态 • SYN_SENT：客户端发出连接请求等待服务器回应时所处的状态 • SYN_RCVD：服务器收到客户端连接请求时所处的状态 • ESTABLISHED：服务器和客户端双方建立连接并能进行双向数据传递的状态 • CLOSE_WAIT：服务器收到客户端关闭连接请求时所处的状态 • FIN_WAIT_1：客户端发出关闭连接请求等待服务器回应时所处的状态 • CLOSING：连接双方在向对端发出关闭连接请求后等待对端回应过程中收到对端发出的关闭连接请求时所处的状态 • LAST_ACK：服务器向客户端发出关闭连接请求等待回应时所处的状态 • FIN_WAIT_2：客户端收到服务器关闭连接回应后所处的状态 • TIME_WAIT：客户端收到服务器的关闭连接请求后所处的状态

字段	描述
PCB	协议控制块索引

1.1.14 display ipv6 tcp verbose

display ipv6 tcp verbose 命令用来显示 IPv6 TCP 连接详细信息。

【命令】

display ipv6 tcp verbose [*slot slot-number* [*pcb pcb-index*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备的 IPv6 TCP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 TCP 连接详细信息。

pcb pcb-index: 显示指定协议控制块索引的 IPv6 TCP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

【举例】

显示 IPv6 TCP 连接详细信息。

```
<Sysname> display ipv6 tcp verbose
```

```
TCP inpcb number: 1(tcpcb number: 1)
```

```
Connection info: src = 2001::1->179 , dst = 2001::2->4181
Location: Slot: 6 Cpu: 0
NSR standby: N/A
Creator: bgpd[199]
State: ISCONNECTED
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/state): 0 / 65536 / 1 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 65536 / 512 / N/A
Type: 1
Protocol: 6
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
```

Connection state: ESTABLISHED
TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
NSR state: READY(M)
Send VRF: 0x0
Receive VRF: 0x0

表1-14 display ipv6 tcp verbose 命令显示信息描述表

字段	描述
TCP inpcb number	IPv6 TCP类型Internet协议控制块个数
Connection info	连接信息，分别为源IPv6地址及端口号、目的IPv6地址及端口号
Location	socket所在位置
tcpcb number	IPv6 TCP控制块个数（处于TIME_WAIT状态的TCP则不列入计数）
NSR standby::	NSR设备所在IRF中的成员编号和槽位号，如果不存在NSR设备，则显示“N/A”
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，可能的状态如下： • NOFDREF: 用户已经关闭 • ISCONNECTED: 连接已经建立 • ISCONNECTING: 正在建立连接 • ISDISCONNECTING: 正在断开连接 • ASYNC: 异步方式 • ISDISCONNECTED: 连接已经断开 • PROTOREF: 协议强关联 • N/A: 不处于上述状态

字段	描述
Options	socket的选项，有以下几种： • SO_DEBUG: 记录套接字的调试信息 • SO_ACCEPTCONN: server 端监听连接请求 • SO_REUSEADDR: 允许本地地址重复使用 • SO_KEEPALIVE: 协议需要查询空闲的连接 • SO_DONTROUTE: 设置不查路由表，由于目的地址是直连网络的情况 • SO_BROADCAST: 套接字支持广播报文 • SO_LINGER: 套接字关闭但仍发送剩余数据 • SO_OOBINLINE: 带外数据采用内联方式存储 • SO_REUSEPORT: 允许本地端口重复使用 • SO_NOSIGPIPE: socket 不能发送数据导致返回失败时不创建 SIGPIPE • SO_TIMESTAMPNS: 和时戳选项功能类似，时间可以精确到纳秒 • SO_KEEPALIVETIME: 设置空闲探测时间，TCP 支持此选项 • SO_FILTER: 设置报文过滤条件，OSI Socket 和 RawIP 支持此选项 • N/A: 没有设置选项
Error	影响socket连接的错误码
Receiving buffer(cc/hiwat/lowat/state)	接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、状态 状态的取值有： • CANTSENDMORE: 不能发送数据到对端 • CANTRCVMORE: 不能从对端接收数据 • RCVATMARK: 接收标记 • N/A: 不处于上述状态
Sending buffer(cc/hiwat/lowat/state)	发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、状态 状态的取值有： • CANTSENDMORE: 不能发送数据到对端 • CANTRCVMORE: 不能从对端接收数据 • RCVATMARK: 接收标记 • N/A: 不处于上述状态

字段	描述
Type	使用的socket类型，类型的取值有： 1: SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 2: SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 3: SOCK_RAW，RAW 模式的通信方式 - N/A: 不是上述类型
Protocol	使用TCP socket的协议号，6表示运用TCP协议
Inpcb flags	Internet协议控制块中的标记，标记的取值有： - INP_RECVOPTS: 接收传入的 IPv6 选项 - INP_RECVRETOPTS: 接收回应的 IPv6 选项 - INP_RECVDSTADDR: 接收目的 IPv6 地址 - INP_HDRINCL: 用户提供整个 IPv6 头 - INP_REUSEADDR: 重复使用地址 - INP_REUSEPORT: 重复使用端口号 - INP_ANONPORT: 用户未指定端口 - INP_PROTOCOL_PACKET: 标识报文为协议报文 - INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 - IN6P_IPV6_V6ONLY: 仅支持 IPv6 协议栈 - IN6P_PKTINFO: 接收报文的源地址和入接口 - IN6P_HOPLIMIT: 接收报文 hoplimit - IN6P_HOPOPTS: 接收报文的逐跳扩展头信息 - IN6P_DSTOPTS: 接收报文的目的扩展头信息 - IN6P_RTHDR: 接收报文的路由扩展头信息 - IN6P_RTHDRDSTOPTS: 接收报文的路由头前的目的扩展头信息 - IN6P_TCLASS: 接收报文的优先级信息 - IN6P_AUTOFLOWLABEL: 使用随机流标签 - IN6P_RFC2292: 使用 RFC2292 API - IN6P_MTU: 感知路径 MTU 的变化，TCP 不支持 - INP_RCVMACADDR: 接收报文的 MAC - INP_SYNCPCB: 阻塞等待 inpcb 同步 - N/A: 不是上述标记

字段	描述
Inpcb extflag	Internet协议控制块中的扩展标记，标记的取值有： • INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 • INP_RCVPWID: 接收报文时记录报文的 PW ID • INP_EXTDONTDROP: 接收报文时设置报文不要丢弃 • INP_EXLISTEN: 监听 socket • N/A: 不是上述标记
Inpcb vflag	Internet协议控制块中的IP版本标记： • INP_IPV4: 运用与 IPv4 通信 • INP_IPV6: 运用与 IPv6 通信 • INP_IPV6PROTO: 运用 IPv6 协议创建的 inpcb • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
Hop limit(minimum hop limit)	Internet协议控制块中的跳数限制，括号中为最小跳数限制
Connection state	TCP连接状态，可能的状态如下： • CLOSED: 服务器收到客户端的关闭连接请求回应后所处的状态 • LISTEN: 服务器在等待连接请求时所处的状态 • SYN_SENT: 客户端发出连接请求等待服务器回应时所处的状态 • SYN_RCVD: 服务器收到客户端连接请求时所处的状态 • ESTABLISHED: 服务器和客户端双方建立连接并能进行双向数据传递的状态 • CLOSE_WAIT: 服务器收到客户端关闭连接请求时所处的状态 • FIN_WAIT_1: 客户端发出关闭连接请求等待服务器回应时所处的状态 • CLOSING: 连接双方在向对端发出关闭连接请求后等待对端回应过程中收到对端发出的关闭连接请求时所处的状态 • LAST_ACK: 服务器向客户端发出关闭连接请求等待回应时所处的状态 • FIN_WAIT_2: 客户端收到服务器关闭连接回应后所处的状态 • TIME_WAIT: 客户端收到服务器的关闭连接请求后所处的状态

字段	描述
TCP options	TCP的选项类型，有以下几种： • TF_MD5SIG: 使能密钥 • TF_PASSWORD: 已经设置密钥 • TF_NODELAY: 关闭延时 ACK • TF_NOOPT: TCP 不使用选项 • TF_NOPUSH: 对写入的最后部分不进行 PUSH 操作 • TF_BINDFOREIGNADDR: 绑定对端 IP 地址 • TF_NSR: 使能 TCP NSR • TF_REQ_SCALE: 使能窗口缩放因子选项 • TF_REQ_TSTMP: 使能事件戳选项 • TF_SACK_PERMIT: 使能选择性 ACK 选项
NSR state	TCP连接NSR状态，可能的状态如下： • CLOSED: 关闭（初始）状态 • CLOSING: 连接待关闭状态 • ENABLED: 使能备份功能状态 • OPEN: 连接开始同步状态 • PENDING: 连接判定状态 • READY: 连接备份就绪状态 • SMOOTH: 连接平滑状态 角色：M表示主连接、S表示备份连接
Send VRF	发送实例
Receive VRF	接收实例

1.1.15 display ipv6 udp

display ipv6 udp 命令用来显示 IPv6 UDP 连接摘要信息。

【命令】

display ipv6 udp [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备的 IPv6 UDP 连接摘要信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 UDP 连接摘要信息。

【举例】

```
# 显示 IPv6 UDP 连接摘要信息。
<Sysname> display ipv6 udp
LAddr->port      FAddr->port      Slot  PCB
2001:2002:2003:2  3001:3002:3003:3  1      0x00000000000000c387
004:2005:2006:20  004:3005:3006:30
07:2008->1200     07:3008->1200
2001::1->23        2001::5->1284     2      0x0000000000000008
2003::1->25        2001::2->1283     3      0x0000000000000009
```

表1-15 display ipv6 udp 命令显示信息描述表

字段	描述
LAddr->port	本端IPv6地址及端口号
FAddr->port	对端IPv6地址及端口号
PCB	协议控制块索引

1.1.16 display ipv6 udp verbose

display ipv6 udp verbose 命令用来显示 IPv6 UDP 连接详细信息。

【命令】

```
display ipv6 udp verbose [ slot slot-number [ pcb pcb-index ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 显示指定成员设备的 IPv6 UDP 连接详细信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 UDP 连接详细信息。

pcb pcb-index: 显示指定协议控制块索引的 IPv6 UDP 连接详细信息。*pcb-index* 表示协议控制块索引，取值范围为 1~16。

【举例】

```
# 显示 IPv6 UDP 连接详细信息。
<Sysname> display ipv6 udp verbose
Total UDP socket number: 1

Connection info: src = ::->69, dst = ::->0
Location: slot: 2
Creator: sock_test_mips[250]
State: N/A
Options: N/A
Error: 0
Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
Type: 2
Protocol: 17
Inpcb flags: N/A
Inpcb extflag: N/A
Inpcb vflag: INP_IPV6
Hop limit: 255 (minimum hop limit: 0)
Send VRF: 0xffff
Receive VRF: 0xffff
```

表1-16 display ipv6 udp verbose 命令显示信息描述表

字段	描述
Total UDP socket number	IPv6 UDP socket总数
Connection info	连接信息，分别为源IPv6地址及端口号、目的IPv6地址及端口号
Location	socket所在位置
Creator	创建socket的任务名称，括号中为创建者的进程号
State	socket的状态，可能的状态如下： - NOFDREF：用户已经关闭 - ISCONNECTED：连接已经建立 - ISCONNECTING：正在建立连接 - ISDISCONNECTING：正在断开连接 - ASYNCR：异步方式 - ISDISCONNECTED：连接已经断开 - PROTODREF：协议强关联 - N/A：不处于上述状态

字段	描述
Options	socket的选项，有以下几种： • SO_DEBUG: 记录套接字的调试信息 • SO_ACCEPTCONN: server 端监听连接请求 • SO_REUSEADDR: 允许本地地址重复使用 • SO_KEEPALIVE: 协议需要查询空闲的连接 • SO_DONTROUTE: 设置不查路由表，由于目的地址是直连网络的情况 • SO_BROADCAST: 套接字支持广播报文 • SO_LINGER: 套接字关闭但仍发送剩余数据 • SO_OOBINLINE: 带外数据采用内联方式存储 • SO_REUSEPORT: 允许本地端口重复使用 • SO_TIMESTAMP: 入报文记录时间戳，只对非连接的协议有效，时间精确到毫秒 • SO_NOSIGPIPE: socket 不能发送数据导致返回失败时不创建SIGPIPE • SO_TIMESTAMPNS: 和时戳选项功能类似，时间可以精确到纳秒 • SO_KEEPALIVETIME: 设置空闲探测时间，TCP 支持此选项 • SO_FILTER: 设置报文过滤条件，OSI Socket 和 RawIP 支持此选项 • N/A: 没有设置选项
Error	影响socket连接的错误码
Receiving buffer(cc/hiwat/lowat/drop/state)	接收缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、丢包数和状态 状态的取值有： • CANTSENDMORE: 不能发送数据到对端 • CANTRCVMORE: 不能从对端接收数据 • RCVATMARK: 接收标记 • N/A: 不处于上述状态

字段	描述
Sending buffer(cc/hiwat/lowat/state)	发送缓冲区信息，括号中分别为：当前使用空间、最大空间、最小空间、状态 状态的取值有： • CANTSENDMORE：不能发送数据到对端 • CANTRCVMORE：不能从对端接收数据 • RCVATMARK：接收标记 • N/A：不处于上述状态
Type	使用的socket类型，类型的取值有： • 1: SOCK_STREAM，流模式，提供可靠的字节流。TCP 协议使用此类型 • 2: SOCK_DGRAM，数据报模式的通信。UDP 协议使用此类型 • 3: SOCK_RAW，RAW 模式的通信方式 • N/A：不是上述类型
Protocol	使用UDP socket的协议号，17表示运用UDP协议

字段	描述
Inpcb flags	Internet协议控制块中的标记，标记的取值有： • INP_RECVOPTS: 接收传入的 IPv6 选项 • INP_RECVRETOPTS: 接收回应的 IPv6 选项 • INP_RECVDSTADDR: 接收目的 IPv6 地址 • INP_HDRINCL: 用户提供整个 IPv6 头 • INP_REUSEADDR: 重复使用地址 • INP_REUSEPORT: 重复使用端口号 • INP_ANONPORT: 用户未指定端口 • INP_PROTOCOL_PACKET: 标识报文为协议报文 • INP_RCVVLANID: 接收报文的 VLAN ID，仅 UDP 和 RawIP 支持 • IN6P_IPV6_V6ONLY: 仅支持 IPv6 协议栈 • IN6P_PKTINFO: 接收报文的源地址和入接口 • IN6P_HOPLIMIT: 接收报文 hoplimit • IN6P_HOPOPTS: 接收报文的逐跳扩展头信息 • IN6P_DSTOPTS: 接收报文的目的扩展头信息 • IN6P_RTHDR: 接收报文的路由扩展头信息 • IN6P_RTHDRDSTOPTS: 接收报文的路由头前的目的扩展头信息 • IN6P_TCLASS: 接收报文的优先级信息 • IN6P_AUTOFLOWLABEL: 使用随机流标签 • IN6P_RFC2292: 使用 RFC2292 API • IN6P_MTU: 感知路径 MTU 的变化，TCP 不支持 • INP_RCVMACADDR: 接收报文的 MAC • INP_SYNCPCB: 阻塞等待 inpcb 同步 • N/A: 不是上述标记
Inpcb extflag	Internet协议控制块中的扩展标记，标记的取值有： • INP_EXTRCVPVCIDX: 接收报文时记录报文的 PVC 索引 • INP_RCVPWID: 接收报文时记录报文的 PW ID • N/A: 不是上述标记

字段	描述
Inpcb vflag	Internet协议控制块中的IP版本标记，标记的取值有： • INP_IPV4: 运用与 IPv4 通信 • INP_IPV6: 运用与 IPv6 通信 • INP_IPV6PROTO: 运用 IPv6 协议创建的 inpcb • INP_TIMEWAIT: 处于等待状态 • INP_ONESBCAST: 发送广播报文 • INP_DROPPED: 协议丢弃标志 • INP_SOCKREF: socket 强关联 • INP_DONTBLOCK: inpcb 同步时不能被阻塞 • N/A: 不是上述标记
Hop limit(minimum hop limit)	Internet协议控制块中的跳数限制，括号中为最小跳数限制
Send VRF	发送实例
Receive VRF	接收实例

1.1.17 ipv6 address

ipv6 address 命令用来手工配置接口的 IPv6 全球单播地址。

undo ipv6 address 命令用来删除接口的 IPv6 地址。

【命令】

```

ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
undo ipv6 address [ ipv6-address prefix-length | ipv6-address/prefix-length ]

```

【缺省情况】

接口上未配置 IPv6 全球单播地址。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address: IPv6 地址。

prefix-length: 前缀长度，取值范围为 1~128。

【使用指导】

IPv6 全球单播地址等同于 IPv4 公网地址，提供给网络服务提供商。这种类型的地址允许路由前缀的聚合，从而限制了全球路由表项的数量。

undo ipv6 address 命令不带参数则删除该接口的所有 IPv6 地址。

【举例】

指定 GigabitEthernet1/0/1 接口的 IPv6 全球单播地址为 2001::1，前缀长度为 64。

方法一：

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1/64
```

方法二：

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1 64
```

1.1.18 ipv6 address anycast

ipv6 address anycast 命令用来给接口配置 IPv6 任播地址。

undo ipv6 address anycast 命令用来删除接口上已配置的 IPv6 任播地址。

【命令】

```
ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
anycast
undo ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
anycast
```

【缺省情况】

接口上未配置 IPv6 任播地址。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address：指定 IPv6 任播地址。

prefix-length：前缀长度，取值范围为 1~128。

【举例】

指定 GigabitEthernet1/0/1 接口的 IPv6 任播地址为 2001::1，前缀长度为 64。

方法一：

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1/64 anycast
```

方法二：

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1 64 anycast
```

1.1.19 ipv6 address auto

ipv6 address auto 命令用来开启无状态地址自动配置功能，使接口通过无状态自动配置方式生成全球单播地址。

undo ipv6 address auto 命令用来关闭无状态地址自动配置功能。

【命令】

```
ipv6 address auto
```

```
undo ipv6 address auto
```

【缺省情况】

无状态地址自动配置功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

通过无状态自动配置方式生成全球单播地址时，会自动生成链路本地地址，生成的全球单播地址和链路本地地址可以通过执行 **undo ipv6 address auto** 命令或 **undo ipv6 address** 命令删除。

【举例】

配置接口 GigabitEthernet1/0/1 通过无状态自动配置方式生成全球单播地址。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 address auto
```

1.1.20 ipv6 address auto link-local

ipv6 address auto link-local 命令用来配置系统自动为接口生成链路本地地址。

undo ipv6 address auto link-local 命令用来恢复缺省情况。

【命令】

```
ipv6 address auto link-local
```

```
undo ipv6 address auto link-local
```

【缺省情况】

接口上没有链路本地地址。当接口配置了 IPv6 全球单播地址后，会自动生成链路本地地址。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

链路本地地址用于邻居发现协议和无状态自动配置中链路本地上节点之间的通信。使用链路本地地址作为源或目的地址的数据报文不会被转发到其他链路上。

接口配置了 IPv6 全球单播地址后，所自动生成的链路本地地址与采用 **ipv6 address auto link-local** 命令生成的链路本地地址相同。

undo ipv6 address auto link-local 命令只能删除使用 **ipv6 address auto link-local** 命令生成的链路本地地址。即如果此时接口已配置了 IPv6 全球单播地址，则接口仍有链路本地地址；如果此时接口未配置 IPv6 全球单播地址，则接口没有链路本地地址。

配置链路本地地址时，手工指定方式的优先级高于自动生成方式。即如果先采用自动生成方式，之后手工指定，则手工指定的地址会覆盖自动生成的地址；如果先手工指定，之后采用自动生成的方式，则自动配置不生效，接口的链路本地地址仍是手工指定的。此时，如果删除手工指定的地址，则自动生成的链路本地地址会生效。关于手工指定方式的介绍请参见命令 **ipv6 address link-local**。

【举例】

```
# 配置 GigabitEthernet1/0/1 接口自动生成链路本地地址。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address auto link-local
```

【相关命令】

- **ipv6 address link-local**

1.1.21 ipv6 address eui-64

ipv6 address eui-64 命令用来为接口配置 EUI-64 格式的 global 单播地址。

undo ipv6 address eui-64 命令用来删除接口上指定的 EUI-64 格式的 global 单播地址。

【命令】

```
ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length } eui-64
undo ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length } eui-64
```

【缺省情况】

接口上未配置 EUI-64 格式的 global 单播地址。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address prefix-length: IPv6 地址和前缀长度，共同指定采用 EUI-64 格式形成的 IPv6 地址的前缀。前缀长度 *prefix-length* 的取值范围为 1~64。IPv6 地址和前缀长度有如下两种输入方式：

- *ipv6-address/prefix-length*，例如 2001::1/64。
- *ipv6-address prefix-length*，例如 2001::1 64。

【使用指导】

EUI-64 格式的地址由指定的地址前缀和自动产生的接口标识符生成，最终生成的地址可以通过 **display ipv6 interface** 命令查看。

在配置 EUI-64 地址时前缀长度取值不能大于 64。

【举例】

配置 GigabitEthernet1/0/1 接口采用 EUI-64 格式形成 IPv6 地址，其地址前缀与 2001::1/64 的前缀相同，接口标识符由设备的 MAC 地址生成。

方法一：

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1/64 eui-64
```

方法二：

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001::1 64 eui-64
```

【相关命令】

- **display ipv6 interface**

1.1.22 ipv6 address link-local

ipv6 address link-local 命令用来手动指定接口的链路本地地址。

undo ipv6 address link-local 命令用来恢复缺省情况。

【命令】

```
ipv6 address ipv6-address link-local
undo ipv6 address ipv6-address link-local
```

【缺省情况】

未指定接口的链路本地地址。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address: IPv6 链路本地地址，地址前面 10 位必须为 111111010（二进制标识），即地址最前面的一组十六进制数为 FE80～FEBF。

【使用指导】

配置链路本地地址时，手工指定方式的优先级高于自动生成方式。即如果先采用自动生成方式，之后手工指定，则手工指定的地址会覆盖自动生成的地址；如果先手工指定，之后采用自动生成的方式，则自动配置不生效，接口的链路本地地址仍是手工指定的。此时，如果删除手工指定的地址，则自动生成的链路本地地址会生效。关于自动生成方式的介绍请参见命令 **ipv6 address auto link-local**。

【举例】

```
# 配置 GigabitEthernet1/0/1 接口的链路本地地址。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ipv6 address fe80::1 link-local
```

【相关命令】

- **ipv6 address auto link-local**

1.1.23 *ipv6 address prefix-number*

ipv6 address prefix-number 命令用来引用前缀生成接口上的 IPv6 地址，并将此前缀分配给终端设备。

undo ipv6 address prefix-number 命令用来恢复缺省情况。

【命令】

```
ipv6 address prefix-number sub-prefix/prefix-length  
undo ipv6 address prefix-number
```

【缺省情况】

接口上未引用前缀，也不会向终端设备分配该前缀。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

prefix-number: 表示 IPv6 前缀编号，取值范围为 1～1024。

sub-prefix: 表示 IPv6 地址的子前缀位和主机位。

prefix-length: 表示地址的前缀长度，取值范围为 1~128。

【使用指导】

配置该命令后，接口的 IPv6 地址由指定编号的前缀、子前缀位和主机位构成。

一个接口上只能有一个引用前缀生成的地址，且不能通过重复执行本命令修改引用前缀生成的地址。

如需修改引用前缀生成的地址，请先通过 **undo ipv6 address prefix-number** 命令取消引用前缀生成接口上的 IPv6 地址，再执行 **ipv6 address prefix-number** 命令。

【举例】

静态配置编号为 1 的 IPv6 前缀为 AAAA::/16，在接口 GigabitEthernet1/0/1 上使用编号为 1 的前缀生成 IPv6 地址为 AAAA:CCCC:DDDD::10/32，并将编号为 1 的 IPv6 前缀分配给终端设备。

```
<Sysname> system-view
[Sysname] ipv6 prefix 1 AAAA::/16
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 1 BBBB:CCCC:DDDD::10/32
```

【相关命令】

- **ipv6 prefix**

1.1.24 ipv6 extension-header drop enable

ipv6 extension-header drop enable 命令用来开启 IPv6 报文扩展头丢弃功能，此功能开启后将包含无法处理的 IPv6 扩展头的报文丢弃。

undo ipv6 extension-header drop enable 命令用来关闭 IPv6 扩展头丢弃功能。

【命令】

```
ipv6 extension-header drop enable
undo ipv6 extension-header drop enable
```

【缺省情况】

IPv6 报文扩展头丢弃功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

开启 IPv6 报文扩展头丢弃功能。

```
<Sysname> system-view
[Sysname] ipv6 extension-header drop enable
```

1.1.25 ipv6 hop-limit

ipv6 hop-limit 命令用来配置设备的跳数限制。

undo ipv6 hop-limit 命令用来恢复缺省情况。

【命令】

```
ipv6 hop-limit value
undo ipv6 hop-limit
```

【缺省情况】

设备的跳数限制为 64 跳。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

value：跳数值，取值范围为 1～255。

【使用指导】

设备的跳数限制有以下两个作用：

- 决定了设备发送的 IPv6 数据报文的跳数，即 IPv6 数据报文的 Hop Limit 字段的值。
- 设备发送的 RA 消息中将携带此处配置的跳数限制值。收到该 RA 消息之后，主机在发送 IPv6 报文时，将使用该跳数值填充 IPv6 报文头中的 Hop Limit 字段。配置命令 **ipv6 nd ra hop-limit unspecified** 可以配置 RA 消息中不指定跳数限制。

【举例】

```
# 配置设备的跳数限制为 100 跳。
<Sysname> system-view
[Sysname] ipv6 hop-limit 100
```

【相关命令】

- **ipv6 nd ra hop-limit unspecified**

1.1.26 ipv6 hoplimit-expires enable

ipv6 hoplimit-expires enable 命令用来开启设备的 ICMPv6 超时报文的发送功能。

undo ipv6 hoplimit-expires enable 命令用来关闭设备的 ICMPv6 超时报文的发送功能。

【命令】

```
ipv6 hoplimit-expires enable
undo ipv6 hoplimit-expires enable
```

【缺省情况】

ICMPv6 超时报文发送功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

ICMPv6 超时报文发送功能是在设备收到 IPv6 数据报文后，如果发生超时（Hop-limit 超时或者重组超时）差错，则将报文丢弃并给源端发送 ICMPv6 超时差错报文。

如果接收到大量需要发送 ICMPv6 差错报文的恶意攻击报文，设备会因为处理大量该类报文而导致性能降低。为了避免该现象发生，可以关闭设备的 ICMPv6 超时报文发送功能，从而减少网络流量、防止遭到恶意攻击。

关闭 ICMPv6 超时报文发送功能后，设备不会再发送“Hop-Limit 超时”ICMPv6 差错报文，但“重组超时”ICMPv6 差错报文仍会正常发送。

【举例】

```
# 关闭设备的 ICMPv6 超时报文发送功能。  
<Sysname> system-view  
[Sysname] undo ipv6 hoplimit-expires enable
```

1.1.27 ipv6 icmpv6 error-interval

ipv6 icmpv6 error-interval 命令用来配置发送 ICMPv6 差错报文对应的令牌桶容量和令牌刷新周期。

undo ipv6 icmpv6 error-interval 命令用来恢复缺省情况。

【命令】

```
ipv6 icmpv6 error-interval interval [ bucketsize ]  
undo ipv6 icmpv6 error-interval
```

【缺省情况】

令牌桶容量为 10，令牌刷新周期为 100 毫秒。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval：令牌刷新周期，取值范围 0～2147483647，单位为毫秒。取值为 0 时，表示不限制 ICMPv6 差错报文的发送。

bucketsize：令牌桶中容纳的令牌数，取值范围 1～200。

【使用指导】

如果网络中短时间内发送的 ICMPv6 差错报文过多，将可能导致网络拥塞。为了避免这种情况，用户可以控制在指定时间内发送 ICMPv6 差错报文的最大个数，目前采用令牌桶算法来实现。

用户可以设置令牌桶的容量，即令牌桶中可以同时容纳的令牌数；同时可以设置令牌桶的刷新周期，即每隔多长时间发放一个令牌到令牌桶中，直到令牌桶中的令牌数达到配置的容量。一个令牌表示允许发送一个 ICMPv6 差错报文，每当发送一个 ICMPv6 差错报文，则令牌桶中减少一个令牌。如果连续发送的 ICMPv6 差错报文超过了令牌桶的容量，则后续的 ICMPv6 差错报文将不能被发送出去，直到按照所设置的刷新频率将新的令牌放入令牌桶中。

【举例】

配置设备发送 ICMPv6 差错报文对应的令牌桶容量为 40，令牌刷新时间为 200 毫秒。

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 error-interval 200 40
```

1.1.28 ipv6 icmpv6 multicast-echo-reply enable

ipv6 icmpv6 multicast-echo-reply enable 命令用来配置允许设备回复组播形式的 Echo request 报文。

undo ipv6 icmpv6 multicast-echo-reply enable 命令用来恢复缺省情况。

【命令】

```
ipv6 icmpv6 multicast-echo-reply enable
undo ipv6 icmpv6 multicast-echo-reply enable
```

【缺省情况】

不允许设备回复组播形式的 Echo request 报文。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

如果主机 B 允许回复组播形式的 Echo request 报文，则主机 A 可以构造目的地址为组播地址、源地址为主机 B 的 Echo request 报文，使该组播组中的所有的主机都向主机 B 发送 Echo reply 报文，从而达到攻击主机 B 的目的。因此，为了避免主机利用设备达到攻击的目的，缺省情况下，不允许设备回复组播形式的 Echo request 报文。

但在某些应用场景下，可能需要使用组播形式的 Echo request 报文来获取信息，此时可以配置允许设备回复组播形式的 Echo request 报文。

【举例】

配置允许设备回复组播形式的 Echo request 报文。

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

1.1.29 ipv6 icmpv6 source

ipv6 icmpv6 source 命令用来开启 ICMPv6 报文指定源地址功能。

undo ipv6 icmpv6 source 命令用来关闭 ICMPv6 报文指定源地址功能。

【命令】

```
ipv6 icmpv6 source [ vpn-instance vpn-instance-name ] ipv6-address  
undo ipv6 icmpv6 source [ vpn-instance vpn-instance-name ]
```

【缺省情况】

ICMPv6 报文指定源地址功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

vpn-instance vpn-instance-name: 指定地址所在的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。指定的 VPN 实例必须已经存在。如果不指定本参数，则表示公网内的 IPv6 地址。

ipv6-address: 表示设备发送 ICMPv6 报文时指定的源地址。

【使用指导】

在网络中 IPv6 地址配置较多的情况下，收到 ICMPv6 报文时，用户很难根据报文的源 IPv6 地址判断报文来自哪台设备。为了简化这一判断过程，可以配置 ICMPv6 报文指定源地址功能。用可配置特定地址（如环回口地址）为 ICMPv6 报文的源地址，可以简化判断。

设备发送 ICMPv6 差错报文（TTL 超时、报文过大、端口不可达和参数错误等）和 ping echo request 报文时，都可以通过上述命令指定报文的源地址。

【举例】

```
# 配置设备发送 ICMPv6 报文时指定的源地址为 1::1。  
<Sysname> system-view  
[Sysname] ipv6 icmpv6 source 1::1
```

1.1.30 ipv6 mtu

ipv6 mtu 命令用来配置接口上发送 IPv6 报文的 MTU。

undo ipv6 mtu 命令用来恢复缺省情况。

【命令】

```
ipv6 mtu size  
undo ipv6 mtu
```

【缺省情况】

未配置接口上发送 IPv6 报文的 MTU。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

size: 接口的 MTU 值，单位为字节。取值范围为 1280~1560。

【使用指导】

由于 IPv6 路由器不支持对报文进行分片，当路由器接口收到一个报文后，如果发现报文长度比转发接口的 MTU 值大，则会将其丢弃；同时将转发接口的 MTU 值通过 ICMPv6 报文的“Packet Too Big”消息发给源端主机，源端主机以该值重新发送 IPv6 报文。为减少报文被丢弃带来的额外流量开销，需要根据实际组网环境设置合适的接口 MTU 值。

【举例】

```
# 配置 GigabitEthernet1/0/1 接口上发送 IPv6 报文的 MTU 为 1280 字节。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 mtu 1280
```

1.1.31 ipv6 nd dad attempts

ipv6 nd dad attempts 命令用来配置进行重复地址检测时发送邻居请求消息的次数。

undo ipv6 nd dad attempts 命令用来恢复缺省情况。

【命令】

```
ipv6 nd dad attempts times
undo ipv6 nd dad attempts
```

【缺省情况】

进行重复地址检测时发送邻居请求消息的次数为 1。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

times: 进行重复地址检测时发送邻居请求消息的次数，取值范围为 0~600。当配置为 0 时，表示禁止重复地址检测。

【使用指导】

接口获得 IPv6 地址后，将发送邻居请求消息进行重复地址检测，如果在指定的时间内（通过 **ipv6 nd ns retrans-timer** 命令配置）没有收到响应，则继续发送邻居请求消息，当发送的次数达到使用 **ipv6 nd dad attempts** 命令所设置的次数后，仍未收到响应，则认为该地址可用。

【举例】

```
# 配置 GigabitEthernet1/0/1 接口进行重复地址检测时发送邻居请求消息的次数为 20 次。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd dad attempts 20
```

【相关命令】

- **display ipv6 interface**
- **ipv6 nd ns retrans-timer**

1.1.32 ipv6 nd ns retrans-timer

ipv6 nd ns retrans-timer 命令用来配置邻居请求消息的重传时间间隔。

undo ipv6 nd ns retrans-timer 命令用来恢复缺省情况。

【命令】

```
ipv6 nd ns retrans-timer value
undo ipv6 nd ns retrans-timer
```

【缺省情况】

接口发送 NS 消息的时间间隔为 1000 毫秒；接口发布的 RA 消息中 Retrans Timer 字段的值为 0，即不对主机进行指定。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

value: NS 消息重传时间间隔，取值范围为 1000～4294967295，单位为毫秒。

【使用指导】

设备发送 NS 消息后，如果未在指定的邻居请求消息重传时间间隔内收到响应，则会重新发送 NS 消息。

本命令配置的时间间隔既用于本接口发送 NS 消息的时间间隔，同时也作为本接口发布的 RA 消息中 Retrans Timer 字段的值。

【举例】

```
# 配置 GigabitEthernet1/0/1 接口发送 NS 消息的时间间隔为 10000 毫秒。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ns retrans-timer 10000
```

【相关命令】

- **display ipv6 interface**

1.1.33 ipv6 nd nud reachable-time

ipv6 nd nud reachable-time 命令用来配置接口保持邻居可达状态的时间。

undo ipv6 nd nud reachable-time 命令用来恢复缺省情况。

【命令】

ipv6 nd nud reachable-time *time*

undo ipv6 nd nud reachable-time

【缺省情况】

接口保持邻居可达状态的时间为 30000 毫秒；接口发布的 RA 消息中 Reachable Timer 字段的值为 0，即不对主机进行指定。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

time：保持邻居可达状态的时间，取值范围为 1~3600000，单位为毫秒。

【使用指导】

当通过邻居可达性检测确认邻居可达后，在所设置的接口保持邻居可达状态的时间内，设备认为邻居可达；超过设置的时间后，如果需要向邻居发送报文，会重新确认邻居是否可达。

本命令配置的时间既用于本接口保持邻居可达状态的时间，同时也作为本接口发布的 RA 消息中 Reachable Timer 字段的值。

【举例】

配置 GigabitEthernet1/0/1 接口上保持邻居可达状态的时间为 10000 毫秒。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 nd nud reachable-time 10000
```

【相关命令】

- **display ipv6 interface**

1.1.34 ipv6 nd ra halt

ipv6 nd ra halt 命令用来抑制 RA 消息的发布。

undo ipv6 nd ra halt 命令用来取消对 RA 消息发布的抑制。

【命令】

ipv6 nd ra halt

undo ipv6 nd ra halt

【缺省情况】

抑制发布 RA 消息。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【举例】

取消对接口 GigabitEthernet1/0/1 发布 RA 消息的抑制。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] undo ipv6 nd ra halt
```

1.1.35 ipv6 nd ra hop-limit unspecified

ipv6 nd ra hop-limit unspecified 命令用来配置 RA 消息中不指定跳数限制。

undo ipv6 nd ra hop-limit unspecified 命令用来恢复缺省情况。

【命令】

ipv6 nd ra hop-limit unspecified

undo ipv6 nd ra hop-limit unspecified

【缺省情况】

RA 消息中发布本设备的跳数限制。本设备的跳数限制默认为 64 跳。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

本设备的跳数限制默认为 64 跳，可以通过命令 **ipv6 hop-limit** 进行配置。

【举例】

配置 GigabitEthernet1/0/1 接口上 RA 消息中不指定跳数限制。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra hop-limit unspecified
```

【相关命令】

- **ipv6 hop-limit**

1.1.36 ipv6 nd ra interval

ipv6 nd ra interval 命令用来配置 RA 消息发布的最大时间间隔和最小时间间隔。

undo ipv6 nd ra interval 命令用来恢复缺省情况。

【命令】

ipv6 nd ra interval *max-interval min-interval*

undo ipv6 nd ra interval

【缺省情况】

RA 消息发布的最大时间间隔为 600 秒，最小时间间隔为 200 秒。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

max-interval: 指定 RA 消息发布的最大时间间隔，取值范围是 4~1800，单位为秒。

min-interval: 指定 RA 消息发布的最小时间间隔，取值范围是 3~ (*max-interval* * 3/4)，单位为秒。

【使用指导】

RA 消息周期性发布时，设备在最大时间间隔与最小时间间隔之间随机选取一个值作为周期性发布 RA 消息的时间间隔。

RA 消息发布的最大实际间隔应该小于或等于 RA 消息中路由器的生存时间。

【举例】

设备周期性发布 RA 消息的最大时间间隔为 1000 秒，最小时间间隔为 700 秒。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra interval 1000 700
```

【相关命令】

- **ipv6 nd ra router-lifetime**

1.1.37 ipv6 nd ra no-advlinkmtu

ipv6 nd ra no-advlinkmtu 命令用来配置 RA 消息中不携带 MTU 选项。

undo ipv6 nd ra no-advlinkmtu 命令用来恢复缺省情况。

【命令】

ipv6 nd ra no-advlinkmtu

undo ipv6 nd ra no-advlinkmtu

【缺省情况】

RA 消息中携带 MTU 选项。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

RA 消息中携带的 MTU 选项可以用来发布链路的 MTU，用于确保同一链路上的所有节点采用相同的 MTU 值。

【举例】

配置 GigabitEthernet1/0/1 接口上 RA 消息中不携带 MTU 选项。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra no-advlinkmtu
```

1.1.38 ipv6 nd ra prefix

ipv6 nd ra prefix 命令用来配置 RA 消息中的前缀信息。

undo ipv6 nd ra prefix 命令用来恢复缺省情况。

【命令】

```
ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length }  
[ valid-lifetime preferred-lifetime [ no-autoconfig | off-link ] * |  
no-advertise ]
```

```
undo ipv6 nd ra prefix { ipv6-prefix | ipv6-prefix/prefix-length }
```

【缺省情况】

未配置 RA 消息中的前缀信息，此时将使用发送 RA 消息的接口 IPv6 地址作为 RA 中的前缀信息，其手工配置地址的有效生命期是 2592000 秒（30 天），首选生命期是 604800（7 天）；其他自动分配地址的有效生命期和首选生命期与地址本身的生命期相同。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-prefix: IPv6 地址前缀。

prefix-length: 前缀长度。

valid-lifetime: 前缀的有效存活时间，即有效生命期。取值范围为 0~4294967295，单位为秒，缺省值为 2592000 秒（30 天）。

preferred-lifetime: 前缀用于无状态地址配置的优选项的存活时间，即首选生命期。取值范围为 0~4294967295，单位为秒。**preferred-lifetime** 的值要小于等于 **valid-lifetime** 的值，缺省值为 604800 秒（7 天）。

no-autoconfig: 指定前缀不用于无状态地址配置。如果不选择该参数，则指定前缀用于无状态地址配置。

off-link: 指定前缀不是该链路上直连可达的。如果不选择该参数，则表示指定前缀是直连可达的。

no-advertise: 指定前缀不在 RA 消息中发布。如果不选择该参数，则表示指定前缀在 RA 消息中发布。

【使用指导】

如果使用本命令配置的前缀和 IPv6 地址生成的前缀相同，则优先使用本命令配置的前缀信息进行 RA 消息发布。

在同一链路上的主机收到设备发布的 RA 消息中后，可以根据 RA 消息中的前缀信息进行无状态自动配置等操作。

配置 RA 消息中的前缀信息时，如果不指定任何参数，在使用 **ipv6 nd ra prefix default** 命令的情况下，采用 **default** 配置参数，否则采用缺省情况下的参数值，即有效生命期是 2592000 秒（30 天），首选生命期是 604800（7 天），配置的前缀可以用于无状态地址配置、在 RA 消息中发布，并且是直连可达的。

【举例】

配置 GigabitEthernet1/0/1 接口上 RA 消息中的前缀信息。

方法一：

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra prefix 2001:10::100/64 100 10
```

方法二：

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra prefix 2001:10::100 64 100 10
```

1.1.39 ipv6 nd ra prefix default

ipv6 nd ra prefix default 命令用来配置通过 RA 消息发布的前缀使用的缺省参数。

undo ipv6 nd ra prefix default 命令用来恢复缺省情况。

【命令】

```
ipv6 nd ra prefix default [ valid-lifetime preferred-lifetime
[ no-autoconfig | off-link ] * | no-advertise ]
undo ipv6 nd ra prefix default
```

【缺省情况】

未配置通过 RA 消息发布的前缀使用的缺省参数。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

valid-lifetime: 前缀的有效存活时间，即有效生命期。取值范围为 0~4294967295，单位为秒，缺省值为 2592000 秒（30 天）。

preferred-lifetime: 前缀用于无状态地址配置的优选项的存活时间，即首选生命期。取值范围为 0~4294967295，单位为秒。**preferred-lifetime** 的值要小于等于 **valid-lifetime** 的值，缺省值为 604800（7 天）。

no-autoconfig: 前缀不用于无状态地址配置。如果不选择该参数，则表示前缀用于无状态地址配置。

off-link: 前缀不是该链路上直连可达的。如果不选择该参数，则表示前缀是直连可达的。

no-advertise: 前缀不在 RA 消息中发布。如果不选择该参数，则表示前缀在 RA 消息中发布。

【使用指导】

对于使用 **ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length }** 命令配置的前缀，本命令的所有配置生效；对于由发布 RA 消息的接口的 IPv6 地址生成的前缀，本命令的配置中只有 **no-advertise** 配置生效。

通过本命令配置缺省参数后，在配置 **ipv6 nd ra prefix { ipv6-prefix prefix-length | ipv6-prefix/prefix-length }** 命令时，如果指定了 **valid-lifetime**、**preferred-lifetime**、**no-autoconfig**、**off-link**、**no-advertise** 等参数，则使用指定的参数，如果没有指定这些参数，则使用本命令配置的缺省参数。

【举例】

配置 GigabitEthernet1/0/1 接口上 RA 消息中的缺省前缀信息。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra prefix default 100 10
```

1.1.40 ipv6 nd ra router-lifetime

ipv6 nd ra router-lifetime 命令用来配置 RA 消息中路由器的生存时间。

undo ipv6 nd ra router-lifetime 命令用来恢复缺省情况。

【命令】

ipv6 nd ra router-lifetime time

undo ipv6 nd ra router-lifetime

【缺省情况】

RA 消息中路由器的生存时间为 1800 秒。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

time: RA 消息中路由器的生存时间，取值范围为 0~9000，单位为秒。当配置为 0 时，表示本设备不作为默认路由器。

【使用指导】

RA 消息中路由器的生存时间用于设置发布 RA 消息的路由器作为主机的默认路由器的时间。主机根据接收到的 RA 消息中的路由器生存时间参数值，就可以确定是否将发布该 RA 消息的路由器作为默认路由器。发布 RA 消息中路由器生存时间为 0 的路由器不能作为默认路由器。

RA 消息中路由器的生存时间应该大于或等于 RA 消息的发布时间间隔。

【举例】

配置 GigabitEthernet1/0/1 接口上 RA 消息中路由器的生存时间为 1000 秒。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 nd ra router-lifetime 1000
```

【相关命令】

- **ipv6 nd ra interval**

1.1.1.41 ipv6 nd router-preference

ipv6 nd router-preference 命令用来配置接口下发送的 RA 消息中的路由器优先级。

undo ipv6 nd router-preference 命令用来恢复缺省情况。

【命令】

ipv6 nd router-preference { high | low | medium }

undo ipv6 nd router-preference

【缺省情况】

设备发送的 RA 消息中的路由器优先级为 **medium**。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

high: 设置发布 RA 的路由器为高优先级。

low: 设置发布 RA 的路由器为低优先级。

medium: 设置发布 RA 的路由器为中优先级。

【使用指导】

主机根据接收到的 RA 消息中的路由器优先级，可以选择优先级最高的路由器作为默认网关。

在路由器的优先级相同的情况下，遵循“先来先用”的原则，优先选择先接收到的 RA 消息对应的发送路由器作为默认网关。

【举例】

配置 GigabitEthernet1/0/1 接口下发送的 RA 消息中的路由优先级为 **low**。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd router-preference low
```

1.1.42 ipv6 neighbor

ipv6 neighbor 命令用来配置静态邻居表项。

undo ipv6 neighbor 命令用来删除邻居表项。

【命令】

```
ipv6 neighbor ipv6-address mac-address { vlan-id port-type port-number |
interface interface-type interface-number } [vpn-instance
vpn-instance-name ]
undo ipv6 neighbor ipv6-address interface-type interface-number
```

【缺省情况】

不存在静态邻居表项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address: 静态邻居表项中的 IPv6 地址。

mac-address: 静态邻居表项中的链路层地址（48 位，格式为 H-H-H）。

vlan-id: 静态邻居表项所对应的 VLAN ID，取值范围为 1~4094。

port-type port-number: 静态邻居表项所对应的二层端口类型和端口号。

interface interface-type interface-number: 静态邻居表项所对应的三层接口类型和接口号。

vpn-instance vpn-instance-name: 指定静态邻居表项所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示静态邻居表项属于公网。

【使用指导】

邻居表项保存的是设备在链路范围内的邻居信息，设备邻居表项可以通过邻居请求消息 NS 及邻居通告消息 NA 来动态创建，也可以通过手工配置来静态创建。

设备根据邻居节点的 IPv6 地址和与此邻居节点相连的三层接口号来唯一标识一个静态邻居表项。目前，静态邻居表项有两种配置方式：

- 配置本节点的三层接口相连的邻居节点的 IPv6 地址和链路层地址；
- 配置本节点 VLAN 中的二层端口相连的邻居节点的 IPv6 地址和链路层地址。

对于 VLAN 接口，可以采用上述两种方式来配置静态邻居表项：

- 采用第一种方式配置静态邻居表项后，该邻居表项处于 INCMP 状态。设备解析该 VLAN 下的二层端口信息后，该邻居表项才会进入 REACH 状态。
- 采用第二种方式配置静态邻居表项，需要保证 *port-type port-number* 指定的二层端口属于 *vlan-id* 指定的 VLAN，且该 VLAN 已经创建了 VLAN 接口。在配置后，设备会将 VLAN 所对应的 VLAN 接口与 IPv6 地址相对应来唯一标识一个静态邻居表项，并且该表项处于 REACH 状态。

执行 **undo ipv6 neighbor** 命令既可以删除静态邻居表项，也可以删除动态邻居表项。

在删除 VLAN 接口对应的邻居表项时，只需要指定 VLAN 对应的 VLAN 接口即可。

【举例】

配置三层以太网接口 GigabitEthernet1/0/1 对应的静态邻居表项。

```
<Sysname> system-view
```

```
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 interface gigabitethernet 1/0/1
```

【相关命令】

- **display ipv6 neighbors**
- **reset ipv6 neighbors**

1.1.43 ipv6 neighbor link-local minimize

ipv6 neighbor link-local minimize 命令用来配置链路本地 ND 表项资源占用最小化。

undo ipv6 neighbor link-local minimize 命令用来恢复缺省情况。

【命令】

```
ipv6 neighbor link-local minimize
```

```
undo ipv6 neighbor link-local minimize
```

【缺省情况】

所有 ND 表项均会下发硬件表项。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

本功能可以对链路本地 ND 表项（该 ND 表项的 IPv6 地址为链路本地地址）占用的资源进行优化。配置本功能后，新学习的、未被引用的链路本地 ND 表项（该 ND 表项的链路本地地址不是某条路由的下一跳）不下发硬件表项，以节省资源。

本功能只对后续新学习的 ND 表项生效，已经存在的 ND 表项不受影响。

【举例】

```
# 配置链路本地 ND 表项资源占用最小化。
<Sysname> system-view
[Sysname] ipv6 neighbor link-local minimize
```

1.1.44 ipv6 neighbor stale-aging

ipv6 neighbor stale-aging 命令用来配置 STALE 状态 ND 表项的老化时间。

undo ipv6 neighbor stale-aging 命令用来恢复缺省情况。

【命令】

```
ipv6 neighbor stale-aging aging-time
undo ipv6 neighbor stale-aging
```

【缺省情况】

STALE 状态 ND 表项的老化时间为 240 分钟。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

aging-time: STALE 状态 ND 表项的老化时间，取值范围为 1~1440，单位为分钟。

【使用指导】

为适应网络的变化，ND 表需要不断更新。ND 表中的 STALE 状态 ND 表项并非永远有效，每一条记录都有一个老化时间。到达老化时间的 STALE 状态 ND 表项将迁移到 DELAY 状态。5 秒钟后 DELAY 状态超时，ND 表项将迁移到 PROBE 状态，并发送 3 次 NS 报文进行可达性探测。若邻居已经下线，则收不到回应的 NA 报文，此时会将该 ND 表项删除。

【举例】

```
# 配置 STALE 状态 ND 表项的老化时间为 120 分钟。
<Sysname> system-view
[Sysname] ipv6 neighbor stale-aging 120
```

1.1.45 ipv6 neighbors max-learning-num

ipv6 neighbors max-learning-num 命令用来配置接口上允许学习的动态邻居表项的最大个数。

undo ipv6 neighbors max-learning-num 命令用来恢复缺省情况。

【命令】

ipv6 neighbors max-learning-num *max-number*

undo ipv6 neighbors max-learning-num

【缺省情况】

接口上允许学习的动态邻居表项的最大个数为 65536。

【视图】

二层接口视图/三层接口视图

二层聚合接口视图/三层聚合接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

max-number：接口上允许学习的动态邻居表项的最大个数。取值范围为 0～65536。

【使用指导】

设备可以通过 NS 消息和 NA 消息来动态获取邻居节点的链路层地址，并将其加入到邻居表中。为了防止部分接口下的用户占用过多的资源，可以通过设置接口学习动态邻居表项的最大数目来进行限制。当接口学习到的动态邻居表项的个数达到所设置的最大值时，该接口将不再学习动态邻居表项。

当参数配置为 0 时，接口将不能学习动态邻居表项，即动态邻居表项学习功能处于关闭状态。

【举例】

指定 GigabitEthernet1/0/1 接口上允许动态学习的邻居的最大个数为 10 个。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 neighbors max-learning-num 10
```

1.1.46 ipv6 pathmtu

ipv6 pathmtu 命令用来配置 IPv6 地址对应的静态 PMTU。

undo ipv6 pathmtu 命令用来删除指定 IPv6 地址的 PMTU 配置。

【命令】

ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] *ipv6-address value*

undo ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] *ipv6-address*

【缺省情况】

未配置 IPv6 地址对应的静态 PMTU 值。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

vpn-instance *vpn-instance-name*: 指定 PMTU 所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示公网。

ipv6-address: 指定的 IPv6 地址。

value: 指定 IPv6 地址对应的 PMTU 值, 取值范围为 1280~10240, 单位为字节。

【使用指导】

用户可以为指定的目的 IPv6 地址配置静态的 PMTU 值。当源端主机从接口发送报文时, 将比较该接口的 MTU 与指定目的 IPv6 地址的静态 PMTU, 如果报文长度大于二者中的最小值, 则采用此最小值对报文进行分片。

【举例】

配置指定 IPv6 地址对应的静态 PMTU 值。

```
<Sysname> system-view
```

```
[Sysname] ipv6 pathmtu fe80::12 1300
```

【相关命令】

- **display ipv6 pathmtu**
- **reset ipv6 pathmtu**

1.1.47 ipv6 pathmtu age

ipv6 pathmtu age 命令用来配置动态 PMTU 的老化时间。

undo ipv6 pathmtu age 命令用来恢复缺省情况。

【命令】

```
ipv6 pathmtu age age-time
```

```
undo ipv6 pathmtu age
```

【缺省情况】

动态 PMTU 的老化时间为 10 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

age-time: PMTU 老化时间，取值范围为 10~100，单位为分钟。

【使用指导】

动态确定源端主机到目的端主机的 PMTU 后，源端主机将使用这个 MTU 值发送后续报文到目的端主机。当 PMTU 老化时间超时后：

- 删除动态 PMTU；
- 源端主机会通过 PMTU 机制重新确定发送报文的 MTU 值。

该配置对静态 PMTU 不起作用。

【举例】

配置动态 PMTU 的老化时间为 40 分钟。

```
<Sysname> system-view  
[Sysname] ipv6 pathmtu age 40
```

【相关命令】

- **display ipv6 pathmtu**

1.1.48 ipv6 prefer temporary-address

ipv6 prefer temporary-address 命令用来开启优先选择临时地址作为报文的源地址功能。

undo ipv6 prefer temporary-address 命令用来关闭优先选择临时地址作为报文的源地址功能。

【命令】

```
ipv6 prefer temporary-address  
undo ipv6 prefer temporary-address
```

【缺省情况】

优先选择临时地址作为报文的源地址功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

在配置了优先选择临时地址功能前提下发送报文，系统将优先选择临时地址作为报文的源地址。如果生成的临时地址因为 DAD 冲突不可用，就采用公共地址作为报文的源地址。

【举例】

开启优先选择临时地址作为报文的源地址功能。

```
<Sysname> system-view  
[Sysname] ipv6 prefer temporary-address
```

【相关命令】

- **ipv6 address auto**
- **ipv6 nd ra prefix**
- **ipv6 temporary-address**

1.1.49 ipv6 prefix

ipv6 prefix 命令用来手工配置静态 IPv6 前缀。

undo ipv6 prefix 命令用来删除指定的静态 IPv6 前缀。

【命令】

ipv6 prefix *prefix-number* *ipv6-prefix/prefix-length*
undo ipv6 prefix *prefix-number*

【缺省情况】

未配置静态 IPv6 前缀。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

prefix-number: 前缀编号，取值范围为 1~1024。

ipv6-prefix/prefix-length: 前缀和前缀长度。*prefix-length* 的取值范围为 1~128。

【使用指导】

不能通过重复执行本命令修改已经创建的静态 IPv6 前缀。如需修改静态 IPv6 前缀，请先通过 **undo ipv6 prefix** 命令删除静态 IPv6 前缀，再执行 **ipv6 prefix** 命令。

手工配置的静态 IPv6 前缀与动态生成的 IPv6 前缀编号允许相同，静态 IPv6 前缀优先。

【举例】

创建 IPv6 静态前缀编号为 1，前缀为 2001:0410::/32。

```
<Sysname> system-view  
[Sysname] ipv6 prefix 1 2001:0410::/32
```

【相关命令】

- **display ipv6 prefix**

1.1.50 ipv6 reassemble local enable

ipv6 reassemble local enable 命令用来开启 IPv6 分片报文本地重组功能。

undo ipv6 reassemble local enable 命令用来关闭 IPv6 分片报文本地重组功能。

【命令】

```
ipv6 reassemble local enable
undo ipv6 reassemble local enable
```

【缺省情况】

IPv6 分片报文本地重组功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

多台设备组成的 IRF 环境下，当某成员设备收到目的为本 IRF 设备的 IPv6 分片报文时，需要把分片报文送到主设备进行重组，这样会导致报文重组性能较低的问题。当开启 IPv6 分片报文本地重组功能后，分片报文会在该成员设备上直接进行报文重组，这样就能提高分片报文的重组性能。开启 IPv6 分片报文本地重组功能后，如果分片报文是从设备上不同的成员设备进入的，会导致 IPv6 分片报文本地无法重组成功。

【举例】

```
# 开启 IPv6 分片报文本地重组功能。
<Sysname> system-view
[Sysname] ipv6 reassemble local enable
```

1.1.51 ipv6 redirects enable

ipv6 redirects enable 命令用来开启设备的 ICMPv6 重定向报文的发送功能。

undo ipv6 redirects enable 命令用来关闭设备的 ICMPv6 重定向报文的发送功能。

【命令】

```
ipv6 redirects enable
undo ipv6 redirects enable
```

【缺省情况】

ICMPv6 重定向报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```


【使用指导】

主机启动时，它的路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时，作为缺省网关的设备会向源主机发送 ICMPv6 重定向报文，通知主机重新选择正确的下一跳进行后续报文的发送。

ICMPv6 重定向报文发送功能可以简化主机的管理，使具有很少选路信息的主机逐渐建立较完善的路由表，从而找到最佳路由。但是由于重定向功能会在主机的路由表中增加主机路由，当增加的主机路由很多时，会降低主机性能。因此默认情况下设备的 ICMPv6 重定向报文发送功能是关闭的。

【举例】

开启设备的 ICMPv6 重定向报文发送功能。

```
<Sysname> system-view  
[Sysname] ipv6 redirects enable
```

1.1.52 ipv6 temporary-address

ipv6 temporary-address 命令用来配置系统生成临时地址。

undo ipv6 temporary-address 命令用来恢复缺省情况。

【命令】

```
ipv6 temporary-address [valid-lifetime preferred-lifetime ]  
undo ipv6 temporary-address
```

【缺省情况】

系统不生成临时地址。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

valid-lifetime: 临时地址的有效生命期，取值范围为 600～4294967295，单位为秒，缺省值为 604800（7 天）。

preferred-lifetime: 临时地址的首选生命期，取值范围为 600～4294967295，单位为秒，缺省值为 86400（1 天）。***preferred-lifetime*** 的值要小于等于 ***valid-lifetime*** 的值。

【使用指导】

配置本功能时需要打开地址无状态自动配置功能。

在配置了无状态自动配置 IPv6 地址功能后，接口会根据接收到的 RA 报文中携带的地址前缀信息和接口 ID，自动生成 IPv6 全球单播地址。如果接口是 IEEE 802 类型的接口（例如，以太网接口、VLAN 接口），其接口 ID 是由 MAC 地址根据一定的规则生成，此接口 ID 具有全球唯一性。对于不同的前缀，接口 ID 部分始终不变，攻击者通过接口 ID 可以很方便的识别出通信流量是由哪台设备产生的，并分析其规律，会造成一定的安全隐患。

如果在地址无状态自动配置时，自动生成接口 ID 不断变化的 IPv6 地址，就可以加大攻击的难度，从而保护网络。为此，设备提供了临时地址功能，使得系统可以生成临时地址。

配置该功能后，通过地址无状态自动配置，IEEE 802 类型的接口可以同时生成两类地址：

- 公共地址：地址前缀采用 RA 报文携带的前缀，接口 ID 由 MAC 地址产生。接口 ID 始终不变。
- 临时地址：地址前缀采用 RA 报文携带的前缀，接口 ID 由系统根据 MD5 算法计算产生。接口 ID 不断变化。

当临时地址的有效生命期过期后，这个临时地址将被删除，同时，系统会通过 MD5 算法重新生成一个接口 ID 不同的临时地址。所以，该接口发送报文的源地址的接口 ID 总是在不停变化。

配置的临时地址的有效生命期要大于或等于首选生命期。

临时地址的首选生命期是如下两个值之中的较小者：

- RA 前缀中的首选生命期
- 配置的临时地址首选生命期减去 DESYNC_FACTOR（DESYNC_FACTOR 是一个 0~600 秒的随机值）。

临时地址的有效生命期是如下两个值之中的较小者：

- RA 前缀中的有效生命期。
- 配置的临时地址有效生命期。

【举例】

```
# 配置系统生成临时地址。  
<Sysname> system-view  
[Sysname] ipv6 temporary-address
```

【相关命令】

- **ipv6 address auto**
- **ipv6 nd ra prefix**
- **ipv6 prefer temporary-address**

1.1.53 ipv6 unreachable enable

ipv6 unreachable enable 命令用来开启设备的 ICMPv6 目的不可达报文的发送功能。

undo ipv6 unreachable enable 命令用来关闭设备的 ICMPv6 目的不可达报文的发送功能。

【命令】

```
ipv6 unreachable enable  
undo ipv6 unreachable enable
```

【缺省情况】

ICMPv6 目的不可达报文发送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

ICMPv6 目的不可达报文发送功能是在设备收到 IPv6 数据报文后，如果发生目的不可达的差错，则将报文丢弃并给源端发送 ICMPv6 目的不可达差错报文。

由于 ICMPv6 目的不可达报文传递给用户进程的信息为不可达信息，如果有用户恶意攻击，可能会影响终端用户的正常使用。为了避免上述现象发生，可以关闭设备的 ICMPv6 目的不可达报文发送功能，从而减少网络流量、防止遭到恶意攻击。

【举例】

开启设备的 ICMPv6 目的不可达报文发送功能。

```
<Sysname> system-view
[Sysname] ipv6 unreachable enable
```

1.1.54 local-proxy-nd enable

local-proxy-nd enable 命令用来开启本地 ND Proxy 功能。

undo local-proxy-nd enable 命令用来关闭本地 ND Proxy 功能。

【命令】

```
local-proxy-nd enable
undo local-proxy-nd enable
```

【缺省情况】

本地 ND Proxy 功能处于关闭状态。

【视图】

VLAN 接口视图
三层以太网接口视图
三层以太网子接口视图
三层聚合接口视图
三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【举例】

在 GigabitEthernet1/0/1 接口上开启本地 ND Proxy 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] local-proxy-nd enable
```

【相关命令】

- **proxy-nd enable**

1.1.55 proxy-nd enable

proxy-nd enable 命令用来开启 ND Proxy 功能。

undo proxy-nd enable 命令用来关闭 ND Proxy 功能。

【命令】

```
proxy-nd enable
undo proxy-nd enable
```

【缺省情况】

ND Proxy 功能处于关闭状态。

【视图】

VLAN 接口视图
三层以太网接口视图
三层以太网子接口视图
三层聚合接口视图
三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 在 GigabitEthernet1/0/1 接口上开启 ND Proxy 功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] proxy-nd enable
```

【相关命令】

- **local-proxy-nd enable**

1.1.56 reset ipv6 neighbors

reset ipv6 neighbors 命令用来清除 IPv6 邻居信息。

【命令】

```
reset ipv6 neighbors { all | dynamic | interface interface-type
interface-number | slot slot-number | static }
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

all: 清除所有接口上的静态与动态邻居信息。

dynamic: 清除所有接口上的动态邻居信息。

interface interface-type interface-number: 清除指定接口上的动态邻居信息。
interface-type interface-number 为接口类型和接口编号

slot slot-number: 清除指定成员设备的动态邻居信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除所有成员设备上的动态邻居信息。

static: 清除所有接口上的静态邻居信息。

【举例】

```
# 清除所有接口上的所有邻居信息。
<Sysname> reset ipv6 neighbors all
This will delete all the entries. Continue? [Y/N]:Y
# 清除所有接口上的动态邻居信息。
<Sysname> reset ipv6 neighbors dynamic
This will delete all the dynamic entries. Continue? [Y/N]:Y
# 清除接口 GigabitEthernet1/0/1 上的所有邻居信息。
<Sysname> reset ipv6 neighbors interface gigabitethernet 1/0/1
This will delete all the dynamic entries by the interface you specified. Continue? [Y/N]:Y
```

【相关命令】

- **display ipv6 neighbors**
- **ipv6 neighbor**

1.1.57 reset ipv6 pathmtu

reset ipv6 pathmtu 命令用来清除 PMTU 信息。

【命令】

reset ipv6 pathmtu { all | dynamic | static }

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

all: 清空所有的 PMTU 信息。

dynamic: 清空所有动态创建的 PMTU 信息。

static: 清空所有的静态 PMTU 信息。

【举例】

```
# 清除所有 PMTU 信息。
<Sysname> reset ipv6 pathmtu all
```

【相关命令】

- **display ipv6 pathmtu**

1.1.58 reset ipv6 statistics

reset ipv6 statistics 命令用来清除 IPv6 报文及 ICMPv6 报文的统计信息。

【命令】

reset ipv6 statistics [*slot slot-number*]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot slot-number: 清除指定成员设备的 IPv6 报文及 ICMPv6 报文统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除所有成员设备上的 IPv6 报文及 ICMPv6 报文统计信息。

【举例】

清除 IPv6 报文及 ICMPv6 报文的统计信息。

```
<Sysname> reset ipv6 statistics
```

【相关命令】

- **display ipv6 statistics**

目 录

1 IPv6 快速转发	1-1
1.1 IPv6 快速转发配置命令	1-1
1.1.1 display ipv6 fast-forwarding aging-time	1-1
1.1.2 display ipv6 fast-forwarding cache	1-1
1.1.3 ipv6 fast-forwarding aging-time	1-3
1.1.4 ipv6 fast-forwarding load-sharing	1-3
1.1.5 reset ipv6 fast-forwarding cache	1-4

1 IPv6 快速转发

1.1 IPv6快速转发配置命令

1.1.1 display ipv6 fast-forwarding aging-time

display ipv6 fast-forwarding aging-time 命令用来显示 IPv6 快速转发表项的老化时间。

【命令】

display ipv6 fast-forwarding aging-time

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 IPv6 快速转发表项的老化时间。

```
<Sysname> display ipv6 fast-forwarding aging-time  
Aging time: 30s
```

表1-1 display ipv6 fast-forwarding aging-time 命令显示信息描述表

字段	描述
Aging time	IPv6快转表项的老化时间，单位为秒

【相关命令】

- **ipv6 fast-forwarding aging-time**

1.1.2 display ipv6 fast-forwarding cache

display ipv6 fast-forwarding cache 命令用来显示 IPv6 快速转发表信息。

【命令】

display ipv6 fast-forwarding cache [*ipv6-address*] [*slot slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

ipv6-address: 显示指定 IPv6 地址的 IPv6 快速转发表信息。如果不指定 **ipv6-address**，将显示所有 IPv6 地址的 IPv6 快速转发表信息。

slot slot-number: 显示指定成员设备的 IPv6 快速转发表信息。**slot-number** 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备上的 IPv6 快速转发表信息。

【举例】

显示 IPv6 快转表信息。

```
<Sysname> display ipv6 fast-forwarding cache
Total number of IPv6 fast-forwarding items: 2
Src IP: 2002::1                               Src port: 129
Dst IP: 2001::1                               Dst port: 65535
Protocol: 58
VPN instance: N/A
Input interface: GE1/0/2
Output interface: GE1/0/1

Src IP: 2001::1                               Src port: 128
Dst IP: 2002::1                               Dst port: 0
Protocol: 58
VPN instance: N/A
Input interface: GE1/0/1
Output interface: GE1/0/2
```

表1-2 display ipv6 fast-forwarding cache 命令显示信息描述表

字段	描述
Total number of IPv6 fast-forwarding items	IPv6快速转发表项数目
Src IP	源IPv6地址
Src port	源端口号
Dst IP	目的IPv6地址
Dst Port	目的端口号
Protocol	协议号
VPN instance	VPN实例名称，（“N/A”表示该表项属于公网）
Input interface	报文入接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及入接口，“-”表示接口不存在）
Output interface	报文出接口类型和接口号（“N/A”表示接口存在但是该快速转发不涉及出接口，“-”表示接口不存在）

【相关命令】

- **reset ipv6 fast-forwarding cache**

1.1.3 ipv6 fast-forwarding aging-time

ipv6 fast-forwarding aging-time 命令用来配置 IPv6 快速转发表项的老化时间。

undo ipv6 fast-forwarding aging-time 命令用来恢复缺省情况。

【命令】

ipv6 fast-forwarding aging-time *aging-time*

undo ipv6 fast-forwarding aging-time

【缺省情况】

IPv6 快速转发表项的老化时间为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

aging-time: IPv6 快速转发表项的老化时间，取值范围为 10～300，单位为秒。

【举例】

配置 IPv6 快速转发表项的老化时间为 20 秒。

```
<Sysname> system-view
```

```
[Sysname] ipv6 fast-forwarding aging-time 20
```

【相关命令】

- **display ipv6 fast-forwarding aging-time**

1.1.4 ipv6 fast-forwarding load-sharing

ipv6 fast-forwarding load-sharing 命令用来开启 IPv6 快转负载分担功能。

undo ipv6 fast-forwarding load-sharing 命令用来关闭 IPv6 快转负载分担功能。

【命令】

ipv6 fast-forwarding load-sharing

undo ipv6 fast-forwarding load-sharing

【缺省情况】

IPv6 快转负载分担功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

开启 IPv6 快速转发负载分担功能后，当一条数据流从不同入接口上来进行转发时，不再根据入接口不同区分数据流，根据报文中的信息标识一条数据流。

关闭 IPv6 快速转发负载分担功能后，将会根据入接口的不同对已标识的数据流再次做出区分，即将入接口作为区分数据流的另一特征标识。

【举例】

```
# 开启 IPv6 快转负载分担功能。  
<Sysname> system-view  
[Sysname] ipv6 fast-forwarding load-sharing
```

1.1.5 reset ipv6 fast-forwarding cache

reset ipv6 fast-forwarding cache 命令用来清除 IPv6 快速转发表信息。

【命令】

reset ipv6 fast-forwarding cache [*slot slot-number*]

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number: 清除指定成员设备的 IPv6 快速转发表信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除所有成员设备的 IPv6 快速转发表信息。

【举例】

```
# 清除 IPv6 快速转发表信息。  
<Sysname> reset ipv6 fast-forwarding cache
```

【相关命令】

- **display ipv6 fast-forwarding cache**



UNIS 入侵检测系统

三层技术-IP 路由命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《三层技术-IP 路由命令参考》主要介绍 IP 路由基础、静态路由、RIP、OSPF、策略路由、IPv6 静态路由、RIPng、OSPFv3、IPv6 策略路由和路由策略的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项中选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。

格 式	意 义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 IP路由基础	1-1
1.1 IP路由基础配置命令	1-1
1.1.1 address-family ipv4	1-1
1.1.2 address-family ipv6	1-1
1.1.3 display ip routing-table	1-2
1.1.4 display ip routing-table acl	1-5
1.1.5 display ip routing-table <i>ip-address</i>	1-8
1.1.6 display ip routing-table prefix-list	1-11
1.1.7 display ip routing-table protocol	1-13
1.1.8 display ip routing-table statistics	1-15
1.1.9 display ip routing-table summary	1-16
1.1.10 display ipv6 rib graceful-restart	1-17
1.1.11 display ipv6 rib nib	1-18
1.1.12 display ipv6 route-direct nib	1-20
1.1.13 display ipv6 routing-table	1-21
1.1.14 display ipv6 routing-table acl	1-25
1.1.15 display ipv6 routing-table <i>ipv6-address</i>	1-29
1.1.16 display ipv6 routing-table prefix-list	1-32
1.1.17 display ipv6 routing-table protocol	1-33
1.1.18 display ipv6 routing-table statistics	1-35
1.1.19 display ipv6 routing-table summary	1-36
1.1.20 display rib graceful-restart	1-37
1.1.21 display rib nib	1-39
1.1.22 display route-direct nib	1-43
1.1.23 fib lifetime	1-45
1.1.24 inter-protocol fast-reroute	1-46
1.1.25 non-stop-routing	1-47
1.1.26 protocol lifetime	1-47
1.1.27 reset ip routing-table statistics protocol	1-48
1.1.28 reset ipv6 routing-table statistics protocol	1-49
1.1.29 rib	1-49

1 IP路由基础

1.1 IP路由基础配置命令

1.1.1 address-family ipv4

address-family ipv4 命令用来创建 RIB IPv4 地址族，并进入 RIB IPv4 地址族视图。

undo address-family ipv4 命令用来删除 RIB IPv4 地址族和 RIB IPv4 地址族视图下的所有配置。

【命令】

```
address-family ipv4
undo address-family ipv4
```

【缺省情况】

不存在 RIB IPv4 地址族。

【视图】

RIB 视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 创建 RIB IPv4 地址族，并进入 RIB IPv4 地址族视图。
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4]
```

1.1.2 address-family ipv6

address-family ipv6 命令用来创建 RIB IPv6 地址族，并进入 RIB IPv6 地址族视图。

undo address-family 命令用来删除 RIB IPv6 地址族和 RIB IPv6 地址族视图下的所有配置。

【命令】

```
address-family ipv6
undo address-family ipv6
```

【缺省情况】

不存在 RIB IPv6 地址族。

【视图】

RIB 视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 创建 RIB IPv6 地址族，并进入 RIB IPv6 地址族视图。  
<Sysname> system-view  
[Sysname] rib  
[Sysname-rib] address-family ipv6  
[Sysname-rib-ipv6]
```

1.1.3 display ip routing-table

display ip routing-table 命令用来显示路由表的信息。

【命令】

display ip routing-table [*vpn-instance vpn-instance-name*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance vpn-instance-name: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

verbose: 显示全部路由表的详细信息，包括激活路由和未激活路由。如果未指定本参数，将显示激活路由的概要信息。

【使用指导】

如果不指定任何参数时，则显示公网的信息。

【举例】

```
# 显示路由表中当前激活路由的概要信息。
```

```
<Sysname> display ip routing-table
```

```
Destinations : 10          Routes : 10
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	Static	60	0	192.168.47.4	GE1/0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0

127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.40/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

表1-1 display ip routing-table 命令显示信息描述表

字段	描述
Destinations	目的地址个数
Routes	路由条数
Destination/Mask	目的地址/掩码长度
Proto	发现该路由的路由协议类型
Pre	路由的优先级
Cost	路由的度量值
NextHop	此路由的下一跳地址
Interface	出接口，即到该目的网段的数据包将从此接口发出
Summary count	路由数目

显示路由表的全部详细信息。

<Sysname> display ip routing-table verbose

Destinations : 2 Routes : 2

Destination: 0.0.0.0/32

Protocol: Direct

Process ID: 0

SubProtID: 0x0

Age: 08h34m37s

Cost: 0

Preference: 0

IpPre: N/A

QosLocalID: N/A

Tag: 0

State: Active NoAdv

OrigTblID: 0x0

OrigVrf: default-vrf

TableID: 0x2

OrigAs: 0

NibID: 0x10000000

LastAs: 0

AttrID: 0xffffffff

Neighbor: 0.0.0.0

Flags: 0x1000c

OrigNextHop: 127.0.0.1

Label: NULL

RealNextHop: 127.0.0.1

BkLabel: NULL

BkNextHop: N/A

SRLLabel: NULL

BkSRLLabel: NULL

Tunnel ID: Invalid

Interface: InLoopBack0

BkTunnel ID: Invalid

BkInterface: N/A

FtnIndex: 0x0

TrafficIndex: N/A

Connector: N/A

VpnPeerId: N/A

Dscp: N/A

Exp: N/A

```

Destination: 1.1.1.0/24
  Protocol: Static
  Process ID: 0
    SubProtID: 0x0                                Age: 04h20m37s
      Cost: 0                                    Preference: 60
        IpPre: N/A                              QosLocalID: N/A
          Tag: 0                                State: Active Adv
    OrigTblID: 0x0                                OrigVrf: default-vrf
      TableID: 0x2                                OrigAs: 0
        NibID: 0x10000003                        LastAs: 0
          AttrID: 0xffffffff                      Neighbor: 0.0.0.0
            Flags: 0x1008c                        OrigNextHop: 192.168.47.4
              Label: NULL                          RealNextHop: 192.168.47.4
                BkLabel: NULL                      BkNextHop: N/A
                  SRLLabel: NULL                  BkSRLLabel: NULL
                    Tunnel ID: Invalid              Interface: GigabitEthernet1/0/1
    BkTunnel ID: Invalid                          BkInterface: N/A
      FtnIndex: 0x0                              TrafficIndex: N/A
        Connector: N/A                          VpnPeerId: N/A
          Dscp: N/A                              Exp: N/A

```

表1-2 display ip routing-table verbose 命令显示信息描述表

字段	描述
Destinations	目的地址个数
Routes	路由条数
Destination	目的地址/掩码
Protocol	发现该路由的路由协议类型
Process ID	进程号
SubProtID	路由子协议ID
Age	此路由在路由表中存在的时间
Cost	路由的度量值
Preference	路由的优先级
IpPre	IP优先级值
QosLocalID	（暂不支持）QoS本地ID
Tag	路由标记
State	路由状态描述： • Active: 有效的单播路由 • Adv: 允许对外发送的路由 • Inactive: 非激活路由标志 • NoAdv: 不允许发布的路由 • Vrrp: VRRP 产生的路由（暂不支持）

字段	描述
	- Nat: NAT 产生的路由（暂不支持） - TunE: Tunnel 隧道的标志（暂不支持）
OrigTblID	原始路由表ID
OrigVrf	路由所属的原始VPN，显示为default-vrf表示公网
TableID	路由所在路由表的ID
OrigAs	初始AS号
NibID	下一跳ID
LastAs	最后AS号
AttrID	路由属性ID号
Neighbor	路由协议的邻居地址
Flags	路由标志位
OrigNextHop	此路由的下一跳地址
Label	标签
RealNextHop	路由真实下一跳
BkLabel	备份标签
BkNextHop	备份下一跳地址
SRLLabel	SR（Segment Routing）标签
BkSRLLabel	SR（Segment Routing）备份标签
Tunnel ID	（暂不支持）隧道ID
Interface	出接口，即到该目的网段的数据包将从此接口发出
BkTunnel ID	（暂不支持）备份隧道ID
BkInterface	备份出接口
FtnIndex	FTN表项索引
TrafficIndex	流量统计索引值，取值范围为1~64，N/A表示无效值
Connector	（暂不支持）表示BGP为MD VPN特性所携带的Connector属性，具体取值为BGP对等体在交换VPN-IPv4路由时携带源PE的地址，N/A表示没有该属性
VpnPeerId	路由所属的VPN peer ID值，取值范围为1~134217727，N/A表示无效值
Dscp	路由的DSCP优先级，取值范围为0~63，N/A表示无效值
Exp	（暂不支持）路由的EXP优先级（仅BGP支持），N/A表示无效值
Summary count	路由数目

1.1.4 display ip routing-table acl

display ip routing-table acl 命令用来显示通过指定 ACL 过滤的路由信息。

【命令】

```
display ip routing-table [ vpn-instance vpn-instance-name ] acl
ipv4-acl-number [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance vpn-instance-name: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

ipv4-acl-number: 基本 ACL 的编号，取值范围为 2000~2999。

verbose: 显示通过指定 ACL 过滤的所有路由的详细信息。如果未指定本参数，将只显示通过指定 ACL 过滤的激活路由的概要信息。

【使用指导】

如果用户指定的 ACL 不存在或者 ACL 中没有任何规则，将显示所有的路由信息。

【举例】

配置 ACL 2000，并设置路由过滤规则。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any
# 显示通过 ACL 2000 过滤的激活路由的概要信息。
[Sysname-acl-ipv4-basic-2000] display ip routing-table acl 2000
```

Summary count : 4

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
192.168.1.0/24	Direct	0	0	192.168.1.111	GE1/0/1
192.168.1.0/32	Direct	0	0	192.168.1.111	GE1/0/1
192.168.1.111/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.255/32	Direct	0	0	192.168.1.111	GE1/0/1

以上显示信息解释请参见 [表 1-1](#)。

显示通过 ACL 2000 过滤的所有路由的详细信息。

```
<Sysname> display ip routing-table acl 2000 verbose
```

Summary count : 4

Destination: 192.168.1.0/24

Protocol: Direct

Process ID: 0

SubProtID: 0x1

Age: 04h20m37s

Cost: 0

Preference: 0

IpPre: N/A

QosLocalID: N/A

Tag: 0

State: Active Adv

OrigTblID: 0x0

OrigVrf: default-vrf

TableID: 0x2

OrigAs: 0

NibID: 0x10000003

LastAs: 0

AttrID: 0xffffffff

Neighbor: 0.0.0.0

Flags: 0x10080

OrigNextHop: 192.168.1.111

Label: NULL

RealNextHop: 192.168.1.111

BkLabel: NULL

BkNextHop: N/A

SRLabel: NULL

BkSRLabel: NULL

Tunnel ID: Invalid

Interface: GigabitEthernet1/0/1

BkTunnel ID: Invalid

BkInterface: N/A

FtnIndex: 0x0

TrafficIndex: N/A

Connector: N/A

VpnPeerId: N/A

Dscp: N/A

Exp: N/A

Destination: 192.168.1.0/32

Protocol: Direct

Process ID: 0

SubProtID: 0x0

Age: 04h20m37s

Cost: 0

Preference: 0

IpPre: N/A

QosLocalID: N/A

Tag: 0

State: Active NoAdv

OrigTblID: 0x0

OrigVrf: default-vrf

TableID: 0x2

OrigAs: 0

NibID: 0x10000003

LastAs: 0

AttrID: 0xffffffff

Neighbor: 0.0.0.0

Flags: 0x1008c

OrigNextHop: 192.168.1.111

Label: NULL

RealNextHop: 192.168.1.111

BkLabel: NULL

BkNextHop: N/A

SRLabel: NULL

BkSRLabel: NULL

Tunnel ID: Invalid

Interface: GigabitEthernet1/0/1

BkTunnel ID: Invalid

BkInterface: N/A

FtnIndex: 0x0

TrafficIndex: N/A

Connector: N/A

VpnPeerId: N/A

Dscp: N/A

Exp: N/A

Destination: 192.168.1.111/32

Protocol: Direct

Process ID: 0

SubProtID: 0x1

Age: 04h20m37s

Cost: 0

Preference: 0

IpPre: N/A

QosLocalID: N/A


```

        Tag: 0                      State: Active NoAdv
OrigTblID: 0x0                    OrigVrf: default-vrf
TableID: 0x2                      OrigAs: 0
NibID: 0x10000000                LastAs: 0
AttrID: 0xffffffff                Neighbor: 0.0.0.0
Flags: 0x10004                   OrigNextHop: 127.0.0.1
Label: NULL                      RealNextHop: 127.0.0.1
BkLabel: NULL                    BkNextHop: N/A
SRLabel: NULL                    BkSRLabel: NULL
Tunnel ID: Invalid               Interface: InLoopBack0
BkTunnel ID: Invalid             BkInterface: N/A
FtnIndex: 0x0                    TrafficIndex: N/A
Connector: N/A                   VpnPeerId: N/A
Dscp: N/A                       Exp: N/A

Destination: 192.168.1.255/32
Protocol: Direct
Process ID: 0
SubProtID: 0x0                   Age: 04h20m37s
Cost: 0                          Preference: 0
IpPre: N/A                       QosLocalID: N/A
Tag: 0                           State: Active NoAdv
OrigTblID: 0x0                   OrigVrf: default-vrf
TableID: 0x2                     OrigAs: 0
NibID: 0x10000003               LastAs: 0
AttrID: 0xffffffff                Neighbor: 0.0.0.0
Flags: 0x1008c                   OrigNextHop: 192.168.1.111
Label: NULL                      RealNextHop: 192.168.1.111
BkLabel: NULL                    BkNextHop: N/A
SRLabel: NULL                    BkSRLabel: NULL
Tunnel ID: Invalid               Interface: GigabitEthernet1/0/1
BkTunnel ID: Invalid             BkInterface: N/A
FtnIndex: 0x0                    TrafficIndex: N/A
Connector: N/A                   VpnPeerId: N/A
Dscp: N/A                       Exp: N/A

```

以上显示信息解释请参见 [表 1-2](#)。

1.1.5 display ip routing-table ip-address

display ip routing-table ip-address 命令用来显示指定目的地址的路由信息。

display ip routing-table ip-address1 to ip-address2 命令用来显示指定目的地址范围内的路由信息。

【命令】

display ip routing-table [vpn-instance vpn-instance-name] ip-address [mask-length | mask] [longer-match] [verbose]

display ip routing-table [vpn-instance vpn-instance-name] ip-address1 to ip-address2 [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance *vpn-instance-name*: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

ip-address: 目的 IP 地址，点分十进制格式。

mask-length: 网络掩码长度，取值范围为 0~32。

mask: 网络掩码，点分十进制格式。

longer-match: 匹配掩码更长的路由。

ip-address1 to ip-address2: IP 地址范围。*ip-address1* 和 *ip-address2* 共同决定一个地址范围，只有地址在此范围内的路由才会被显示。

verbose: 显示全部路由表的详细信息，包括激活路由和未激活路由。如果未指定本参数，将显示激活路由的概要信息。

【使用指导】

使用不同的可选参数，命令的输出也不相同，以下是对该命令不同形式的输出说明：

- **display ip routing-table ip-address**
显示满足如下条件的所有激活路由：
 - 用户输入的目的 IP 地址同路由表中各条路由的子网掩码值进行与运算；
 - 路由表中各条路由的目的 IP 地址同其自身子网掩码值进行与运算；
 - 两次运算结果相同的路由条目将被显示出来。
- **display ip routing-table ip-address mask**
显示满足如下条件的所有激活路由：
 - 用户输入的目的 IP 地址同用户输入的子网掩码值进行与运算；
 - 路由表中各条路由的目的 IP 地址同用户输入的子网掩码值进行与运算；
 - 两次运算结果相同，并且掩码小于等于用户输入的子网掩码的路由条目将被显示出来。
- **display ip routing-table ip-address longer-match**
显示满足如下条件的所有激活路由：
 - 用户输入的目的 IP 地址同路由表中各条路由的子网掩码值进行与运算；
 - 路由表中各条路由的目的 IP 地址同其自身子网掩码值进行与运算；
 - 两次运算结果相同，并且子网掩码最长匹配的路由条目将被显示出来。
- **display ip routing-table ip-address mask longer-match**
显示满足如下条件的所有激活路由：

- 用户输入的目的 IP 地址同用户输入的子网掩码值进行与运算；
- 路由表中各条路由的目的 IP 地址同用户输入的子网掩码值进行与运算；
- 两次运算结果相同，掩码小于等于用户输入的子网掩码，同时子网掩码最长匹配的路由条目将被显示出来。

- **display ip routing-table ip-address1 to ip-address2**

显示 *ip-address1/32* 到 *ip-address2/32* 之间的激活路由，目的地址与掩码（32 位）同时在指定范围内才会显示。

【举例】

显示目的地址为 11.0.0.1 的路由信息。

```
<Sysname> display ip routing-table 11.0.0.1
```

Summary count : 3

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.0.0.0/8	Static	60	0	0.0.0.0	NULL0
11.0.0.0/16	Static	60	0	0.0.0.0	NULL0
11.0.0.0/24	Static	60	0	0.0.0.0	NULL0

显示目的地址/掩码为 11.0.0.1/20 的路由信息。

```
<Sysname> display ip routing-table 11.0.0.1 20
```

Summary count : 2

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.0.0.0/8	Static	60	0	0.0.0.0	NULL0
11.0.0.0/16	Static	60	0	0.0.0.0	NULL0

显示目的地址为 11.0.0.1 并且掩码最长匹配的路由信息。

```
<Sysname> display ip routing-table 11.0.0.1 longer-match
```

Summary count : 1

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.0.0.0/24	Static	60	0	0.0.0.0	NULL0

显示目的地址/掩码为 11.0.0.1/20 并且掩码最长匹配的路由信息。

```
<Sysname> display ip routing-table 11.0.0.1 20 longer-match
```

Summary count : 1

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.0.0.0/16	Static	60	0	0.0.0.0	NULL0

显示目的地址从 1.1.1.0 到 5.5.5.0 范围内的路由信息。

```
<Sysname> display ip routing-table 1.1.1.0 to 5.5.5.0
```

Summary count : 5

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
3.3.3.0/24	Direct	0	0	3.3.3.1	GE1/0/2
3.3.3.1/32	Direct	0	0	127.0.0.1	InLoop0
4.4.4.0/24	Direct	0	0	4.4.4.1	GE1/0/1
4.4.4.1/32	Direct	0	0	127.0.0.1	InLoop0

显示目的地址为 1.2.3.4 的路由的详细信息。

```
<Sysname> display ip routing-table 1.2.3.4 verbose
```

Summary count : 1

Destination: 1.2.3.4/32

Protocol: 0_INTRA

Process ID: 0

SubProtID: 0x1

Age: 00h00m37s

Cost: 0

Preference: 255

IpPre: N/A

QosLocalID: N/A

Tag: 0

State: Active Adv

OrigTblID: 0x0

OrigVrf: default-vrf

TableID: 0x2

OrigAs: 200

NibID: 0x15000000

LastAs: 200

AttrID: 0x0

Neighbor: 192.168.47.2

Flags: 0x10060

OrigNextHop: 192.168.47.2

Label: NULL

RealNextHop: 192.168.47.2

BkLabel: NULL

BkNextHop: N/A

SRLabel: NULL

BkSRLabel: NULL

Tunnel ID: Invalid

Interface: GigabitEthernet1/0/1

BkTunnel ID: Invalid

BkInterface: N/A

FtnIndex: 0x0

TrafficIndex: N/A

Connector: N/A

VpnPeerId: N/A

Dscp: N/A

Exp: N/A

以上显示信息的解释请参见 [表 1-1](#)。

1.1.6 display ip routing-table prefix-list

display ip routing-table prefix-list 命令用来显示通过指定前缀列表过滤的路由信息。

【命令】

```
display ip routing-table [ vpn-instance vpn-instance-name ] prefix-list  
prefix-list-name [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

vpn-instance vpn-instance-name: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

prefix-list-name: 前缀列表名称，为 1~63 个字符的字符串，区分大小写。

verbose: 当使用该参数时，显示通过过滤规则的所有路由的详细信息。如果未指定本参数，将只显示通过过滤规则的激活路由的概要信息。

【使用指导】

如果指定的前缀列表不存在，将显示所有的路由信息。

【举例】

配置地址前缀列表 **test** 允许前缀为 1.1.1.0，掩码长度为 24 的路由通过。

```
<Sysname> system-view
```

```
[Sysname] ip prefix-list test permit 1.1.1.0 24
```

显示通过前缀列表 **test** 过滤的激活路由的概要信息。

```
[Sysname] display ip routing-table prefix-list test
```

Summary count : 1

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.1.1.0/24	Direct	0	0	1.1.1.2	GE1/0/2

以上显示信息的解释请参见 [表 1-1](#)。

显示通过前缀列表 **test** 过滤的所有路由的详细信息。

```
[Sysname] display ip routing-table prefix-list test verbose
```

Summary count : 1

Destination: 1.1.1.0/24

Protocol: Direct

Process ID: 0

SubProtID: 0x1

Age: 04h20m37s

Cost: 0

Preference: 0

IpPre: N/A

QosLocalID: N/A

Tag: 0

State: Active Adv

OrigTblID: 0x0

OrigVrf: default-vrf

TableID: 0x2

OrigAs: 0

NibID: 0x10000003

LastAs: 0

AttrID: 0xffffffff

Neighbor: 0.0.0.0

Flags: 0x1008c

OrigNextHop: 1.1.1.2

Label: NULL

RealNextHop: 1.1.1.2

BkLabel: NULL

BkNextHop: N/A

SRLabel: NULL

BkSRLabel: NULL

Tunnel ID: Invalid

Interface: GigabitEthernet1/0/2

BkTunnel ID: Invalid

BkInterface: N/A

```
FtnIndex: 0x0          TrafficIndex: N/A
Connector: N/A         VpnPeerId: N/A
Dscp: N/A             Exp: N/A
```

以上显示信息的解释请参见 [表 1-2](#)。

1.1.7 display ip routing-table protocol

display ip routing-table protocol 命令用来显示指定协议生成或发现的路由信息。

【命令】

```
display ip routing-table [ vpn-instance vpn-instance-name ] protocol  
protocol [ inactive | verbose ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

vpn-instance vpn-instance-name: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

protocol: 显示指定路由协议的信息。

inactive: 显示未激活路由的信息。如果未指定本参数，则显示激活路由和未激活路由的信息。

verbose: 当使用该参数时，显示路由的详细信息。如果未指定本参数，将显示路由的概要信息。

【举例】

显示所有直连路由的概要信息。

```
<Sysname> display ip routing-table protocol direct
```

```
Summary count : 9
```

```
Direct Routing table status : <Active>
```

```
Summary count : 9
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.80.0/24	Direct	0	0	192.168.80.10	GE1/0/1
192.168.80.0/32	Direct	0	0	192.168.80.10	GE1/0/1

192.168.80.10/32	Direct	0	0	127.0.0.1	InLoop0
192.168.80.255/32	Direct	0	0	192.168.80.10	GE1/0/1

Direct Routing table status : <Inactive>

Summary count : 0

显示静态路由表。

<Sysname> display ip routing-table protocol static

Summary count : 1

Static Routing table status : <Active>

Summary count : 0

Static Routing table status : <Inactive>

Summary count : 1

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
3.0.0.0/8	Static	60	0	2.2.2.2	GE1/0/1

显示所有 OSPF 路由的详细信息。

<Sysname> display ip routing-table protocol ospf verbose

Summary count : 1

Destination: 1.1.1.2/32

Protocol: 0_INTRA

Process ID: 0

SubProtID: 0x6

Age: 00h03m54s

Cost: 0

Preference: 255

IpPre: N/A

QosLocalID: N/A

Tag: 0

State: Active Adv

OrigTblID: 0x0

OrigVrf: default-vrf

TableID: 0x2

OrigAs: 200

NibID: 0x16000000

LastAs: 200

AttrID: 0x0

Neighbor: 192.168.47.2

Flags: 0x10060

OrigNextHop: 192.168.47.2

Label: NULL

RealNextHop: 192.168.47.2

BkLabel: NULL

BkNextHop: N/A

SRLLabel: NULL

BkSRLLabel: NULL

Tunnel ID: Invalid

Interface: GigabitEthernet1/0/1

BkTunnel ID: Invalid

BkInterface: N/A

FtnIndex: 0x0

TrafficIndex: N/A

Connector: N/A

VpnPeerId: N/A

Dscp: N/A

Exp: N/A

以上显示信息的解释请参见 [表 1-1](#)。

1.1.8 display ip routing-table statistics

display ip routing-table statistics 命令用来显示路由表中的综合路由统计信息。综合路由统计信息包括路由总数目、路由协议添加/删除路由数目、激活路由数目。

【命令】

display ip routing-table [vpn-instance vpn-instance-name] statistics

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance vpn-instance-name: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

如果不指定任何参数时，则显示公网的信息。

【举例】

显示路由表中的综合路由统计信息。

```
<Sysname> display ip routing-table statistics
```

Total prefixes: 15 Active prefixes: 15

Proto	route	active	added	deleted
DIRECT	12	12	30	18
STATIC	3	3	5	2
RIP	0	0	0	0
OSPF	0	0	0	0
LISP	0	0	0	0
Total	15	15	35	20

表1-3 display ip routing-table statistics 命令显示信息描述表

字段	描述
Total prefixes	总的前缀数目
Active prefixes	总的激活前缀数目
Proto	路由协议
route	总的路由数目
active	活跃的、正在使用的路由数目

字段	描述
added	路由器启动后或在上一次清除路由表后，路由表中添加的路由数目
deleted	标记为删除的路由数目（此类路由在等待一段时间后会释放）
Total	各种类型路由数目的总和

1.1.9 display ip routing-table summary

display ip routing-table summary 命令用来显示路由表的概要信息，包括最大等价路由数、最大可激活路由前缀数、剩余可激活路由前缀数等。

【命令】

display ip routing-table [vpn-instance *vpn-instance-name*] summary

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance *vpn-instance-name*: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

【举例】

显示公网的路由表概要信息。

```
<Sysname> display ip routing-table summary
```

```
Max ECMP: 32
```

```
Max Active Route: 262144
```

```
Remain Active Route: 262126
```

显示 vpn1 实例的路由表概要信息。

```
<Sysname> display ip routing-table vpn-instance vpn1 summary
```

```
Max ECMP: 32
```

```
Max Active Route: 262144
```

```
Remain Active Route: 262134
```

```
Threshold value percentage of max active routes: 100%
```

表1-4 display ip routing-table summary 命令显示信息描述表

字段	描述
Max ECMP	最大等价路由数
Max Active Route	最多支持激活路由前缀数
Remain Active Route	剩余可激活路由前缀数
Threshold value of active routes alert	显示最多支持激活路由前缀数的告警门限： - 如果在 VPN 实例中配置了 routing-table limit number simply-alert 命令，则显示信息字段为 Threshold value of active routes alert，取值表示产生告警的门限值。当 VPN 实例的激活路由前缀数超过该取值时，可以继续激活新的路由前缀，但会产生 Trap 告警和日志信息 - 若在 VPN 实例中未配置 routing-table limit 命令或配置了 routing-table limit number warn-threshold 命令，则显示信息字段为 Threshold value percentage of max active routes，取值表示当（VPN 实例中的激活路由前缀数/最多支持激活路由前缀数×100）达到 warn-threshold 时，产生 Trap 告警和日志信息，但仍然允许增加激活路由前缀。当 VPN 实例中的激活路由前缀数达到最多支持激活路由前缀数目时，不再激活新的路由前缀

1.1.10 display ipv6 rib graceful-restart

display ipv6 rib graceful-restart 命令用来显示 IPv6 RIB 的 GR 状态信息。

【命令】

display ipv6 rib graceful-restart

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 IPv6 RIB 的 GR 状态信息。

```
<Sysname> display ipv6 rib graceful-restart
RIB GR state      : Phase2-calculation end
RCOM GR state     : Flush end
Protocol GR state:
No.  Protocol    Lifetime FD   State   Start/End
-----
1    DIRECT6      480        29    End     No/No
2    STATIC6      480        32    End     No/No
3    ISISV6       480        30    End     No/No
```

以上显示信息的解释请参见 [表 1-8](#)。

1.1.11 display ipv6 rib nib

display ipv6 rib nib 命令用来显示 IPv6 RIB 的下一跳信息。

【命令】

```
display ipv6 rib nib [ self-originated ] [ nib-id ] [ verbose ]
display ipv6 rib nib protocol protocol [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

self-originated: 路由管理自己生成的下一跳。

nib-id: 路由下一跳 ID 值，取值范围为十六进制数 1~ffffff。

verbose: 显示详细信息。如果未指定本参数，则显示概要信息。

protocol protocol: 显示指定路由协议的下一跳信息。

【举例】

显示 IPv6 RIB 的下一跳信息。

```
<Sysname> display ipv6 rib nib
Total number of nexthop(s): 151
```

```
      NibID: 0x20000000      Sequence: 0
      Type: 0x1              Flushed: Yes
      UserKey0: 0x0          VrfNthp: 0
      UserKey1: 0x0          Nexthop: ::
      IFIndex: 0x111         LocalAddr: ::
      TopoNthp: Invalid
```

```
      NibID: 0x20000001      Sequence: 1
      Type: 0x1              Flushed: Yes
      UserKey0: 0x0          VrfNthp: 0
      UserKey1: 0x0          Nexthop: ::1
      IFIndex: 0x112         LocalAddr: ::1
      TopoNthp: Invalid
```

.....（省略部分显示信息）

显示 IPv6 RIB 下一跳的详细信息。

```
<Sysname> display ipv6 rib nib verbose
```

Total number of nexthop(s): 151

NibID: 0x20000000 Sequence: 0
Type: 0x1 Flushed: Yes
UserKey0: 0x0 VrfNthp: 0
UserKey1: 0x0 Nexthop: ::
IFIndex: 0x111 LocalAddr: ::
TopoNthp: Invalid
RefCnt: 4 FlushRefCnt: 1
Flag: 0x84 Version: 1
1 nexthop(s):
PrefixIndex: 0 OrigNexthop: ::
RelyDepth: 0 RealNexthop: ::
Interface: NULL0 LocalAddr: ::
TunnelCnt: 0 Vrf: default-vrf
TunnelID: N/A Topology:
Weight: 0

NibID: 0x20000001 Sequence: 1
Type: 0x1 Flushed: Yes
UserKey0: 0x0 VrfNthp: 0
UserKey1: 0x0 Nexthop: ::1
IFIndex: 0x112 LocalAddr: ::1
TopoNthp: Invalid
RefCnt: 4 FlushRefCnt: 1
Flag: 0x84 Version: 1
1 nexthop(s):
PrefixIndex: 0 OrigNexthop: ::1
RelyDepth: 0 RealNexthop: ::1
Interface: InLoop0 LocalAddr: ::1
TunnelCnt: 0 Vrf: default-vrf
TunnelID: N/A Topology:
Weight: 0

NibID: 0x26000001 Sequence: 1
Type: 0x1 Flushed: Yes
UserKey0: 0x0 VrfNthp: 0
UserKey1: 0x0 Nexthop: 121::2
IFIndex: 0x112 LocalAddr: ::
TopoNthp: Invalid
Instance: default

NibID: 0x26000002 Sequence: 1
Type: 0x1 Flushed: Yes
UserKey0: 0x0 VrfNthp: 0
UserKey1: 0x0 Nexthop: 122::2
IFIndex: 0x112 LocalAddr: ::
TopoNthp: Invalid

Instance: abc

..... (省略部分显示信息)

以上显示信息的解释请参见 [表 1-9](#) 和 [表 1-10](#)。

1.1.12 display ipv6 route-direct nib

display ipv6 route-direct nib 命令用来显示 IPv6 直连路由下一跳信息。

【命令】

display ipv6 route-direct nib [*nib-id*] [*verbose*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

nib-id: 路由邻居 ID 值，取值范围为十六进制数 1~ffffff。

verbose: 显示详细信息。如果未指定本参数，则显示概要信息。

【举例】

显示 IPv6 直连路由下一跳信息。

```
<Sysname> display ipv6 route-direct nib
Total number of nexthop(s): 115
```

NibID: 0x20000000	Sequence: 0
Type: 0x1	Flushed: Yes
UserKey0: 0x0	VrfNthp: 0
UserKey1: 0x0	Nexthop: ::
IFIndex: 0x111	LocalAddr: ::
TopoNthp: Invalid	

NibID: 0x20000001	Sequence: 1
Type: 0x1	Flushed: Yes
UserKey0: 0x0	VrfNthp: 0
UserKey1: 0x0	Nexthop: ::1
IFIndex: 0x112	LocalAddr: ::1
TopoNthp: Invalid	

..... (省略部分显示信息)

显示 IPv6 直连路由下一跳详细信息。

```
<Sysname> display ipv6 route-direct nib verbose
Total number of nexthop(s): 115
```

```

        NibID: 0x20000000      Sequence: 0
        Type: 0x1              Flushed: Yes
    UserKey0: 0x0              VrfNthp: 0
    UserKey1: 0x0              Nexthop: ::
    IFIndex: 0x111            LocalAddr: ::
    RefCnt: 1                  FlushRefCnt: 0
    Flag: 0x2                  Version: 1
1 nexthop(s):
PrefixIndex: 0                OrigNexthop: ::
RelyDepth: 0                  RealNexthop: ::
Interface: NULL0              LocalAddr: ::
TunnelCnt: 0                  Vrf: default-vrf
TunnelID: N/A                 Topology:
Weight: 0

```

```

        NibID: 0x20000001      Sequence: 1
        Type: 0x1              Flushed: Yes
    UserKey0: 0x0              VrfNthp: 0
    UserKey1: 0x0              Nexthop: ::1
    IFIndex: 0x112            LocalAddr: ::1
    RefCnt: 1                  FlushRefCnt: 0
    Flag: 0x2                  Version: 1
1 nexthop(s):
PrefixIndex: 0                OrigNexthop: ::1
RelyDepth: 0                  RealNexthop: ::1
Interface: InLoop0            LocalAddr: ::1
TunnelCnt: 0                  Vrf: default-vrf
TunnelID: N/A                 Topology:
Weight: 0

```

.....（省略部分显示信息）

以上显示信息的解释请参见 [表 1-11](#) 和 [表 1-12](#)。

1.1.13 display ipv6 routing-table

display ipv6 routing-table 命令用来显示 IPv6 路由表的信息。

【命令】

display ipv6 routing-table [*vpn-instance vpn-instance-name*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin

```

context-operator

【参数】

vpn-instance *vpn-instance-name*: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

verbose: 显示 IPv6 路由表的详细信息，包括激活路由和未激活路由。如果未指定本参数，将显示激活路由的概要信息。

【使用指导】

如果不指定任何参数时，则显示公网的信息。

【举例】

```
# 显示当前路由表的概要信息。
<Sysname> display ipv6 routing-table

Destinations : 2 Routes : 2

Destination: ::1/128                Protocol : Direct
NextHop      : ::1                  Preference: 0
Interface    : InLoop0              Cost      : 0

Destination: FE80::/10               Protocol : Direct
NextHop      : ::                   Preference: 0
Interface    : InLoop0              Cost      : 0
```

表1-5 display ipv6 routing-table 命令显示信息描述表

字段	描述
Destinations	目的地址个数
Routes	路由条数
Destination	目的网络/主机的IPv6地址和前缀
NextHop	下一跳地址
Preference	路由优先级
Interface	出接口，即到该目的地址的数据包将从此接口发出
Protocol	发现该路由的路由协议类型
Cost	路由的开销值
Summary count	路由数目

```
# 显示路由表的详细路由信息。
<Sysname> display ipv6 routing-table verbose

Destinations : 2 Routes : 2

Destination: ::1/128
```

```

Protocol: Direct
Process ID: 0
SubProtID: 0x0                                Age: 19h23m02s
Cost: 0                                         Preference: 0
IpPre: N/A                                    QosLocalID: N/A
Tag: 0                                         State: Active NoAdv
OrigTblID: 0x0                                OrigVrf: default-vrf
TableID: 0xa                                  OrigAs: 0
NibID: 0x20000000                             LastAs: 0
AttrID: 0xffffffff                           Neighbor: ::
Flags: 0x10004                                OrigNextHop: ::1
Label: NULL                                   RealNextHop: ::1
BkLabel: NULL                                 BkNextHop: N/A
SRLabel: NULL                                BkSRLabel: NULL
Tunnel ID: Invalid                            Interface: InLoopBack0
BkTunnel ID: Invalid                          BkInterface: N/A
FtnIndex: 0x0                                TrafficIndex: N/A
Connector: N/A                                VpnPeerId: N/A
Dscp: N/A                                     Exp: N/A

Destination: 12::/96
Protocol: Direct
Process ID: 0
SubProtID: 0x0                                Age: 00h01m47s
Cost: 0                                         Preference: 0
IpPre: N/A                                    QosLocalID: N/A
Tag: 0                                         State: Active Adv
OrigTblID: 0x0                                OrigVrf: default-vrf
TableID: 0xa                                  OrigAs: 0
NibID: 0x20000003                             LastAs: 0
AttrID: 0xffffffff                           Neighbor: ::
Flags: 0x10080                                OrigNextHop: ::
Label: NULL                                   RealNextHop: ::
BkLabel: NULL                                 BkNextHop: N/A
SRLabel: NULL                                BkSRLabel: NULL
Tunnel ID: Invalid                            Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid                          BkInterface: N/A
FtnIndex: 0x0                                TrafficIndex: N/A
Connector: N/A                                VpnPeerId: N/A
Dscp: N/A                                     Exp: N/A

```

表1-6 display ipv6 routing-table verbose 命令显示信息描述表

字段	描述
Destination	目的网络/主机的IPv6地址和前缀
Protocol	发现该路由的路由协议类型
Process ID	进程号
SubProtID	路由子协议ID

字段	描述
Age	此路由在路由表中存在的时间
Cost	路由的度量值
Preference	路由的优先级
IpPre	IP优先级值
QoSLocalID	（暂不支持）QoS本地ID
Tag	路由标记
State	路由状态描述： • Active: 有效的单播路由 • Adv: 允许对外发送的路由 • Inactive: 非激活路由标志 • NoAdv: 不允许发布的路由 • Vrrp: VRRP 产生的路由（暂不支持） • Nat: NAT 产生的路由（暂不支持） • TunE: Tunnel 隧道的标志（暂不支持）
OrigTblID	原始路由表ID
OrigVrf	路由所属的原始VPN，显示为default-vrf表示公网
TableID	路由所在路由表的ID
OrigAs	初始AS号
NibID	下一跳ID
LastAs	最后AS号
AttrID	路由属性ID号
Neighbor	路由协议的邻居地址
Flags	路由标志位
OrigNextHop	此路由的下一跳地址
Label	标签
RealNextHop	路由真实下一跳
BkLabel	备份标签
BkNextHop	备份下一跳地址
SRLabel	SR（Segment Routing）标签
BkSRLabel	SR（Segment Routing）备份标签
Tunnel ID	（暂不支持）隧道ID
Interface	出接口，即到该目的网段的数据包将从此接口发出
BkTunnel ID	（暂不支持）备份隧道ID
BkInterface	备份出接口

字段	描述
FtnIndex	FTN表项索引
TrafficIndex	流量统计索引值，取值范围为1~64，N/A表示无效值
Connector	（暂不支持）表示BGP为MD VPN特性所携带的Connector属性，具体取值为BGP对等体在交换VPN-IPv4路由时携带源PE的地址，N/A表示没有该属性
VpnPeerId	路由所属的VPN peer ID值，取值范围为1~134217727，N/A表示无效值
Dscp	路由的DSCP优先级，取值范围为0~63，N/A表示无效值
Exp	（暂不支持）路由的EXP优先级（仅BGP支持），N/A表示无效值
Summary count	路由数目

1.1.14 display ipv6 routing-table acl

display ipv6 routing-table acl 命令用来显示通过指定 IPv6 ACL 过滤的 IPv6 路由信息。

【命令】

```
display ipv6 routing-table [ vpn-instance vpn-instance-name ] acl
ipv6-acl-number [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

vpn-instance *vpn-instance-name*: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

ipv6-acl-number: 基本 IPv6 ACL 编号，取值范围为 2000~2999。

verbose: 显示通过指定 IPv6 ACL 过滤的所有路由的详细信息。如果未指定本参数，只显示通过 IPv6 ACL 过滤的激活路由的概要信息。

【使用指导】

如果指定的 IPv6 ACL 不存在或者 IPv6 ACL 中没有任何规则，将显示所有的 IPv6 路由信息。

【举例】

显示通过 IPv6 ACL 2000 过滤的激活路由的概要信息。

```
<Sysname> display ipv6 routing-table acl 2000
```

```
Summary count : 6
```

Destination : ::1/128	Protocol : Direct
NextHop : ::1	Preference: 0
Interface : InLoop0	Cost : 0
Destination: 12::/96	Protocol : Direct
NextHop : ::	Preference: 0
Interface : GE1/0/2	Cost : 0
Destination: 12::1/128	Protocol : Direct
NextHop : ::1	Preference: 0
Interface : InLoop0	Cost : 0
Destination: FF::11/128	Protocol : 0_INTER
NextHop : 12::2	Preference: 255
Interface : GE1/0/2	Cost : 0
Destination: FE80::/10	Protocol : Direct
NextHop : ::	Preference: 0
Interface : InLoop0	Cost : 0
Destination: FF00::/8	Protocol : Direct
NextHop : ::	Preference: 0
Interface : NULL0	Cost : 0

以上显示信息的解释请参见 [表 1-5](#)。

显示通过 IPv6 ACL 2000 过滤的所有路由的详细信息。

<Sysname> display ipv6 routing-table acl 2000 verbose

Summary count : 6

Destination: ::1/128	
Protocol: Direct	
Process ID: 0	
SubProtID: 0x0	Age: 19h29m12s
Cost: 0	Preference: 0
IpPre: N/A	QosLocalID: N/A
Tag: 0	State: Active NoAdv
OrigTblID: 0x0	OrigVrf: default-vrf
TableID: 0xa	OrigAs: 0
NibID: 0x20000000	LastAs: 0
AttrID: 0xffffffff	Neighbor: ::
Flags: 0x10004	OrigNextHop: ::1
Label: NULL	RealNextHop: ::1
BkLabel: NULL	BkNextHop: N/A
SRLabel: NULL	BkSRLabel: NULL
Tunnel ID: Invalid	Interface: InLoopBack0
BkTunnel ID: Invalid	BkInterface: N/A
FtnIndex: 0x0	TrafficIndex: N/A

Connector: N/A	VpnPeerId: N/A
Dscp: N/A	Exp: N/A

Destination: 12::/96

Protocol: Direct

Process ID: 0

SubProtID: 0x0	Age: 00h07m57s
Cost: 0	Preference: 0
IpPre: N/A	QosLocalID: N/A
Tag: 0	State: Active Adv
OrigTblID: 0x0	OrigVrf: default-vrf
TableID: 0xa	OrigAs: 0
NibID: 0x20000003	LastAs: 0
AttrID: 0xffffffff	Neighbor: ::
Flags: 0x10080	OrigNextHop: ::
Label: NULL	RealNextHop: ::
BkLabel: NULL	BkNextHop: N/A
SRLabel: NULL	BkSRLabel: NULL
Tunnel ID: Invalid	Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid	BkInterface: N/A
FtnIndex: 0x0	TrafficIndex: N/A
Connector: N/A	VpnPeerId: N/A
Dscp: N/A	Exp: N/A

Destination: 12::1/128

Protocol: Direct

Process ID: 0

SubProtID: 0x0	Age: 00h07m55s
Cost: 0	Preference: 0
IpPre: N/A	QosLocalID: N/A
Tag: 0	State: Active NoAdv
OrigTblID: 0x0	OrigVrf: default-vrf
TableID: 0xa	OrigAs: 0
NibID: 0x20000000	LastAs: 0
AttrID: 0xffffffff	Neighbor: ::
Flags: 0x10004	OrigNextHop: ::1
Label: NULL	RealNextHop: ::1
BkLabel: NULL	BkNextHop: N/A
SRLabel: NULL	BkSRLabel: NULL
Tunnel ID: Invalid	Interface: InLoopBack0
BkTunnel ID: Invalid	BkInterface: N/A
FtnIndex: 0x0	TrafficIndex: N/A
Connector: N/A	VpnPeerId: N/A
Dscp: N/A	Exp: N/A

Destination: FF::11/128

Protocol: 0_INTER

Process ID: 0

SubProtID: 0x6	Age: 00h06m43s

Cost: 0	Preference: 255
IpPre: N/A	QosLocalID: N/A
Tag: 0	State: Active Adv
OrigTblID: 0x0	OrigVrf: default-vrf
TableID: 0xa	OrigAs: 200
NibID: 0x26000000	LastAs: 200
AttrID: 0x1	Neighbor: 12::2
Flags: 0x10060	OrigNextHop: 12::2
Label: NULL	RealNextHop: 12::2
BkLabel: NULL	BkNextHop: N/A
SRLabel: NULL	BkSRLabel: NULL
Tunnel ID: Invalid	Interface: GigabitEthernet1/0/2
BkTunnel ID: Invalid	BkInterface: N/A
FtnIndex: 0x0	TrafficIndex: N/A
Connector: N/A	VpnPeerId: N/A
Dscp: N/A	Exp: N/A

Destination: FE80::/10

Protocol: Direct

Process ID: 0

SubProtID: 0x0

Age: 19h29m12s

Cost: 0

Preference: 0

IpPre: N/A

QosLocalID: N/A

Tag: 0

State: Active NoAdv

OrigTblID: 0x0

OrigVrf: default-vrf

TableID: 0xa

OrigAs: 0

NibID: 0x20000002

LastAs: 0

AttrID: 0xffffffff

Neighbor: ::

Flags: 0x10084

OrigNextHop: ::

Label: NULL

RealNextHop: ::

BkLabel: NULL

BkNextHop: N/A

SRLabel: NULL

BkSRLabel: NULL

Tunnel ID: Invalid

Interface: InLoopBack0

BkTunnel ID: Invalid

BkInterface: N/A

FtnIndex: 0x0

TrafficIndex: N/A

Connector: N/A

VpnPeerId: N/A

Dscp: N/A

Exp: N/A

Destination: FF00::/8

Protocol: Direct

Process ID: 0

SubProtID: 0x0

Age: 19h29m12s

Cost: 0

Preference: 0

IpPre: N/A

QosLocalID: N/A

Tag: 0

State: Active NoAdv

OrigTblID: 0x0

OrigVrf: default-vrf

TableID: 0xa

OrigAs: 0

NibID: 0x20000001

LastAs: 0

AttrID: 0xffffffff

Neighbor: ::

Flags: 0x10014	OrigNextHop: ::
Label: NULL	RealNextHop: ::
BkLabel: NULL	BkNextHop: N/A
SRLabel: NULL	BkSRLabel: NULL
Tunnel ID: Invalid	Interface: NULL0
BkTunnel ID: Invalid	BkInterface: N/A
FtnIndex: 0x0	TrafficIndex: N/A
Connector: N/A	VpnPeerId: N/A
Dscp: N/A	Exp: N/A

以上显示信息的解释请参见 [表 1-6](#)。

1.1.15 display ipv6 routing-table ipv6-address

display ipv6 routing-table ipv6-address 命令用来显示指定目的地址的 IPv6 路由信息。

display ipv6 routing-table ipv6-address1 to ipv6-address2 命令用来显示指定目的地址范围内的 IPv6 路由信息。

【命令】

display ipv6 routing-table [vpn-instance *vpn-instance-name*] *ipv6-address*
[*prefix-length*] [**longer-match**] [**verbose**]

display ipv6 routing-table [vpn-instance *vpn-instance-name*] *ipv6-address1*
to ipv6-address2 [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance *vpn-instance-name*: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

ipv6-address: IPv6 目的地址。

prefix-length: 前缀长度，取值范围为 0~128。

longer-match: 匹配并显示前缀最长的路由条目。

ipv6-address1 to ipv6-address2: IPv6 地址范围。*ipv6-address1* 和 *ipv6-address2* 共同决定一个地址范围，只有地址在此范围内的路由才会被显示。

verbose: 显示激活和未激活路由的详细信息。如果未指定本参数，将显示激活路由的概要信息。

【使用指导】

使用不同的可选参数，命令的输出也不相同，以下是对该命令不同形式的输出说明：

- **display ipv6 routing-table ipv6-address**
显示满足如下条件的所有激活路由：
 - 用户输入的目的 IPv6 地址同路由表中各条路由的前缀长度值进行与运算；
 - 路由表中各条路由的目的 IPv6 地址同其自身前缀长度值进行与运算；
 - 两次运算结果相同的路由条目将被显示出来。
- **display ipv6 routing-table ipv6-address prefix-length**
显示满足如下条件的所有激活路由：
 - 用户输入的目的 IPv6 地址同用户输入的前缀长度值进行与运算；
 - 路由表中各条路由的目的 IPv6 地址同用户输入的前缀长度值进行与运算；
 - 两次运算结果相同，并且路由表中前缀长度小于等于用户输入的前缀长度的路由条目将被显示出来。
- **display ipv6 routing-table ipv6-address longer-match**
显示满足如下条件的所有激活路由：
 - 用户输入的目的 IPv6 地址同路由表中各条路由的前缀长度值进行与运算；
 - 路由表中各条路由的目的 IPv6 地址同其自身前缀长度值进行与运算；
 - 两次运算结果相同，同时前缀长度最长匹配的路由条目将被显示出来。
- **display ipv6 routing-table ipv6-address prefix-length longer-match**
显示满足如下条件的所有激活路由：
 - 用户输入的目的 IPv6 地址同用户输入的前缀长度值进行与运算；
 - 路由表中各条路由的目的 IPv6 地址同用户输入的前缀长度值进行与运算；
 - 两次运算结果相同，路由表中前缀长度小于等于用户输入的前缀长度，同时前缀长度最长匹配的路由条目将被显示出来。
- **display ipv6 routing-table ipv6-address1 to ipv6-address2**
显示 *ipv6-address1/128* 到 *ipv6-address2/128* 之间的路由，目的 IPv6 地址与前缀长度（128 位）同时在指定范围内才会显示。

【举例】

显示目的 IPv6 地址/前缀为 10::1/127 的 IPv6 路由信息。

```
<Sysname> display ipv6 routing-table 10::1 127
```

```
Summary count: 3
```

Destination: 10::/64	Protocol : Static
NextHop : ::	Preference: 60
Interface : NULL0	Cost : 0

Destination: 10::/68	Protocol : Static
NextHop : ::	Preference: 60
Interface : NULL0	Cost : 0

Destination: 10::/120	Protocol : Static
NextHop : ::	Preference: 60

Interface : NULL0 Cost : 0

显示目的 IPv6 地址/前缀为 10::1/127 并且掩码最长匹配的 IPv6 路由信息。

<Sysname> display ipv6 routing-table 10::1 127 longer-match

Summary count : 1

Destination: 10::/120	Protocol : Static
NextHop : ::	Preference: 60
Interface : NULL0	Cost : 0

显示目的 IPv6 地址从 100::到 300::范围内的 IPv6 路由信息。

<Sysname> display ipv6 routing-table 100:: to 300::

Summary count : 3

Destination: 100::/64	Protocol : Static
NextHop : ::	Preference: 60
Interface : NULL0	Cost : 0

Destination: 200::/64	Protocol : Static
NextHop : ::	Preference: 60
Interface : NULL0	Cost : 0

Destination: 300::/64	Protocol : Static
NextHop : ::	Preference: 60
Interface : NULL0	Cost : 0

显示目的 IPv6 地址/前缀为 1:2::3:4/128 的 IPv6 路由的详细信息。

<Sysname> display ipv6 routing-table 1:2::3:4 128 verbose

Summary count : 1

Destination: 1:2::3:4/128

Protocol: 0_INTER

Process ID: 0

SubProtID: 0x1 Age: 00h01m14s

Cost: 0 Preference: 255

IpPre: N/A QoSLocalID: N/A

Tag: 0 State: Active Adv

OrigTblID: 0x0 OrigVrf: default-vrf

TableID: 0x1 OrigAs: 200

NibID: 0x26000000 LastAs: 200

AttrID: 0x0 Neighbor: 2:2::3:4

Flags: 0x10060 OrigNextHop: 2:2::3:4

Label: NULL RealNextHop: 2:2::3:4

BkLabel: NULL BkNextHop: N/A

SRLabel: NULL BkSRLabel: NULL

Tunnel ID: Invalid Interface: GigabitEthernet1/0/1

BkTunnel ID: Invalid BkInterface: N/A

FtnIndex: 0x0 TrafficIndex: N/A

Connector: N/A VpnPeerId: N/A
Dscp: N/A Exp: N/A

以上显示信息的解释请参见 [表 1-5](#)。

1.1.16 display ipv6 routing-table prefix-list

display ipv6 routing-table prefix-list 命令用来显示通过指定前缀列表过滤的 IPv6 路由信息。

【命令】

display ipv6 routing-table [vpn-instance vpn-instance-name] prefix-list prefix-list-name [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance vpn-instance-name: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

prefix-list-name: IPv6 前缀列表的名称，为 1~63 个字符的字符串，区分大小写。

verbose: 显示所有路由的详细信息。如果未指定本参数，只显示激活路由的概要信息。

【使用指导】

如果指定的前缀列表不存在，将显示所有的路由信息。

【举例】

配置地址前缀列表 test 允许前缀为::1，前缀长度为 128 的 IPv6 路由通过。

```
<Sysname> system-view
```

```
[Sysname] ipv6 prefix-list test permit ::1 128
```

显示通过前缀列表 test 过滤的 IPv6 激活路由的概要信息。

```
[Sysname] display ipv6 routing-table prefix-list test
```

```
Summary count : 1
```

```
Destination: ::1/128
```

```
Protocol : Direct
```

```
NextHop : ::1
```

```
Preference: 0
```

```
Interface : InLoop0
```

```
Cost : 0
```

以上显示信息的解释请参见 [表 1-5](#)。

显示通过前缀列表 test 过滤的所有 IPv6 路由的详细信息。

```
[Sysname] display ipv6 routing-table prefix-list test verbose
```

Summary count : 1

Destination: ::1/128
Protocol: Direct
Process ID: 0
SubProtID: 0x0 Age: 08h57m19s
Cost: 0 Preference: 0
IpPre: N/A QosLocalID: N/A
Tag: 0 State: Active NoAdv
OrigTblID: 0x0 OrigVrf: default-vrf
TableID: 0xa OrigAs: 0
NibID: 0x20000000 LastAs: 0
AttrID: 0xffffffff Neighbor: ::
Flags: 0x10004 OrigNextHop: ::1
Label: NULL RealNextHop: ::1
BkLabel: NULL BkNextHop: N/A
SRLabel: NULL BkSRLabel: NULL
Tunnel ID: Invalid Interface: InLoopBack0
BkTunnel ID: Invalid BkInterface: N/A
FtnIndex: 0x0 TrafficIndex: N/A
Connector: N/A VpnPeerId: N/A
Dscp: N/A Exp: N/A

以上显示信息的解释请参见 [表 1-6](#)。

1.1.17 display ipv6 routing-table protocol

display ipv6 routing-table protocol 命令用来显示指定协议生成或发现的 IPv6 路由信息。

【命令】

display ipv6 routing-table [vpn-instance *vpn-instance-name*] protocol *protocol* [inactive | verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance *vpn-instance-name*: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

protocol: 显示指定路由协议的信息。

inactive: 如果配置了该参数，此命令只显示未激活路由信息。如果未指定本参数，将显示所有激活和未激活路由信息。

verbose: 显示激活和未激活路由的详细信息。如果未指定本参数，将显示路由的概要信息。

【举例】

显示所有 IPv6 直连路由的概要信息。

```
<Sysname> display ipv6 routing-table protocol direct
```

```
Summary count : 3
```

```
Direct Routing table status : <Active>
```

```
Summary count : 3
```

Destination: ::1/128	Protocol : Direct
NextHop : ::1	Preference: 0
Interface : InLoop0	Cost : 0

Destination: FE80::/10	Protocol : Direct
NextHop : ::	Preference: 0
Interface : InLoop0	Cost : 0

Destination: FF00::/8	Protocol : Direct
NextHop : ::	Preference: 0
Interface : NULL0	Cost : 0

```
Direct Routing table status : <Inactive>
```

```
Summary count : 0
```

显示 IPv6 静态路由表。

```
<Sysname> display ipv6 routing-table protocol static
```

```
Summary count : 3
```

```
Static Routing table status : <Active>
```

```
Summary count : 3
```

Destination: 2::2/128	Protocol : Static
NextHop : fe80::2	Preference: 60
Interface : GE1/0/2	Cost : 0

Destination: 2::2/128	Protocol : Static
NextHop : fe80::3	Preference: 60
Interface : GE1/0/2	Cost : 0

Destination: 3::3/128	Protocol : Static
NextHop : 2::2	Preference: 60
Interface : GE1/0/2	Cost : 0

```

Static Routing table status : <Inactive>
Summary count : 0
# 显示所有 OSPFv3 路由的详细信息。
<Sysname> display ipv6 routing-table protocol ospfv3 verbose

Summary count : 1

Destination: 22::22/128
  Protocol: O_INTER
  Process ID: 0
  SubProtID: 0x6                      Age: 00h04m15s
    Cost: 0                          Preference: 255
    IpPre: N/A                       QosLocalID: N/A
    Tag: 0                           State: Active Adv
  OrigTblID: 0x0                      OrigVrf: default-vrf
  TableID: 0xa                       OrigAs: 200
  NibID: 0x25000001                 LastAs: 200
  AttrID: 0x3                       Neighbor: 121::2
  Flags: 0x10060                    OrigNextHop: 121::2
  Label: NULL                       RealNextHop: 121::2
  BkLabel: NULL                     BkNextHop: N/A
  SRLabel: NULL                     BkSRLabel: NULL
  Tunnel ID: Invalid                Interface: GigabitEthernet1/0/1
  BkTunnel ID: Invalid              BkInterface: N/A
  FtnIndex: 0x0                     TrafficIndex: N/A
  Connector: N/A                    VpnPeerId: N/A
  Dscp: N/A                         Exp: N/A

```

以上显示信息的解释请参见 [表 1-5](#)。

1.1.18 display ipv6 routing-table statistics

display ipv6 routing-table statistics 命令用来显示 IPv6 路由表中的综合路由统计信息。综合路由统计信息包括路由总数、路由协议添加/删除路由数目、激活路由数目。

【命令】

display ipv6 routing-table [vpn-instance *vpn-instance-name*] statistics

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

vpn-instance *vpn-instance-name*: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

如果不指定任何参数时，则显示公网的信息。

【举例】

显示综合路由统计信息。

```
<Sysname> display ipv6 routing-table statistics
```

Total prefixes: 8 Active prefixes: 8

Proto	route	active	added	deleted
DIRECT	5	5	5	0
STATIC	3	3	3	0
RIPng	0	0	0	0
OSPFv3	0	0	0	0
LISP	0	0	0	0
Total	8	8	8	0

表1-7 display ipv6 routing-table statistics 命令显示信息描述表

字段	描述
Total prefixes	总的前缀数目
Active prefixes	总的激活前缀数目
Proto	路由协议
route	总的路由数目
active	激活的、正在使用的路由数目
added	路由器启动后或在上一次清除路由表后，路由表中添加的路由数目
deleted	标记为删除的路由数目（此类路由在等待一段时间后会释放）
Total	各种类型路由数目的总和

1.1.19 display ipv6 routing-table summary

display ipv6 routing-table summary 命令用来显示 IPv6 路由表的概要信息，包括最大等价路由数、最大可激活路由前缀数、剩余可激活路由前缀数等。

【命令】

display ipv6 routing-table [vpn-instance *vpn-instance-name*] summary

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance vpn-instance-name: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

【举例】

显示公网的路由表概要信息。

```
<Sysname> display ipv6 routing-table summary
```

```
Max ECMP: 32  
Max Active Route: 262144  
Remain Active Route: 262126
```

显示实例 vpn1 的路由表概要信息。

```
<Sysname> display ipv6 routing-table vpn-instance vpn1 summary
```

```
Max ECMP: 32  
Max Active Route: 262144  
Remain Active Route: 262134  
Threshold value of active routes alert: 65100
```

以上显示信息的解释请参见 [表 1-4](#)。

1.1.20 display rib graceful-restart

display rib graceful-restart 命令用来显示 RIB 的 GR 状态信息。

【命令】

display rib graceful-restart

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 RIB 的 GR 状态信息。

```
<Sysname> display rib graceful-restart
```

```
RIB GR state      : Phase2-calculation end
RCOM GR state     : Flush end
Protocol GR state:
No.  Protocol  Lifetime FD   State   Start/End
-----
1    DIRECT    100      30    End     No/No
2    STATIC    480      34    End     No/No
3    OSPF      480      36    End     No/No
4    ISIS      480      32    End     No/No
```

表1-8 display rib graceful-restart 命令显示信息描述表

字段	描述
RIB GR state	RIB GR状态: - Start: 协议 GR 开始 - IGP end: 所有 IGP 协议 GR 结束 - VPN-triggering end: VPN 路由触发优选结束 - VPN-calculation end: VPN 路由优选结束 - Routing protocol end: 所有路由协议 GR 结束 - NSR-calculation unfinished: NSR 优选未完成状态 - Triggering start: 所有路由触发优选开始 - Triggering end: 所有路由触发优选结束 - Phase1-calculation end: 第一阶段优选结束 - All end: 所有协议 GR 结束 - Phase2-calculation end: 第二阶段优选结束
RCOM GR state	RCOM GR状态: - Start: 协议 GR 开始 - VPN-calculation end: VPN 路由优选结束 - VPN-notification end: VPN 路由上报结束 - Routing protocol end: 所有路由协议 GR 结束 - NSR-calculation unfinished: NSR 优选未完成状态 - Phase1-calculation end: 第一阶段优选结束 - Notification end: 所有路由上报结束 - Phase2-calculation end: 第二阶段优选结束 - Flush start: 开始下刷 FIB - Flush end: 下刷 FIB 结束
Protocol GR state	协议GR状态
No.	编号
Protocol	协议名称
Lifetime	倒换过程中协议的路由信息/标签信息在RIB中的存活时间，单位为秒
FD	协议进程与RIB连接的句柄

字段	描述
State	协议GR状态： • Init: 协议 GR 初始化状态 • Listen: 协议 GR 监听状态 • Idle: 协议 GR 空闲状态 • Active: 协议 GR 激活状态 • Start: 协议 GR 开始状态 • End: 协议 GR 结束状态
Start/End	• No: 表示该消息未发送 • Yes: 表示该消息已发送

1.1.21 display rib nib

display rib nib 命令用来显示 RIB 的下一跳信息。

【命令】

```
display rib nib [ self-originated ] [ nib-id ] [ verbose ]
display rib nib protocol protocol [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

self-originated: 路由管理自己生成的下一跳信息。

nib-id: 路由下一跳信息的 ID 值，取值范围为十六进制数 1~ffffff。

verbose: 显示详细信息。如果未指定本参数，则显示概要信息。

protocol protocol: 显示指定路由协议生成的下一跳信息。

【举例】

显示 RIB 的下一跳信息。

```
<Sysname> display rib nib
```

```
Total number of nexthop(s): 176
```

```

      NibID: 0x10000000      Sequence: 0
      Type: 0x1              Flushed: Yes
      UserKey0: 0x0          VrfNthp: 0
      UserKey1: 0x0          Nexthop: 0.0.0.0
```



```

    IFIndex: 0x111          LocalAddr: 0.0.0.0
    TopoNthp: 0

    NibID: 0x10000001      Sequence: 1
    Type: 0x1              Flushed: Yes
    UserKey0: 0x0           VrfNthp: 0
    UserKey1: 0x0           Nexthop: 127.0.0.1
    IFIndex: 0x112         LocalAddr: 127.0.0.1
    TopoNthp: 0

    NibID: 0x10000002      Sequence: 2
    Type: 0x5              Flushed: Yes
    UserKey0: 0x0           VrfNthp: 0
    UserKey1: 0x0           Nexthop: 127.0.0.1
    IFIndex: 0x112         LocalAddr: 127.0.0.1
    TopoNthp: 0

    NibID: 0x16000000      Sequence: 3
    Type: 0x21             Flushed: No
    UserKey0: 0x0           VrfNthp: 0
    UserKey1: 0x0           Nexthop: 12.1.1.2
    IFIndex: 0x0            LocalAddr: 0.0.0.0
    TopoNthp: 0
    Instance: abc

```

.....（省略部分显示信息）

表1-9 display rib nib 命令显示信息描述表

字段	描述
Total number of Nexthop(s)	总的下一跳个数
NibID	下一跳ID
Sequence	下一跳序列号
Type	下一跳类型
Flushed	是否下刷
UserKey0	第一个协议保留数据
UserKey1	第二个协议保留数据
VrfNthp	下一跳所在VPN索引，显示为0表示公网
Nexthop	下一跳地址
IFIndex	接口索引
LocalAddr	本地接口地址
TopoNthp	（暂不支持）下一跳所在拓扑索引，显示为0表示公网拓扑（目前IPv6不支持子拓扑，显示为Invalid）

字段	描述
SubNibID	子下一跳的ID
SubSeq	子下一跳的序列号
NthpCnt	子下一跳的下一跳计数
Samed	子下一跳中相同下一跳计数
NthpType	子下一跳类型： - IP：下一跳是 IP 转发类型 - MPLS：下一跳是 MPLS 转发类型（暂不支持）

显示 RIB 下一跳详细信息。

```
<Sysname> display rib nib verbose
```

```
Total number of nexthop(s): 176
```

```

      NibID: 0x10000000      Sequence: 0
      Type: 0x1              Flushed: Yes
      UserKey0: 0x0          VrfNthp: 0
      UserKey1: 0x0          Nexthop: 0.0.0.0
      IFIndex: 0x111        LocalAddr: 0.0.0.0
      TopoNthp: 0
      RefCnt: 6              FlushRefCnt: 2
      Flag: 0x84             Version: 1
1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 0.0.0.0
RelyDepth: 0                RealNexthop: 0.0.0.0
Interface: NULL0            LocalAddr: 0.0.0.0
TunnelCnt: 0                Vrf: default-vrf
TunnelID: N/A               Topology: base
Weight: 0

      NibID: 0x10000001      Sequence: 1
      Type: 0x1              Flushed: Yes
      UserKey0: 0x0          VrfNthp: 0
      UserKey1: 0x0          Nexthop: 127.0.0.1
      IFIndex: 0x112        LocalAddr: 127.0.0.1
      TopoNthp: 0
      RefCnt: 13             FlushRefCnt: 5
      Flag: 0x84             Version: 1
1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 127.0.0.1
RelyDepth: 0                RealNexthop: 127.0.0.1
Interface: InLoop0          LocalAddr: 127.0.0.1
TunnelCnt: 0                Vrf: default-vrf
TunnelID: N/A               Topology: base
Weight: 0
```

```

        NibID: 0x15000003      Sequence: 3
        Type: 0x43             Flushed: Yes
    UserKey0: 0x100010000      VrfNthp: 0
    UserKey1: 0x0              Nextthop: 22.22.22.22
        IFIndex: 0x0           LocalAddr: 0.0.0.0
    TopoNthp: 0
    Instance: default
        RefCnt: 9              FlushRefCnt: 3
        Flag: 0x84             Version: 1
        Policy: tnl-policy1
1 nexthop(s):
PrefixIndex: 0                OrigNextthop: 22.22.22.22
    RelyDepth: 1               RealNextthop: 13.1.1.2
    Interface: GE0/1/3         LocalAddr: 13.1.1.1
    TunnelCnt: 1               Vrf: default-vrf
    TunnelID: 1025             Topology: base
    Weight: 0

```

.....（省略部分显示信息）

表1-10 display rib nib verbose 命令显示信息描述表

字段	描述
x nexthop (s)	下一跳具体值（前面数值表示下一跳个数）
PrefixIndex	等价时下一跳序号
Vrf	VPN实例名，显示为default-vrf表示公网
OrigNextthop	原始下一跳
RealNextthop	真实下一跳
Interface	出接口
LocalAddr	本地接口地址
RelyDepth	迭代深度
TunnelCnt	（暂不支持）迭代到隧道的个数
TunnelID	（暂不支持）迭代到隧道的ID
Topology	（暂不支持）拓扑名称，显示为base表示公网拓扑（目前IPv6不支持子拓扑，显示为空）
Weight	等价路由各路由的权重，取值为0表示不是等价路由
RefCnt	下一跳信息的引用计数
FlushRefCnt	下一跳信息的下刷引用计数
Flag	下一跳信息的标志位
Version	下一跳信息的版本号

1.1.22 display route-direct nib

display route-direct nib 命令用来显示直连路由下一跳信息。

【命令】

display route-direct nib [nib-id] [verbose]

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

nib-id: 路由邻居 ID 值，取值范围为十六进制数 1~ffffff。
verbose: 显示详细信息。如果未指定本参数，则显示概要信息。

【举例】

```
# 显示直连路由下一跳信息。
<Sysname> display route-direct nib
Total number of nexthop(s): 116

      NibID: 0x10000000      Sequence: 0
      Type: 0x1             Flushed: Yes
      UserKey0: 0x0         VrfNthp: 0
      UserKey1: 0x0         Nexthop: 0.0.0.0
      IFIndex: 0x111       LocalAddr: 0.0.0.0
      TopoNthp: 0

      NibID: 0x10000001      Sequence: 1
      Type: 0x1             Flushed: Yes
      UserKey0: 0x0         VrfNthp: 0
      UserKey1: 0x0         Nexthop: 127.0.0.1
      IFIndex: 0x112       LocalAddr: 127.0.0.1
      TopoNthp: 0

..... (省略部分显示信息)
```

表1-11 display route-direct nib 命令显示信息描述表

字段	描述
Total number of nexthop(s)	总的下一跳个数
NibID	NIB ID号
Sequence	NIB序列号

字段	描述
Type	NIB类型
Flushed	是否下刷FIB
UserKey0	NIB协议保留数据1
UserKey1	NIB协议保留数据2
VrfNthp	下一跳所在VPN索引，显示为0表示公网
Nexthop	下一跳信息
IFIndex	接口索引
LocalAddr	本地接口地址
TopoNthp	（暂不支持）下一跳所在拓扑索引，显示为0表示公网拓扑（目前IPv6不支持子拓扑，显示为Invalid）

显示直连路由下一跳详细信息。

```
<Sysname> display route-direct nib verbose
```

Total number of nexthop(s): 116

```

      NibID: 0x10000000      Sequence: 0
      Type: 0x1              Flushed: Yes
      UserKey0: 0x0          VrfNthp: 0
      UserKey1: 0x0          Nexthop: 0.0.0.0
      IFIndex: 0x111         LocalAddr: 0.0.0.0
      RefCnt: 2              FlushRefCnt: 0
      Flag: 0x2              Version: 1
1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 0.0.0.0
RelyDepth: 0                RealNexthop: 0.0.0.0
Interface: NULL0            LocalAddr: 0.0.0.0
TunnelCnt: 0                Vrf: default-vrf
TunnelID: N/A               Topology: base
Weight: 0

```

```

      NibID: 0x10000001      Sequence: 1
      Type: 0x1              Flushed: Yes
      UserKey0: 0x0          VrfNthp: 0
      UserKey1: 0x0          Nexthop: 127.0.0.1
      IFIndex: 0x112         LocalAddr: 127.0.0.1
      RefCnt: 5              FlushRefCnt: 0
      Flag: 0x2              Version: 1
1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 127.0.0.1
RelyDepth: 0                RealNexthop: 127.0.0.1
Interface: InLoop0          LocalAddr: 127.0.0.1
TunnelCnt: 0                Vrf: default-vrf
TunnelID: N/A               Topology: base

```

Weight: 0

..... (省略部分显示信息)

表1-12 display route-direct nib verbose 命令显示信息描述表

字段	描述
x nexthop (s)	下一跳具体值（前面数值表示下一跳个数）
PrefixIndex	等价时下一跳序号
Vrf	VPN实例名，显示为default-vrf表示公网
OrigNexthop	原始下一跳
RealNexthop	真实下一跳
Interface	出接口
localAddr	本地接口地址
RelyDepth	迭代深度
TunnelCnt	迭代到隧道的个数
TunnelID	（暂不支持）迭代到隧道的ID
Topology	（暂不支持）拓扑名称，显示为base表示公网拓扑（目前IPv6不支持子拓扑，显示为空）
Weight	等价路由各路由的权重，取值为0表示不是等价路由
RefCnt	下一跳信息的引用计数
FlushRefCnt	下一跳信息的下刷引用计数
Flag	下一跳信息的标志位
Version	下一跳信息的版本号

1.1.23 fib lifetime

fib lifetime 命令用来配置 IPv4/IPv6 路由在 FIB 中的最大存活时间。

undo fib lifetime 命令用来恢复缺省情况。

【命令】

fib lifetime seconds

undo fib lifetime

【缺省情况】

IPv4/IPv6 路由在 FIB 中的最大存活时间为 600 秒。

【视图】

RIB IPv4 地址族视图

RIB IPv6 地址族视图

【缺省用户角色】

network-admin
context-admin

【参数】

seconds: 路由在 FIB 中的最大存活时间，取值范围为 0~6000，单位为秒。取值为 0 时表示，协议或 RIB 进程倒换并重新恢复后，会立即通知 FIB 老化表项。

【使用指导】

配置本命令后，协议在未配置 GR 或 NSR 的情况下，协议或 RIB 倒换重新恢复后，会延迟配置的 **seconds**，再通知 FIB 老化表项。

【举例】

配置 IPv4 路由在 FIB 中的最大存活时间为 60 秒。

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] fib lifetime 60
```

1.1.24 inter-protocol fast-reroute

inter-protocol fast-reroute 命令用来开启 RIB IPv4/IPv6 地址族的不同协议间快速重路由功能。

undo inter-protocol fast-reroute 命令用来关闭 RIB IPv4/IPv6 地址族的不同协议间快速重路由功能。

【命令】

```
inter-protocol fast-reroute [ vpn-instance vpn-instance-name ]
undo inter-protocol fast-reroute [ vpn-instance vpn-instance-name ]
```

【缺省情况】

不同协议间快速重路由功能处于关闭状态。

【视图】

RIB IPv4 地址族视图
RIB IPv6 地址族视图

【缺省用户角色】

network-admin
context-admin

【参数】

vpn-instance vpn-instance-name: 开启指定 VPN 实例的不同协议间快速重路由功能。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则开启 RIB IPv4/IPv6 地址族中公网的不同协议间快速重路由功能。

【使用指导】

通过配置不同协议间快速重路由功能，可将不同协议的下一跳作为备份下一跳。当路由器检测到网络故障时，将使用备份下一跳替换失效下一跳，通过备份下一跳来指导报文的转发，从而大大缩短了流量中断的时间。

如果 RIB 表中去往同一目的地的不同路由的下一跳和出接口均相同，使用该命令不会生成备份下一跳。

使用不同协议间的快速重路由功能生成备份下一跳时可能会造成环路。

【举例】

开启 RIB IPv4 地址族中公网的不同协议间快速重路由功能。

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] inter-protocol fast-reroute
```

1.1.25 non-stop-routing

non-stop-routing 命令用来使能路由的 NSR 功能。

undo non-stop-routing 命令用来关闭路由的 NSR 功能。

【命令】

non-stop-routing

undo non-stop-routing

【缺省情况】

路由的 NSR 功能处于关闭状态。

【视图】

RIB IPv4 地址族视图

RIB IPv6 地址族视图

【缺省用户角色】

network-admin

context-admin

【举例】

使能 IPv4 路由的 NSR 功能。

```
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] non-stop-routing
```

1.1.26 protocol lifetime

protocol lifetime 命令用来配置 IPv4/IPv6 路由和标签在 RIB 中的最大存活时间。

undo protocol lifetime 命令用来恢复缺省情况。

【命令】

```
protocol protocol lifetime seconds
undo protocol protocol lifetime
```

【缺省情况】

IPv4/IPv6 路由和标签在 RIB 中的最大存活时间为 480 秒。

【视图】

RIB IPv4 地址族视图
RIB IPv6 地址族视图

【缺省用户角色】

network-admin
context-admin

【参数】

protocol: 路由协议。
seconds: 最大存活时间，取值范围为 1~6000，单位为秒。

【使用指导】

如果配置了该命令，且协议配置 GR 的情况下，需要注意该时间不要与 GR 时间冲突，即必须要保证协议能够在该时间内完成 GR 并将全部表项下发 RIB，否则会导致 GR 失败并断流。

【举例】

```
# 配置 RIB 中 RIP 路由和标签的最大存活时间为 60 秒。
<Sysname> system-view
[Sysname] rib
[Sysname-rib] address-family ipv4
[Sysname-rib-ipv4] protocol rip lifetime 60
```

1.1.27 reset ip routing-table statistics protocol

reset ip routing-table statistics protocol 命令用来清除路由表中的路由统计信息。

【命令】

```
reset ip routing-table statistics protocol [ vpn-instance
vpn-instance-name ] { protocol | all }
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

vpn-instance *vpn-instance-name*: 清除指定 VPN 的路由统计信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则清除公网的路由统计信息。

protocol: 清除 IPv4 路由表中指定路由协议的统计信息。

all: 清除 IPv4 路由表中所有路由协议的统计信息。

【使用指导】

执行本命令只能清除路由统计信息中路由协议添加/删除路由的数目信息。

【举例】

清除路由表中的路由统计信息。

```
<Sysname> reset ip routing-table statistics protocol all
```

1.1.28 reset ipv6 routing-table statistics protocol

reset ipv6 routing-table statistics protocol 命令用来清除 IPv6 路由表中的综合路由统计信息。

【命令】

```
reset ipv6 routing-table statistics protocol [ vpn-instance  
vpn-instance-name ] { protocol | all }
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

vpn-instance *vpn-instance-name*: 清除指定 VPN 的路由统计信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则清除公网的路由统计信息。

protocol: 清除 IPv6 路由表中指定路由协议的统计信息。

all: 清除 IPv6 路由表中所有路由协议的统计信息。

【使用指导】

执行本命令只能清除路由统计信息中路由协议添加/删除路由的数目信息。

【举例】

清除 IPv6 路由表中所有路由协议的综合路由统计信息。

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

1.1.29 rib

rib 命令用来进入 RIB 视图。

undo rib 命令用来删除 RIB 视图下的所有配置。

【命令】

```
rib
undo rib
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 进入 RIB 视图。
<Sysname> system-view
[Sysname] rib
[Sysname-rib]
```

目 录

1 静态路由	1-1
1.1 静态路由配置命令	1-1
1.1.1 delete static-routes all	1-1
1.1.2 display route-static nib	1-1
1.1.3 display route-static routing-table	1-5
1.1.4 ip route-static	1-7
1.1.5 ip route-static default-preference	1-9
1.1.6 ip route-static fast-reroute auto	1-10
1.1.7 ip route-static primary-path-detect bfd echo	1-10
1.1.8 ip route-static-group	1-11
1.1.9 prefix	1-12

1 静态路由

1.1 静态路由配置命令

1.1.1 delete static-routes all

delete static-routes all 命令用来删除所有静态路由。

【命令】

delete [vpn-instance *vpn-instance-name*] static-routes all

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

vpn-instance *vpn-instance-name*：删除指定 VPN 实例的所有静态路由。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示删除公网的所有静态路由。

【使用指导】

使用本命令删除静态路由时，系统会提示确认，确认后才会删除所配置的所有静态路由。

使用 **undo ip route-static** 命令可以删除一条静态路由，而使用 **delete static-routes all** 命令可以删除包括缺省路由在内的所有静态路由。

【举例】

```
# 删除所有静态路由。
<Sysname> system-view
[Sysname] delete static-routes all
This will erase all IPv4 static routes and their configurations, you must reconfigure all static routes.
Are you sure?[Y/N]:y
```

【相关命令】

- **ip route-static**

1.1.2 display route-static nib

display route-static nib 命令用来显示静态路由下一跳信息。

【命令】

display route-static nib [*nib-id*] [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

nib-id: 路由邻居 ID 值，取值范围为十六进制数 1~ffffff。如果未指定本参数，则显示所有的静态路由下一跳信息。

verbose: 显示详细信息。如果未指定本参数，则显示概要信息。

【举例】

```
# 显示静态路由下一跳信息。
<Sysname> display route-static nib
Total number of nexthop(s): 44

      NibID: 0x11000000      Sequence: 0
      Type: 0x21            Flushed: Yes
UserKey0: 0x111             VrfNthp: 0
UserKey1: 0x0               Nexthop: 0.0.0.0
      IFIndex: 0x111        LocalAddr: 0.0.0.0
      TopoNthp: 0

      NibID: 0x11000001      Sequence: 1
      Type: 0x41            Flushed: Yes
UserKey0: 0x0               VrfNthp: 5
UserKey1: 0x0               Nexthop: 2.2.2.2
      IFIndex: 0x0          LocalAddr: 0.0.0.0
      TopoNthp: 0

.....（省略部分显示信息）
```

表1-1 display route-static nib 命令显示信息描述表

字段	描述
Total number of nexthop(s)	总的下一跳个数
NibID	NIB ID号
Sequence	NIB序列号
Type	NIB类型
Flushed	是否下刷FIB
UserKey0	NIB协议保留数据1
UserKey1	NIB协议保留数据2

字段	描述
VrfNthp	下一跳所在VPN索引，显示为0表示公网
Nexthop	下一跳信息
IFIndex	接口索引
LocalAddr	本地接口地址
TopoNthp	（暂不支持）下一跳所在拓扑索引，显示为0表示公网拓扑

显示静态路由下一跳详细信息。

```
<Sysname> display route-static nib verbose
```

Total number of nexthop(s): 44

```

      NibID: 0x11000000      Sequence: 0
      Type: 0x21             Flushed: Yes
      UserKey0: 0x111        VrfNthp: 0
      UserKey1: 0x0          Nexthop: 0.0.0.0
      IFIndex: 0x111        LocalAddr: 0.0.0.0
      TopoNthp: 0
      RefCnt: 2              FlushRefCnt: 0
      Flag: 0x2              Version: 1
1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 0.0.0.0
RelyDepth: 0                RealNexthop: 0.0.0.0
Interface: NULL0            LocalAddr: 0.0.0.0
TunnelCnt: 0                Vrf: default-vrf
TunnelID: N/A               Topology: base
Weight: 1000000

      NibID: 0x11000001      Sequence: 1
      Type: 0x41             Flushed: Yes
      UserKey0: 0x0          VrfNthp: 5
      UserKey1: 0x0          Nexthop: 2.2.2.2
      IFIndex: 0x0          LocalAddr: 0.0.0.0
      TopoNthp: 0
      RefCnt: 1              FlushRefCnt: 0
      Flag: 0x12             Version: 1
2 nexthop(s):
PrefixIndex: 0              OrigNexthop: 2.2.2.2
RelyDepth: 7                RealNexthop: 8.8.8.8
Interface: GE1/0/1          LocalAddr: 12.12.12.12
TunnelCnt: 0                Vrf: default-vrf
TunnelID: N/A               Topology: base
Weight: 1000000
PrefixIndex: 0              OrigNexthop: 2.2.2.2
RelyDepth: 9                RealNexthop: 0.0.0.0
Interface: NULL0            LocalAddr: 0.0.0.0

```

```

TunnelCnt: 0                      Vrf: default-vrf
TunnelID: N/A                     Topology: base
Weight: 1000000

```

.....（省略部分显示信息）

表1-2 display route-static nib verbose 命令显示信息描述表

字段	描述
Total number of nexthop(s)	总的下一跳个数
NibID	NIB ID号
Sequence	NIB序列号
Type	NIB类型
Flushed	是否下刷FIB
UserKey0	NIB协议保留数据1
VrfNthp	下一跳所在VPN索引，显示为0表示公网
UserKey1	NIB协议保留数据2
Nexthop	下一跳信息
IFIndex	接口索引
LocalAddr	本地接口地址
TopoNthp	下一跳所在拓扑索引，显示为0表示公网拓扑
RefCnt	下一跳信息的引用计数
FlushRefCnt	下一跳信息的下刷引用计数
Flag	下一跳信息的标志位
Version	下一跳信息的版本号
x nexthop (s)	下一跳具体值（前面数值表示下一跳个数）
PrefixIndex	等价时下一跳序号
OrigNexthop	原始下一跳
RelyDepth	迭代深度
RealNexthop	真实下一跳
Interface	出接口
localAddr	本地接口地址
TunnelCnt	（暂不支持）迭代到隧道的个数
Vrf	VPN实例名，显示为default-vrf表示公网
TunnelID	（暂不支持）迭代到隧道的ID
Topology	（暂不支持）拓扑名称，显示为base表示公网拓扑
Weight	等价路由各路由的权重，取值为0表示不是等价路由

1.1.3 display route-static routing-table

display route-static routing-table 命令用来显示静态路由表信息。

【命令】

```
display route-static routing-table [ vpn-instance vpn-instance-name ]  
[ ip-address { mask-length | mask } ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance *vpn-instance-name*: 显示指定 VPN 实例的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

ip-address: 目的 IP 地址，点分十进制。如果未指定本参数，则显示所有的静态路由表信息。

mask-length: 网络掩码长度，取值范围为 0~32。

mask: 网络掩码，点分十进制格式。

【举例】

显示静态路由表信息。

```
<Sysname> display route-static routing-table
```

```
Total number of routes: 24
```

```
Status: * - valid
```

```
*Destination: 0.0.0.0/0
```

```
    NibID: 0x1100000a
```

```
    NextHop: 2.2.2.10
```

```
    MainNibID: N/A
```

```
    BkNextHop: N/A
```

```
    BkNibID: N/A
```

```
    Interface: GigabitEthernet1/0/1
```

```
    TableID: 0x2
```

```
    BkInterface: GigabitEthernet1/0/2
```

```
    Flag: 0x82d01
```

```
    BfdSrcIp: N/A
```

```
    DbIndex: 0xd
```

```
    BfdIfIndex: 0x0
```

```
    Type: Normal
```

```
    BfdVrfIndex: 0
```

```
    TrackIndex: 0xffffffff
```

```
    Label: NULL
```

```
    Preference: 60
```

```
    vrfIndexDst: 0
```

```
    BfdMode: N/A
```

```
    vrfIndexNH: 0
```

```
    Permanent: 0
```

```
    Tag: 0
```

```

Destination: 0.0.0.0/0
    NibID: 0x1100000b      NextHop: 2.2.2.11
MainNibID: N/A             BkNextHop: N/A
    BkNibID: N/A           Interface: GigabitEthernet1/0/3
    TableID: 0x2           BkInterface: GigabitEthernet1/0/4
        Flag: 0x82d01      BfdSrcIp: N/A
    DbIndex: 0xd           BfdIfIndex: 0x0
        Type: Normal        BfdVrfIndex: 0
TrackIndex: 0xffffffff     Label: NULL
Preference: 60             vrfIndexDst: 0
    BfdMode: N/A           vrfIndexNH: 0
    Permanent: 0           Tag: 0

```

.....（省略部分显示信息）

表1-3 display route-static routing-table 命令显示信息描述表

字段	描述
Total number of routes	总的路由条数
Destination	目的地址/掩码
NibID	下一跳信息ID
MainNibID	FRR静态路由主下一跳信息ID
BkNibID	FRR静态路由备下一跳信息ID
NextHop	此路由的下一跳地址
BkNextHop	此路由的备份下一跳地址
Interface	出接口，即到该目的网段的数据包将从此接口发出
BkInterface	备份出接口
TableID	路由所在的表ID
Flag	路由标志位
DbIndex	路由所在DB的DB索引
Type	路由类型： Normal: 普通类型的静态路由
BfdSrcIp	BFD非直连会话源地址
BfdIfIndex	BFD使用的接口索引
BfdVrfIndex	BFD所在VPN索引，显示为0表示公网
BfdMode	BFD模式： - N/A: 未配置 BFD 会话 - Ctrl: 控制报文方式的 BFD 会话 - Echo: echo 报文方式的 BFD 会话
TrackIndex	NQA Track索引

字段	描述
Label	标签
Preference	路由优先级
vrflIndexDst	目的所在VPN索引，显示为0表示公网
vrflIndexNH	下一跳所在VPN索引，显示为0表示公网
Permanent	永久静态路由标志（1表示永久静态路由）
Tag	路由标记

1.1.4 ip route-static

ip route-static 命令用来配置静态路由。

undo ip route-static 命令用来删除指定的静态路由。

【命令】

```
ip route-static { dest-address { mask-length | mask } | group group-name }
{ interface-type interface-number [ next-hop-address ] [ backup-interface
interface-type interface-number [ backup-nexthop backup-nexthop-address ]
[ permanent ] | bfd { control-packet | echo-packet } | permanent | track
track-entry-number ] } [ preference preference ] [ tag tag-value ]
[ description text ]
```

```
ip route-static { dest-address { mask-length | mask } | group group-name }
next-hop-address [ bfd control-packet bfd-source ip-address | permanent |
track track-entry-number ] [ preference preference ] [ tag tag-value ]
[ description text ]
```

```
ip route-static { dest-address { mask-length | mask } | group group-name }
vpn-instance d-vpn-instance-name next-hop-address [ bfd control-packet
bfd-source ip-address | permanent | track track-entry-number ] [ preference
preference ] [ tag tag-value ] [ description text ]
```

```
undo ip route-static { dest-address { mask-length | mask } | group group-name }
[ interface-type interface-number [ next-hop-address ] | next-hop-address |
vpn-instance d-vpn-instance-name next-hop-address ] [ preference
preference ]
```

【缺省情况】

未配置静态路由。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

dest-address: 静态路由的目的 IP 地址，点分十进制格式。

mask-length: 网络掩码长度，取值范围为 0~32。

mask: 网络掩码，点分十进制格式。

group group-name: 指定静态路由配置组。*group-name* 表示配置组名称，为 1~31 个字符的字符串，区分大小写。

vpn-instance d-vpn-instance-name: 指定目的 VPN 实例。*d-vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果指定目的 VPN 实例，静态路由将根据配置的 *next-hop-address* 在目的 VPN 中查找出接口。

interface-type interface-number: 指定静态路由的出接口类型和接口号。在指定静态路由的出接口类型和接口号时需要注意的事项，详见使用指导。

next-hop-address: 指定路由的下一跳的 IP 地址，点分十进制格式。在指定路由的下一跳的 IP 地址时需要注意的事项，详见使用指导。

backup-interface interface-type interface-number: 备份出接口。对于备份出接口为非 P2P 类型的接口时（包括 NBMA 类型接口或广播类型接口），必须同时指定其对应的备份下一跳地址。*interface-type interface-number* 为指定的接口类型和编号。

backup-nexthop backup-nexthop-address: 备份下一跳地址。

bfd: 使能 BFD（Bidirectional Forwarding Detection，双向转发检测）功能，对静态路由下一跳的可达性进行快速检测，当下一跳不可达时可以快速切换到备份路由。

control-packet: 通过 BFD 控制报文方式实现 BFD 功能。

bfd-source ip-address: BFD 源 IP 地址。建议配置为 Loopback 接口 IP 地址。

echo-packet: 通过 BFD echo 报文方式实现 BFD 功能。

permanent: 指定为永久静态路由。即使在出接口 down 时，配置的永久静态路由仍然保持 active 状态。

track track-entry-number: 将静态路由与 Track 项相关联，*track-entry-number* 为 Track 项的序号，取值范围为 1~1024。关于 Track 的详细介绍，请参见“可靠性配置指导”中的“Track”。

public: 指定静态路由下一跳处于公网实例。

preference preference: 指定静态路由的优先级，取值范围为 1~255，缺省值为 60。

tag tag-value: 静态路由 Tag 值，用于标识该条静态路由，以便在路由策略中根据 Tag 对路由进行灵活的控制。*tag-value* 的取值范围为 1~4294967295，缺省值为 0。关于路由策略的详细信息，请参见“三层技术-IP 路由配置指导”中的“路由策略”。

description text: 配置的静态路由描述信息，取值范围为 1~60 个字符。除“?”外，可以包含空格等特殊字符。

【使用指导】

如果目的 IP 地址和掩码都为 0.0.0.0（或掩码为 0），则配置的路由为缺省路由。当没有匹配的路由表项时，将使用缺省路由进行报文转发。

对不同的优先级配置，可采用不同的路由管理策略。例如，为同一目的地配置多条路由，如果指定相同的优先级，则实现路由负载分担；如果指定不同的优先级，则实现路由备份。

配置静态路由时，可根据实际需要指定出接口或下一跳地址。需要注意的是：

- 对于 Null0 接口，配置了出接口就不需要配置下一跳地址。
- 对于点到点接口，配置时可以只指定出接口，不指定下一跳地址。这样，即使对端地址发生了变化也无须改变配置。
- 对于 NBMA、P2MP 等接口，需要进行 IP 地址到链路层地址的映射，建议同时配置出接口和下一跳 IP 地址。
- 对于广播类型接口，如以太网接口、VLAN 接口等，因为可能有多个下一跳，配置时必须同时指定出接口和下一跳。

配置静态路由时需要注意的是：

- 路由振荡时，使能 BFD 检测功能可能会加剧振荡，需谨慎使用。关于 BFD 的详细介绍，请参考“可靠性配置指导”中的“BFD”。
- 如果 Track 模块通过 NQA 探测私网静态路由中下一跳的可达性，静态路由下一跳的 VPN 实例号与 NQA 测试组配置的实例号必须相同，才能进行正常的探测。
- 在静态路由进行迭代时，Track 项监测的应该是静态路由真正的下一跳，而不是配置的下一跳。否则，可能导致错误地将有效路由判断为无效路由。

按配置组配置静态路由时，配置组下的所有前缀会应用相同的下一跳、出接口信息。如果配置组不存在或者配置组中没有任何前缀，则不会创建静态路由。

【举例】

配置静态路由，其目的地址为 1.1.1.1/24，指定下一跳为 2.2.2.2，Tag 值为 45，描述信息为“for internet”。

```
<Sysname> system-view
```

```
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for internet
```

【相关命令】

- **display ip routing-table protocol**（三层技术-IP 路由命令参考/IP 路由基础）
- **ip route-static-group**
- **prefix**

1.1.5 ip route-static default-preference

ip route-static default-preference 命令用来配置静态路由的缺省优先级。

undo ip route-static default-preference 命令用来恢复缺省情况。

【命令】

```
ip route-static default-preference default-preference
```

```
undo ip route-static default-preference
```

【缺省情况】

静态路由的缺省优先级为 60。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

default-preference: 静态路由缺省优先级的值，取值范围为 1~255。

【使用指导】

如果在配置静态路由时没有指定优先级，就会使用缺省优先级。

重新配置缺省优先级后，新设置的缺省优先级仅对新增的静态路由有效。

【举例】

```
# 配置静态路由的缺省优先级为 120。
<Sysname> system-view
[Sysname] ip route-static default-preference 120
```

【相关命令】

- **display ip routing-table protocol**（三层技术-IP 路由命令参考/IP 路由基础）

1.1.6 ip route-static fast-reroute auto

ip route-static fast-reroute auto 命令用来配置静态路由自动快速重路由功能。

undo ip route-static fast-reroute auto 命令用来关闭静态路由自动快速重路由功能。

【命令】

```
ip route-static fast-reroute auto
undo ip route-static fast-reroute auto
```

【缺省情况】

静态路由自动快速重路由功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 配置静态路由自动快速重路由功能。
<Sysname> system-view
[Sysname] ip route-static fast-reroute auto
```

1.1.7 ip route-static primary-path-detect bfd echo

ip route-static primary-path-detect bfd echo 命令用来使能静态路由中主用链路的 BFD（Echo 方式）检测功能。

undo ip route-static primary-path-detect bfd 命令用来关闭静态路由中主用链路的 BFD（Echo 方式）检测功能。

【命令】

```
ip route-static primary-path-detect bfd echo
undo ip route-static primary-path-detect bfd
```

【缺省情况】

静态路由中主用链路的 BFD（Echo 方式）检测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

配置本功能后，静态路由的快速重路由特性中的主用链路将使用 BFD（Echo 方式）进行检测。

【举例】

```
# 配置静态路由快速重路由特性中主用链路使能 BFD（Echo 方式）功能。
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 32 gigabitethernet 1/0/1 2.2.2.2 backup-interface
gigabitethernet 1/0/2 backup-nexthop 3.3.3.3
[Sysname] ip route-static primary-path-detect bfd echo
```

1.1.8 ip route-static-group

ip route-static-group 命令用来创建静态路由配置组，并进入静态路由配置组视图。如果指定的静态路由配置组已经存在，则直接进入静态路由配置组视图。

undo ip route-static-group 命令用来删除静态路由配置组。

【命令】

```
ip route-static-group group-name
undo ip route-static-group group-name
```

【缺省情况】

不存在静态路由配置组。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

group-name：指定静态路由配置组。**group-name** 表示静态路由配置组名称，为 1~31 个字符的字符串，区分大小写。

【举例】

```
# 创建静态路由配置组 test，并进入静态路由配置组视图。  
<Sysname> system-view  
[Sysname] ip route-static-group test  
[Sysname-route-static-group-test]
```

【相关命令】

- **ip route-static**
- **prefix**

1.1.9 prefix

prefix 命令用来在静态路由配置组中增加前缀。

undo prefix 命令用来在静态路由配置组中删除前缀。

【命令】

```
prefix dest-address { mask-length | mask }  
undo prefix dest-address { mask-length | mask }
```

【缺省情况】

静态路由配置组中未配置前缀。

【视图】

静态路由配置组视图

【缺省用户角色】

network-admin
context-admin

【参数】

dest-address: 静态路由的目的 IP 地址，点分十进制格式。

mask-length: 网络掩码长度，取值范围为 0~32。

mask: 网络掩码，点分十进制格式。

【使用指导】

在静态路由配置组视图下可以多次配置该命令，添加多个前缀，并通过命令 **ip route-static group** 批量创建静态路由；如果已经通过命令 **ip route-static group** 批量创建了静态路由，后续向配置组中增加前缀，则会一并生成该前缀对应的静态路由。

【举例】

```
# 在静态路由配置组 test 中，增加前缀 1.1.1.1/32。  
<Sysname> system-view  
[Sysname] ip route-static-group test  
[Sysname-route-static-group-test] prefix 1.1.1.1 32
```

【相关命令】

- **ip route-static**

- **ip route-static-group**

目 录

1 RIP	1-1
1.1 RIP配置命令	1-1
1.1.1 bfd all-interfaces enable	1-1
1.1.2 checkzero	1-2
1.1.3 default cost	1-2
1.1.4 default-route	1-3
1.1.5 display rip	1-4
1.1.6 display rip database	1-6
1.1.7 display rip graceful-restart	1-7
1.1.8 display rip interface	1-8
1.1.9 display rip neighbor	1-10
1.1.10 display rip non-stop-routing	1-11
1.1.11 display rip route	1-12
1.1.12 fast-reroute	1-14
1.1.13 filter-policy export	1-15
1.1.14 filter-policy import	1-17
1.1.15 graceful-restart	1-18
1.1.16 graceful-restart interval	1-19
1.1.17 host-route	1-19
1.1.18 import-route	1-20
1.1.19 maximum load-balancing	1-21
1.1.20 network	1-22
1.1.21 non-stop-routing	1-23
1.1.22 output-delay	1-24
1.1.23 peer	1-25
1.1.24 preference	1-25
1.1.25 reset rip process	1-26
1.1.26 reset rip statistics	1-27
1.1.27 rip	1-27
1.1.28 rip authentication-mode	1-28
1.1.29 rip bfd	1-29
1.1.30 rip default-route	1-30
1.1.31 rip enable	1-31

1.1.32 rip input	1-32
1.1.33 rip max-packet-length	1-32
1.1.34 rip metricin	1-33
1.1.35 rip metricout.....	1-34
1.1.36 rip mib-binding.....	1-35
1.1.37 rip output.....	1-36
1.1.38 rip output-delay.....	1-36
1.1.39 rip poison-reverse	1-37
1.1.40 rip primary-path-detect bfd	1-38
1.1.41 rip split-horizon	1-38
1.1.42 rip summary-address	1-39
1.1.43 rip version	1-40
1.1.44 silent-interface	1-41
1.1.45 summary	1-42
1.1.46 timer triggered	1-42
1.1.47 timers	1-43
1.1.48 validate-source-address	1-44
1.1.49 version	1-45

1 RIP

1.1 RIP配置命令

1.1.1 bfd all-interfaces enable

bfd all-interfaces enable 命令用来在运行当前 RIP 进程的所有接口上使能 BFD 功能。

undo bfd all-interfaces enable 命令用来恢复缺省情况。

【命令】

```
bfd all-interfaces enable [ ctrl ]  
undo bfd all-interfaces enable
```

【缺省情况】

运行 RIP 进程的接口上未使能 BFD 功能。

【视图】

RIP 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

ctrl: 配置直连和非直连邻居均使用 control 报文双向检测方式。如果不指定本参数，对于直连邻居 RIP BFD 将使用 echo 报文单跳检测方式，对于非直连邻居 RIP BFD 将使用 control 报文双向检测方式。

【使用指导】

目前 RIP 支持 BFD 提供了下面几种检测方式：

- **echo 报文单跳检测方式**：直连邻居使用。在对端有 RIP 路由发送时才能建立 BFD 会话。
- **指定目的地址的 echo 报文单跳检测方式**：直连邻居使用，并且在接口上直接指定 RIP 邻居的 IP 地址。当该接口使能了 RIP 功能，会建立到指定目的 IP 地址的 BFD 会话。
- **control 报文双向检测方式**：直连邻居和非直连邻居均可以使用。当两端互有 RIP 路由发送时，且使能 BFD 的接口与接收接口为同一接口，邻居之间才能建立 BFD 会话。

本端使用 control 报文双向检测方式时，需要对端也使用 control 报文双向检测方式，才能正常工作。

接口视图下使能 RIP BFD 功能的配置，其优先级高于 RIP 视图下使能 BFD 的配置。

由于 **peer** 命令与邻居之间没有对应关系，**undo peer** 操作并不能立刻删除邻居，因此不能立刻删除 BFD 会话。

【举例】

RIP 进程 1 在所有接口上使能 RIP BFD。

```
<Sysname> system-view  
[Sysname] rip 1
```

```
[Sysname-rip-1] bfd all-interfaces enable
```

【相关命令】

- **rip bfd**

1.1.2 checkzero

checkzero 命令用来使能 RIP-1 报文的零域检查功能。

undo checkzero 命令用来关闭零域检查功能。

【命令】

checkzero

undo checkzero

【缺省情况】

RIP-1 报文的零域检查功能处于使能状态。

【视图】

RIP 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

使能零域检查功能后，零域中包含非零位的 RIP-1 报文将被拒绝处理。如果用户能确保所有报文都是可信任的，则可以不进行该项检查，以节省 CPU 处理时间。

【举例】

关闭进程号为 1 的 RIP 进程对 RIP-1 报文的零域检查功能。

```
<Sysname> system-view
```

```
[Sysname] rip
```

```
[Sysname-rip-1] undo checkzero
```

1.1.3 default cost

default cost 命令用来配置引入路由的缺省度量值。

undo default cost 命令用来恢复缺省情况。

【命令】

default cost *cost-value*

undo default cost

【缺省情况】

引入路由的缺省度量值为 0。

【视图】

RIP 视图

【缺省用户角色】

network-admin
context-admin

【参数】

cost-value: 引入路由的缺省度量值，取值范围为 0~16。

【使用指导】

当使用 **import-route** 命令从其它协议引入路由时，如果不指定具体的度量值，则引入路由的度量值为 **default cost** 所指定的值。

【举例】

```
# 配置从其它路由协议引入路由的缺省度量值为 3。  
<Sysname> system-view  
[Sysname] rip 1  
[Sysname-rip-1] default cost 3
```

【相关命令】

- **import-route**

1.1.4 default-route

default-route 命令用来配置 RIP 进程下的所有接口以指定度量值向 RIP 邻居发布一条缺省路由。
undo default-route 命令用来恢复缺省情况。

【命令】

```
default-route { only | originate } [ cost cost-value | route-policy  
route-policy-name ] *  
undo default-route
```

【缺省情况】

不向 RIP 邻居发送缺省路由。

【视图】

RIP 视图

【缺省用户角色】

network-admin
context-admin

【参数】

only: 配置只发送缺省路由，不发送普通路由。

originate: 配置既发送普通路由，又发送缺省路由。

cost-value: 缺省路由的度量值，取值范围为 1~15，缺省值为 1。

route-policy route-policy-name: 路由策略名称，**route-policy-name** 为 1~63 个字符的字符串，区分大小写。只有当前路由器的路由表中有路由匹配 **route-policy-name** 指定的路由策略时，才发送缺省路由。

【使用指导】

配置了发布缺省路由的 RIP 路由器不接收来自 RIP 邻居的缺省路由。

【举例】

配置 RIP 进程 100 的所有接口向 RIP 邻居发布一条度量值为 2 的缺省路由, 而且只发送缺省路由, 不发送普通路由。

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default-route only cost 2
```

【相关命令】

- **rip default-route**

1.1.5 display rip

display rip 命令用来显示 RIP 的当前运行状态及配置信息。

【命令】

display rip [*process-id*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: RIP 进程号, 取值范围为 1~65535。如果未指定本参数, 则显示所有 RIP 进程的当前运行状态及配置信息。

【举例】

显示所有 RIP 进程的当前运行状态及配置信息。

```
<Sysname> display rip
Public VPN-instance name:
RIP process: 1
  RIP version: 1
  Preference: 100
    Routing policy: abc
  Fast-reroute:
    Routing policy: frr
  Checkzero: Enabled
  Default cost: 0
  Summary: Enabled
  Host routes: Enabled
  Maximum number of load balanced routes: 8
```

```

Update time      : 30 secs  Timeout time      : 180 secs
Suppress time   : 120 secs  Garbage-collect time : 120 secs
Update output delay: 20(ms) Output count:    3
Graceful-restart interval: 60 secs
Triggered Interval : 5 50 200
BFD: Enabled (ctrl)
Silent interfaces: None
Default routes: Originate  Default routes cost: 3
Verify-source: Enabled
Networks:
    1.0.0.0
Configured peers:
    197.168.6.2
Triggered updates sent: 0
Number of routes changes: 1
Number of replies to queries: 0

```

表1-1 display rip 命令显示信息描述表

字段	描述
Public VPN-instance name	RIP进程运行在公网实例下
Private VPN-instance name	RIP进程应用于指定VPN实例
RIP process	RIP进程号
RIP version	RIP版本，取值为1或2
Preference	RIP路由优先级
Fast-reroute	RIP快速重路由
Routing policy	路由策略
Checkzero	是否使能对RIP-1报文的零域进行检查的功能 • Enable 表示已使能 • Disabled 表示关闭
Default cost	引入路由的缺省度量值
Summary	路由聚合功能是否使能 • Enabled 表示已使能 • Disabled 表示关闭
Host routes	是否允许接收主机路由 • Enabled 表示允许 • Disabled 表示不允许
Maximum number of load balanced routes	等价路由的最大数目
Update time	Update定时器的值，单位为秒
Timeout time	Timeout定时器的值，单位为秒
Suppress time	Suppress定时器的值，单位为秒

字段	描述
Garbage-collect time	Garbage-Collect定时器的值，单位为秒
Update output delay	接口发送RIP报文的时间间隔
Output count	接口一次发送RIP报文的最大个数
Graceful-restart interval	GR重启间隔时间，单位为秒
Triggered Interval	发送触发更新的时间间隔
BFD	是否使能了RIP的BFD功能 • Disabled: 表示未使能 • Enabled: 表示在 RIP 视图下使能了 BFD 功能（直连邻居使用 echo 报文单跳检测方式，非直连邻居使用 control 报文双向检测方式） • Enabled (ctrl): 表示在 RIP 视图下使能了 BFD 功能（直连邻居和非直连邻居均使用 control 报文双向检测方式）
Silent interfaces	工作在抑制状态的接口（这些接口不发送周期更新报文）
Default routes	是否向RIP邻居发布一条缺省路由 • Only: 表示只发布缺省路由 • Originate: 表示同时发布缺省路由和普通路由 • Disabled: 表示不发布缺省路由
Default routes cost	RIP进程下发布缺省路由的度量值
Verify-source	是否使能对接收到的RIP路由更新报文进行源IP地址检查的功能 • Enable 表示已使能 • Disabled 表示关闭
Networks	使能RIP的网段地址
Configured peers	配置的邻居
Triggered updates sent	发送的触发更新报文数
Number of routes changes	RIP进程改变路由数据库的统计数据
Number of replies to queries	RIP请求的响应报文数

1.1.6 display rip database

display rip database 命令用来显示 RIP 数据库的激活路由。

【命令】

display rip process-id database [ip-address { mask-length | mask }]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

process-id: RIP 进程号，取值范围为 1~65535。
ip-address { mask-length | mask }: 显示指定目的地址和掩码的激活路由信息。如果未指定本参数，将显示 RIP 的所有激活路由信息。

【举例】

显示 RIP 进程 100 数据库的所有激活路由。
<Sysname> display rip 100 database
1.0.0.0/8, auto-summary
1.1.1.0/24, cost 16, interface summary
1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface
1.1.2.0/24, cost 0, imported
2.0.0.0/8, auto-summary
2.0.0.0/8, cost 1, nexthop 1.1.1.2
显示 RIP 进程 100 数据库中指定地址和掩码为 1.1.1.0/24 的激活路由。
<Sysname> display rip 100 database 1.1.1.0 24
1.1.1.0/24, cost 16, interface summary
1.1.1.0/24, cost 0, nexthop 1.1.1.1, RIP-interface

表1-2 display rip database 命令显示信息描述表

字段	描述
cost	度量值
auto-summary	表示该条路由是RIP的自动聚合路由
interface summary	表示该条路由是RIP的接口聚合路由
nexthop	下一跳地址
RIP-interface	使能RIP协议的接口的直连路由
imported	表示该条路由是从其它路由协议引入的

1.1.7 display rip graceful-restart

display rip graceful-restart 命令用来显示 RIP 进程的 GR 状态信息。

【命令】

display rip [process-id] graceful-restart

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

process-id: RIP 进程号，取值范围为 1~65535。如果未指定本参数，则显示所有 RIP 进程的 GR 状态信息。

【举例】

显示 RIP 1 进程的 GR 状态信息。

```
<Sysname> display rip 1 graceful-restart
RIP process: 1
Graceful Restart capability      : Enabled
Current GR state                : Normal
Graceful Restart period         : 60 seconds
Graceful Restart remaining time : 0 seconds
```

表1-3 display rip graceful-restart 命令显示信息描述表

字段	描述
RIP process	RIP进程号
Graceful Restart capability	GR使能状态 - Enabled: 使能了 GR 能力 - Disabled: 关闭了 GR 能力
Current GR state	当前GR所处状态 - Under GR: 进程正在 GR - Normal: 普通状态
Graceful Restart period	GR重启间隔时间
Graceful Restart remaining time	GR结束剩余时间

1.1.8 display rip interface

display rip interface 命令用来显示 RIP 的接口信息。

【命令】

display rip process-id interface [interface-type interface-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin

context-operator

【参数】

process-id: RIP 进程号，取值范围为 1~65535。
interface-type interface-number: 接口类型和编号。如果未指定本参数，将显示 RIP 的所有接口信息。

【举例】

```
# 显示 RIP 进程 1 的接口信息。
<Sysname> display rip 1 interface
Total: 1

Interface: GigabitEthernet1/0/2
  Address/Mask: 1.1.1.1/24      Version: RIPv1
  MetricIn: 0                  MetricIn route policy: Not designated
  MetricOut: 1                 MetricOut route policy: Not designated
  Split-horizon/Poison-reverse: On/Off  Input/Output: On/On
  Default route: Off
  Update output delay: 20(ms)      Output count: 3
  BFD: Enabled (ctrl), inherited
  Current number of packets/Maximum number of packets: 0/2000
```

表1-4 display rip interface 命令显示信息描述表

字段	描述
Total	运行RIP协议的接口总数
Interface	运行RIP协议的接口的名称
Address/Mask	运行RIP协议的接口的IP地址/掩码
Version	接口上运行的RIP协议的版本
MetricIn	接收路由的附加度量值
MetricIn route policy	接收路由的附加度量值应用的路由策略，取值为Not designated表示没有对接收路由的附加度量值使用路由策略，如果对接收路由的附加度量值使用了路由策略，取值为使用的路由策略名称
MetricOut	发送路由的附加度量值
MetricOut route policy	发送路由的附加度量值应用的路由策略，取值为Not designated表示没有对发送路由的附加度量值使用路由策略，如果对发送路由的附加度量值使用了路由策略，取值为使用的路由策略名称
Split-horizon	是否使能了水平分割（On表示使能，Off表示关闭）
Poison-reverse	是否使能了毒性逆转（On表示使能，Off表示关闭）
Input/Output	是否允许接口接收（Input）/发送（Output）RIP报文（On表示允许，Off表示不允许）

字段	描述
Default route	是否允许向RIP邻居发送缺省路由 • Only: 表示只发布缺省路由 • Originate: 表示同时发布缺省路由和普通路由 • No-originate: 表示只发布普通路由 • Off: 表示不发布缺省路由
Default route cost	RIP接口下配置发布缺省路由的度量值
Update output delay	接口发送RIP报文的时间间隔
Output count	接口一次发送RIP报文的最大个数
BFD	RIP接口上是否使能了BFD功能，其中： • Disabled: 表示未使能 • Enabled: 表示在接口视图下使能了RIP的BFD功能（直连邻居使用echo报文单跳检测方式，非直连邻居使用control报文双向检测方式） • Enabled (ctrl): 表示在接口视图下使能了RIP的BFD功能（直连邻居和非直连邻居均使用control报文双向检测方式） • Enabled, inherited: 表示在RIP视图下使能了BFD功能（直连邻居使用echo报文单跳检测方式，非直连邻居使用control报文双向检测方式），且接口继承了RIP视图下的配置 • Enabled (ctrl), inherited: 表示在RIP视图下使能了BFD功能（直连邻居和非直连邻居均使用control报文双向检测方式），且接口继承了RIP视图下的配置 • Enabled (destination): 表示在接口视图下使能了RIP的BFD功能，且使用指定了BFD链路检测的目的地址的echo报文单跳检测方式
Current number of packets /Maximum number of packets	显示当前接口待发送的报文数量和最多可以发送的报文数量

1.1.9 display rip neighbor

display rip neighbor 命令用来显示RIP进程的邻居信息。

【命令】

display rip process-id neighbor [interface-type interface-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: RIP进程号，取值范围为1~65535。

interface-type interface-number: 接口类型和编号。如果未指定本参数，将显示 RIP 的所有邻居信息。

【举例】

显示 RIP 进程 1 的邻居信息。

```
<Sysname> display rip 1 neighbor
```

```
Neighbor address: 197.168.2.3
```

```
Interface : GigabitEthernet1/0/2
```

```
Version : RIPv2 Last update: 00h00m02s
```

```
Relay nbr : N/A BFD session: N/A
```

```
Bad packets: 0 Bad routes : 0
```

表1-5 display rip neighbor 命令显示信息描述表

字段	描述
Neighbor address	邻居地址
Interface	出接口
Version	收到邻居RIP报文的版本
Last update	上次收到邻居更新报文距离现在时间
Relay nbr	是否是非直连邻居
BFD session	BFD会话类型
Bad packets	接口收到的错误报文数目
Bad routes	接口收到的错误路由数目

1.1.10 display rip non-stop-routing

display rip non-stop-routing 命令用来显示 RIP 进程的 NSR 状态信息。

【命令】

display rip [*process-id*] non-stop-routing

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

process-id: RIP 进程号，取值范围为 1~65535。如果未指定本参数，则显示所有 RIP 进程的 NSR 状态信息。

【举例】

```
# 显示 RIP 1 进程的 NSR 状态信息。  
<Sysname> display rip 1 non-stop-routing  
RIP process: 1  
Nonstop Routing capability: Enabled  
Current NSR state      : Finish
```

表1-6 display rip non-stop-routing 命令显示信息描述表

字段	描述
RIP process	RIP进程号
Nonstop Routing capability	NSR使能状态 - Enabled: 使能 NSR - Disabled: 不使能 NSR
Current NSR state	当前NSR所处状态 - Initialization: 初始准备 - Smooth: 数据平滑 - Advertising: 发布路由 - Redistribution: 路由引入处理 - Finish: 完成

1.1.11 display rip route

display rip route 命令用来显示 RIP 的路由信息。

【命令】

```
display rip process-id route [ ip-address { mask-length | mask } [ verbose ]  
| peer ip-address | statistics ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: RIP 进程号，取值范围为 1~65535。
ip-address { mask-length | mask }: 显示指定目的地址和掩码的路由信息。
verbose: 显示当前 RIP 路由表中指定目的地址和掩码的所有路由信息。如果未指定本参数，则只
显示指定目的地址和掩码的最优 RIP 路由。
peer ip-address: 显示从指定邻居学到的所有路由信息。

statistics: 显示路由的统计信息。路由的统计信息包括路由总数目，各个邻居的路由数目。

【使用指导】

如果未指定任何参数，将显示 RIP 的所有路由信息。

【举例】

显示进程号为 1 的 RIP 进程所有的路由信息。

```
<Sysname> display rip 1 route
Route Flags: R - RIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
-----
Peer 1.1.1.1 on GigabitEthernet1/0/2
  Destination/Mask    Nexthop          Cost    Tag    Flags  Sec
  3.0.0.0/8           1.1.1.1          1       0      RAOF   24
Local route
  Destination/Mask    Nexthop          Cost    Tag    Flags  Sec
  4.4.4.4/32          0.0.0.0          0       0      RD0F   -
  1.1.1.0/24          0.0.0.0          0       0      RD0F   -
```

显示进程号为 1 的 RIP 进程指定路由的全部路由信息。

```
<Sysname> display rip 1 route 3.0.0.0 8 verbose
Route Flags: R - RIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
-----
Peer 1.1.1.1 on GigabitEthernet1/0/2
  Destination/Mask    OrigNexthop/RealNexthop    Cost    Tag    Flags  Sec
  3.0.0.0/8           1.1.1.1/1.1.1.1           1       0      RAOF   16
```

表1-7 display rip route 命令显示信息描述表

字段	描述
Route Flags	路由标志： • R: RIP 生成的路由 • P: 该路由永久有效 • A: 该路由处于老化时期 • S: 该路由处于抑制时期 • G: 该路由处于 Garbage-collect 时期 • D: RIP 生成的直连路由 • O: 该路由处于最优路由状态 • F: 该路由已经被下刷到 RIB
Peer X.X.X.X on interface-type interface-number	在RIP接口上从指定邻居学到的路由信息
Local route	RIP本地生成的直连路由
Destination/Mask	目的IP地址/掩码
Nexthop	路由的下一跳地址

字段	描述
OrigNexthop/RealNexthop	如果路由来自直连邻居，那么路由的真实下一跳就是原始下一跳；如果路由来自非直连邻居，对于成功迭代的路由RealNexthop则显示迭代出来的下一跳，否则不显示
Cost	度量值
Tag	路由标记
Flags	路由信息所处状态
Sec	路由信息所处状态对应的定时器时间

显示进程号为 1 的 RIP 进程的路由统计信息。

```
<Sysname> display rip 1 route statistics
```

Peer	Optimal/Aging	Optimal/Permanent	Garbage
1.1.1.1	1/1	0/0	0
Local	2/0	0/0	0
Total	3/1	0/0	0

表1-8 display rip route statistics 命令显示信息描述表

字段	描述
Peer	RIP邻居IP地址
Optimal	路由信息中处于最优路由状态的路由条数
Aging	路由信息中处于老化状态的路由条数
Permanent	路由信息中处于永久有效状态的路由条数
Garbage	路由信息中处于Garbage-collection状态的路由条数
Local	RIP本地生成的直连路由条数的总和
Total	从所有RIP邻居学习到的路由条数的总和

1.1.12 fast-reroute

fast-reroute 命令用来配置 RIP 快速重路由功能。

undo fast-reroute 命令用来关闭 RIP 快速重路由功能。

【命令】

fast-reroute route-policy route-policy-name

undo fast-reroute

【缺省情况】

RIP 快速重路由功能处于关闭状态。

【视图】

RIP 视图

【缺省用户角色】

network-admin
context-admin

【参数】

route-policy *route-policy-name* : 为通过策略的路由指定备份下一跳。
route-policy-name 为路由策略名, 为 1~63 个字符的字符串, 区分大小写。

【使用指导】

RIP 快速重路由功能只适合在主链路三层接口 **up**, 主链路由双通变为单通或者不通的情况下使用。在主链路三层接口 **down** 的情况下, 本功能不可用。单通现象, 即一条链路上的两端, 有且只有一端可以收到另一端发来的报文, 此链路称为单向链路。

RIP 快速重路由功能仅对非迭代 RIP 路由 (即从直连邻居学到 RIP 路由) 有效。
等价路由不支持快速重路由功能。

【举例】

配置对通过策略 frr 的路由指定备份下一跳信息。

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 100.1.1.0 24
[Sysname] route-policy frr permit node 10
[Sysname-route-policy-frr-10] if-match ip address prefix-list abc
[Sysname-route-policy-frr-10] apply fast-reroute backup-interface gigabitethernet 1/0/1
backup-nexthop 193.1.1.8
[Sysname-route-policy-frr-10] quit
[Sysname] rip 100
[Sysname-rip-100] fast-reroute route-policy frr
```

1.1.13 filter-policy export

filter-policy export 命令用来配置 RIP 对发布的路由信息进行过滤。

undo filter-policy export 命令用来取消 RIP 对发布路由信息的过滤。

【命令】

```
filter-policy { ipv4-acl-number | prefix-list prefix-list-name } export
[ interface-type interface-number | direct | { ospf | rip } [ process-id ] |
static ]
undo filter-policy export [ interface-type interface-number | direct | { ospf
| rip } [ process-id ] | static ]
```

【缺省情况】

RIP 不对发布的路由信息进行过滤。

【视图】

RIP 视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-acl-number: 用于过滤发布的路由信息的 IPv4 ACL 编号，取值范围为 2000~3999。

prefix-list prefix-list-name: 指定用于过滤发布路由信息的 IP 地址前缀列表名称。

prefix-list-name 为 IP 地址前缀列表名称，为 1~63 个字符的字符串，区分大小写。

interface-type interface-number: 过滤指定接口发布的路由信息，**interface-type** **interface-number** 为接口类型和编号。

direct: 对引入的直连路由进行过滤。

ospf: 对引入的 OSPF 路由进行过滤。

rip: 对引入的 RIP 路由进行过滤。

process-id: OSPF 或 RIP 协议的进程号，取值范围为 1~65535，缺省值为 1。

【使用指导】

一个协议或接口只能配置一个过滤策略。如果未指定协议或接口，就认为是配置全局过滤策略，同样每次只能配置一个。多次执行本命令，最后一次执行的命令生效。

如果已经配置了基于协议或接口的过滤策略，删除时必须指定协议或接口。

当配置的是高级 ACL（3000~3999）时，其使用规则如下：

- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard** 来过滤指定目的地址的路由。
- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard destination dest-addr dest-wildcard** 来过滤指定目的地址和掩码的路由。

其中，**source** 用来过滤路由目的地址，**destination** 用来过滤路由掩码，配置的掩码应该是连续的（当配置的掩码不连续时该过滤掩码的条件不生效）。

【举例】

配置使用编号为 2000 的基本 ACL 来对发布的路由信息进行过滤。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 export
```

配置按照地址前缀列表来过滤发布的路由信息。

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 11.0.0.0 8
[Sysname] rip 1
[Sysname-rip-1] filter-policy prefix-list abc export
```

使用编号为 3000 的高级 ACL 对发布的路由进行过滤，只允许 113.0.0.0/16 通过。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
```

```
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] rip 1
[Sysname-rip 1] filter-policy 3000 export
```

【命令参考】

- **acl** (ACL 命令参考/ACL)
- **import-route**
- **ip prefix-list** (三层技术-IP 路由命令参考/路由策略)

1.1.14 filter-policy import

filter-policy import 命令用来配置 RIP 对接收的路由信息进行过滤。

undo filter-policy import 命令用来取消对接收路由信息的过滤。

【命令】

```
filter-policy { ipv4-acl-number | gateway prefix-list-name | prefix-list
prefix-list-name [ gateway prefix-list-name ] } import [ interface-type
interface-number ]
undo filter-policy import [ interface-type interface-number ]
```

【缺省情况】

RIP 不对接收的路由信息进行过滤。

【视图】

RIP 视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4-acl-number: 用于过滤发布的路由信息的 IPv4 ACL 编号，取值范围为 2000~3999。

prefix-list prefix-list-name: 指定用于过滤接收路由信息的 IP 地址前缀列表名称。
prefix-list-name 为 IP 地址前缀列表名称，为 1~63 个字符的字符串，区分大小写。

gateway prefix-list-name: 基于要加入到路由表的路由信息的下一跳进行过滤。
prefix-list-name 为 IP 地址前缀列表名称，为 1~63 个字符的字符串，区分大小写。

interface-type interface-number: 过滤指定接口接收的路由信息，*interface-type interface-number* 为接口类型和编号。

【使用指导】

一个接口只能配置一个过滤策略。如果未指定接口，就认为是配置全局过滤策略，同样每次只能配置一个。多次执行本命令，最后一次执行的命令生效。

如果已经配置了基于接口的过滤策略，删除时必须指定 *interface-type interface-number*。
当配置的是高级 ACL（3000~3999）时，其使用规则如下：

- 使用命令 **rule [rule-id] { deny | permit } ip source *sour-addr* *sour-wildcard*** 来过滤指定目的地址的路由。

- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard destination dest-addr dest-wildcard** 来过滤指定目的地址和掩码的路由。

其中，**source** 用来过滤路由目的地址，**destination** 用来过滤路由掩码，配置的掩码应该是连续的（当配置的掩码不连续时该过滤掩码的条件不生效）。

【举例】

配置使用编号为 2000 的基本 ACL 来对接收的路由信息进行过滤。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 import
```

配置按照地址前缀列表来过滤接收的路由信息。

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 11.0.0.0 8
[Sysname] rip 1
[Sysname-rip-1] filter-policy prefix-list abc import
```

使用编号为 3000 的高级 ACL 对接收的路由进行过滤，只允许 113.0.0.0/16 通过。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] rip 1
[Sysname-rip-1] filter-policy 3000 import
```

【命令参考】

- **acl**（ACL 命令参考/ACL）
- **ip prefix-list**（三层技术-IP 路由命令参考/路由策略）

1.1.15 graceful-restart

graceful-restart 命令用来使能 RIP 协议的 GR 能力。

undo graceful-restart 命令用来关闭 RIP 协议的 GR 能力。

【命令】

```
graceful-restart
undo graceful-restart
```

【缺省情况】

RIP 协议的 GR 能力处于关闭状态。

【视图】

RIP 视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

RIP GR 特性与 RIP NSR 特性互斥,即 **graceful-restart** 和 **non-stop-routing** 命令互斥,不能同时配置。

【举例】

```
# 使能 RIP 进程 1 的 GR 能力。  
<Sysname> system-view  
[Sysname] rip 1  
[Sysname-rip-1] graceful-restart
```

1.1.16 graceful-restart interval

graceful-restart interval 命令用来配置 RIP 协议的 GR 重启间隔时间。

undo graceful-restart interval 命令用来恢复缺省情况。

【命令】

```
graceful-restart interval interval  
undo graceful-restart interval
```

【缺省情况】

RIP 协议的 GR 重启间隔时间为 60 秒。

【视图】

RIP 视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval: 指定 RIP 协议的 GR 重启间隔时间（期望重启时间），取值范围为 5～360，单位为秒。

【举例】

```
# 配置 RIP 进程 1 的 GR 重启间隔时间为 200 秒。  
<Sysname> system-view  
[Sysname] rip 1  
[Sysname-rip-1] graceful-restart interval 200
```

1.1.17 host-route

host-route 命令用来允许 RIP 接收主机路由。

undo host-route 命令用来禁止 RIP 接收主机路由。

【命令】

```
host-route
undo host-route
```

【缺省情况】

允许 RIP 接收主机路由。

【视图】

RIP 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

在某些特殊情况下，路由器会收到大量来自同一网段的主机路由。这些路由对于路由寻址没有多少作用，却占用了大量的资源；此时可以使用 **undo host-route** 命令禁止接收主机路由，以节省网络资源。

该命令仅对 RIPv2 报文携带的路由有效，对 RIPv1 报文携带的路由无效。

【举例】

```
# 禁止 RIP 接收主机路由。
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] undo host-route
```

1.1.18 import-route

import-route 命令用来从其它路由协议引入路由。

undo import-route 命令用来取消引入外部路由信息。

【命令】

```
import-route { direct | static } [ cost cost-value | route-policy
route-policy-name | tag tag ] *
import-route { ospf | rip } [ process-id | all-processes ] [ allow-direct | cost
cost-value | route-policy route-policy-name | tag tag ] *
undo import-route { direct { ospf | rip } [ process-id | all-processes ] |
static }
```

【缺省情况】

RIP 不引入其它路由。

【视图】

RIP 视图

【缺省用户角色】

```
network-admin
```

context-admin

【参数】

direct: 引入直连路由。

ospf: 引入 OSPF 协议的路由。

rip: 引入 RIP 协议的路由。

static: 引入静态路由。

process-id: OSPF 或 RIP 路由协议的进程号，取值范围为 1~65535，缺省值为 1。

all-processes: 引入 OSPF 或 RIP 路由协议所有进程的路由。

allow-direct: 在引入的路由中包含使能了该协议的接口网段路由。如果未指定本参数，在引入协议路由时不会包含使能了该协议的接口网段路由。当 **allow-direct** 与 **route-policy route-policy-name** 参数一起使用时，需要注意路由策略中配置的匹配规则不要与接口路由信息存在冲突，否则会导致 **allow-direct** 配置失效。例如，当配置 **allow-direct** 参数引入 OSPF 直连时，在路由策略中不要配置 **if-match route-type** 匹配条件，否则，**allow-direct** 参数失效。

cost cost-value: 所要引入路由的度量值，取值范围为 0~16，缺省值为 0。

route-policy route-policy-name: 路由策略名称，**route-policy-name** 为 1~63 个字符的字符串，区分大小写。

tag tag: 所要引入路由的标记值，取值范围为 0~65535，缺省值为 0。

【使用指导】

只能引入路由表中状态为 **active** 的路由，是否为 **active** 状态可以通过 **display ip routing-table protocol** 命令来查看。

undo import-route { ospf | rip } all-processes 命令只能取消 **import-route { ospf | rip } all-processes** 命令的配置，不能取消 **import-route { ospf | rip } process-id** 命令的配置。

【举例】

引入静态路由，并将其度量值设置为 4。

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4
```

【命令参考】

- **default cost**

1.1.19 maximum load-balancing

maximum load-balancing 命令用来配置 RIP 最大等价路由条数。

undo maximum load-balancing 命令用来恢复缺省情况。

【命令】

```
maximum load-balancing number
undo maximum load-balancing
```

【缺省情况】

RIP 支持的等价路由的最大条数与系统支持最大等价路由的条数相同。

【视图】

RIP 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

number：等价路由的最大条数，当 **number** 取值为 1 时，相当于不进行负载分担。

设备各款型中本参数的取值范围有所不同，详细差异信息如下：

型号	参数	描述
T5000-G20	等价路由的 最大条数	1~16
T5000-G30		1~32
T1000-G20/T1000-G50/T1000-G60/T1000-G80		1~16
T1000-CN60/T1000-CN80		1~32

【使用指导】

通过配置 **max-ecmp-num** 命令，对系统支持最大等价路由的条数进行修改，导致当前 RIP 支持的等价路由的最大条数大于 **max-ecmp-num** 命令的取值，那么设备重启后，RIP 支持的等价路由的最大条数自动修改为 **max-ecmp-num** 的取值。

【举例】

```
# 配置 RIP 最大等价路由条数为 2。
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] maximum load-balancing 2
```

【相关命令】

- **max-ecmp-num**（三层技术-IP 路由命令参考/IP 路由基础）

1.1.20 network

network 命令用来在指定网段上使能 RIP。

undo network 命令用来在指定网段上关闭 RIP。

【命令】

```
network network-address [ wildcard-mask ]  
undo network network-address
```

【缺省情况】

没有网段使能 RIP。

【视图】

RIP 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

network-address: 指定网段的地址，其取值可以为各个接口的 IP 网络地址。

wildcard-mask: IP 地址掩码的反码，相当于将 IP 地址的掩码取反（0 变 1，1 变 0）。其中，“1”表示忽略 IP 地址中对应的位，“0”表示必须保留此位。（例如：子网掩码 255.0.0.0，该掩码的反码为 0.255.255.255）。如果未指定本参数，将按照自然网段进行。

【使用指导】

RIP 只在指定网段的接口上运行，指定网段可以配置掩码；对于不在指定网段上的接口，RIP 既不在它上面接收和发送路由，也不将它的接口路由发布出去。因此，RIP 启动后必须指定其工作网段。在单进程情况下，可以使用 **network 0.0.0.0** 命令在所有接口上使能 RIP；在多进程情况下，无法使用 **network 0.0.0.0** 命令。

RIP 不支持将同一物理接口下的不同网段使能到不同的 RIP 进程中。

【举例】

```
# 在指定网段 129.102.0.0 上使能 RIP 进程 100。  
<Sysname> system-view  
[Sysname] rip 100  
[Sysname-rip-100] network 129.102.0.0
```

【相关命令】

- **rip enable**

1.1.21 non-stop-routing

non-stop-routing 命令用来使能 RIP 协议的 NSR 功能。

undo non-stop-routing 命令用来关闭 RIP 协议的 NSR 功能。

【命令】

```
non-stop-routing  
undo non-stop-routing
```

【缺省情况】

RIP 协议的 NSR 功能处于关闭状态。

【视图】

RIP 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

各个进程的 NSR 功能是相互独立的，只对本进程生效。如果存在多个 RIP 进程，建议在各个进程下使能 RIP NSR 功能。

RIP NSR 特性与 RIP GR 特性互斥，即 **non-stop-routing** 和 **graceful-restart** 命令互斥，不能同时配置。

【举例】

```
# 配置 RIP 进程 1 使能 NSR 功能。
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] non-stop-routing
```

1.1.22 output-delay

output-delay 用来配置 RIP 报文的发送速率。

undo output-delay 命令用来恢复缺省情况。

【命令】

```
output-delay time count count
undo output-delay
```

【缺省情况】

接口发送 RIP 报文的时间间隔为 20 毫秒，一次最多发送 3 个 RIP 报文。

【视图】

RIP 视图

【缺省用户角色】

network-admin

context-admin

【参数】

time: 接口发送 RIP 报文的时间间隔，取值范围为 10~100，单位为毫秒。

count: 接口一次发送 RIP 报文的最大个数，取值范围为 1~30。

【举例】

```
# 配置 RIP 进程 1 的所有接口发送 RIP 报文的时间间隔为 60 毫秒，一次最多发送 10 个 RIP 报文。
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] output-delay 60 count 10
```

1.1.23 peer

peer 命令用来配置 NBMA（Non-Broadcast Multi-Access，非广播多路访问）网络中 RIP 邻居的 IP 地址，并使更新报文以单播形式发送到对端，而不采用正常的组播或广播的形式。

undo peer 命令用来取消指定邻居 IP 地址。

【命令】

```
peer ip-address
undo peer ip-address
```

【缺省情况】

RIP 不向任何定点地址发送单播更新报文。

【视图】

RIP 视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: RIP 邻居 IP 地址，用点分十进制格式表示。

【使用指导】

当 RIP 邻居与当前设备直连时不推荐使用该命令，因为这样可能会造成对端同时收到同一路由信息的组播（或广播）和单播两种形式的报文。

配置本命令时，必须同时配置 **undo validate-source-address** 命令，即取消对接收到的 RIP 路由更新报文进行源 IP 地址检查。

【举例】

```
# 配置 RIP 邻居的 IP 地址为 202.38.165.1。
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] peer 202.38.165.1
```

【相关命令】

- **validate-source-address**

1.1.24 preference

preference 命令用来配置 RIP 路由的优先级。

undo preference 命令用来恢复缺省情况。

【命令】

```
preference { preference | route-policy route-policy-name } *
undo preference
```

【缺省情况】

RIP 路由的优先级为 100。

【视图】

RIP 视图

【缺省用户角色】

network-admin

context-admin

【参数】

preference: RIP 路由优先级的值，取值范围为 1~255，取值越小，优先级越高。

route-policy route-policy-name: 路由策略名称，*route-policy-name* 为 1~63 个字符的字符串，区分大小写。对满足特定条件的路由设置优先级。

【使用指导】

通过指定 **route-policy** 参数，可应用路由策略对特定的路由设置优先级：

- 如果在路由策略中已经设置了匹配路由的优先级，则匹配路由取路由策略设置的优先级，其它路由取 **preference** 命令所设优先级。
- 如果在路由策略中没有设置匹配路由的优先级，则所有路由都取 **preference** 命令所设优先级。

【举例】

```
# 配置 RIP 路由的优先级为 120。  
<Sysname> system-view  
[Sysname] rip 1  
[Sysname-rip-1] preference 120
```

1.1.25 reset rip process

reset rip process 命令用来重启指定 RIP 进程。

【命令】

reset rip process-id process

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: RIP 进程号，取值范围为 1~65535。

【使用指导】

执行该命令后，系统提示用户确认是否重启 RIP 协议。

【举例】

```
# 重启进程号为 100 的 RIP 进程。  
<Sysname> reset rip 100 process  
Reset RIP process? [Y/N]:y
```

1.1.26 reset rip statistics

reset rip statistics 命令用来清除指定 RIP 进程的统计信息，便于在调试时重新记录统计数据。

【命令】

```
reset rip process-id statistics
```

【视图】

用户视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

process-id: RIP 进程号，取值范围为 1~65535。

【举例】

```
# 清除进程号为 100 的 RIP 进程的统计信息。  
<Sysname> reset rip 100 statistics
```

1.1.27 rip

rip 命令用来启动 RIP，并进入 RIP 视图。

undo rip 命令用来关闭 RIP。

【命令】

```
rip [ process-id ] [ vpn-instance vpn-instance-name ]  
undo rip [ process-id ]
```

【缺省情况】

系统没有运行 RIP。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

process-id: RIP 进程号，取值范围为 1~65535，缺省值为 1。

vpn-instance vpn-instance-name: 指定 RIP 所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 RIP 位于公网中。

【使用指导】

必须先启动 RIP 进程，才能配置 RIP 的各种全局性参数，而配置与接口相关的参数时，可以不受这个限制。

关闭 RIP 进程后，原来配置的接口参数也同时失效。

【举例】

启动 RIP 进程 1，并进入 RIP 视图。

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1]
```

1.1.28 rip authentication-mode

rip authentication-mode 命令用来配置 RIP-2 的验证方式及验证参数。

undo rip authentication-mode 命令用来恢复缺省情况。

【命令】

```
rip authentication-mode { md5 { rfc2082 { cipher | plain } string key-id |
rfc2453 { cipher | plain } string } | simple { cipher | plain } string }
undo rip authentication-mode
```

【缺省情况】

未配置 RIP-2 的验证方式。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

md5: MD5 验证方式。

rfc2082: 指定 MD5 验证报文使用 RFC 2082 规定的报文格式。

cipher: 以密文方式设置密钥。

plain: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~16 个字符的字符串，密文密钥为 33~53 个字符的字符串。

key-id: 验证字标识符，取值范围为 1~255。

rfc2453: 指定 MD5 验证报文使用 RFC 2453 规定的报文格式（IETF 标准）。

simple: 简单验证方式。

【使用指导】

每次验证只支持一个验证字，新输入的验证字将覆盖旧验证字。

当 RIP 的版本为 RIP-1 时，虽然在接口视图下仍然可以配置验证方式，但由于 RIP-1 不支持认证，因此该配置不会生效。

【举例】

在接口 GigabitEthernet1/0/1 上配置 RFC 2453 格式的 MD5 明文验证，密钥为 rose。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip version 2
[Sysname-GigabitEthernet1/0/1] rip authentication-mode md5 rfc2453 plain rose
```

【命令参考】

- **rip version**

1.1.29 rip bfd

rip bfd 命令用来使能 RIP 的 BFD 功能。

undo rip bfd 命令用来关闭 RIP 的 BFD 功能。

【命令】

```
rip bfd { disable | enable [ ctrl | destination ip-address ] }
undo rip bfd
```

【缺省情况】

RIP 的 BFD 功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

disable: 在接口上关闭 RIP 的 BFD 功能。

enable: 在接口上使能 RIP 的 BFD 功能。

ctrl: 直连或非直连邻居均使用 control 报文双向检测方式。如果不指定该参数，对于直连邻居 RIP BFD 将使用 echo 报文单跳检测方式，对于非直连邻居 RIP BFD 将使用 control 报文双向检测方式。

destination ip-address: 指定 BFD 链路检测的目的地址。如果不指定该参数，RIP BFD 将使用邻居的 IP 地址作为链路检测的目的地址。

【使用指导】

目前 RIP 支持 BFD 提供了下面几种检测方式：

- **echo 报文单跳检测方式：**直连邻居使用。在对端有 RIP 路由发送时才能建立 BFD 会话。

- 指定目的地址的 echo 报文单跳检测方式: 直连邻居使用, 并且在接口上直接指定 RIP 邻居的 IP 地址。当该接口使能了 RIP 功能, 会建立到指定目的 IP 地址的 BFD 会话。
- control 报文双向检测方式: 直连邻居和非直连邻居均可以使用。当两端互有 RIP 路由发送时, 且使能 BFD 的接口与接收接口为同一接口, 邻居之间才能建立 BFD 会话。

如果指定了 **destination ip-address** 参数, RIP 会在该接口创建目的地址为 *ip-address* 的 echo 报文方式的 BFD 会话, 当检测到到达该目的地址的链路出现故障时, 便不再从该接口收、发任何 RIP 报文。

在 RIP 视图下配置了 **bfd all-interfaces enable** 后, 如果某接口的链路状态不稳定, 可能会导致 BFD 会话震荡, 继而影响网络的稳定性。这种情况下, 如需在该接口上关闭 RIP 的 BFD 功能, 减少对网络稳定性的影响, 必须使用 **rip bfd disable** 命令。

本端使用 control 报文双向检测方式时, 需要对端也使用 control 报文双向检测方式, 才能正常工作。由于 **peer** 命令与邻居之间没有对应关系, **undo peer** 操作并不能立刻删除邻居, 因此不能立刻删除 BFD 会话。

【举例】

```
# 在接口 GigabitEthernet1/0/1 使能 RIP 的 BFD 功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip bfd enable
```

1.1.30 rip default-route

rip default-route 命令用来配置 RIP 接口以指定度量值向 RIP 邻居发布一条缺省路由。

undo rip default-route 命令用来禁止 RIP 接口向 RIP 邻居发布缺省路由。

【命令】

```
rip default-route { { only | originate } [ cost cost-value | route-policy
route-policy-name ] * | no-originate }
undo rip default-route
```

【缺省情况】

RIP 接口是否发布缺省路由以 RIP 进程配置为准。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

only: 配置只发送缺省路由, 不发送普通路由。

originate: 配置既发送普通路由, 又发送缺省路由。

cost-value: 缺省路由的度量值, 取值范围为 1~15, 缺省值为 1。

route-policy route-policy-name: 路由策略名称, *route-policy-name* 为 1~63 个字符的字符串, 区分大小写。只有当前路由器的路由表中有路由匹配 *route-policy-name* 指定的路由策略时, 才发送缺省路由。

no-originate: 配置只发送普通路由, 不发布缺省路由。

【使用指导】

配置了发布缺省路由的 RIP 路由器不接收来自 RIP 邻居的缺省路由。

【举例】

配置接口 GigabitEthernet1/0/1 以指定度量值 2 向 RIP 邻居发布一条缺省路由, 而且只发送缺省路由, 不发送普通路由。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] rip default-route only cost 2
```

指定接口 GigabitEthernet1/0/1 以指定度量值 4 向 RIP 邻居既发布缺省路由, 而且发送普通路由。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] rip default-route originate cost 4
```

【相关命令】

- **default-route**

1.1.31 rip enable

rip enable 命令用来在接口上使能 RIP。

undo rip enable 命令用来在接口上关闭 RIP。

【命令】

rip process-id enable [exclude-subip]

undo rip enable

【缺省情况】

接口上没有使能 RIP。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: RIP 进程号, 取值范围为 1~65535。

exclude-subip: 不包括接口的从 IP 地址。如果未指定本参数, 将包括接口的从 IP 地址。

【使用指导】

本命令的优先级高于 **network** 命令。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上使能 RIP 进程 100。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip 100 enable
```

【相关命令】

- **network**

1.1.32 rip input

rip input 命令用来允许接口接收 RIP 报文。

undo rip input 命令用来禁止接口接收 RIP 报文。

【命令】

```
rip input
undo rip input
```

【缺省情况】

允许接口接收 RIP 报文。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 禁止接口 GigabitEthernet1/0/1 接收 RIP 报文。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo rip input
```

1.1.33 rip max-packet-length

rip max-packet-length 命令用来配置 RIP 报文的最大长度。

undo rip max-packet-length 命令用来恢复缺省情况。

【命令】

```
rip max-packet-length value
undo rip max-packet-length
```

【缺省情况】

RIP 报文的最大长度为 512 字节。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

value: 指定 RIP 报文的最大长度，取值范围为 32~65535，单位为字节。

【使用指导】

由于不同厂商对 RIP 报文最大长度的支持情况不同，要谨慎使用本特性，以免出现不兼容的情况。在配置认证的情况下，如果配置不当可能会造成报文无法发送，建议用户按照下面进行配置：

- 简单验证方式时，RIP 报文的最大长度不小于 52 字节；
- MD5 验证方式（使用 RFC 2453 规定的报文格式）时，RIP 报文的最大长度不小于 56 字节；
- MD5 验证方式（使用 RFC 2082 规定的报文格式）时，RIP 报文的最大长度不小于 72 字节。

如果配置值大于接口 MTU，则报文的最大长度为接口 MTU。

【举例】

```
# 在接口 GigabitEthernet1/0/1 配置 RIP 报文的最大长度为 1024 字节。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] rip max-packet-length 1024
```

1.1.34 rip metricin

rip metricin 命令用来配置接口接收 RIP 路由时的附加度量值。

undo rip metricin 命令用来恢复缺省情况。

【命令】

```
rip metricin [ route-policy route-policy-name ] value  
undo rip metricin
```

【缺省情况】

接口接收 RIP 路由时的附加度量值为 0。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

route-policy *route-policy-name*: 路由策略名称，*route-policy-name* 为 1~63 个字符的字符串，区分大小写。对满足特定条件的路由设置附加度量值。

value: 接收附加度量值，取值范围为 0~16。

【使用指导】

当接口收到一条合法的 RIP 路由，在将其加入路由表前，附加度量值会被加到该路由上。因此，增加接口的接收附加度量值，该接口收到的 RIP 路由的度量值也会相应增加，当附加度量值与原路由度量值之和大于 16，该条路由的度量值取 16。

通过指定 **route-policy** 参数，可应用路由策略对接口接收的特定路由设置附加度量值：

- 如果通过 **apply cost** 命令设置了匹配路由的附加度量值，则匹配路由的附加度量值取 **apply cost** 命令 *value* 参数设置的值，不匹配路由的附加度量值取本命令 *value* 参数所设的值。本命令不支持通过 **apply cost** 命令中的 **+**、**-** 关键字对接口接收 RIP 路由的附加度量值进行增加、减少的设置。
- 如果没有通过 **apply cost** 命令设置路由的附加度量值，则所有接收路由的附加度量值都取本命令 *value* 参数所设的值。

【举例】

对接口 GigabitEthernet1/0/1 接收的 RIP 路由附加度量值进行设置。其中，1.0.0.0/8 网段路由的附加度量值设置为 6，其它网段路由的附加度量值设置为 2。

```
<Sysname> system-view
[Sysname] ip prefix-list 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 10
[Sysname-route-policy-abc-10] if-match ip address prefix-list 123
[Sysname-route-policy-abc-10] apply cost 6
[Sysname-route-policy-abc-10] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip metricin route-policy abc 2
```

【相关命令】

- **apply cost**（三层技术-IP 路由命令参考/路由策略）

1.1.35 rip metricout

rip metricout 命令用来配置接口发送 RIP 路由时的附加度量值。

undo rip metricout 命令用来恢复缺省情况。

【命令】

```
rip metricout [ route-policy route-policy-name ] value
undo rip metricout
```

【缺省情况】

接口发送 RIP 路由时的附加度量值为 1。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

route-policy route-policy-name: 路由策略名称, *route-policy-name* 为 1~63 个字符的字符串, 区分大小写。对满足特定条件的路由设置附加度量值。

value: 发送附加度量值, 取值范围为 1~16。

【使用指导】

当发布一条 RIP 路由时, 附加度量值会在发布该路由之前附加在这条路由上。因此, 增加一个接口的发送附加度量值, 该接口发送的 RIP 路由的度量值也会相应增加。

通过指定 **route-policy** 参数, 可应用路由策略对接口发布的特定路由设置附加度量值:

- 如果通过 **apply cost** 命令设置了匹配路由的附加度量值, 则匹配路由的附加度量值取 **apply cost** 命令 *value* 参数设置的值, 不匹配路由的附加度量值取本命令 *value* 参数所设的值。本命令不支持通过 **apply cost** 命令中的 +、- 关键字对接口发布 RIP 路由的附加度量值进行增加、减少的设置。
- 如果没有通过 **apply cost** 命令设置路由的附加度量值, 则所有发布路由的附加度量值都取本命令 *value* 参数所设的值。

【举例】

对接口 GigabitEthernet1/0/1 发送的 RIP 路由附加度量值进行设置。其中, 1.0.0.0/8 网段路由的附加度量值设置为 6, 其它网段路由的附加度量值设置为 2。

```
<Sysname> system-view
[Sysname] ip prefix-list 123 permit 1.0.0.0 8
[Sysname] route-policy abc permit node 10
[Sysname-route-policy-abc-10] if-match ip address prefix-list 123
[Sysname-route-policy-abc-10] apply cost 6
[Sysname-route-policy-abc-10] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip metricout route-policy abc 2
```

【相关命令】

- **apply cost** (三层技术-IP 路由命令参考/路由策略)

1.1.36 rip mib-binding

rip mib-binding 命令用来配置 RIP 进程绑定 MIB。

undo rip mib-binding 命令用来恢复缺省情况。

【命令】

```
rip mib-binding process-id
undo rip mib-binding
```

【缺省情况】

MIB 绑定在进程号最小的 RIP 进程上。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

process-id: RIP 进程号，取值范围为 1~65535。

【使用指导】

如果指定的 *process-id* 不存在，配置 RIP 进程绑定命令不生效。

如果配置了 RIP 进程绑定 MIB，若删除 *process-id* 对应的 RIP 进程，则同时删除 RIP 进程绑定 MIB 配置，MIB 绑定到进程号最小的 RIP 进程上。

【举例】

```
# 配置 RIP 进程 100 绑定 MIB。  
<Sysname> system-view  
[Sysname] rip mib-binding 100
```

1.1.37 rip output

rip output 命令用来允许接口发送 RIP 报文。

undo rip output 命令用来禁止接口发送 RIP 报文。

【命令】

```
rip output  
undo rip output
```

【缺省情况】

允许接口发送 RIP 报文。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 禁止接口 GigabitEthernet1/0/1 发送 RIP 报文。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] undo rip output
```

1.1.38 rip output-delay

rip output-delay 命令用来配置接口下 RIP 报文的发送速率。

undo rip output-delay 命令用来恢复缺省情况。

【命令】

```
rip output-delay time count count
undo rip output-delay
```

【缺省情况】

RIP 报文的发包速率由进程全局的配置决定。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

time: 接口发送 RIP 报文的时间间隔，取值范围为 10~100，单位为毫秒。

count: 接口一次发送 RIP 报文的最大个数，取值范围为 1~30。

【举例】

在接口 GigabitEthernet1/0/1 配置发送 RIP 报文的时间间隔为 30 毫秒，一次最多发送 6 个 RIP 报文。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip output-delay 30 count 6
```

【相关命令】

- **output-delay**

1.1.39 rip poison-reverse

rip poison-reverse 命令用来使能毒性逆转功能。

undo rip poison-reverse 命令用来关闭毒性逆转功能。

【命令】

```
rip poison-reverse
undo rip poison-reverse
```

【缺省情况】

毒性逆转功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```


【举例】

```
# 在接口 GigabitEthernet1/0/1 上配置对 RIP 更新报文进行毒性逆转。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip poison-reverse
```

1.1.40 rip primary-path-detect bfd

rip primary-path-detect bfd 命令用来使能 RIP 协议中主用链路使能 BFD 检测功能。

undo rip primary-path-detect bfd 命令用来关闭 RIP 协议中主用链路的 BFD 检测功能。

【命令】

```
rip primary-path-detect bfd { ctrl | echo }
undo rip primary-path-detect bfd
```

【缺省情况】

RIP 协议中主用链路的 BFD 检测功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ctrl: 通过控制报文方式的 BFD 会话对主用链路进行检测。

echo: 通过 echo 报文方式的 BFD 会话对主用链路进行检测。

【使用指导】

配置本功能后，RIP 协议的快速重路由特性中的主用链路将使用 BFD 进行检测。

本端使用 control 报文双向检测方式时，需要对端也使用 control 报文双向检测方式，才能正常工作。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上配置 RIP 协议快速重路由特性中主用链路使能 BFD（Echo 方式）检测功能。
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] fast-reroute route-policy frr
[Sysname-rip-1] quit
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip primary-path-detect bfd echo
```

1.1.41 rip split-horizon

rip split-horizon 命令用来使能水平分割功能。

undo rip split-horizon 命令用来关闭水平分割功能。

【命令】

```
rip split-horizon
undo rip split-horizon
```

【缺省情况】

水平分割功能处于使能状态。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

通常情况下，为了防止路由环路的出现，水平分割是必要的，因此，建议不要关闭水平分割。当因为特殊需要，如为保证协议的正确执行，需要关闭水平分割时，请一定要确认是否必要。

如果同时使能了水平分割和毒性逆转，则只有毒性逆转功能生效。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上配置水平分割。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip split-horizon
```

1.1.42 rip summary-address

rip summary-address 命令用来配置一条聚合路由。

undo rip summary-address 命令用来取消指定的聚合路由。

【命令】

```
rip summary-address ip-address { mask-length | mask }
undo rip summary-address ip-address { mask-length | mask }
```

【缺省情况】

未配置聚合路由。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ip-address: 聚合路由的目的 IP 地址。

mask-length: 聚合路由的网络掩码长度，取值范围为 0~32。

mask: 聚合路由的网络掩码，点分十进制格式。

【使用指导】

该功能仅在自动路由聚合功能被关闭时才能生效。

【举例】

在接口 GigabitEthernet1/0/1 下配置一条聚合路由。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip summary-address 10.0.0.0 255.255.255.0
```

【相关命令】

- **summary**

1.1.43 rip version

rip version 命令用来配置接口运行的 RIP 版本。

undo rip version 命令用来恢复缺省情况。

【命令】

```
rip version { 1 | 2 [ broadcast | multicast ] }
undo rip version
```

【缺省情况】

未配置接口运行的 RIP 版本。接口只能发送 RIP-1 广播报文，可以接收 RIP-1 广播/单播报文、RIP-2 广播/组播/单播报文。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

1: 接口运行 RIP 协议的版本为 RIP-1。

2: 接口运行 RIP 协议的版本为 RIP-2。

[**broadcast | multicast**]: RIP-2 报文的发送方式为广播方式（**broadcast**）还是组播方式（**multicast**），缺省为组播方式（**multicast**）。

【使用指导】

如果接口上配置了 RIP 版本，以接口配置的为准；如果接口上没有配置 RIP 版本，接口运行的 RIP 版本以全局配置的为准。

当接口运行的 RIP 版本为 RIP-1 时：

- 发送 RIP-1 广播报文
- 接收 RIP-1 广播/单播报文

当接口运行在 RIP-2 广播方式时：

- 发送 RIP-2 广播报文
- 接收 RIP-1 广播/单播报文、RIP-2 广播/组播/单播报文

当接口运行在 RIP-2 组播方式时：

- 发送 RIP-2 组播报文
- 接收 RIP-2 广播/组播/单播报文

【举例】

```
# 配置接口 GigabitEthernet1/0/1 以广播方式发送 RIP-2 报文。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rip version 2 broadcast
```

【相关命令】

- **version**

1.1.14 silent-interface

silent-interface 命令用来配置接口工作在抑制状态，即接口只接收 RIP 报文而不发送 RIP 报文。

undo silent-interface 命令用来取消接口的抑制状态。

【命令】

```
silent-interface { interface-type interface-number | all }
undo silent-interface { interface-type interface-number | all }
```

【缺省情况】

允许所有接口发送 RIP 报文。

【视图】

RIP 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interface-type interface-number：接口类型和编号。
all：抑制所有接口。

【举例】

```
# 将所有接口设置为抑制状态，随后激活指定接口 GigabitEthernet1/0/1。
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] silent-interface all
[Sysname-rip-100] undo silent-interface gigabitethernet 1/0/1
[Sysname-rip-100] network 131.108.0.0
```

1.1.45 summary

summary 命令用来使能 RIP-2 自动路由聚合功能, 聚合后的路由以使用自然掩码的路由形式发布, 减小了路由表的规模。

undo summary 命令用来关闭 RIP-2 自动路由聚合功能, 以便将所有子网路由广播出去。

【命令】

```
summary
undo summary
```

【缺省情况】

RIP-2 自动路由聚合功能处于使能状态。

【视图】

RIP 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

使能 RIP-2 自动路由聚合功能可以减小路由表规模, 提高大型网络的可扩展性和效率。

【举例】

```
# 关闭 RIP-2 自动路由聚合功能。
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] undo summary
```

【相关命令】

- **rip summary-address**
- **rip version**

1.1.46 timer triggered

timer triggered 命令用来配置触发更新的时间间隔。

undo timer triggered 命令用来恢复缺省情况。

【命令】

```
timer          triggered          maximum-interval          [          minimum-interval
[ incremental-interval ] ]
undo timer triggered
```

【缺省情况】

发送触发更新的最大时间间隔为 5 秒, 最小间隔为 50 毫秒, 增量惩罚间隔为 200 毫秒。

【视图】

RIP 视图

【缺省用户角色】

network-admin
context-admin

【参数】

maximum-interval: 触发更新的最大间隔时间。取值范围为 1~5，单位为秒。

minimum-interval: 触发更新的最小间隔时间。取值范围为 10~5000，单位为毫秒。

incremental-interval: 触发更新间隔的增加时间。取值范围为 100~1000，单位为毫秒。

【使用指导】

本命令在网络变化不频繁的情况下将触发更新的时间间隔缩小到 *minimum-interval*，而在网络变化频繁的情况下可以进行相应惩罚，将时间间隔按照配置的惩罚增量延长，最大不超过 *maximum-interval*。

minimum-interval 和 *incremental-interval* 配置值不允许大于 *maximum-interval* 配置值。

【举例】

```
# 配置发送触发更新的最大时间间隔为 2 秒，最小时间间隔为 100 毫秒，惩罚增量为 100 毫秒。  
<Sysname> system-view  
[Sysname] rip 1  
[Sysname-rip-1] timer triggered 2 100 100
```

1.1.47 timers

timers 命令用来配置 RIP 定时器的值，可通过调节 RIP 定时器来调整路由协议的性能，以满足网络需要。

undo timers 命令用来恢复 RIP 定时器的缺省值。

【命令】

```
timers { garbage-collect garbage-collect-value | suppress suppress-value |  
timeout timeout-value | update update-value } *  
undo timers { garbage-collect | suppress | timeout | update } *
```

【缺省情况】

Garbage-collect 定时器的值为 120 秒，Suppress 定时器的值为 120 秒，Timeout 定时器的值为 180 秒，Update 定时器的值为 30 秒。

【视图】

RIP 视图

【缺省用户角色】

network-admin
context-admin

【参数】

garbage-collect-value: Garbage-collect 定时器的值，取值范围为 1~3600，单位为秒。

suppress-value: Suppress 定时器的值，取值范围为 0~3600，单位为秒。

timeout-value: Timeout 定时器的值，取值范围为 1~3600，单位为秒。

update-value: Update 定时器的值，取值范围为 1~3600，单位为秒。

【使用指导】

RIP 受四个定时器的控制，分别是 Update、Timeout、Suppress 和 Garbage-Collect，其中：

- Update 定时器，定义了发送更新报文的时间间隔。
- Timeout 定时器，定义了路由老化时间。如果在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16。
- Suppress 定时器，定义了 RIP 路由处于抑制状态的时间段长度。当一条路由的度量值变为 16 时，该路由将进入被抑制状态。在被抑制状态，只有来自同一邻居，且度量值小于 16 的路由更新才会被路由器接收，取代不可达路由。
- Garbage-Collect 定时器，定义了一条路由从度量值变为 16 开始，直到它从路由表里被删除所经过的时间。在 Garbage-Collect 时间内，RIP 以 16 作为度量值向外发送这条路由的更新，如果 Garbage-Collect 超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除。

通常情况下，无需改变各定时器的缺省值，该命令须谨慎使用。

各个定时器的值在网络中所有的路由器上必须保持一致。

Timeout 定时器的值要大于 Update 定时器的值。

【举例】

分别设置 RIP 各定时器的值：其中，Update 定时器的值为 5 秒、Timeout 定时器的值为 15 秒、Suppress 定时器的值为 15 秒、Garbage-Collect 定时器的值为 30 秒。

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

1.1.48 validate-source-address

validate-source-address 命令用来使能对接收到的 RIP 路由更新报文进行源 IP 地址检查的功能。

undo validate-source-address 命令用来关闭对接收到的 RIP 路由更新报文进行源 IP 地址检查的功能。

【命令】

validate-source-address

undo validate-source-address

【缺省情况】

对接收到的 RIP 路由更新报文进行源 IP 地址检查的功能处于使能状态。

【视图】

RIP 视图

【缺省用户角色】

network-admin

context-admin

【举例】

关闭对接收到的 RIP 路由更新报文进行源 IP 地址检查的功能。

```
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] undo validate-source-address
```

1.1.49 version

version 命令用来配置全局 RIP 版本。

undo version 命令用来恢复缺省情况。

【命令】

```
version { 1 | 2 }
undo version
```

【缺省情况】

未配置全局 RIP 版本。接口只能发送 RIP-1 广播报文，可以接收 RIP-1 广播/单播报文、RIP-2 广播/组播/单播报文。

【视图】

RIP 视图

【缺省用户角色】

network-admin
context-admin

【参数】

- 1: 指定为 RIP-1 版本。
- 2: 指定为 RIP-2 版本，RIP-2 报文的发送方式为组播方式。

【使用指导】

配置全局 RIP 版本时，其生效规则如下：

- 如果接口上配置了 RIP 版本，以接口配置的为准。
- 如果接口没有配置 RIP 版本，将全局 RIP 版本配置为 1 时，接口运行的 RIP 版本为 RIP-1，发送 RIP-1 广播报文，可以接收 RIP-1 广播/单播报文。
- 如果接口没有配置 RIP 版本，将全局 RIP 版本配置为 2 时，接口运行的 RIP 版本为 RIP-2 且工作在组播方式，发送 RIP-2 组播报文，可以接收 RIP-2 广播/组播/单播。

【举例】

```
# 指定全局 RIP 版本为 RIP-2。
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] version 2
```

【相关命令】

- **rip version**

目 录

1 OSPF.....	1-1
1.1 OSPF配置命令	1-1
1.1.1 abr-summary (OSPF area view).....	1-1
1.1.2 area (OSPF view)	1-2
1.1.3 asbr-summary (OSPF view)	1-2
1.1.4 authentication-mode.....	1-3
1.1.5 bandwidth-reference (OSPF view)	1-5
1.1.6 database-filter peer (OSPF view)	1-6
1.1.7 default (OSPF view)	1-7
1.1.8 default-cost (OSPF area view)	1-8
1.1.9 default-route-advertise (OSPF view)	1-9
1.1.10 description (OSPF/OSPF area view)	1-10
1.1.11 discard-route.....	1-11
1.1.12 display ospf	1-12
1.1.13 display ospf abr-asbr	1-19
1.1.14 display ospf abr-summary	1-21
1.1.15 display ospf asbr-summary	1-23
1.1.16 display ospf event-log	1-24
1.1.17 display ospf event-log hello	1-28
1.1.18 display ospf fast-reroute lfa-candidate	1-33
1.1.19 display ospf graceful-restart	1-34
1.1.20 display ospf hostname-table	1-37
1.1.21 display ospf interface	1-38
1.1.22 display ospf interface hello	1-41
1.1.23 display ospf lsdb	1-43
1.1.24 display ospf nexthop	1-50
1.1.25 display ospf non-stop-routing status	1-51
1.1.26 display ospf peer.....	1-52
1.1.27 display ospf peer statistics	1-57
1.1.28 display ospf request-queue	1-58
1.1.29 display ospf retrans-queue	1-59
1.1.30 display ospf routing	1-61
1.1.31 display ospf spf-tree	1-65

1.1.32 display ospf statistics	1-68
1.1.33 display ospf vlink.....	1-73
1.1.34 display router id	1-75
1.1.35 dscp.....	1-75
1.1.36 ecmp-group enable	1-76
1.1.37 enable link-local-signaling	1-76
1.1.38 enable out-of-band-resynchronization.....	1-77
1.1.39 event-log	1-77
1.1.40 fast-reroute (OSPF view)	1-78
1.1.41 filter (OSPF area view)	1-79
1.1.42 filter-policy export (OSPF view)	1-80
1.1.43 filter-policy import (OSPF view)	1-81
1.1.44 graceful-restart (OSPF view)	1-83
1.1.45 graceful-restart helper enable	1-84
1.1.46 graceful-restart helper strict-lsa-checking	1-85
1.1.47 graceful-restart interval (OSPF view).....	1-85
1.1.48 host-advertise	1-86
1.1.49 hostname	1-87
1.1.50 import-route (OSPF view)	1-88
1.1.51 ispf enable (OSPF view)	1-89
1.1.52 log-peer-change	1-90
1.1.53 lsa-arrival-interval.....	1-90
1.1.54 lsa-generation-interval.....	1-91
1.1.55 lsdb-overflow-interval	1-92
1.1.56 lsdb-overflow-limit	1-93
1.1.57 maximum load-balancing (OSPF view)	1-94
1.1.58 network (OSPF area view)	1-94
1.1.59 non-stop-routing	1-95
1.1.60 nssa (OSPF area view)	1-96
1.1.61 opaque-capability enable	1-97
1.1.62 ospf	1-98
1.1.63 ospf area.....	1-99
1.1.64 ospf authentication-mode.....	1-100
1.1.65 ospf bfd enable.....	1-102
1.1.66 ospf cost (Interface view)	1-103
1.1.67 ospf database-filter.....	1-103

1.1.68 ospf dr-priority	1-104
1.1.69 ospf fast-reroute lfa-backup	1-105
1.1.70 ospf mib-binding	1-106
1.1.71 ospf mtu-enable	1-106
1.1.72 ospf network-type	1-107
1.1.73 ospf prefix-suppression	1-108
1.1.74 ospf primary-path-detect bfd	1-109
1.1.75 ospf timer dead	1-110
1.1.76 ospf timer hello	1-111
1.1.77 ospf timer poll	1-112
1.1.78 ospf timer retransmit	1-112
1.1.79 ospf trans-delay	1-113
1.1.80 ospf ttl-security	1-114
1.1.81 peer (OSPF view)	1-115
1.1.82 pic (OSPF view)	1-116
1.1.83 preference (OSPF view)	1-117
1.1.84 prefix-priority (OSPF view)	1-118
1.1.85 prefix-suppression	1-119
1.1.86 reset ospf event-log	1-120
1.1.87 reset ospf event-log hello	1-120
1.1.88 reset ospf process	1-121
1.1.89 reset ospf redistribution	1-122
1.1.90 reset ospf statistics	1-122
1.1.91 rfc1583 compatible	1-123
1.1.92 router id	1-123
1.1.93 silent-interface (OSPF view)	1-124
1.1.94 snmp trap rate-limit	1-125
1.1.95 snmp-agent trap enable ospf	1-126
1.1.96 spf-schedule-interval (OSPF view)	1-127
1.1.97 stub (OSPF area view)	1-128
1.1.98 stub-router (OSPF view)	1-129
1.1.99 transmit-pacing	1-130
1.1.100 ttl-security	1-131
1.1.101 vlink-peer (OSPF area view)	1-132

1 OSPF

1.1 OSPF配置命令

1.1.1 abr-summary (OSPF area view)

abr-summary 命令用来配置 ABR 路由聚合。

undo abr-summary 命令用来取消 ABR 对指定网段的路由聚合。

【命令】

```
abr-summary ip-address { mask-length | mask } [ advertise | not-advertise ]  
[ cost cost-value ]  
undo abr-summary ip-address { mask-length | mask }
```

【缺省情况】

ABR 不对路由进行聚合。

【视图】

OSPF 区域视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: 聚合路由的目的 IP 地址。

mask-length: 聚合路由的网络掩码长度，取值范围为 0~32。

mask: 聚合路由的网络掩码，点分十进制形式。

advertise | not-advertise: 是否发布这条聚合路由。缺省时发布聚合路由。

cost cost-value: 聚合路由的开销值，取值范围为 1~16777215，缺省值为所有被聚合的路由中最大的开销值。

【使用指导】

本命令只适用于区域边界路由器（ABR），用来对某一个区域内的路由信息进行聚合。对于属于该聚合网段范围的路由，ABR 向其它区域只发送一条聚合后的路由。一个区域可配置多条聚合网段，这样 OSPF 可对多个网段进行聚合。

当配置了 **undo abr-summary** 命令后，原来被聚合的路由又重新被发布。

【举例】

将 OSPF 区域 1 中两个网段 36.42.10.0/24 和 36.42.110.0/24 的路由聚合成一条聚合路由 36.42.0.0/16 向其它区域发布。

```
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] area 1
```

```
[Sysname-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

1.1.2 area (OSPF view)

area 命令用来创建 OSPF 区域，并进入 OSPF 区域视图。

undo area 命令用来删除指定的 OSPF 区域。

【命令】

```
area area-id
undo area area-id
```

【缺省情况】

不存在 OSPF 区域。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

area-id: 区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其转换成 IP 地址格式）或者是 IP 地址格式。

【举例】

创建 OSPF 区域 0 并进入 OSPF 区域视图。

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]
```

1.1.3 asbr-summary (OSPF view)

asbr-summary 命令用来配置 ASBR 路由聚合。

undo asbr-summary 命令用来取消 ASBR 对指定网段的路由聚合。

【命令】

```
asbr-summary ip-address { mask-length | mask } [ cost cost-value |
not-advertise | nssa-only | tag tag ] *
undo asbr-summary ip-address { mask-length | mask }
```

【缺省情况】

ASBR 不对路由进行聚合。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: 聚合路由的目的 IP 地址。

mask-length: 聚合路由的网络掩码长度，取值范围为 0~32。

mask: 聚合路由的网络掩码，点分十进制格式。

cost cost-value: 聚合路由的开销值，取值范围为 1~16777214。如果未指定本参数，**cost-value** 取所有被聚合的路由中最大的开销值作为聚合路由的开销值；如果是 Type-7 LSA 转化成的 Type-5 LSA 描述的路由匹配聚合、且是 Type2 外部路由，则 **cost-value** 取所有被聚合的路由中最大的开销值加 1 作为聚合路由的开销值。

not-advertise: 不通告聚合路由。如果未指定本参数，将通告聚合路由。

nssa-only: 设置 Type-7 LSA 的 P 比特位为不置位，即在对端路由器上不能转为 Type-5 LSA。缺省时，Type-7 LSA 的 P 比特位被置位，即在对端路由器上可以转为 Type-5 LSA（如果本地路由器是 ABR，则会检查骨干区域是否存在 FULL 状态的邻居，当 FULL 状态的邻居存在时，产生的 Type-7 LSA 中 P 比特位不置位）。

tag tag: 聚合路由的标识，可以通过路由策略控制聚合路由的发布，取值范围为 0~4294967295，缺省值为 1。

【使用指导】

如果本地路由器是 ASBR，对引入的聚合地址范围内的 Type-5 LSA 描述的路由进行聚合；当配置了 NSSA 区域时，对引入的聚合地址范围内的 Type-7 LSA 描述的路由进行聚合。

如果本地路由器同时是 ASBR 和 ABR，并且是 NSSA 区域的转换路由器，将对由 Type-7 LSA 转化成的 Type-5 LSA 进行聚合处理；如果不是 NSSA 区域的转换路由器，则不进行聚合处理。

配置 **asbr-summary** 命令后，对处于聚合地址范围内的外部路由，本地路由器只向邻居路由器发布一条聚合后的路由；配置 **undo asbr-summary** 命令后，原来被聚合的外部路由将重新被发布。

【举例】

配置 OSPF 对引入的路由进行聚合，聚合路由的标识为 2，开销值为 100。

```
<Sysname> system-view
[Sysname] ip route-static 10.2.1.0 24 null 0
[Sysname] ip route-static 10.2.2.0 24 null 0
[Sysname] ospf 100
[Sysname-ospf-100] import-route static
[Sysname-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 tag 2 cost 100
```

1.1.4 authentication-mode

authentication-mode 命令用来配置 OSPF 区域所使用的验证模式。

undo authentication-mode 命令用来取消 OSPF 区域所使用的验证模式。

【命令】

MD5/HMAC-MD5 验证模式：

```
authentication-mode { hmac-md5 | md5 } key-id { cipher | plain } string  
undo authentication-mode [ { hmac-md5 | md5 } key-id ]
```

简单验证模式：

```
authentication-mode simple { cipher | plain } string  
undo authentication-mode
```

keychain 验证模式：

```
authentication-mode keychain keychain-name  
undo authentication-mode
```

【缺省情况】

未配置区域验证模式。

【视图】

OSPF 区域视图

【缺省用户角色】

network-admin
context-admin

【参数】

hmac-md5：HMAC-MD5 验证模式。

md5：MD5 验证模式。

simple：简单验证模式。

key-id：验证字标识符，取值范围为 0～255。

cipher：以密文方式设置密钥。

plain：以明文方式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。简单验证模式下，明文密钥为 1～8 个字符的字符串；密文密钥为 33～41 个字符的字符串。MD5/HMAC-MD5 验证模式下，明文密钥为 1～16 个字符的字符串；密文密钥为 33～53 个字符的字符串。

keychain：使用 keychain 验证方式。

keychain-name：keychain 名称，为 1～63 个字符的字符串，区分大小写。

【使用指导】

一个区域中所有路由器的验证模式和验证密码必须一致。

OSPF 可指定区域下使用 MD5/HMAC-MD5 验证或简单验证两种方式，但不能同时指定；使用 MD5/HMAC-MD5 验证方式时，可配置多条 MD5/HMAC-MD5 验证命令，但 **key-id** 是唯一的，同一 **key-id** 只能配置一个验证字。

修改 OSPF 区域的 MD5/HMAC-MD5 验证字的步骤如下：

- 首先在该区域配置新的 MD5/HMAC-MD5 验证字；此时若邻居设备尚未配置新的 MD5/HMAC-MD5 验证字，便会触发 MD5/HMAC-MD5 验证平滑迁移过程。在这个过程中，OSPF 会发送分别携带各个 MD5/HMAC-MD5 验证字的多份报文，使得已配置新验证字的邻居设备和尚未配置新验证字的邻居设备都能通过验证，保持邻居关系。

- 然后在各个邻居设备上也都配置相同的新 MD5/HMAC-MD5 验证字；当本设备上收到所有邻居的携带新验证字的报文后，便会退出 MD5/HMAC-MD5 验证平滑迁移过程。
- 最后在本设备和所有邻居上都删除旧的 MD5/HMAC-MD5 验证字；建议区域下不要保留多个 MD5/HMAC-MD5 验证字，每次 MD5/HMAC-MD5 验证字修改完毕后，应当及时删除旧的验证字，这样可以防止与持有旧验证字的系统继续通信、减少被攻击的可能，还可以减少验证迁移过程对系统、带宽的消耗。

在 OSPF 区域使用 keychain 验证方式时，报文的收、发过程如下：

- OSPF 在发送报文前，会先从 keychain 获取当前的有效发送 key，然后发送报文。如果当前不存在有效发送 key，则不会发送报文。
- OSPF 在收到报文后，会根据报文携带的 key 的标识符从本地 keychain 中查找具有相同标识符的 key，找到且该 key 为有效 key，则根据该 key 的认证算法和认证密钥对报文进行校验，校验成功后再对报文进行下一步处理。如果报文校验失败，或者根据报文中携带的 key 的标识符无法从 keychain 中获取到有效接收 key，则该报文将被丢弃。

对于 keychain 认证算法和 key 的标识符的范围，OSPF 的支持情况如下：

- OSPF 仅支持 MD5 和 HMAC-MD5 认证算法。
- OSPF 仅支持 keychain 中 key-id 的范围在 0~255 内的 key，如果接收报文的 key-id 不在这个范围内，则该报文将被丢弃。

【举例】

配置 OSPF 区域 0 使用 MD5 明文验证模式，验证字标识符为 15，验证密钥为 abc。

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] authentication-mode md5 15 plain abc
```

【相关命令】

- **ospf authentication-mode**

1.1.5 bandwidth-reference (OSPF view)

bandwidth-reference 命令用来配置计算链路开销时所依据的带宽参考值。

undo bandwidth-reference 命令用来恢复缺省情况。

【命令】

```
bandwidth-reference value
undo bandwidth-reference
```

【缺省情况】

计算链路开销时所依据的带宽参考值为 100Mbps。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

value: 计算链路开销时所依据的带宽参考值，取值范围为 1~4294967，单位为 Mbps。

【使用指导】

如果没有配置链路的开销值，OSPF 根据链路带宽来计算开销值，接口开销=带宽参考值÷接口期望带宽（接口期望带宽通过命令 **bandwidth** 进行配置，具体情况请参见接口分册命令参考中的介绍）。当计算出来的开销值大于 65535 时，开销取最大值 65535；当计算出来的开销值小于 1 时，开销取最小值 1。

【举例】

```
# 配置链路的带宽参考值为 1000Mbps。
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] bandwidth-reference 1000
```

【相关命令】

- **ospf cost**

1.1.6 database-filter peer (OSPF view)

database-filter peer 命令用来对发送给指定邻居的 LSA 进行过滤。

undo database-filter peer 命令用来恢复缺省情况。

【命令】

```
database-filter peer ip-address { all | { ase [ acl ipv4-acl-number ] | nssa  
[ acl ipv4-acl-number ] | summary [ acl ipv4-acl-number ] } * }  
undo database-filter peer ip-address
```

【缺省情况】

不对发送给指定邻居的 LSA 进行过滤。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: 接口的网络类型为 P2MP 的邻居的 IP 地址。

all: 对发送给接口的网络类型为 P2MP 的邻居的所有 LSA 进行过滤（除了 Grace LSA）。

ase: 对发送给接口的网络类型为 P2MP 的邻居的 Type-5 LSA 进行过滤。

nssa: 对发送给接口的网络类型为 P2MP 的邻居的 Type-7 LSA 进行过滤。

summary: 对发送给接口的网络类型为 P2MP 的邻居的 Type-3 LSA 进行过滤。

acl ipv4-acl-number: 指定的基本或高级 IPv4 ACL 编号，取值范围为 2000~3999。

【使用指导】

当两台路由器之间存在多条 P2MP 链路时，路由器上会存在多个接口的网络类型为 P2MP 的 OSPF 邻居。不愿让某个指定邻居收到的 LSA，通过该功能可在本地将其过滤掉。

当配置的是高级 ACL（3000~3999）时，其使用规则如下：

- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard** 来过滤携带指定链路状态 ID 的 LSA。
- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard destination dest-addr dest-wildcard** 来过滤携带指定链路状态 ID 和掩码的 LSA。

其中，**source** 用来过滤 LSA 的链路状态 ID，**destination** 用来过滤 LSA 的掩码，配置的掩码应该是连续的（当配置的掩码不连续时该过滤掩码的规则不生效）。

如果在配置该命令前邻居路由器就已经收到了将要进行过滤的 LSA，那么配置该命令后，这些 LSA 仍存在于邻居路由器的 LSDB 中。

【举例】

配置对发送给接口的网络类型为 P2MP 的邻居的所有 LSA 进行过滤。

```
<Sysname> system-view
```

```
[Sysname] ospf 1
```

```
[Sysname-ospf-1] database-filter peer 121.20.20.121 all
```

配置编号为 3000 的高级 ACL 对发送给邻居 121.20.20.121 的 Type-3 LSA 进行过滤。

```
<Sysname> system-view
```

```
[Sysname] acl advanced 3000
```

```
[Sysname-acl-ipv4-adv-3000] rule 10 deny ip source 121.20.0.0 0 destination 255.255.0.0 0
```

```
[Sysname-acl-ipv4-adv-3000] rule 100 permit ip
```

```
[Sysname-acl-ipv4-adv-3000] quit
```

```
[Sysname] ospf 1
```

```
[Sysname-ospf-1] database-filter peer 121.20.20.121 summary acl 3000
```

【相关命令】

- **ospf database-filter**

1.1.7 default (OSPF view)

default 命令用来配置引入外部路由时的缺省参数，包括 OSPF 引入外部路由的开销、类型和标记。

undo default 命令用来取消引入外部路由时的缺省参数的配置。

【命令】

```
default { cost cost-value | tag tag | type type } *
```

```
undo default { cost | tag | type } *
```

【缺省情况】

OSPF 引入的外部路由的度量值为 1，引入的外部路由的标记为 1，引入的外部路由类型为 2。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

cost *cost-value*: OSPF 引入的外部路由的缺省度量值, *cost-value* 的取值范围为 0~16777214。

tag *tag*: 外部路由的标记, *tag* 的取值范围为 0~4294967295。

type *type*: 外部路由类型, *type* 的取值范围为 1~2。

【举例】

配置外部路由开销、标记和类型的缺省值分别为 10、100 和 2。

```
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] default cost 10 tag 100 type 2
```

【相关命令】

- **import-route**

1.1.8 default-cost (OSPF area view)

default-cost 命令用来配置发送到 Stub 区域或 NSSA 区域的缺省路由的开销。

undo default-cost 命令用来恢复缺省情况。

【命令】

default-cost *cost-value*
undo default-cost

【缺省情况】

发送到 Stub 区域或 NSSA 区域的缺省路由的开销为 1。

【视图】

OSPF 区域视图

【缺省用户角色】

network-admin
context-admin

【参数】

cost-value: 发送到 Stub 区域或 NSSA 区域的缺省路由的开销值, 取值范围为 0~16777214。

【使用指导】

该命令只有在 Stub 区域的 ABR 或 NSSA 区域的 ABR/ASBR 上配置才能生效。

【举例】

将区域 1 设置成 Stub 区域, 配置发送到该 Stub 区域的缺省路由的开销为 20。

```
<Sysname> system-view  
[Sysname] ospf 100
```

```
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
[Sysname-ospf-100-area-0.0.0.1] default-cost 20
```

【相关命令】

- **nssa**
- **stub**

1.1.9 default-route-advertise (OSPF view)

default-route-advertise 命令用来将缺省路由引入到 OSPF 路由区域。

undo default-route-advertise 命令用来恢复缺省情况。

【命令】

```
default-route-advertise [ [ always | permit-calculate-other ] | cost
cost-value | route-policy route-policy-name | type type ] *
default-route-advertise [ summary cost cost-value ]
undo default-route-advertise
```

【缺省情况】

未引入缺省路由。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

always: 如果当前路由器的路由表中没有缺省路由,使用此参数可产生一个描述缺省路由的 Type-5 LSA 发布出去。如果没有指定该关键字,仅当本地路由器的路由表中存在缺省路由时,才可以产生一个描述缺省路由的 Type-5 LSA 发布出去。

permit-calculate-other: 当路由器产生并发布了一个描述缺省路由的 Type-5 LSA 时,指定此参数的路由器仍然会计算来自于其他路由器的缺省路由,未指定此参数的路由器不再计算来自其他路由器的缺省路由。当路由器没有产生一个描述缺省路由的 Type-5 LSA 时,无论是否指定此参数,路由器都会计算来自其他路由器的缺省路由。

cost cost-value: 该缺省路由的度量值,取值范围为 0~16777214,如果没有指定,缺省路由的度量值将取 **default cost** 命令配置的值。

route-policy route-policy-name: 路由策略名,为 1~63 个字符的字符串,区分大小写。只有当前路由器的路由表中存在缺省路由,并且有路由匹配 **route-policy-name** 指定的路由策略,才可以产生一个描述缺省路由的 Type-5 LSA 发布出去,指定的路由策略会影响 Type-5 LSA 中的值。如果同时指定 **always** 参数,不论当前路由器的路由表中是否有缺省路由,只要有路由匹配指定的路由策略,就将产生一个描述缺省路由的 Type-5 LSA 发布出去,指定的路由策略会影响 Type-5 LSA 中的值。

type type: 该 Type-5 LSA 的类型，取值范围为 1~2，如果没有指定，Type-5 LSA 的缺省类型将取 **default type** 命令配置的值。

summary: 发布指定缺省路由的 Type-3 LSA。在选用该参数时，必须首先使能 VPN，否则路由不能发布。

【使用指导】

使用 **import-route** 命令不能引入缺省路由，如果要引入缺省路由，必须使用该命令。当本地路由器的路由表中没有缺省路由时，要产生一个描述缺省路由的 Type-5 LSA 应使用 **always** 关键字。

default-route-advertise summary cost 命令仅在 VPN 中应用，以 Type-3 LSA 引入缺省路由，PE 路由器会将引入的缺省路由发布给 CE 路由器。

【举例】

不管本地路由器的路由表中是否存在缺省路由，将产生的缺省路由引入到 OSPF 路由区域（本地路由器没有缺省路由）。

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default-route-advertise always
```

【相关命令】

- **default**
- **import-route**

1.1.10 description (OSPF/OSPF area view)

description 命令用来配置 OSPF 进程/OSPF 区域的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

未配置 OSPF 进程和区域的描述信息。

【视图】

OSPF 视图
OSPF 区域视图

【缺省用户角色】

network-admin
context-admin

【参数】

text: 在 OSPF 视图下，该参数用来描述 OSPF 进程；在 OSPF 区域视图下，该参数用来描述 OSPF 区域，为 1~80 个字符的字符串，区分大小写。

【使用指导】

本命令仅仅用于标识某 OSPF 进程/OSPF 区域，并无特别的意义和用途。

【举例】

```
# 配置 OSPF 进程 100 的描述信息为 “abc”。
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] description abc
# 配置 OSPF 区域 0 的描述信息为 “bone area”。
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] description bone area
```

1.1.11 discard-route

discard-route 命令用来配置 NULL0 路由以及 NULL0 路由的优先级。

undo discard-route 命令用来将 NULL0 路由的优先级恢复为 255。

【命令】

discard-route { **external** { *preference* | **suppression** } | **internal** { *preference* | **suppression** } } *

undo discard-route [**external** | **internal**] *

【缺省情况】

产生引入聚合 NULL0 路由和区域间聚合 NULL0 路由，且 NULL0 路由优先级为 255。

【视图】

OSPF 视图

【缺省用户角色】

network-admin

context-admin

【参数】

external: 引入聚合 NULL0 路由。

preference: 引入聚合 NULL0 路由的优先级，取值范围为 1~255。

suppression: 抑制产生引入聚合 NULL0 路由。

internal: 区域间聚合 NULL0 路由。

preference: 区域间聚合 NULL0 路由的优先级，取值范围为 1~255。

suppression: 抑制产生区域间聚合 NULL0 路由。

【举例】

```
# 配置引入聚合路由的 NULL0 路由的优先级为 100，区域间聚合 NULL0 路由的优先级为 200。
<Sysname> system-view
[Sysname] ospf 100
```

```
[Sysname-ospf-100] discard-route external 100 internal 200
```

1.1.12 display ospf

display ospf 命令用来显示 OSPF 的进程信息。

【命令】

```
display ospf [ process-id ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin  
network-operator  
context-admin  
context-operator
```

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 的进程信息。

verbose: 显示 OSPF 进程的详细信息。如果未指定本参数，将显示 OSPF 进程的概要信息。

【举例】

显示 OSPF 的详细信息。

```
<Sysname> display ospf verbose
```

```
OSPF Process 1 with Router ID 192.168.1.2  
OSPF Protocol Information
```

```
RouterID: 192.168.1.2      Router type: NSSA  
Route tag: 0  
Multi-VPN-Instance is not enabled  
Ext-community type: Domain ID 0x105, Route Type 0x8000, Router ID 0x8001  
Domain ID: 0.0.0.0:23  
Opaque capable  
Originating router-LSAs with maximum metric  
    Condition: On startup for 600 seconds, State: Inactive  
    Advertise stub links with maximum metric in router-LSAs  
    Advertise summary-LSAs with metric 16711680  
    Advertise external-LSAs with metric 16711680  
ECMP group is enabled  
ISPF is enabled  
SPF-schedule-interval: 5 50 200  
LSA generation interval: 5  
LSA arrival interval: 1000  
Transmit pacing: Interval: 20 Count: 3  
Default ASE parameters: Metric: 1 Tag: 1 Type: 2
```



```

Route preference: 10
ASE route preference: 150
SPF computation count: 22
RFC 1583 compatible
Graceful restart interval: 120
SNMP trap rate limit interval: 2 Count: 300
This process is currently bound to MIB
Area count: 1  NSSA area count: 1
Normal areas with up interfaces: 0
NSSA areas with up interfaces: 1
Up interfaces: 1
ExChange/Loading neighbors: 0
Full neighbors:3
Calculation trigger type: Full
Current calculation type: SPF calculation
Current calculation phase: Calculation area topology
Process reset state: N/A
Current reset type: N/A
Next reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
    M-N/A, P-N/A, L-N/A, C-N/A, R-N/A
MPLS segment routing: Disabled
    Segment routing adjacency    : Disabled
    Segment routing global block: 16000 24000

Area: 0.0.0.1          (MPLS TE not enabled)
Authtype: None      Area flag: NSSA
7/5 translator state: Disabled
7/5 translate stability timer interval: 0
SPF scheduled count: 5
ExChange/Loading neighbors: 0
Up interfaces: 1

Interface: 192.168.1.2 (GigabitEthernet1/0/1)
Cost: 1      State: DR      Type: Broadcast      MTU: 1500
Priority: 1
Designated router: 192.168.1.2
Backup designated router: 192.168.1.1
Timers: Hello 10 , Dead 40 , Poll 40 , Retransmit 5 , Transmit Delay 1
FRR backup: Enabled
Enabled by network configuration
Prefix-SID type: Index
    Value: 101
    Process ID: ospf 1
    Prefix-SID validity: Invalid

```

表1-1 display ospf verbose 命令显示信息描述表

字段	描述
OSPF Process 1 with Router ID 192.168.1.2	OSPF进程号以及OSPF Router ID
RouterID	本路由器的Router ID
Router type	路由器类型，取值为： • ABR：表示区域边界路由器 • ASBR：表示自治系统边界路由器 • NSSA：表示支持 NSSA 区域 • 为空：表示非上面三种情况
Route tag	与外部路由相关联的标记
Multi-VPN-Instance is not enabled	当前进程不支持多VPN实例
Ext-community type	OSPF扩展团体属性类型编码。其中： • Domain ID：表示 domain ID 属性编码 • Route Type：表示 route type 属性编码 • Router ID：表示 router ID 属性编码
Domain ID	OSPF域标识符（主标识符）
Opaque capable	使能OSPF的Opaque LSA发布接收能力
Originating router-LSAs with maximum metric	Router LSA中除Stublink外使用最大开销值发布
Condition	Stub路由器的状态： • Always：表示始终生效 • On startup for XXX seconds：表示重启后生效时间
State	Stub路由器是否生效： • Active 表示生效 • Inactive 表示不生效
Advertise stub links with maximum metric in router-LSAs	Router LSA使用最大开销值发布
Advertise summary-LSAs with metric	Summary LSA发布使用的开销值
Advertise external-LSAs with metric	外部LSA发布使用的开销值
ECMP group is enabled	等价路由组功能处于开启状态。如果未开启等价路由组功能，则不显示该字段
ISPF is enabled	使能增量SPF计算功能
SPF-schedule-interval	进行SPF计算的时间间隔，in milliseconds表示以固定的时间间隔进行SPF计算，单位为毫秒
LSA generation interval	LSA生成时间间隔
LSA arrival interval	LSA重复到达的最小时间间隔
Transmit pacing	接口发送LSU报文的速率，其中： • Interval 表示接口发送 LSU 报文的时间间隔

字段	描述
	Count 表示接口一次发送 LSU 报文的最大个数
Default ASE parameters	引入外部路由的缺省参数值，其中： - Metric: 表示度量值 - Tag: 表示路由标记 - Type: 表示路由类型
Route preference	OSPF协议对自治系统内部路由的优先级
ASE route preference	OSPF协议对自治系统外部路由的优先级
SPF computation count	OSPF进程的路由计算总数
RFC1583 compatible	兼容RFC 1583路由选择优先规则
Graceful restart interval	GR重启间隔时间
SNMP trap rate limit interval	TRAP发送间隔
Count	TRAP发送个数
This process is currently bound to MIB	当前进程绑定MIB
Area count	当前进程中的区域数
NSSA area count	当前进程中的NSSA区域数
Normal areas with up interfaces	有Up接口的外部能力区域个数
NSSA areas with up interfaces	有Up接口的NSSA区域个数
Up interfaces	处于Up状态的接口计数
ExChange/Loading neighbors	处于ExChange/Loading状态的邻居数
Full neighbors	处于Full状态的邻居数
Calculation trigger type	触发路由计算的类型，具体如下： - Full: 触发全部路由计算 - Area topology change: 区域拓扑改变触发路由计算 - Intra router change: 增量的区域内路由由器路由变化 - ASBR change: 增量的 ASBR 路由变化 7to5 translator: 7 转 5 角色变化 - Full IP prefix: 触发全部 IP 前缀计算 - Full intra AS: 触发全部 AS 内部前缀计算 - Inc intra AS: 触发增量 AS 内部前缀计算 - Full inter AS: 触发全部 AS 外部前缀计算 - Inc inter AS: 触发增量 AS 外部前缀计算 - N/A: 未触发计算
Current calculation type	当前路由计算的类型，具体如下： - SPF calculation: 进行区域 SPF 计算 - Intra router calculation: 区域内路由由器路由计算

字段	描述
	- ASBR calculation: 区域间 ASBR 路由计算 - Inc intra router: 增量区域内路由器路由计算 - Inc ASBR calculation: 增量区域间 ASBR 路由计算 7to5 translator: 7 转 5 角色路由计算 - Full intra AS: 进行全部 AS 内部前缀计算 - Inc intra AS: 进行增量 AS 内部前缀计算 - Full inter AS: 进行全部 AS 外部前缀计算 - Inc inter AS: 进行增量 AS 外部前缀计算 - Forward address: 转发地址计算 - N/A: 未触发计算
Current calculation phase	当前路由计算调度运行到的阶段，具体如下： - Calculation area topology: 计算区域拓扑 - Calculation router: 计算路由器路由 - Calculation intra AS: 计算 AS 内部路由 7to5 translator: 计算 7 转 5 角色路由 - Forward address: 计算转发地址 - Calculation inter AS: 计算 AS 外部路由 - Calculation end: 计算收尾阶段 - N/A: 未触发计算
Process reset state	进程重启状态，具体如下： - N/A: 进程未重启 - Under reset: 进程重启过程中 - Under RIB smooth: 进程正在同步 RIB 路由
Current reset type	当前进程重启类型，具体如下： - N/A: 进程未重启 - Normal: 普通重启 - GR quit: GR 异常退出进行普通重启 - Delete: 删除 OSPF 进程 - VPN delete: 删除 VPN
Next reset type	即将调度进程重启类型，具体如下： - N/A: 进程未重启 - Normal: 普通重启 - GR quit: GR 异常退出进行普通重启 - Delete: 删除 OSPF 进程 - VPN delete: 删除 VPN
Reset prepare message replied	响应准备重启消息的模块，具体如下： - P: 表示邻居维护模块 - L: 表示 LSDB 同步模块

字段	描述
	• C: 表示路由计算模块 • R: 表示路由引入模块
Reset process message replied	响应进程重启消息的模块，具体如下： • P: 表示邻居维护模块 • L: 表示 LSDB 同步模块 • C: 表示路由计算模块 • R: 表示路由引入模块
Reset phase of module	各模块所处重启阶段。其中M代表主控制模块，其阶段有： • N/A: 未重启 • Delete area: 删除区域 • Delete process: 删除进程 P代表邻居维护模块，其阶段有： • N/A: 未重启 • Delete neighbor: 删除邻居 • Delete interface: 删除接口 • Delete vlink: 删除虚连接 L代表LSDB同步模块，其阶段有： • N/A: 未重启 • Stop timer: 停止计时器 • Delete ASE: 删除所有 ASE LSA • Delete ASE maps: 删除 ASE LSA 的 map • Clear process data: 清除进程数据 • Delete area LSA: 删除区域相关 LSA 及其 map • Delete area interface: 删除区域下接口 • Delete process: 删除进程相关资源 • Restart: 重启进程相关资源 C代表路由计算模块，其阶段有： • N/A: 未重启 • Delete topology: 删除区域拓扑 • Delete router: 删除路由器路由 • Delete intra AS: 删除 AS 内部路由 • Delete inter AS: 删除 AS 外部路由 • Delete forward address: 删除转发地址列表 • Delete advertise: 删除发布源列表 R代表路由引入模块，其阶段有： • N/A: 未重启 • Delete ABR summary: 删除 ABR 聚合路由 • Delete ASBR summary: 删除 ASBR 聚合路由 • Delete import: 删除引入路由

字段	描述
MPLS segment routing	是否开启MPLS SR功能： - Disabled: 表示未开启 - Enabled: 表示开启
Segment routing adjacency	是否开启MPLS SR邻居标签分配功能： - Disabled: 表示未开启 - Enabled: 表示开启
Segment routing global bloack	基于MPLS的SRGB的标签范围
Area	列举当前进程中各区域的信息。显示当前区域ID, IP地址格式
MPLS TE not enabled	(暂不支持) 是否开启OSPF区域的MPLS TE能力 - MPLS TE not enabled: 表示关闭 - MPLS TE enabled: 表示开启
Authtype	区域验证模式, 取值为: - None: 表示无验证 - Simple: 表示简单验证模式 - MD5: 表示 MD5 验证模式
Area flag	区域类型: - Normal: 普通区域 - Stub: Stub 区域 - StubNoSummary: 完全 Stub 区域 - NSSA: NSSA 区域 - NSSANoSummary: 完全 NSSA 区域
7/5 translator state	Type-7 LSA转换为Type-5 LSA的转换者状态, 取值为: - Enabled: 表示通过命令指定 Type-7 LSA 转换为 Type-5 LSA 的转换者 - Elected: 表示通过选举指定 Type-7 LSA 转换为 Type-5 LSA 的转换者 - Disabled: 表示不是 Type-7 LSA 转换为 Type-5 LSA 的转换者
7/5 translate stability timer interval	Type-7 LSA转换为Type-5 LSA转换稳定定时器超时时间间隔
SPF scheduled Count	OSPF区域的路由计算总数
Interface	区域内的接口信息
Cost	接口的开销值
State	接口状态
Type	接口的网络类型
MTU	接口的MTU值

字段	描述
Priority	路由器优先级
Designated router	接口所属网段的DR
Backup designated router	接口所属网段的BDR
Timers	OSPF定时器的值，其中： • Hello: 表示接口发送 Hello 报文的时间间隔 • Dead: 表示邻居的失效时间 • Poll: 表示接口发送轮询 Hello 报文的时间间隔 • Retransmit: 表示定接口重传 LSA 时间间隔
Transmit Delay	接口对LSA的传输延迟时间
FRR backup	是否使能接口参与LFA（Loop Free Alternate）计算： • Enabled: 使能 • Disabled: 关闭
Enabled by network configuration	接口由网络配置使能到该区域
Simple authentication enabled	采用Simple验证模式
Keychain authentication enabled, name is xx	采用keychain验证模式，keychain名称为xx
MD5 authentication enabled	采用MD5/HMAC-MD5验证模式
The last key is xx	最新的MD5/HMAC-MD5验证密钥为xx
The rollover is in progress, xx neighbor(s) left	正在进行MD5/HMAC-MD5验证平滑迁移，尚未完成MD5/HMAC-MD5验证平滑迁移的邻居个数为xx
Prefix-SID type	表示前缀SID的类型： • Absolute: 前缀 SID 绝对值 • Index: 前缀 SID 相对值
Value	前缀SID的取值
Process ID	配置前缀SID时实际指定的进程号
Prefix-SID validity	配置的Prefix SID是否为有效值： • Invalid: 表示无效值，即前缀 SID 的值不在 SRGB 范围内或 Loopback 接口上使能的 OSPF 进程和配置前缀 SID 时实际指定的进程号不一致 • Valid: 表示有效值

1.1.13 display ospf abr-asbr

display ospf abr-asbr 命令用来显示到 OSPF 的区域边界路由器和自治系统边界路由器的路由信息。

【命令】

display ospf [process-id] abr-asbr [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程下到区域边界路由器和自治系统边界路由器的路由信息。
verbose: 显示详细信息。如果未指定本参数，将显示概要信息。

【使用指导】

如果在 Stub 区域的路由器上执行此命令，不显示有关 ASBR 的信息。

【举例】

显示到 OSPF 的区域边界路由器和自治系统边界路由器的路由概要信息。
<Sysname> display ospf abr-asbr

```
OSPF Process 1 with Router ID 192.168.1.112
Routing Table to ABR and ASBR

Type      Destination      Area            Cost      Nexthop        RtType
Inter     3.3.3.3          0.0.0.0         3124      10.1.1.2       ASBR
Intra     2.2.2.2          0.0.0.0         1562      10.1.1.2       ABR
```

显示到 OSPF 的区域边界路由器和自治系统边界路由器的路由详细信息。
<Sysname> display ospf abr-asbr verbose

```
OSPF Process 10 with Router ID 101.1.1.11
Routing Table to ABR and ASBR

Destination: 1.1.1.1          RtType      : ASBR
Area      : 0.0.0.1           Type        : Intra
Nexthop    : 150.0.1.12       BkNexthop   : 0.0.0.0
Interface  : GE1/0/1          BkInterface  : N/A
Cost       : 1000
```

表1-2 display ospf abr-asbr 命令显示信息描述表

字段	描述
Type	到ABR或ASBR的路由类型，取值为： - Inter 表示区域间路由 - Intra 表示区域内路由
Destination	ABR或ASBR的路由器ID

字段	描述
Area	下一跳地址所在的区域ID
Cost	从本路由器到达ABR或ASBR的开销
Nexthop	下一跳地址
BkNexthop	备份下一跳地址
RtType	路由器类型，包括ABR和ASBR
Interface	路由出接口
BkInterface	路由备份出接口

1.1.14 display ospf abr-summary

display ospf abr-summary 命令用来显示 OSPF 的 ABR 聚合信息。

【命令】

```
display ospf [ process-id ] [ area area-id ] abr-summary [ ip-address
{ mask-length | mask } ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的 ABR 聚合信息。

area area-id: 显示指定区域的 ABR 聚合相关信息。**area-id** 表示区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其转换成 IP 地址格式）或者是 IP 地址格式。如果未指定本参数，将显示所有区域的信息。

ip-address: 指定的聚合路由的目的 IP 地址。

mask-length: 网络掩码长度，取值范围为 0~32。

mask: 网络掩码，点分十进制格式。

verbose: 显示 ABR 聚合的详细信息。如果未指定本参数，将显示 ABR 聚合的概要信息。

【使用指导】

如果未指定 IP 地址和掩码，将显示所有的 ABR 聚合信息。

【举例】

显示 OSPF 的 ABR 聚合信息。

```
<Sysname> display ospf abr-summary
```

```
OSPF Process 1 with Router ID 2.2.2.2
  ABR Summary Addresses

      Area: 0.0.0.1
Total summary addresses: 1
Net      Mask      Status      Count      Cost
100.0.0.0 255.0.0.0  Advertise    1          (Not Configured)
```

表1-3 display ospf abr-summary 命令显示信息描述表

字段	描述
Area	聚合路由所在的区域
Total summary addresses	聚合路由的路由数
Net	聚合路由的网络地址
Mask	聚合路由的网络掩码
Status	聚合路由的状态： • Advertise: 已发布 • Not-Advertise: 未发布
Count	被聚合的路由数
Cost	聚合路由的开销

显示 OSPF 的 ABR 聚合详细信息。

```
<Sysname> display ospf abr-summary verbose
```

```
OSPF Process 1 with Router ID 2.2.2.2
  ABR Summary Addresses

      Area: 0.0.0.1
Total summary addresses: 1

Net      : 100.0.0.0
Mask     : 255.0.0.0
Status   : Advertise
Cost     : (Not Configured)
Routes count: 1
  Destination      NetMask      Metric
  100.1.1.0        255.255.255.0  1000
```

表1-4 display ospf abr-summary verbose 命令显示信息描述表

字段	描述
Destination	被聚合路由的网络地址
NetMask	被聚合路由的网络掩码

字段	描述
Metric	路由的开销值

1.1.15 display ospf asbr-summary

display ospf asbr-summary 命令用来显示 OSPF 的 ASBR 聚合信息。

【命令】

display ospf [*process-id*] **asbr-summary** [*ip-address* { *mask-length* | *mask* }]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的 ASBR 聚合信息。

ip-address: 指定的聚合路由的目的 IP 地址。

mask-length: 网络掩码长度，取值范围为 0~32。

mask: 网络掩码，点分十进制格式。

【使用指导】

如果未指定 IP 地址和掩码，将显示所有的 ASBR 聚合信息。

【举例】

显示 OSPF 进程 1 的 ASBR 聚合信息。

```
<Sysname> display ospf 1 asbr-summary
```

```
OSPF Process 1 with Router ID 2.2.2.2
Summary Addresses
```

```
Total Summary Address Count: 1
```

```
Summary Address
```

```
Net       : 30.1.0.0
Mask      : 255.255.0.0
Tag       : 20
Status    : Advertise
Cost      : 10 (Configured)
```

The Count of Route is : 2

Destination	Net Mask	Proto	Process	Type	Metric
30.1.2.0	255.255.255.0	OSPF	2	2	1
30.1.1.0	255.255.255.0	OSPF	2	2	1

表1-5 display ospf asbr-summary 命令显示信息描述表

字段	描述
Total Summary Address Count	聚合路由的路由数
Net	聚合路由的网络地址
Mask	聚合路由的网络掩码
Tag	聚合路由的标记字段
Status	聚合路由的发布状态
Cost	聚合路由的开销
The Count of Route is	被聚合的路由数
Destination	被聚合路由的网络地址
Net Mask	被聚合路由的网络掩码
Proto	引入路由的协议类型
Process	引入路由的协议进程号
Type	外部路由类型
Metric	路由的开销值

1.1.16 display ospf event-log

display ospf event-log 命令用来显示 OSPF 的日志信息。

【命令】

```
display ospf [process-id] event-log { lsa-flush | peer [neighbor-id] [slot  
slot-number] | spf }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号, 取值范围为 1~65535。如果未指定本参数, 将显示所有进程的日志信息。

lsa-flush: 显示 LSA 老化的日志信息。

peer: 显示邻居状态变化的日志信息。

neighbor-id: 显示指定邻居状态变化的日志信息, *neighbor-id* 表示邻居路由器的 Router ID。如果未指定本参数, 将显示所有 OSPF 邻居状态变化的日志信息。

slot slot-number: 显示指定成员设备的 OSPF 日志信息, *slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数, 将显示主进程所在成员设备上 OSPF 邻居状态变化的日志信息。

spf: 路由计算的日志信息。

【使用指导】

路由计算的日志信息是指更新到 IP 路由表的路由计数信息。

邻居的日志信息包括 OSPF 邻居状态倒退到 DOWN, 以及收到 BadLSReq、SeqNumberMismatch 和 1-Way 事件导致邻居状态倒退的信息。

【举例】

显示 OSPF 的 LSA 老化日志信息。

```
<Sysname> display ospf event-log lsa-flush
```

```
OSPF Process 1 with Router ID 1.1.1.1
LSA Flush Log

Date: 2013-09-22 Time: 14:47:33 Received MaxAge LSA from 10.1.1.1
Type: 1   LS ID: 2.2.2.2           AdvRtr: 2.2.2.2           Seq#: 80000001

Date: 2013-09-22 Time: 14:47:33 Flushed MaxAge LSA by the self
Type: 1   LS ID: 1.1.1.1           AdvRtr: 1.1.1.1           Seq#: 80000001

Date: 2013-09-22 Time: 14:47:33 Received MaxAge LSA from 10.1.2.2
Type: 1   LS ID: 2.2.2.2           AdvRtr: 2.2.2.2           Seq#: 80000001

Date: 2013-09-22 Time: 14:47:33 Flushed MaxAge LSA by the self
Type: 1   LS ID: 1.1.1.1           AdvRtr: 1.1.1.1           Seq#: 80000001
```

表1-6 display ospf event-log lsa-flush 命令显示信息描述表

字段	描述
Date &Time	收到MaxAge LSA的时间
Received MaxAge LSA from X.X.X.X	从源地址收到MaxAge LSA
Flushed MaxAge LSA by the self	由自己发起老化, 洪泛MaxAge LSA
Type	LSA类型
LS ID	LSA链路状态ID
AdvRtr	LSA发布路由器

字段	描述
Seq#	LSA序列号

显示 OSPF 路由计算的日志信息。

<Sysname> display ospf event-log spf

OSPF Process 1 with Router ID 1.1.1.2

SPF Log

Date	Time	Duration	Intra	Inter	External	Reason
2012-06-27	15:28:26	0.95	1	1	10000	Intra-area LSA
2012-06-27	15:28:23	0.2	0	0	0	Area 0 full neighbor
2012-06-27	15:28:19	0	0	0	0	Intra-area LSA
2012-06-27	15:28:19	0	0	0	0	external LSA
2012-06-27	15:28:19	0.3	0	0	0	Intra-area LSA
2012-06-27	15:28:12	0	1	0	0	Intra-area LSA
2012-06-27	15:28:11	0	0	0	0	Routing policy
2012-06-27	15:28:11	0	0	0	0	Intra-area LSA

表1-7 display ospf event-log spf 命令显示信息描述表

字段	描述
Date/Time	路由计算开始的时间
Duration	路由计算持续时间，单位为秒
Intra	区域内路由变化的个数
Inter	区域间路由变化的个数
External	外部路由变化的个数
Reason	路由计算的原因： • Intra-area LSA: 区域内 LSA 变化 • Inter-area LSA: 区域间 LSA 变化 • External LSA: 外部 LSA 变化 • Configuration: 配置变化 • Area 0 full neighbor: 区域 0FULL 邻居个数变化 • Area 0 up interface: 区域 0UP 接口个数变化 • LSDB overflow state: overflow 状态变化 • AS number: AS 号变化 • ABR summarization: ABR 聚合变化 • GR end: GR 结束 • Routing policy: 路由策略变化 • Intra-area tunnel: 区域内隧道变化 • Others: 除上述原因之外的其他原因

显示 OSPF 邻居的日志信息。

```
<Sysname> display ospf 1 event-log peer
```

```
OSPF Process 1 with Router ID 1.1.1.1
Neighbors Log
```

Date	Time	Local Address	Remote Address	Router ID	Reason
2012-12-31	12:35:45	197.168.1.1	197.168.1.2	2.2.2.2	IntPhyChange
2012-12-31	12:35:19	197.168.1.1	197.168.1.2	2.2.2.2	ConfNssaArea
2012-12-31	12:34:59	197.168.1.1	197.168.1.2	2.2.2.2	SilentInt

表1-8 display ospf event-log peer 命令显示信息描述表

字段	描述
Date &Time	邻居状态变化的时间
Local Address	建立邻居关系的本端地址
Remote Address	建立邻居关系的对端地址
Router ID	邻居的Router ID
Reason	邻居状态变化的原因： • ResetConnect: 内存不足断连接 • IntChange: 接口参数改变 • VlinkChange: 虚连接参数改变 • ResetOspf: 重启 OSPF 进程 • UndoOspf: 删除 OSPF 进程 • UndoArea: 删除 OSPF 区域 • UndoNetwork: 接口去使能 • SilentInt: 配置抑制接口 • IntLogChange: 接口逻辑属性变化 • IntPhyChange: 接口物理属性变化 • IntVliChange: 接口虚连接属性变化 • VlinkDown: 虚连接 Down • DeadExpired: Dead Timer 超时 • ConfStubArea: 配置 Stub 区域参数 • ConfNssaArea: 配置 NSSA 区域参数 • AuthChange: 认证类型变化 • OpaqueChange: Opaque 能力改变 • Retrans: 重传过多 • LLSChange: LLS 能力变化 • OOBChange: OOB 能力变化 • GRChange: GR 能力变化 • BFDDown: BFD Down • BadLSReq: 收到 BadLSReq 事件

字段	描述
	- SeqMismatch: 收到 SeqNumberMismatch 事件 1-Way: 收到 1-Way 事件

【相关命令】

- reset ospf event-log**

1.1.17 display ospf event-log hello

display ospf event-log hello 命令用来显示 OSPF 接收或发送 Hello 报文的日志信息。

【命令】

```
display ospf [ process-id ] event-log hello { received [ abnormal | dropped ]
| sent } [ neighbor-id ] [ slot slot-number ]
display ospf [ process-id ] event-log hello sent { abnormal | failed }
[ neighbor-address ] [ slot slot-number ]
```

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

process-id: OSPF 进程号, 取值范围为 1~65535。如果未指定本参数, 将显示所有进程的日志信息。

received: 显示接收到的 Hello 报文的日志信息。

sent: 显示发送 Hello 报文的日志信息。

abnormal: 显示接收或发送异常 Hello 报文的日志信息。异常 Hello 报文指的是发送或接收到的 Hello 报文的时间间隔大于或等于 1.5 倍 Hello 定时器的报文。

dropped: 显示丢弃接收到的 Hello 报文的日志信息。

failed: 显示发送失败的 Hello 报文的日志信息。

neighbor-address: 邻居的 IP 地址, 显示指定邻居接收或发送 Hello 报文的日志信息。如果未指定本参数, 将显示所有 OSPF 邻居接收或发送 Hello 报文的日志信息。

neighbor-id: 邻居的 Router ID, 显示指定邻居接收或发送 Hello 报文的日志信息。如果未指定本参数, 将显示所有 OSPF 邻居接收或发送 Hello 报文的日志信息。

slot slot-number: 显示指定成员设备接收或发送 Hello 报文的日志信息, *slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数, 将显示主进程所在的成员设备接收或发送 Hello 报文的日志信息。

【举例】

显示发送 Hello 报文的日志信息。

```
<Sysname> display ospf event-log hello sent
```


OSPF Process 1 with Router ID 5.5.5.5
Hello Log

Interface: GE1/0/1
Neighbor address: 10.1.1.2, NbrID: 1.0.0.2
First 4 hello packets sent:
2018-08-05 20:10:10:121, failed, errno: 132
2018-08-05 20:10:30:121, succeeded
2018-08-05 20:10:20:121, succeeded
2018-08-05 20:10:40:121, succeeded
Last 4 hello packets sent before Full->Down at 2018-08-06 14:52:10:121
2018-08-06 14:51:40:021, succeeded
2018-08-06 14:51:50:021, succeeded
2018-08-06 14:52:00:021, failed, errno: 132
2018-08-06 14:52:10:010, failed, errno: 132

Interface: GE1/0/1
Neighbor address: 10.1.1.2, NbrID: 1.0.0.2
First 4 hello packets sent:
2018-08-05 20:10:10:121, failed, errno: 132
2018-08-05 20:10:30:121, succeeded
2018-08-05 20:10:20:121, succeeded
2018-08-05 20:10:40:121, succeeded
Last 4 hello packets sent before Full->Init at 2018-08-06 11:16:20:171
2018-08-06 11:15:20:121, succeeded
2018-08-06 11:15:30:121, succeeded
2018-08-06 11:15:40:121, succeeded
2018-08-06 11:15:50:121, succeeded

表1-9 display ospf event-log hello sent 命令显示信息描述表

字段	描述
Interface	发送Hello报文的接口
Neighbor address	邻居的IP地址
NbrID	邻居的路由器ID
First 4 hello packets sent	最开始发送的4个Hello报文的时间，以及报文是否发送成功的信息 • succeeded: 发送成功 • failed: 发送失败 • errno: 错误码，表明了报文发送失败的原因
Last 4 hello packets sent before Full->Down at 2018-01-06 14:52:10:121	邻居状态改变的时间，以及状态改变前发送的4个Hello报文的时间和报文是否发送成功的信息 • succeeded: 发送成功 • failed: 发送失败 • errno: 错误码，表明了报文发送失败的原因

显示发送失败的 Hello 报文的日志信息。

```
<Sysname> display ospf event-log hello sent failed
```

```
OSPF Process 1 with Router ID 5.5.5.5
```

```
Hello Log
```

```
Date: 2018-08-06 Time: 14:51:20:121 Interface: GE1/0/1
```

```
Destination address: 224.0.0.5, sent failed, errno: 132
```

```
Date: 2018-08-06 Time: 11:20:20:116 Interface: GE1/0/2
```

```
Destination address: 10.1.1.2, sent failed, errno: 132
```

表1-10 display ospf event-log hello sent failed 命令显示信息描述表

字段	描述
Date	Hello报文发送失败的日期，单位为YYYY-MM-DD，其中YYYY为年，MM为月，DD为日
Time	Hello报文发送失败的时间，单位为hh:mm:ss:xxx，其中hh为小时，mm为分钟，ss为秒，xxx为毫秒
Interface	发送Hello报文的接口
Destination address	Hello报文的目的IP地址
sent failed	发送失败
error	发送失败的错误码

查看发送异常 Hello 报文的日志信息。

```
<Sysname> display ospf event-log hello sent abnormal
```

```
OSPF Process 1 with Router ID 5.5.5.5
```

```
Hello Log
```

```
Date: 2018-08-06 Time: 11:21:12:121 Interface: GE1/0/2
```

```
Destination address: 224.0.0.5, last one sent: 2018-08-06 11:20:51:916
```

```
Date: 2018-08-06 Time: 11:56:21:312 Interface: GE1/0/2
```

```
Destination address: 10.1.1.2, last one sent: 2018-08-06 11:56:02:691
```

表1-11 display ospf event-log hello sent abnormal 命令显示信息描述表

字段	描述
Date	发送异常Hello报文的日期，单位为YYYY-MM-DD，其中YYYY为年，MM为月，DD为日
Time	发送异常Hello报文的时间，单位为hh:mm:ss:xxx，其中hh为小时，mm为分钟，ss为秒，xxx为毫秒
Interface	发送异常Hello报文的接口
Destination address	异常Hello报文的目的IP地址

last one sent	发送异常Hello报文前，最后一次发送Hello报文的时间

显示接收 Hello 报文的日志信息。

<Sysname> display ospf event-log hello received

OSPF Process 1 with Router ID 5.5.5.5
Hello Log

Interface: GE1/0/1

Neighbor address: 10.1.1.2, NbrID: 1.0.0.2

First 4 hello packets received:

2018-08-05 20:11:10:121
2018-08-05 20:11:30:121
2018-08-05 20:11:20:121
2018-08-05 20:11:40:121

Last 4 hello packets received before Exchange->Down at 2018-08-06 14:52:10:121

2018-08-06 14:51:10:121
2018-08-06 14:51:30:121
2018-08-06 14:51:20:121
2018-08-06 14:51:40:121

Interface: GE1/0/1

Neighbor address: 10.1.1.1, NbrID: 1.0.0.1

First 4 hello packets received:

2018-08-06 19:11:15:121
2018-08-06 19:11:35:121
2018-08-06 19:11:25:121
2018-08-06 19:11:45:121

Last 4 hello packets received before Full->Init at 2018-08-06 21:16:20:171

2018-08-06 21:15:45:121
2018-08-06 21:15:55:121
2018-08-06 21:16:05:121
2018-08-06 21:16:15:121

表1-12 display ospf event-log hello received 命令显示信息描述表

字段	描述
Interface	发送Hello报文的接口
Neighbor address	邻居的IP地址
NbrID	邻居的路由器ID
First 4 hello packets received	最开始接收的4个Hello报文的时间
Last 4 hello packets received before Full->Init at 2018-01-06 21:16:20:171	邻居状态改变的时间，以及状态改变前接收的4个Hello报文的时间信息。其中，日期单位为YYYY-MM-DD，其中YYYY为年，MM为月，DD为日；时间单位为hh:mm:ss:xxx，其中hh为小时，mm为分钟，ss为秒，xxx为毫秒

显示丢弃接收到的 Hello 报文的日志信息。

```
<Sysname> display ospf event-log hello received dropped
```

```
OSPF Process 1 with Router ID 5.5.5.5
Hello Log
```

```
Date: 2018-08-06 Time: 14:51:22:791 Interface: GE1/0/1
Source address: 10.1.1.1, NbrID: 1.0.0.1, area: 0.0.0.1
Drop reason: Hello-time mismatch
```

```
Date: 2018-08-06 Time: 14:51:20:121 Interface: GE1/0/1
Source address: 10.1.1.2, NbrID: 1.0.0.2, area: 0.0.0.1
Drop reason: NP-bit mismatch
```

表1-13 display ospf event-log hello received dropped 命令显示信息描述表

字段	描述
Date	丢弃接收到的Hello报文的日期，单位为YYYY-MM-DD，其中YYYY为年，MM为月，DD为日
Time	丢弃接收到的Hello报文的时间，单位为hh:mm:ss:xxx，其中hh为小时，mm为分钟，ss为秒，xxx为毫秒
Interface	接收Hello报文的接口
Source address	接收到的Hello报文中的源IP地址
NbrID	邻居路由器的Router ID
area	邻居接口所在区域
Drop reason	丢弃Hello报文的原因： • Area under reset: 正在进行区域重置 • Router ID conflict: Router ID 冲突 • Area mismatch: 区域 ID 不一致 • Unknown virtual link: Hello 报文来自未知的虚连接 • Authentication failure: Hello 报文认证检查失败 • Peer address check failure: Hello 报文的邻居地址检查失败 • Not DR or BDR: Hello 报文目的地址与接口 DR/BDR 状态不一致 • Unknown unicast peer: Hello 报文来自未知的单播邻居 • Option mismatch: Hello 报文 Option 字段不匹配 • Subnet mask mismatch: Hello 报文的网络掩码不匹配 • Address mismatch: Hello 报文的地址段不匹配 • Hello timer mismatch: Hello 报文的 Hello 定时器不匹配 • Dead timer mismatch: Hello 报文的 Dead 定时器不匹配 • Peer change: Hello 报文的源地址或 Router ID 发生变化

显示接收到异常的 Hello 报文的日志信息。

```
<Sysname> display ospf event-log hello received abnormal
```

OSPF Process 1 with Router ID 5.5.5.5
Hello Log

Date: 2018-08-06 Time: 10:12:22:121 Interface: GE1/0/1
Source address: 10.1.1.2, NbrID: 1.0.0.2, area: 0.0.0.1
Last one received: 2018-08-06 10:12:04:212

Date: 2018-08-06 Time: 14:51:20:121 Interface: GE1/0/1
Source address: 10.1.1.2, NbrID: 1.0.0.2, area: 0.0.0.1
Last one received: 2018-08-06 14:51:05:113

表1-14 display ospf event-log hello receiverd abnormal 命令显示信息描述表

字段	描述
Date&Tme	收到异常Hello报文的日期，单位为YYYY-MM-DD，其中YYYY为年，MM为月，DD为日
Time	收到异常Hello报文的时间，单位为hh:mm:ss:xxx，其中hh为小时，mm为分钟，ss为秒，xxx为毫秒
Interface	收到异常Hello报文的接口
Source address	收到异常Hello报文的源IP地址
NbrID	邻居路由器的Router ID
area	邻居接口所在区域
Last one received	接收到异常的Hello报文前，最后一次收到Hello报文的时间

【相关命令】

- **reset ospf event-log hello**

1.1.18 display ospf fast-reroute lfa-candidate

display ospf fast-reroute lfa-candidate 命令用来显示区域中 FRR 备份下一跳候选列表。

【命令】

display ospf [process-id] [area area-id] fast-reroute lfa-candidate

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有进程的备份下一跳候选列表。

area area-id: 显示指定区域 FRR 备份下一跳候选列表。**area-id** 表示区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其转换成 IP 地址格式）或者是 IP 地址格式。如果未指定本参数，将显示所有区域的信息。

【举例】

显示 OSPF 的 FRR 备份下一跳候选列表。
<Sysname> display ospf 1 area 0 fast-reroute lfa-candidate

```
OSPF Process 1 with Router ID 2.2.2.2
    LFA Candidate List

Area: 0.0.0.0
Candidate nexthop count: 2
NextHop          IntIP           Interface
10.0.1.1          10.0.1.2         GE1/0/2
10.0.11.1         10.0.11.2        GE1/0/3
```

表1-15 display ospf fast-reroute lfa-candidate 命令显示信息描述表

字段	描述
Area	显示该区域的备份下一跳信息
Candidate nexthop count	备份下一跳个数
NextHop	备份下一跳地址
IntIP	出接口IP地址
Interface	出接口

1.1.19 display ospf graceful-restart

display ospf graceful-restart 命令用来查看 OSPF 进程的 GR 状态信息。

【命令】

display ospf [process-id] graceful-restart [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的 GR 状态信息。

verbose: 显示 GR 详细状态信息。如果未指定本参数，将显示 OSPF 进程的 GR 状态概要信息。

【举例】

显示 OSPF 进程的 GR 详细状态信息。

```
<Sysname> display ospf graceful-restart verbose
```

```
OSPF Process 1 with Router ID 1.1.1.1
```

```
Graceful Restart information
```

```
Graceful Restart capability      : Enable(IETF)
Graceful Restart support        : Planned and un-planned,Partial
Helper capability                : Enable(IETF)
Helper support                  : Planned and un-planned (IETF),Strict LSA check
Current GR state                 : Normal
Graceful Restart period         : 40 seconds
Number of neighbors under Helper: 0
Number of restarting neighbors  : 0
Last exit reason:
  Restarter   : None
  Helper      : None
```

```
Area: 0.0.0.0
```

```
Authtype: None Area flag: Normal
```

```
Area up Interface count: 2
```

```
Interface: 40.4.0.1 (GigabitEthernet1/0/2)
```

```
Restarter state: Normal State: P-2-P Type: PTP
```

```
Last exit reason:
```

```
Restarter   : None
Helper      : None
```

```
Neighbor count of this interface: 1
```

```
Number of neighbors under Helper: 0
```

Neighbor	IP address	GR state	Last Helper exit reason
3.3.3.3	40.4.0.3	Normal	None

```
Virtual-link Neighbor-ID -> 4.4.4.4, Neighbor-State: Full
```

```
Restarter state: Normal
```

```
Interface: 20.2.0.1 (Vlink)
```

```
Transit Area: 0.0.0.1
```

```
Last exit reason:
```

```
Restarter   : None
Helper      : None
```

Neighbor	IP address	GR state	Last Helper exit reason
4.4.4.4	20.2.0.4	Normal	Reset neighbor

表1-16 display ospf graceful-restart 命令显示信息描述表

字段	描述
OSPF Process 1 with Router ID 1.1.1.1 Graceful Restart information	OSPF进程是1，Router ID是1.1.1.1的GR状态信息
Graceful Restart capability	进程GR能力配置： • Enable(IETF)：使能 IETF GR 能力 • Enable(Nonstandard)：使能非 IETF GR 能力 • Disable：关闭了 GR 能力
Graceful Restart support	进程GR支持模式（GR使能时才显示）： • Planned and un-planned：支持计划和非计划 GR • Planned only：只支持计划性 GR • Partial：支持接口级 GR • Global：不支持接口级 GR，支持全局 GR
Helper capability	进程Helper能力配置： • Enable(IETF)：支持作为标准 GR Helper 的能力 • Enable(Nonstandard)：支持作为非标准 GR Helper 的能力 • Enable(IETF and nonstandard)：同时支持作为标准和非标准 GR Helper 的能力 • Disable：不支持作为 GR Helper 的能力
Helper support	显示支持Helper的策略（Helper使能时才显示）： • Strict LSA check：Helper 端支持严格的 LSA 检查 • Planned and un-planned：支持作为计划和非计划重启的 Helper • Planned only：只支持作为计划 GR 的 Helper
Current GR state	当前OSPF进程的GR状态： • Normal：普通状态 • Under GR：进程正在 GR • Under Helper：进程正在作为 GR Helper
Graceful-restart period	GR周期
Number of neighbors under helper	处于Helper状态的邻居数量
Number of restarting neighbors	Helper端显示的处于重启路由器的数量
Last exit reason	上次退出原因，其中： • Restarter：表示退出 Restarter 的原因 • Helper：表示退出 Helper 的原因
Area	开始列举当前进程中各区域的信息。显示当前区域ID，IP地址格式
Authtype	区域验证模式，取值为： • None：表示无验证

字段	描述
	- Simple: 表示简单验证模式 - MD5: 表示 MD5 验证模式
Area flag	区域类型: - Normal: 普通区域 - Stub: Stub 区域 - StubNoSummary: 完全 Stub 区域 - NSSA: NSSA 区域 - NSSANoSummary: 完全 NSSA 区域
Area up Interface count	区域下UP的接口计数
Interface	区域内的接口信息
Restarter state	作为Restarter的状态
State	接口状态
Type	接口的网络类型
Neighbor count of this interface	接口下的邻居
Neighbor	邻居Router ID
IP address	邻居IP地址
GR state	邻居的GR状态: - Normal: 普通状态 - Under GR: 进程正在 GR - Under Helper: 进程正在作为 GR Helper
Last Helper exit reason	上一次作为该邻居Helper退出的原因
Virtual-link Neighbor-ID	Vlink的邻居Router ID
Neighbor-State	Vlink和邻居的状态, 包括Down、Init、2-Way、ExStart、Exchange、Loading和Full
Interface	Vlink接口所属的出接口

1.1.20 display ospf hostname-table

display ospf hostname-table 命令用来显示 Router ID 到主机名称的映射关系表。

【命令】

display ospf [process-id] hostname-table

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535，显示指定 OSPF 进程中 Router ID 到主机名称的映射关系表。如果未指定本参数，将显示所有 OSPF 进程中 Router ID 到主机名称的映射关系表。

【举例】

#显示所有 OSPF 进程中 Router ID 到主机名称的映射关系表。
<Sysname> display ospf hostname-table

```
OSPF Process 1 with Router ID 192.168.56.21
      Hostname Table Information

Area: 0.0.0.1
Router ID      Hostname
192.168.56.21  RouterA
```

表1-17 display ospf hostname-table 命令输出信息描述表

字段	描述
Router ID	路由器ID
Hostname	主机名称

1.1.21 display ospf interface

display ospf interface 命令用来显示 OSPF 的接口信息。

【命令】

display ospf [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的接口信息。

interface-type interface-number: 接口类型和编号。显示指定接口的 OSPF 详细信息。
verbose: 显示所有接口的 OSPF 详细信息。

【使用指导】

如果未指定接口或参数 **verbose**，将显示所有接口的 OSPF 概要信息。

【举例】

显示所有接口的 OSPF 概要信息。
<Sysname> display ospf interface

```
OSPF Process 1 with Router ID 192.168.1.1
  Interfaces

Area: 0.0.0.1
IP Address      Type      State    Cost  Pri   DR           BDR
172.16.0.1      Broadcast DR        1      1    172.16.0.1   0.0.0.0
```

表1-18 display ospf interface 命令显示信息描述表

字段	描述
Area	接口所属的区域ID
IP Address	接口IP地址（不管是否使能了流量工程）
Type	接口的网络类型，取值为： - PTMP 表示网络类型为点对多点 - Broadcast 表示网络类型为广播 - NBMA 表示网络类型为 NBMA
State	根据OSPF接口状态机确定的当前接口状态，取值为： - Down 表示在接口上没有发送和接收任何路由协议的报文 - Loopback 表示路由器到网络的接口处于环回状态，不能用于正常的数据传输 - Waiting 表示接口开始发送和接收 Hello 报文，并试图去识别网络上的 DR 和 BDR - P-2-P 表示接口将每隔 HelloInterval 的时间间隔发送 Hello 报文，并尝试和接口链路另一端相连的路由器建立邻接关系 - DR 表示路由器是所连网络的指定路由器 - BDR 表示路由器是所连网络的备份指定路由器 - DROther 表示路由器既不是所连网络的指定路由器，也不是所连网络的备份指定路由器
Cost	接口开销
Pri	路由器优先级
DR	接口所属网段的DR
BDR	接口所属网段的BDR

显示 OSPF 指定接口 GigabitEthernet1/0/1 的详细信息。

<Sysname> display ospf interface gigabitethernet 1/0/1

OSPF Process 1 with Router ID 192.168.1.1
Interfaces

Area: 0.0.0.0

Interface: 172.16.0.1 (GigabitEthernet1/0/1)
Cost: 1 State: DR Type: Broadcast MTU: 1500
Priority: 1
Designated router: 172.16.0.1
Backup designated router: 0.0.0.0
Timers: Hello 10, Dead 40, Poll 40, Retransmit 5, Transmit Delay 1
FRR backup: Enabled
Primary path detection mode: BFD ctrl
Enabled by interface configuration (including secondary IP addresses)
BFD: echo
MD5 authentication enabled.
 The last key is 3.
 The rollover is in progress, 2 neighbor(s) left.
LDP state: No-LDP
LDP sync state: Achieved
Prefix-SID type: Index
 Value: 876, Explicit-null, N-flag-clear
 Process ID: ospf 1
 Prefix-SID validity: Invalid

表1-19 display ospf interface verbose 命令显示信息描述表

字段	描述
Interface	接口IP地址等信息
MTU	最大传输单元
Timers	OSPF定时器的值，其中： • Hello: 表示接口发送 Hello 报文的时间间隔 • Dead: 表示邻居的失效时间 • Poll: 表示接口发送轮询 Hello 报文的时间间隔 • Retransmit: 表示接口重传 LSA 时间间隔
Transmit Delay	接口对LSA的传输延迟时间
FRR backup	是否使能接口参与LFA（Loop Free Alternate）计算： • Enabled: 使能 • Disabled: 关闭
Primary path detection mode	主链路检测方式： • BFD ctrl: BFD 控制报文检测方式 • BFD echo: BFD echo 报文检测方式

字段	描述
Enabled by interface configuration (including secondary IP addresses)	接口使能OSPF，包括接口从IP地址
BFD	接口使能OSPF的BFD功能： - ctrl: 通过 BFD 控制报文方式实现 BFD 功能 - echo: 通过 BFD echo 报文方式实现 BFD 功能
Simple authentication enabled	采用Simple验证模式
Keychain authentication enabled, name is xx	采用keychain验证模式，keychain名称为xx
MD5 authentication enabled	采用MD5/HMAC-MD5验证模式
The last key is xx	最新的MD5/HMAC-MD5验证字标识符为xx
The rollover is in progress, xx neighbor(s) left.	正在进行MD5/HMAC-MD5验证平滑迁移，尚未完成MD5/HMAC-MD5验证平滑迁移的邻居个数为xx
Prefix-SID type	表示前缀SID的类型： - Absolute: 前缀 SID 绝对值 - Index: 前缀 SID 相对值
Value	前缀SID的取值以及标志信息： - Explicit-null: 表示上游邻居用显式空标签代替前缀 SID - N-flag-clear: 表示前缀 SID 为到达一组 SR 节点的 SID
ProcessID	配置前缀SID时实际指定的进程号
Prefix-SID validity	配置的Prefix SID是否为有效值： - Invalid: 表示无效值，即前缀 SID 的值不在 SRGB 范围内或 Loopback 接口上使能的 OSPF 进程和配置前缀 SID 时实际指定的进程号不一致 - Valid: 表示有效值

1.1.22 display ospf interface hello

display ospf interface hello 命令用来显示接口发送 Hello 报文的信息。

【命令】

```
display ospf [ process-id ] interface [ interface-type interface-number ]  
hello
```

【视图】

任意视图

【缺省用户角色】

```
network-admin  
network-operator  
context-admin
```

context-operator

【参数】

process-id: 显示指定 OSPF 进程发送 Hello 报文的信息，*process-id* 表示 OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程发送 Hello 报文的信息。

interface-type interface-number: 显示指定 OSPF 接口发送 Hello 报文的信息，*interface-type interface-number* 表示接口类型和编号。如果未指定本参数，将显示所有 OSPF 接口发送 Hello 报文的信息。

【使用指导】

本命令仅显示以组播形式发送 Hello 报文的信息。

【举例】

显示 OSPF 接口发送 Hello 报文的信息。
<Sysname> display ospf interface hello

```
OSPF Process 1 with Router ID 192.168.1.1
  Interfaces

Area: 0.0.0.0

Interface: 172.16.0.1 (GigabitEthernet1/0/1)
First 4 hello packets sent:
  2018-08-05 11:05:10:121, succeeded
  2018-08-05 11:05:20:121, succeeded
  2018-08-05 11:05:30:121, succeeded
  2018-08-05 11:05:40:121, succeeded
Last 4 hello packets sent:
  2018-08-06 11:15:10:121, succeeded
  2018-08-06 11:15:20:121, succeeded
  2018-08-06 11:15:30:121, succeeded
  2018-08-06 11:15:40:121, succeeded
```

表1-20 display ospf interface hello 命令显示信息描述表

字段	描述
Area	接口所在区域
Interface	接口IP地址
First 4 hello packets sent	最先发送的4个Hello报文的时间，以及报文是否发送成功 - succeeded: 发送成功 - failed: 发送失败
Last 4 hello packets sent	执行本命令时，最近发送的4个Hello报文的时间，以及报文是否发送成功的信息 - succeeded: 发送成功 - failed: 发送失败

1.1.23 display ospf lsdb

display ospf lsdb 命令用来显示 OSPF 的链路状态数据库信息。

【命令】

```
display ospf [ process-id ] lsdb [ brief | originate-router  
advertising-router-id | self-originate ] [ age { max-value max-age-value |  
min-value min-age-value } * ] [ resolve-hostname ]  
display ospf [ process-id ] lsdb hostname host-name [ age { max-value  
max-age-value | min-value min-age-value } * ]  
display ospf [ process-id ] lsdb { ase | opaque-as } [ link-state-id ]  
[ originate-router advertising-router-id | self-originate ] [ age { max-value  
max-age-value | min-value min-age-value } * ] [ resolve-hostname ]  
display ospf [ process-id ] lsdb { ase | opaque-as } [ link-state-id ] hostname  
host-name [ age { max-value max-age-value | min-value min-age-value } * ]  
display ospf [ process-id ] [ area area-id ] lsdb { asbr | network | nssa |  
opaque-area | opaque-link | router | summary } [ link-state-id ]  
[ originate-router advertising-router-id | self-originate ] [ age { max-value  
max-age-value | min-value min-age-value } * ] [ resolve-hostname ]  
display ospf [ process-id ] [ area area-id ] lsdb { asbr | network | nssa |  
opaque-area | opaque-link | router | summary } [ link-state-id ] hostname  
host-name [ age { max-value max-age-value | min-value min-age-value } * ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的链路状态数据库信息。

age: 显示数据库中老化时间在指定范围内的 LSA 的信息。如果未指定本参数，则显示数据库中所有 LSA 的信息。

max-value max-age-value: 指定 LSA 老化时间的最大值，单位为秒，缺省值为 3600。如果未指定 **min-value min-age-value**，取值范围为 0~3600；如果指定了 **min-value min-age-value**，取值范围为 **min-age-value**~3600。

min-value min-age-value: 指定 LSA 老化时间的最小值，单位为秒，缺省值为 0。如果未指定 **max-value max-age-value**，取值范围为 0~3600；如果指定了 **max-value max-age-value**，取值范围为 0~**max-age-value**。

area area-id: 显示数据库中指定区域的 LSA 信息。*area-id* 表示区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其转换成 IP 地址格式）或者是 IP 地址格式。如果未指定本参数，将显示所有区域的信息。

brief: 显示数据库的概要信息。

asbr: 显示数据库中 Type-4 LSA（ASBR Summary LSA）的信息。

ase: 显示数据库中 Type-5 LSA（AS External LSA）的信息。

network: 显示数据库中 Type-2 LSA（Network LSA）的信息。

nssa: 显示数据库中 Type-7 LSA（NSSA External LSA）的信息。

opaque-area: 显示数据库中 Type-10 LSA（Opaque-area LSA）的信息。

opaque-as: 显示数据库中 Type-11 LSA（Opaque-AS LSA）的信息。

opaque-link: 显示数据库中 Type-9 LSA（Opaque-link LSA）的信息。

router: 显示数据库中 Type-1 LSA（Router LSA）的信息。

summary: 显示数据库中 Type-3 LSA（Network Summary LSA）的信息。

link-state-id: 链路状态 ID，IP 地址格式。

originate-router advertising-router-id: 发布 LSA 报文的路由器的 Router ID。

self-originate: 显示本地路由器自己产生的 LSA 的数据库信息。

hostname host-name: 发布 LSA 报文的路由器的主机名。如果未指定本参数，则显示数据库中所有 LSA 的信息。

resolve-hostname: 显示包含主机名的链路状态数据库信息。如果未指定本参数，显示的链路状态数据库信息中将不包含主机名。

【使用指导】

min-age-value 配置值不允许大于 *max-age-value*。

【举例】

显示 OSPF 的链路状态数据库信息。

```
<Sysname> display ospf lsdb
```

```
OSPF Process 1 with Router ID 192.168.0.1
Link State Database
```

Area: 0.0.0.0						
Type	LinkState ID	AdvRouter	Age	Len	Sequence	Metric
Router	192.168.0.2	192.168.0.2	474	36	80000004	0
Router	192.168.0.1	192.168.0.1	21	36	80000009	0
Network	192.168.0.1	192.168.0.1	321	32	80000003	0
Sum-Net	192.168.1.0	192.168.0.1	321	28	80000002	1
Sum-Net	192.168.2.0	192.168.0.2	474	28	80000002	1

Area: 0.0.0.1						
Type	LinkState ID	AdvRouter	Age	Len	Sequence	Metric
Router	192.168.0.1	192.168.0.1	21	36	80000005	0
Sum-Net	192.168.2.0	192.168.0.1	321	28	80000002	2
Sum-Net	192.168.0.0	192.168.0.1	321	28	80000002	1

```
Type 9 Opaque (Link-Local Scope) Database
```



```
Flags: * -Vlink interface LSA
Type      LinkState ID    AdvRouter      Age  Len  Sequence  Interfaces
*Opq-Link  3.0.0.0                7.2.2.1        8   14   80000001  10.1.1.2
*Opq-Link  3.0.0.0                7.2.2.2        8   14   80000001  20.1.1.2
```

显示 OSPF 的链路状态数据库信息，其中包含数据库中 LSA 的主机名信息。

```
<Sysname> display ospf lsdb resolve-hostname
```

```
OSPF Process 1 with Router ID 2.2.2.2
```

```
Link State Database
```

```
Area: 0.0.0.0
```

Type	LinkState ID	AdvRouter	Age	Len	Sequence	Metric
Router	1.1.1.1	1.1.1.1	1419	36	80000004	0
Router	2.2.2.2	RouterB	1420	36	80000004	0
Network	192.168.12.2	RouterB	1420	32	80000001	0
Sum-Net	192.168.13.0	1.1.1.1	1456	28	80000001	1

```
Area: 0.0.0.1
```

Type	LinkState ID	AdvRouter	Age	Len	Sequence	Metric
Router	3.3.3.3	3.3.3.3	1416	36	80000003	0
Router	1.1.1.1	1.1.1.1	1415	36	80000003	0
Network	192.168.13.2	3.3.3.3	1416	32	80000001	0
Sum-Net	192.168.12.0	1.1.1.1	1456	28	80000001	1

```
Type 10 Opaque (Area-Local Scope) Database
```

Type	LinkState ID	AdvRouter	Age	Len	Sequence	Area
Opq-Area	4.0.0.0	RouterB	470	32	80000001	0.0.0.0

表1-21 display ospf lsdb 命令显示信息描述表

字段	描述
Area	显示该区域的LSDB信息
Type	LSA类型
LinkState ID	LSA链路状态ID
AdvRouter	LSA发布路由器
Age	LSA的老化时间
Len	LSA的长度
Sequence	LSA序列号
Metric	度量值
*Opq-Link	表示Vlink接口产生的Opaque LSA
Opq-Area	表示接收到的Type-10 LSA

显示进程号为 1 的 OSPF 进程的链路状态数据库中网络 LSA 的信息。

```
<Sysname> display ospf 1 lsdb network
```

OSPF Process 1 with Router ID 192.168.1.1
Link State Database

Area: 0.0.0.0

Type : Network
LS ID : 192.168.0.2
Adv Rtr : 192.168.2.1
LS age : 922
Len : 32
Options : E
Seq# : 80000003
Checksum : 0x8d1b
Net Mask : 255.255.255.0
Attached Router 192.168.1.1
Attached Router 192.168.2.1

Area: 0.0.0.1

Type : Network
LS ID : 192.168.1.2
Adv Rtr : 192.168.1.2
LS age : 782
Len : 32
Options : NP
Seq# : 80000003
Checksum : 0x2a77
Net Mask : 255.255.255.0
Attached Router 192.168.1.1
Attached Router 192.168.1.2

显示进程号为 1 的 OSPF 进程的链路状态数据库中网络 LSA 的信息, 其中包含发布路由器的主机名信息。

<Sysname> display ospf 1 lsdB network resolve-hostname

OSPF Process 1 with Router ID 2.2.2.2
Link State Database

Area: 0.0.0.0

Type : Network
LS ID : 192.168.12.2
Adv Rtr : 2.2.2.2
Hostname : RouterB
LS age : 1552
Len : 32
Options : 0 E
Seq# : 80000001

```
Checksum : 0xbdd0
Net Mask : 255.255.255.0
Attached Router 1.1.1.1
Attached Router 2.2.2.2
```

Area: 0.0.0.1

```
Type : Network
LS ID : 192.168.13.2
Adv Rtr : 3.3.3.3
LS age : 1548
Len : 32
Options : 0 E
Seq# : 80000001
Checksum : 0xc6be
Net Mask : 255.255.255.0
Attached Router 1.1.1.1
Attached Router 3.3.3.3
```

表1-22 display ospf lsdb network 命令显示信息描述表

字段	描述
Type	LSA类型
LS ID	DR的IP地址
Adv Rtr	发布路由器
Hostname	LSA发布路由器主机名
LS age	LSA的老化时间
Len	LSA的长度
Options	LSA选项，各选项含义如下： • O: Opaque LSA 发布接受能力 • E: AS 外部 LSA 的接受能力 • EA: 外部扩展属性 LSA 的接受和转发能力 • DC: 支持按需链路 • N: 是否支持 NSSA 外部 LSA • P: 非纯末梢区域中的 ABR 路由器将 Type-7 LSA 转换为 Type-5 LSA 的能力
Seq#	LSA序列号
Checksum	LSA校验和
Net Mask	网络掩码
Attached Router	与DR形成了完全邻接关系的路由器的Router ID，也包括DR自身的Router ID

显示进程号为 1 的 OSPF 进程的链路状态数据库中网络 Type-10 LSA 的信息。

<Sysname> display ospf 1 lsdb opaque-area

OSPF Process 1 with Router ID 2.2.2.2

Link State Database

Area: 0.0.0.0

Type : Opq-Area
LS ID : 4.0.0.0
Adv Rtr : 1.1.1.1
LS age : 1311
Len : 52
Options : 0 E
Seq# : 8000015c
Checksum : 0x4323
Opaque type: 4(Router information)
Opaque ID: 0

Router information TLV:

Length : 4
Capabilities:
All Capability Bits: 0x60000000
Graceful restart helper capable
Stub router capable

Segment routing algorithm TLV:

Length : 1
Algorithm: 0

Segment routing range TLV:

Length: 12
Range : 1001

SID sub-TLV:

Length: 3
Label : 16000

Type : Opq-Area
LS ID : 7.0.0.0
Adv Rtr : 1.1.1.1
LS age : 1311
Len : 44
Options : 0 E
Seq# : 8000012f
Checksum : 0xabcf
Opaque type: 7(Extended prefix)
Opaque ID: 0

Extended prefix TLV:

Length : 20
Route type: 1

AF : 0
 Flags : N
 Prefix : 23.1.1.1/32

SID sub-TLV:
 Length : 8
 Flags : NP/-/E/-/-
 MTID : 0
 Algorithm : 0
 SID index : 101

表1-23 display ospf 1 lsdb opaque-area 命令显示信息描述表

字段	描述
Opaque type	Opaque类型
Opaque ID	Opaque ID
Router information TLV	路由能力TLV相关信息
Length	TLV长度，单位为字节
Capabilities	路由能力
All capability bits	所有能力比特位，标明设备支持的特性
Graceful restart helper capable	支持GR Restart Helper
Stub router capable	支持Stub Router
Segment routing algorithm TLV	SR算法TLV
Algorithm	前缀关联的算法类型
Segment routing range TLV	SR标签范围TLV
Range	标签范围
SID sub-TLV	前缀SID子TLV
Label	最小标签值
Route type	- 前缀来源路由类型： 1: Intra-Area 3: Inter-Area
AF	地址族
Flags	前缀SID标志信息： - A: A-Flag (Attach Flag)标志，如果置位，显示为“A”，表示 ABR 产生的区域间前缀 - N: N-Flag (Node Flag)标志，如果置位，显示为“N”，表示前缀 SID 为到达某一台 SR 节点的 SID
Prefix	前缀信息
SID sub-TLV	前缀SID子TLV的长度

字段	描述
Flags	- 前缀 SID 子 TLV 携带的标志信息： - NP: No-PHP 标志，如果置位，显示为“NP”，倒数第二跳不允许弹出前缀 SID - E: 显式空标志，如果置位，显示为“E”，该 SID 节点的上游邻居在转发报文前必须将该 SID 修改为显式空标签 - V: Value/Index 标志，如果置位，显示为“V”，表明携带的前缀 SID 是一个绝对值
MTID	多拓扑ID
Algorithm	前缀关联的算法类型
SID index	SID的相对值

1.1.24 display ospf nexthop

display ospf nexthop 命令用来显示进程中的下一跳信息。

【命令】

display ospf [*process-id*] nexthop

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有进程的下一跳信息。

【举例】

显示 OSPF 路由下一跳信息。

<Sysname> display ospf nexthop

OSPF Process 1 with Router ID 1.1.1.2
Neighbor Nexthop Information

NbrID	Nexthop	Interface	RefCount	Status
192.168.12.1	0.0.0.0	GE1/0/2	4	Valid
192.168.12.2	192.168.12.2	GE1/0/2	3	Valid
192.168.12.1	0.0.0.0	Loop100	1	Valid

表1-24 display ospf nexthop 命令显示信息描述表

字段	描述
NbrID	邻居路由器ID
Nexthop	下一跳地址
Interface	出接口
RefCount	该下一跳被引用次数
Status	该下一跳状态： - Valid: 生效 - Invalid: 未生效 - Valid-SR: 下一跳类型为 SR 隧道，且该 SR 隧道已生效 - Invalid-SR: 下一跳类型为 SR 隧道，该 SR 隧道未生效

1.1.25 display ospf non-stop-routing status

display ospf non-stop-routing status 命令用来显示 OSPF 的 NSR 阶段信息。

【命令】

display ospf [*process-id*] non-stop-routing status

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的 NSR 阶段信息。

【举例】

显示 OSPF 的 NSR 阶段信息。

```
<Sysname> display ospf non-stop-routing status
```

```
OSPF Process 1 with Router ID 192.168.33.12
Non Stop Routing information
```

```
Non Stop Routing capability : Enabled
Upgrade phase : Normal
```

表1-25 display ospf non-stop-routing status 命令显示信息描述表

字段	描述
Non Stop Routing capability	是否使能NSR功能，其中： • Enabled: 使能 NSR • Disabled: 不使能 NSR
Upgrade phase	升级的各个阶段： • Prepare: 升级准备阶段 • Restore Smooth: 升级数据平滑阶段 • Preroute: 路由计算预处理阶段 • Calculating: 路由计算阶段 • Redisting: 路由引入阶段 • Original and age: LSA 生成和老化阶段 • Normal: 普通状态

1.1.26 display ospf peer

display ospf peer 命令用来显示 OSPF 中各区域邻居的信息。

【命令】

```
display ospf [ process-id ] peer [ hello | verbose ] [ interface-type
interface-number ] [ [ neighbor-id ] [ resolve-hostname ] | hostname
host-name ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的各区域邻居的信息。

hello: 显示发送给邻居路由器或从邻居路由器收到 Hello 报文的信息。以组播形式发送 Hello 报文的场景中，仅显示从邻居路由器接收 Hello 报文的信息。

verbose: 显示 OSPF 各区域邻居的详细信息。如果未指定本参数，将显示 OSPF 进程各区域邻居的概要信息。

interface-type interface-number: 接口类型和编号。如果未指定本参数，将显示所有接口的 OSPF 邻居的信息。

neighbor-id: 邻居路由器的 Router ID。如果未指定本参数，将显示所有邻居路由器的 OSPF 邻居的信息。

resolve-hostname: 显示邻居路由器信息，且可以解析其中包含的主机名。如果未指定本参数，将无法解析邻居路由器信息中包含的主机名。

hostname host-name: 邻居路由器的主机名，取值范围为 1~255 个字符的字符串，区分大小写。如果未指定本参数，将显示所有邻居路由器的 OSPF 邻居的信息。

【举例】

显示 OSPF 邻居详细信息。

<Sysname> display ospf peer verbose

```
OSPF Process 1 with Router ID 1.1.1.1
Neighbors

Area 0.0.0.0 interface 1.1.1.1(GigabitEthernet1/0/1)'s neighbors
Router ID: 1.1.1.2           Address: 1.1.1.2           GR State: Normal
State: Full  Mode: Nbr is master  Priority: 1
DR: 1.1.1.2  BDR: 1.1.1.1  MTU: 0
Options is 0x02 (-|-|-|-|E|-)
Dead timer due in 33 sec
Neighbor is up for 02:03:35
Authentication Sequence: [ 0 ]
Neighbor state change count: 6
BFD status: Disabled
Adjacency SID: 24253

Last Neighbor Down Event:
Router ID: 22.22.22.22
Local Address: 11.11.11.11
Remote Address: 22.22.22.22
Time: Apr  9 03:18:19 2014
Reason: Ospf_ifachange
```

表1-26 display ospf peer verbose 命令显示信息描述表

字段	描述
Area <i>areaID</i> interface <i>IPAddress(InterfaceName)</i> 's neighbors	显示接口在指定区域邻居信息，其中： <i>areaID</i> 表示邻居所属的区域 <i>IPAddress</i> 表示接口 IP 地址 <i>InterfaceName</i> 表示接口名称
Router ID	邻居路由器ID
Address	邻居接口地址
GR State	GR状态，取值为： - Normal: 普通状态 - Restarter: 正在作为 GR Restarter

字段	描述
	- Complete: GR 完成 - Helper: 正在作为 GR Helper
Hostname	邻居路由器主机名
State	邻居状态，取值为： - Down 表示邻居关系的初始状态 - Init 表示在邻居失效时间内收到来自邻居路由器的 Hello 报文，但该 Hello 数据包内没有包含自己的 Router ID，双向通信还没有建立起来 - Attempt 该状态仅对 NBMA 网络上的邻居有效，表示最近没有从邻居收到信息，但仍需作出进一步的尝试，用以与邻居联系 2-Way 表示双向通信已经建立，在从邻居路由器收到的 Hello 报文中看到了自己的 Router ID - Exstart 表示路由器和邻居建立主/从关系、确定初始 DD 报文的序列号，为交换 DD 报文做好准备 - Exchange 表示路由器向其邻居发送描述自己 LSDB 的 DD 报文 - Loading 表示路由器向邻居发送链路状态请求报文，请求最新的 LSA - Full 表示路由器与邻居路由器之间建立起完全邻接关系
Mode	路由器在数据库同步阶段，路由器与邻居协商的主从关系，取值为： - Nbr is master 表示邻居路由器为主路由器 - Nbr is slave 表示邻居路由器为从路由器
Priority	邻居路由器优先级
DR	接口所属网段的DR
BDR	接口所属网段的BDR
MTU	接口MTU的值
Options	邻居的LSA选项，各选项含义如下： - O: Opaque LSA 发布接受能力 - E: AS 外部 LSA 的接受能力 - EA: 外部扩展属性 LSA 的接受和转发能力 - DC: 支持按需链路 - N: 是否支持 NSSA 外部 LSA - P: 非纯末稍区域中的 ABR 路由器将 Type-7 LSA 转换为 Type-5 LSA 的能力
Dead timer due in 33 sec	邻居将在33秒后被认为不可达
Neighbor is up for 02:03:35	与邻居建立的时长02:03:35
Authentication Sequence	验证序列号
Neighbor state change count	邻居状态发生改变的次数
BFD status	BFD状态，各状态含义如下： - Disabled: 未使能 BFD - Enabled (Control mode): 已使能 BFD，并处于控制模式

字段	描述
	Enabled (Echo mode): 已使能 BFD, 并处于回应模式
Adjacency SID	邻接链路通告的SID
Last Neighbor Down Event	最后一次邻居down事件
Local Address	本端IP地址
Remote Address	对端IP地址
Time	邻居down的时间
Reason	邻居down的原因

显示 OSPF 邻居概要信息。

<Sysname> display ospf peer

```

      OSPF Process 1 with Router ID 1.1.1.1
        Neighbor Brief Information

```

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	State	Interface
1.1.1.2	1.1.1.2	1	40	Full/DR	GE1/0/1

Sham link: 11.11.11.11 -> 22.22.22.22

Router ID	Address	Pri	Dead-Time	State
22.22.22.22	22.22.22.22	1	36	Full

显示 OSPF 邻居概要信息，并解析其中的主机名。

<Sysname> display ospf peer resolve-hostname

```

      OSPF Process 1 with Router ID 1.1.1.1
        Neighbor Brief Information

```

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	State	Interface
RouterA	1.1.1.2	1	34	Full/DR	GE1/0/1

Sham link: 11.11.11.11 -> 22.22.22.22

Router ID	Address	Pri	Dead-Time	State
22.22.22.22	22.22.22.22	1	36	Full

显示 OSPF 邻居概要信息，并解析其中的主机名。

<Sysname> display ospf peer resolve-hostname

```

      OSPF Process 1 with Router ID 1.1.1.1
        Neighbor Brief Information

```

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	State	Interface
RouterA	1.1.1.2	1	34	Full/DR	Vlan10

Sham link: 11.11.11.11 -> 22.22.22.22

Router ID	Address	Pri	Dead-Time	State
22.22.22.22	22.22.22.22	1	36	Full

表1-27 display ospf peer 命令显示信息描述表

字段	描述
Area	邻居所属的区域
Router ID	邻居路由器ID或邻居路由器主机名
Address	邻居接口IP地址
Pri	邻居路由器优先级
Dead-Time	OSPF的邻居失效时间
Interface	与邻居相连的接口
State	邻居状态（Down、Init、Attempt、2-Way、Exstart、Exchange、Loading、Full）

显示发送给邻居路由器以及从邻居路由器收到 Hello 报文的详细信息。

<Sysname> display ospf peer hello

```
OSPF Process 1 with Router ID 1.1.1.1
Neighbors
```

```
Area 0.0.0.0 interface 1.1.1.1(GigabitEthernet1/0/1)'s neighbors
```

```
Router ID: 1.1.1.2          Address: 1.1.1.2
```

```
First 4 hello packets received:
```

```
2018-01-06 09:12:10:121
```

```
2018-01-06 09:12:20:121
```

```
2018-01-06 09:12:30:121
```

```
2018-01-06 09:12:40:121
```

```
Last 4 hello packets received:
```

```
2018-01-06 11:15:10:121
```

```
2018-01-06 11:15:20:121
```

```
2018-01-06 11:15:30:121
```

```
2018-01-06 11:15:40:121
```

```
First 4 hello packets sent:
```

```
2018-01-06 09:12:12:121, failed, errno:132
```

```
2018-01-06 09:12:22:121, succeeded
```

```
2018-01-06 09:12:32:121, succeeded
```

```
2018-01-06 09:12:42:121, succeeded
```

```
Last 4 hello packets sent:
```

```
2018-01-06 11:15:12:121, succeeded
```

```
2018-01-06 11:15:22:121, succeeded
```

```
2018-01-06 11:15:32:121, failed, errno:132
```

```
2018-01-06 11:15:42:121, failed, errno:132
```

表1-28 display ospf peer hello 命令显示信息描述表

字段	描述
Router ID	邻居路由器的Router ID
Address	邻居接口的IP地址
First 4 hello packets received	最先收到邻居发送的4个Hello报文的时间
Last 4 hello packets received	最近收到邻居发送的4个Hello报文的时间
First 4 hello packets sent	最先发送给邻居的4个Hello报文的时间，以及报文是否发送成功的信息（以组播形式发送Hello报文的场景中，不显示该字段）： • succeeded: 发送成功 • failed: 发送失败 • errno: 错误码，表明了报文发送失败的原因
Last 4 hello packets sent	执行本命令时，最近发送给邻居的4个Hello报文的时间，以及报文是否发送成功的信息（以组播形式发送Hello报文的场景中，不显示该字段）： • succeeded: 发送成功 • failed: 发送失败 • errno: 错误码，表明了报文发送失败的原因

1.1.27 display ospf peer statistics

display ospf peer statistics 命令用来显示本地路由器所有 OSPF 邻居的统计信息，即处于各种状态的邻居数目。

【命令】

display ospf [*process-id*] peer statistics

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的邻居统计信息。

【举例】

显示所有 OSPF 邻居的统计信息。

```
<Sysname> display ospf peer statistics
```

OSPF Process 1 with Router ID 192.168.1.112
Neighbor Statistics

Area ID	Down	Attempt	Init	2-Way	ExStart	Exchange	Loading	Full	Total
0.0.0.0	0	0	0	0	0	0	0	1	1
0.0.0.2	0	0	0	0	0	0	0	1	1
Total	0	0	0	0	0	0	0	2	2

Sham links' neighbors (Total: 1):

Down: 0, Init: 0, 2-Way: 0, ExStart: 0, Exchange: 0, Loading: 0, Full: 1

表1-29 display ospf peer statistics 命令显示信息描述表

字段	描述
Area ID	区域ID，显示当前路由器位于该区域所有邻居路由器的状态统计信息
Down	同一个区域内状态为Down的邻居路由器数目
Attempt	同一个区域内状态为Attempt的邻居路由器数目
Init	同一个区域内状态为Init的邻居路由器数目
2-Way	同一个区域内状态为2-Way的邻居路由器数目
ExStart	同一个区域内状态为ExStart的邻居路由器数目
Exchange	同一个区域内状态为Exchange的邻居路由器数目
Loading	同一个区域内状态为Loading的邻居路由器数目
Full	同一个区域内状态为Full的邻居路由器数目
Total	处于各种状态（Down/Attempt/Init/2-Way/ExStart/Exchange/Loading/Full）邻居路由器的总和

1.1.28 display ospf request-queue

display ospf request-queue 命令用来显示 OSPF 的请求列表信息。

【命令】

display ospf [*process-id*] **request-queue** [*interface-type interface-number*]
[*neighbor-id*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的请求列表信息。

interface-type interface-number: 接口类型和编号。如果未指定本参数，将显示所有接口的请求列表信息。

neighbor-id: 邻居路由器的 Router ID。如果未指定本参数，将显示所有邻居路由器的请求列表信息。

【举例】

显示 OSPF 请求列表信息。

<Sysname> display ospf request-queue

```
OSPF Process 100 with Router ID 192.168.1.59
Link State Request List

The Router's Neighbor is Router ID 2.2.2.2      Address 10.1.1.2
Interface 10.1.1.1      Area 0.0.0.0
Request list:
  Type      LinkState ID      AdvRouter      Sequence      Age
  Router    2.2.2.2      1.1.1.1      80000004      1
  Network   192.168.0.1    1.1.1.1      80000003      1
  Sum-Net   192.168.1.0    1.1.1.1      80000002      2
```

表1-30 display ospf request-queue 命令显示信息描述表

字段	描述
The Router's Neighbor is Router ID	邻居路由器的Router ID
Address	邻居接口IP地址
Interface	本地接口IP地址
Area	区域ID
Request list	请求列表信息
Type	LSA类型
LinkState ID	链路状态ID
AdvRouter	发布路由器的Router ID
Sequence	LSA的序列号
Age	LSA的老化时间

1.1.29 display ospf retrans-queue

display ospf retrans-queue 命令用来显示 OSPF 的重传列表信息。

【命令】

display ospf [*process-id*] **retrans-queue** [*interface-type interface-number*]
[*neighbor-id*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的重传列表信息。

interface-type interface-number: 接口类型和编号。如果未指定本参数，将显示所有接口的重传列表信息。

neighbor-id: 邻居路由器的 Router ID。如果未指定本参数，将显示所有邻居路由器的重传列表信息。

【举例】

显示 OSPF 重传列表信息。
<Sysname> display ospf retrans-queue

```
OSPF Process 100 with Router ID 192.168.1.59
Link State Retransmission List

The Router's Neighbor is Router ID 192.168.1.111   Address 111.1.1.1
Interface 111.1.1.2           Area 0.0.0.1
Retransmit list:
  Type      LinkState ID      AdvRouter      Sequence      Age
  Router    2.2.2.2                 2.2.2.2        80000004      1
  Network   12.18.0.1                2.2.2.2        80000003      1
  Sum-Net   12.18.1.0                2.2.2.2        80000002      2
```

表1-31 display ospf retrans-queue 命令显示信息描述表

字段	描述
The Router's Neighbor is Router ID	邻居路由器ID
Address	邻居接口IP地址
Interface	本地接口IP地址
Area	区域ID
Retransmit list	重传列表信息
Type	LSA类型

字段	描述
LinkState ID	链路状态ID
AdvRouter	发布路由器的Router ID
Sequence	LSA的序列号
Age	LSA的老化时间

1.1.30 display ospf routing

display ospf routing 命令用来显示 OSPF 路由表的信息。

【命令】

```
display ospf [ process-id ] routing [ ip-address { mask-length | mask } ]
[ interface interface-type interface-number ] [ nexthop nexthop-address ]
[ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的路由表信息。

ip-address: 路由的目的 IP 地址。

mask-length: 网络掩码长度，取值范围为 0~32。

mask: 网络掩码，点分十进制格式。

interface interface-type interface-number: 显示指定出接口的路由信息。

interface-type interface-number 为接口类型和编号。如果未指定本参数，将显示所有接口的路由表信息。

nexthop nexthop-address: 显示指定下一跳 IP 地址的路由信息。如果未指定本参数，将显示所有的 OSPF 路由表信息。

verbose: 显示路由表详细信息。如果未指定本参数，将显示路由表的概要信息。

【举例】

显示 OSPF 路由表的信息。

```
<Sysname> display ospf routing
```

```
OSPF Process 1 with Router ID 192.168.1.112
Routing Table
```

```

Routing for network
Destination      Cost      Type      NextHop      AdvRouter      Area
192.168.1.0/24   1562      Stub      192.168.1.2   192.168.1.2    0.0.0.0
172.16.0.0/16    1563      Inter     192.168.1.1   192.168.1.1    0.0.0.0

```

```

Total nets: 2
Intra area: 1  Inter area: 1  ASE: 0  NSSA: 0

```

表1-32 display ospf routing 命令显示信息描述表

字段	描述
Destination	目的网络
Cost	到达目的地址的开销
Type	路由类型（Intra、Transit、Stub、Inter、Type1和Type2）
NextHop	下一跳地址
AdvRouter	发布路由器
Area	区域ID
Total nets	区域内部、区域间、ASE和NSSA区域的路由总数
Intra area	区域内部路由总数
Inter area	区域间路由总数
ASE	OSPF区域外路由总数
NSSA	NSSA区域路由总数

显示 OSPF 路由表的详细信息。

```
<Sysname> display ospf routing verbose
```

```

      OSPF Process 2 with Router ID 192.168.1.112
      Routing Table

```

```
Routing for network
```

```

Destination: 192.168.1.0/24
  Priority: Low                      Type: Stub
  AdvRouter: 192.168.1.2            Area: 0.0.0.0
  SubProtoID: 0x1                   Preference: 10
    NextHop: 192.168.1.2             BkNextHop: N/A
      IfType: Broadcast              BkIfType: N/A
        Interface: GE1/0/2           BkInterface: N/A
          NibID: 0x1300000c          Status: Normal
            Cost: 1562
              InLabel: 4294967295     Tunnel type: -
                OutLabel: 4294967295  OutLabel flag: -
                  BkOutLabel: 4294967295 BkOutLabel flag: -

```

```

Destination: 172.16.0.0/16
  Priority: Low                                Type: Inter
  AdvRouter: 192.168.1.1                      Area: 0.0.0.0
  SubProtoID: 0x1                             Preference: 10
  NextHop: 192.168.1.1                       BkNextHop: N/A
  IfType: Broadcast                          BkIfType: N/A
  Interface: GE1/0/3                         BkInterface: N/A
  NibID: 0x1300000c                          Status: Normal
  Cost: 1563
  InLabel: 4294967295                        Tunnel type: -
  OutLabel: 4294967295                      OutLabel flag: -
  BkOutLabel: 4294967295                    BkOutLabel flag: -

Destination: 91.1.0.0/16
  Priority: Low                                Type: Type2
  AdvRouter: 2.2.2.2                          Tag: 0
  SubProtoID: 0x8                             Preference: 150
  NextHop: 21.41.0.2                         BkNextHop: N/A
  IfType: PTP                                BkIfType: N/A
  Interface: GE1/0/4                         BkInterface: N/A
  NibID: 0x13000003                          Status: Normal
  Cost: 1                                     ECMP group: 0x1300001a
  InLabel: 4294967295                        Tunnel type: -
  OutLabel: 4294967295                      OutLabel flag: -
  BkOutLabel: 4294967295                    BkOutLabel flag: -

Destination: 91.1.0.0/16
  Priority: Low                                Type: Type2
  AdvRouter: 3.3.3.3                          Tag: 0
  SubProtoID: 0x8                             Preference: 150
  NextHop: 31.41.0.3                         BkNextHop: N/A
  IfType: PTP                                BkIfType: N/A
  Interface: GE1/0/3                         BkInterface: N/A
  NibID: 0x13000005                          Status: Normal
  Cost: 1                                     ECMP group: 0x1300001a
  InLabel: 4294967295                        Tunnel type: -
  OutLabel: 4294967295                      OutLabel flag: -
  BkOutLabel: 4294967295                    BkOutLabel flag: -

```

```

Total nets: 4
Intra area: 2  Inter area: 0  ASE: 2  NSSA: 0

```

表1-33 display ospf routing verbose 命令显示信息描述表

字段	描述
Priority	前缀优先级，取值为：Critical、High、Medium和Low
Type	路由类型（Intra-area、Transit、Stub、Inter-Area、Type1 External和Type2 External）

字段	描述
AdvRouter	发布路由器
Area	区域ID
SubProtocolID	子协议ID
Preference	OSPF路由优先级
NextHop	主下一跳IP地址
BkNextHop	备份下一跳IP地址
IfType	路由主下一跳网络类型
BkIfType	路由备份下一跳网络类型
Interface	路由出接口
BkInterface	路由备份出接口
NibID	路由下一跳信息的ID值
Status	路由状态，具体如下： • Local: 该条路由在本地，未发送给路由管理模块 • Invalid: 路由下一跳无效 • Stale: 该路由下一跳较旧 • Normal: 正常可用状态 • Delete: 处于删除状态 • Host-Adv: 该条路由为主机路由 • Rely: 该条路由为迭代路由
Cost	到达目的地址的开销
ECMP group	等价路由组ID，开启等价路由组功能且形成等价路由组时才会显示该字段
InLabel	路由入标签
Tunnel type	隧道类型，目前取值只能为SR，表示SR隧道
OutLabel	路由出标签
OutLabel flag	出标签标志位 • E: 显式空标志，如果置位，显示为“E”，则该SID节点的上游邻居在转发报文前必须将该SID修改为显式空标签 • I: 隐式空标志，如果置位，显示为“I”，则该SID节点的上游邻居在转发报文前必须将该SID修改为隐式空标签（暂不支持） • N: 普通标志 • P: SR标签优先标志
BkOutLabel	路由备份出标签
BkOutLabel flag	备份出标签标志位 • E: 显式空标志，如果置位，显示为“E”，则该SID节点的上游邻居在转发报文前必须将该SID修改为显式空标签 • I: 隐式空标志，如果置位，显示为“I”，则该SID节点的上游邻居在转发报文

字段	描述
	前必须将该 SID 修改为隐式空标签
	• N: 普通标志 • P: SR 标签优先标志

1.1.31 display ospf spf-tree

display ospf spf-tree 命令用来显示 OSPF 区域的最短路径树信息。

【命令】

display ospf [*process-id*] [*area area-id*] **spf-tree** [*verbose*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程下区域的最短路径树信息。

area area-id: 显示指定 OSPF 区域的最短路径树信息。*area-id* 表示区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其转换成 IP 地址格式）或者是 IP 地址格式。如果未指定本参数，将显示所有区域的最短路径树信息。

verbose: 显示 OSPF 区域的最短路径树的详细信息。如果未指定本参数，将显示 OSPF 区域的最短路径树的概要信息。

【举例】

显示进程 1 下区域 0 的最短路径树信息。

```
<Sysname> display ospf 1 area 0 spf-tree
```

```
OSPF Process 1 with Router ID 100.0.0.4
```

```
Flags: S-Node is on SPF tree      R-Node is directly reachable
      I-Node or Link is init      D-Node or Link is to be deleted
      P-Neighbor is parent        A-Node is in candidate list
      C-Neighbor is child         T-Node is tunnel destination
      H-Nexthop changed           N-Link is a new path
      V-Link is involved          G-Link is in change list
```

```
Area: 0.0.0.0 Shortest Path Tree
```

```

SpfNode      Type    Flag      SpfLink      Type    Cost    Flag
>192.168.119.130 Network S R
                                -->114.114.114.111 NET2RT 0      C
                                -->100.0.0.4      NET2RT 0      P
>114.114.114.111 Router  S
                                -->192.168.119.130 RT2NET 65535 P
>100.0.0.4      Router  S
                                -->192.168.119.130 RT2NET 10     C

```

表1-34 display ospf spf-tree 命令显示信息描述表

字段	描述
SpfNode	SPF节点，若节点类型为路由器，则为路由器ID；若节点类型为网络，则为该网络DR接口IP地址。其中，Type为节点类型： • Network：表示网络节点 • Router：表示路由器节点 Flag为节点标志： • I：节点处于初始化状态 • A：节点在候选列表上 • S：节点在 SPF 树上 • R：该节点与根节点直连 • D：该节点将被删除 • T：该节点为隧道的终点
SpfLink	SPF链路，其值表示对端节点。其中，Cost为链路开销，Type为链路类型： • RT2RT：表示路由器到路由器链路 • NET2RT：表示网络到路由器链路 • RT2NET：表示路由器到网络链路 Flag为链路标志： • I：链路处于初始化状态 • P：目的节点是父节点 • C：目的节点是子节点 • D：链路将要被删除 • H：下一跳发生改变 • V：目的节点删除或者是新增节点时，链路的目的节点不在 SPF 树上或处于删除状态 • N：新增链路，并且源节点和目的节点都在 SPF 树上 • G：链路在区域变化列表中

显示进程 1 下区域 0 的最短路径树详细信息。

```
<Sysname> display ospf 1 area 0 spf-tree verbose
```

```
OSPF Process 1 with Router ID 100.0.0.4
```

```

Flags: S-Node is on SPF tree      R-Node is directly reachable
      I-Node or Link is init      D-Node or Link is to be deleted

```

P-Neighbor is parent	A-Node is in candidate list
C-Neighbor is child	T-Node is tunnel destination
H-Nexthop changed	N-Link is a new path
V-Link is involved	G-Link is in change list

Area: 0.0.0.0 Shortest Path Tree

```
>LsId(192.168.119.130)
  AdvId   : 100.0.0.4      NodeType   : Network
  Mask    : 255.255.255.0  SPFLinkCnt : 2
  Distance : 10
  VlinkData: 0.0.0.0      ParentLinkCnt: 1      NodeFlag: S R
  NextHop  : 1
    192.168.119.130      Interface: GE1/0/2      Flag: -
  BkNextHop: 1
    0.0.0.0              Interface: GE1/0/2      Flag: -
-->LinkId(114.114.114.111)
  AdvId   : 100.0.0.4      LinkType   : NET2RT
  LsId    : 192.168.119.130 LinkCost    : 0      NextHopCnt: 1
  LinkData: 0.0.0.0      LinkNewCost: 0      LinkFlag  : C
-->LinkId(100.0.0.4)
  AdvId   : 100.0.0.4      LinkType   : NET2RT
  LsId    : 192.168.119.130 LinkCost    : 0      NextHopCnt: 1
  LinkData: 0.0.0.0      LinkNewCost: 0      LinkFlag  : P
```

表1-35 display ospf spf-tree verbose 命令显示信息描述表

字段	描述
LsId	链路状态ID
AdvId	通告路由器ID
NodeType	节点类型，其中： • Network: 表示网络节点 • Router: 表示路由器节点
Mask	网络掩码，若为路由器节点掩码为0
SPFLinkCnt	SPF链路个数
Distance	表示到根节点的开销
VlinkData	Vlink报文的目的地址
ParentLinkCnt	父链路个数
NodeFlag	节点标志： • I: 节点处于初始化状态 • A: 节点在候选列表上 • S: 节点在 SPF 树上 • R: 该节点与根节点直连 • D: 该节点将被删除

字段	描述
	T: 该节点为隧道的终点
NextHop	下一跳信息
Interface	出接口
Flag	标识下一跳的类型，SR表示为SR隧道，其他类型显示为“-”
BkNextHop	备份下一跳信息
LinkId	链路ID
LinkType	链路类型，其中： - RT2RT: 表示路由器到路由器链路 - NET2RT: 表示网络到路由器链路 - RT2NET: 表示路由器到网络链路
LinkCost	当前链路开销
NextHopCnt	下一跳个数
LinkData	链路数据
LinkNewCost	新的链路开销
LinkFlag	链路标志： - I: 链路处于初始化状态 - P: 目的节点是父节点 - C: 目的节点是子节点 - D: 链路将要被删除 - H: 下一跳发生改变 - V: 目的节点删除或者是新增节点时，链路的目的节点不在 SPF 树上或处于删除状态 - N: 新增链路，并且源节点和目的节点都在 SPF 树上 - G: 链路在区域变化列表中

1.1.32 display ospf statistics

display ospf statistics 命令用来显示 OSPF 的统计信息。

【命令】

```
display ospf [ process-id ] statistics [ error | packet [ hello | interface-type interface-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

context-admin
context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的统计信息。

error: 显示错误统计信息。如果未指定本参数，将显示 OSPF 进程的报文、LSA 和路由的统计信息。

packet: 显示 OSPF 的报文统计信息。

hello: 显示接收和发送 Hello 报文的统计信息。如果未指定本参数，将显示接收和发送所有类型的 OSPF 协议报文的统计信息。

interface-type interface-number: 接口类型和编号。显示指定接口的统计信息。如果未指定本参数，将显示所有接口的统计信息。

【举例】

显示 OSPF 进程的统计信息。

```
<Sysname> display ospf statistics
```

```
OSPF Process 1 with Router ID 2.2.2.2
Statistics
```

```
I/O statistics
```

Type	Input	Output
Hello	61	122
DB Description	2	3
Link-State Req	1	1
Link-State Update	3	3
Link-State Ack	3	2

```
LSAs originated by this router
```

```
Router   : 4
Network  : 0
Sum-Net   : 0
Sum-Asbr : 0
External : 0
NSSA      : 0
Opq-Link : 0
Opq-Area : 0
Opq-As    : 0
```

```
LSAs originated: 4  LSAs received: 7
```

```
Routing table:
```

```
Intra area: 2  Inter area: 3  ASE/NSSA: 0
```

表1-36 display ospf statistics 命令显示信息描述表

字段	描述
I/O statistics	收发报文和LSA的详细统计信息
Type	OSPF报文类型
Input	接收报文数
Output	发送报文数
Hello	OSPF Hello报文
DB Description	OSPF数据库描述报文
Link-State Req	OSPF链路状态请求报文
Link-State Update	OSPF链路状态更新报文
Link-State Ack	OSPF链路状态确认报文
LSAs originated by this router	本路由器发布LSA的详细统计信息
Router	生成Type-1 LSA的数目
Network	生成Type-2 LSA的数目
Sum-Net	生成Type-3 LSA的数目
Sum-Asbr	生成Type-4 LSA的数目
External	生成Type-5 LSA的数目
NSSA	生成Type-7 LSA的数目
Opq-Link	生成Type-9 LSA的数目
Opq-Area	生成Type-10 LSA的数目
Opq-As	生成Type-11 LSA的数目
LSA originated	生成的LSA的总数
LSA received	接收的LSA的总数
Routing table	路由表信息
Intra area	区域内路由的数量
Inter area	区域间路由的数量
ASE/NSSA	自治系统外部/NSSA区域路由的数量

显示 OSPF 进程的错误统计信息。

```
<Sysname> display ospf statistics error
```

```
OSPF Process 1 with Router ID 192.168.1.112
```

```
OSPF Packet Error Statistics
```

```
0          : Router ID confusion      0          : Bad packet
0          : Bad version              0          : Bad checksum
```

0	: Bad area ID	0	: Drop on unnumbered link
0	: Bad virtual link	0	: Bad authentication type
0	: Bad authentication key	0	: Packet too small
0	: Neighbor state low	0	: Transmit error
0	: Interface down	0	: Unknown neighbor
0	: HELLO: Netmask mismatch	0	: HELLO: Hello-time mismatch
0	: HELLO: Dead-time mismatch	0	: HELLO: Ebit option mismatch
0	: DD: MTU option mismatch	0	: DD: Unknown LSA type
0	: DD: Ebit option mismatch	0	: ACK: Bad ack
0	: ACK: Unknown LSA type	0	: REQ: Empty request
0	: REQ: Bad request	0	: UPD: LSA checksum bad
0	: UPD: Unknown LSA type	0	: UPD: Less recent LSA

表1-37 display ospf statistics error 命令显示信息描述表

字段	描述
Router ID confusion	含有重复路由器ID的OSPF报文数
Bad packet	非法的OSPF报文数
Bad version	错误版本号的OSPF报文数
Bad checksum	校验和出错的OSPF报文数
Bad area ID	非法的区域ID的OSPF报文数
Drop on unnumbered link	在地址借用链路上丢弃的OSPF报文数
Bad virtual link	错误的虚链路的OSPF报文数
Bad authentication type	含有非法验证类型的OSPF报文数
Bad authentication key	含有错误验证码的OSPF报文数
Packet too small	报文长度太小的OSPF报文数
Neighbor state low	在低邻居状态收到的OSPF报文数
Transmit error	传输出错的OSPF报文数
Interface down	接口down的计数
Unknown neighbor	未知的邻居发来的OSPF报文数
HELLO: Netmask mismatch	网络掩码不匹配的Hello报文数
HELLO: Hello-time mismatch	Hello定时器不匹配的Hello报文数
HELLO: Dead-time mismatch	Dead定时器不匹配的Hello报文数
HELLO: Ebit option mismatch	Option字段E位不匹配的Hello报文数
DD: MTU option mismatch	MTU不匹配的DD报文数
DD: Unknown LSA type	DD报文中描述未知类型LSA数目
DD: Ebit option mismatch	Option字段E位不匹配的DD报文数
ACK: Bad ack	收到不匹配的ack数目
ACK: Unknown LSA type	收到LSA类型未知的ack数目

字段	描述
REQ: Empty request	不含有任何请求信息的LSR报文数
REQ: Bad request	请求错误LSA的LSR报文数
UPD: LSA checksum bad	LSU报文中LSA校验和出错的LSA数目
UPD: Unknown LSA type	LSU报文中含有未知类型LSA数目
UPD: Less recent LSA	LSU报文中含有不是最新的LSA数目

显示 OSPF 进程和接口的报文统计信息。

<Sysname> display ospf statistics packet

```

OSPF Process 100 with Router ID 192.168.1.59
  Packet Statistics

Waiting to send packet count: 0

      Hello      DD      LSR      LSU      ACK      Total
Input  : 489      6      2      44      40      581
Output: 492      8      2      45      40      587

Area: 0.0.0.1
Interface: 20.1.1.1 (GigabitEthernet1/0/1)
      DD      LSR      LSU      ACK      Total
Input  : 0      0      0      0      0
Output: 0      0      0      0      0

Interface: 100.1.1.1 (GigabitEthernet1/0/2)
      DD      LSR      LSU      ACK      Total
Input  : 3      1      22     16      42
Output: 2      1      19     20      42

```

表1-38 display ospf statistics packet 命令显示信息描述表

字段	描述
Waiting to send packet count	等待发送报文数
Hello	Hello报文
DD	数据库描述报文
LSR	链路状态请求报文
LSU	链路状态更新报文
ACK	链路状态确认报文
Total	报文总数
Input	接收报文数
Output	发送报文数
Area	区域ID

字段	描述
Interface	接口地址和接口名

显示 OSPF 接收和发送 Hello 报文的统计信息。

```
<Sysname> display ospf statistics packet hello
```

```

      OSPF Process 1 with Router ID 1.1.1.1
        Hello statistics
      Total sent                               : 201
      Total sent failed                       : 0
      Sent after one and a half intervals    : 0
      Total received                         : 221
      Total received dropped                 : 0
      Received after one and a half intervals: 0

```

表1-39 display ospf peer hello 命令显示信息描述表

字段	描述
Total sent	发送Hello报文的总数
Total sent failed	发送Hello报文失败的总数
Sent after one and a half intervals	发送Hello报文的时间间隔超过1.5倍Hello定时器的报文总数
Total received	接收Hello报文的总数
Total received dropped	丢弃接收到的Hello报文总数
Received after one and a half intervals	接收Hello报文的时间间隔超过1.5倍Hello定时器的报文总数

【相关命令】

- **reset ospf statistics**

1.1.33 display ospf vlink

display ospf vlink 命令用来显示 OSPF 的虚连接信息。

【命令】

```
display ospf [ process-id ] vlink
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin

```

context-operator

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPF 进程的虚连接信息。

【举例】

显示 OSPF 的虚连接信息。

<Sysname> display ospf vlink

```
OSPF Process 1 with Router ID 3.3.3.3
Virtual Links

Virtual-link Neighbor-ID -> 2.2.2.2, Neighbor-State: Full
Interface: 10.1.2.1 (GigabitEthernet1/0/1)
Cost: 1562 State: P-2-P Type: Virtual
Transit Area: 0.0.0.1
Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
MD5 authentication enabled.
    The last key is 3.
    The rollover is in progress, 2 neighbor(s) left.
```

表1-40 display ospf vlink 命令显示信息描述表

字段	描述
Virtual-link Neighbor-id	通过虚连接相连的邻居路由器的Router ID
Neighbor-State	邻居状态，包括Down、Init、2-Way、ExStart、Exchange、Loading和Full
Interface	此虚连接的本端接口的IP地址和名称
Cost	接口的路由开销
State	接口状态
Type	类型：虚连接
Transit Area	传输区域ID（如果当前接口为虚连接，则显示）
Timers	OSPF定时器，分别定义如下： • Hello: 表示接口发送 Hello 报文的时间间隔，单位为秒 • Dead: 表示邻居的失效时间，单位为秒 • Retransmit: 表示接口重传 LSA 时间间隔，单位为秒
Transmit Delay	接口对LSA的传输延迟时间，单位为秒
Simple authentication enabled	采用Simple验证模式
Keychain authentication enabled, name is xx	采用keychain验证模式，keychain名称为xx
MD5 authentication enabled	采用MD5/HMAC-MD5验证模式
The last key is xx	最新的MD5/HMAC-MD5验证字标识符为xx

字段	描述
The rollover is in progress, xx neighbor(s) left	正在进行MD5/HMAC-MD5验证平滑迁移，尚未完成MD5验证平滑迁移的邻居个数为xx

1.1.34 display router id

display router id 命令用来显示全局 Router ID。

【命令】

display router id

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 显示已配置的全局 Router ID。
<Sysname> display router id
    Configured router ID is 1.1.1.1
```

1.1.35 dscp

dscp 命令用来配置 OSPF 发送协议报文的 DSCP 优先级。

undo dscp 命令用来恢复缺省情况。

【命令】

dscp *dscp-value*
undo dscp

【缺省情况】

OSPF 发送协议报文的 DSCP 优先级为 48。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

dscp-value: DSCP 优先级，取值范围为 0~63。

【举例】

```
# 配置 OSPF 进程 1 发送协议报文的 DSCP 优先级为 63。
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] dscp 63
```

1.1.36 ecmp-group enable

ecmp-group enable 命令用来开启等价路由组功能。

undo ecmp-group enable 命令用来恢复缺省情况。

【命令】

```
ecmp-group enable
undo ecmp-group enable
```

【缺省情况】

等价路由组功能处于关闭状态。

【视图】

OSPF 进程视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

本功能适用于存在大量 OSPF 等价路由且不同前缀都具有相同的等价下一跳场景中。例如，OSPF 学到了 1 万条不同的路由前缀且每条前缀都具有 1.1.1.1~1.1.1.16 的 16 个下一跳。缺省情况下，OSPF 会向路由管理分别下发各条等价路由，开启本功能后，OSPF 会将等价路由组合起来统一下发给路由管理，从而加快收敛速度。

【举例】

```
# 为 OSPF 进程 1 开启等价路由组功能。
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] ecmp-group enable
```

1.1.37 enable link-local-signaling

enable link-local-signaling 命令用来使能 OSPF 本地链路的信令能力。

undo enable link-local-signaling 命令用来关闭 OSPF 本地链路的信令能力。

【命令】

```
enable link-local-signaling
undo enable link-local-signaling
```

【缺省情况】

OSPF 本地链路的信令能力处于关闭状态。

【视图】

OSPF 视图

【缺省用户角色】

network-admin

context-admin

【举例】

使能 OSPF 进程 1 的本地链路的信令能力。

```
<Sysname> system-view
```

```
[Sysname] ospf 1
```

```
[Sysname-ospf-1] enable link-local-signaling
```

1.1.38 enable out-of-band-resynchronization

enable out-of-band-resynchronization 命令用来使能 OSPF 带外同步能力。

undo enable out-of-band-resynchronization 命令用来关闭 OSPF 带外同步能力。

【命令】

enable out-of-band-resynchronization

undo enable out-of-band-resynchronization

【缺省情况】

OSPF 带外同步能力处于关闭状态。

【视图】

OSPF 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

在配置本命令之前，必须先使能 OSPF 本地链路的信令能力。

【举例】

使能 OSPF 进程 1 的带外同步能力。

```
<Sysname> system-view
```

```
[Sysname] ospf 1
```

```
[Sysname-ospf-1] enable link-local-signaling
```

```
[Sysname-ospf-1] enable out-of-band-resynchronization
```

【相关命令】

- **enable link-local-signaling**

1.1.39 event-log

event-log 命令用来配置 OSPF 的日志信息个数。

undo event-log 命令用来取消 OSPF 的日志信息个数的配置。

【命令】

```
event-log { hello { received [ abnormal | dropped ] | sent [ abnormal | failed ] }  
| lsa-flush | peer | spf } size count  
undo event-log { hello { received [ abnormal | dropped ] | sent [ abnormal |  
failed ] } | lsa-flush | peer | spf } size
```

【缺省情况】

接收 Hello 报文、接收异常 Hello 报文、丢弃接收到的 Hello 报文、发送 Hello 报文、发送异常 Hello 报文以及发送失败的 Hello 报文、LSA 老化、邻居状态变化、路由计算的日志信息个数均为 100。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

hello: 接收或发送 Hello 报文的日志信息个数。

received: 接收 Hello 报文的日志信息个数。

sent: 发送 Hello 报文的日志信息个数。

abnormal: 发送或接收异常 Hello 报文的日志信息个数。异常 Hello 报文指的是发送或接收到的 Hello 报文的时间间隔大于或等于 1.5 倍 Hello 定时器的报文。

dropped: 丢弃接收到的 Hello 报文的日志信息个数。

failed: 发送失败的 Hello 报文的日志信息个数。

lsa-flush: LSA 老化日志信息个数。

peer: 邻居状态变化的日志信息个数。

spf: SPF 日志信息个数。

size count: 指定日志信息个数，取值范围为 0~65535。

【举例】

```
# 配置 OSPF 进程 100 的路由计算日志信息个数为 50。  
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] event-log spf size 50
```

1.1.40 fast-reroute (OSPF view)

fast-reroute 命令用来配置 OSPF 快速重路由功能。

undo fast-reroute 命令用来关闭 OSPF 快速重路由功能。

【命令】

```
fast-reroute { lfa [ abr-only ] | route-policy route-policy-name }  
undo fast-reroute
```

【缺省情况】

OSPF 快速重路由功能处于关闭状态。

【视图】

OSPF 视图

【缺省用户角色】

network-admin

context-admin

【参数】

lfa: 为所有路由通过 LFA（Loop Free Alternate）算法选取备份下一跳信息。

abr-only: 仅选取到 ABR 设备的路由作为备份下一跳。

route-policy route-policy-name : 为通过策略的路由指定备份下一跳，*route-policy-name* 为路由策略名，为 1~63 个字符的字符串，区分大小写。

【使用指导】

OSPF 快速重路由功能和前缀无关收敛功能同时配置时，OSPF 快速重路由功能生效。

OSPF 快速重路由功能（通过 LFA 算法选取备份下一跳信息）不能与 **vlink-peer** 命令同时使用。

【举例】

使能 OSPF 进程 1 的快速重路由功能，为所有路由通过 LFA 算法选取备份下一跳信息。

```
<Sysname> system-view
```

```
[Sysname] ospf 1
```

```
[Sysname-ospf-1] fast-reroute lfa
```

1.1.41 filter (OSPF area view)

filter 命令用来配置对 Type-3 LSA 进行过滤。

undo filter 命令用来取消对 Type-3 LSA 的过滤。

【命令】

```
filter { ipv4-acl-number | prefix-list prefix-list-name | route-policy route-policy-name } { export | import }
```

```
undo filter { export | import }
```

【缺省情况】

不对 Type-3 LSA 进行过滤。

【视图】

OSPF 区域视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-acl-number: 指定的基本或高级 IPv4 ACL 编号，对进出本区域的 Type-3 LSA 进行过滤，取值范围为 2000~3999。

prefix-list-name: 指定的地址前缀列表，对进出本区域的 Type-3 LSA 进行过滤，为 1~63 个字符的字符串，区分大小写。

route-policy-name: 指定的路由策略，对进出本区域的 Type-3 LSA 进行过滤，为 1~63 个字符的字符串，区分大小写。

export: 对 ABR 向其它区域发布的 Type-3 LSA 进行过滤。

import: 对 ABR 向本区域发布的 Type-3 LSA 进行过滤。

【使用指导】

此命令只在 ABR 路由器上有效，对区域内部路由器无效。

【举例】

根据地址前缀列表 my-prefix-list 和编号为 2000 的基本 ACL 分别对进出 OSPF 区域 1 的 Type-3 LSA 进行过滤。

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] filter prefix-list my-prefix-list import
[Sysname-ospf-100-area-0.0.0.1] filter 2000 export
```

1.1.42 filter-policy export (OSPF view)

filter-policy export 命令用来配置 OSPF 对引入的路由信息进行过滤。

undo filter-policy export 命令用来取消 OSPF 对引入的路由信息进行过滤。

【命令】

```
filter-policy { ipv4-acl-number | prefix-list prefix-list-name } export [ |
direct | { ospf | rip } [ process-id ] | static ]
undo filter-policy export [ | direct | { ospf | rip } [ process-id ] | static ]
```

【缺省情况】

OSPF 不对引入的路由信息进行过滤。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4-acl-number: 用于过滤路由信息目的地址的基本或高级 IPv4 ACL 编号，取值范围为 2000~3999。

prefix-list-name: 用于过滤路由信息目的地址的 IP 地址前缀列表的名称, 为 1~63 个字符的字符串, 区分大小写。

direct: 对引入的直连路由进行过滤。

ospf: 对引入的 OSPF 路由进行过滤。

rip: 对引入的 RIP 路由进行过滤。

process-id: 路由协议进程号, 取值范围为 1~65535, 缺省值为 1。

【使用指导】

如果没有指定任何参数, 则表示 OSPF 对引入的所有路由信息进行过滤。

当配置的是高级 ACL (3000~3999) 时, 其使用规则如下:

- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard** 来过滤指定目的地址的路由。
- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard destination dest-addr dest-wildcard** 来过滤指定目的地址和掩码的路由。

其中, **source** 用来过滤路由目的地址, **destination** 用来过滤路由掩码, 配置的掩码应该是连续的 (当配置的掩码不连续时该过滤掩码的条件不生效)。

【举例】

配置 OSPF 进程 100 使用编号为 2000 的基本 ACL 对引入的路由进行过滤。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 export
```

配置 OSPF 进程 100 使用编号为 3000 的高级 ACL 对引入的路由进行过滤, 只允许 113.0.0.0/16 通过。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 3000 export
```

【相关命令】

- **import-route**

1.1.43 filter-policy import (OSPF view)

filter-policy import 命令用来配置 OSPF 对通过接收到的 LSA 计算出来的路由信息进行过滤。

undo filter-policy import 命令用来恢复缺省情况。

【命令】

```
filter-policy { ipv4-acl-number [ gateway prefix-list-name ] | gateway  
prefix-list-name | prefix-list prefix-list-name [ gateway prefix-list-name ]  
| route-policy route-policy-name } import  
undo filter-policy import
```

【缺省情况】

OSPF 不对通过接收到的 LSA 计算出来的路由信息进行过滤。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv4-acl-number: 用于过滤路由信息目的地址的基本或高级 IPv4 ACL 编号, 取值范围为 2000~3999。

gateway prefix-list-name: 指定的地址前缀列表, 基于要加入到路由表的路由信息的下一跳进行过滤。prefix-list-name 为 1~63 个字符的字符串, 区分大小写。

prefix-list prefix-list-name: 指定的地址前缀列表, 基于目的地址对接收的路由信息进行过滤。prefix-list-name 为 1~63 个字符的字符串, 区分大小写。

route-policy route-policy-name: 指定路由策略名, 基于路由策略对接收的路由信息进行过滤。route-policy-name 为 1~63 个字符的字符串, 区分大小写。

【使用指导】

当配置的是高级 ACL (3000~3999) 或者指定的路由策略中配置的是高级 ACL 时, 其使用规则如下:

- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard** 来过滤指定目的地址的路由。
- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard destination dest-addr dest-wildcard** 来过滤指定目的地址和掩码的路由。

其中, **source** 用来过滤路由目的地址, **destination** 用来过滤路由掩码, 配置的掩码应该是连续的 (当配置的掩码不连续时该过滤掩码的条件不生效)。

【举例】

使用编号为 2000 的基本 ACL 对接收的路由信息进行过滤。

```
<Sysname> system-view  
[Sysname] acl basic 2000  
[Sysname-acl-ipv4-basic-2000] rule deny source 192.168.10.0 0.0.0.255  
[Sysname-acl-ipv4-basic-2000] quit  
[Sysname] ospf 100  
[Sysname-ospf-100] filter-policy 2000 import
```

```
# 使用编号为 3000 的高级 ACL 对接收的路由进行过滤，只允许 113.0.0.0/16 通过。
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 10 permit ip source 113.0.0.0 0 destination 255.255.0.0 0
[Sysname-acl-ipv4-adv-3000] rule 100 deny ip
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 3000 import
```

1.1.44 graceful-restart (OSPF view)

graceful-restart 命令用来使能 OSPF 协议的 GR 能力。

undo graceful-restart 命令用来关闭 OSPF 协议的 GR 能力。

【命令】

```
graceful-restart [ ietf | nonstandard ] [ global | planned-only ] *
undo graceful-restart
```

【缺省情况】

OSPF 协议的 GR 能力处于关闭状态。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ietf: IETF 标准 GR 能力选项。

nonstandard: 非 IETF 标准 GR 能力选项。

global: 全局 GR，必须保证所有的 GR Helper 都存在，整个 GR 才会完成，如果有一个 GR Helper 失效（比如，接口 down），则整个 GR 失败。如果未指定本参数，表示支持接口级 GR，即只要有一个 GR Helper 存在，则整个 GR 会完成。

planned-only: 表示只支持计划重启。如果未指定本参数，表示计划重启和非计划重启都支持。

【使用指导】

GR 包括计划重启和非计划重启：

- 计划重启指的是手动通过命令 **reset ospf process** 执行重启，或通过命令 **placement reoptimize** 触发进程的主备倒换，在进行重启或主备倒换前 GR Restarter 会先发送 Grace-LSA。
- 非计划重启指的是由于设备故障等原因进行重启或主备倒换，在进行重启或主备倒换前 GR Restarter 不会事先发送 Grace-LSA。

在使能 OSPF 协议的 IETF 标准 GR 能力前，需要先使能 OSPF 不透明链路状态发布接收能力（**opaque-capability enable**）。

在使能 OSPF 协议的非 IETF 标准的 GR 能力前，需要先使能 OSPF 本地链路的信令能力（**enable link-local-signaling**）和 OSPF 带外同步能力（**enable out-of-band-resynchronization**）。

如果在使能 OSPF 协议的 GR 能力时不指定可选参数 **nonstandard** 和 **ietf**，则 **nonstandard** 为缺省配置。

OSPF GR 特性与 OSPF NSR 特性互斥，即 **graceful-restart** 和 **non-stop-routing** 命令互斥，不能同时配置。

【举例】

使能 OSPF 进程 1 的 IETF 标准 GR 能力。

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] opaque-capability enable
[Sysname-ospf-1] graceful-restart ietf
```

使能 OSPF 进程 1 的非 IETF 标准 GR 能力。

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart nonstandard
```

【相关命令】

- **enable link-local-signaling**
- **enable out-of-band-resynchronization**
- **opaque-capability enable**

1.1.45 graceful-restart helper enable

graceful-restart helper enable 命令用来使能 OSPF 的 GR Helper 能力。

undo graceful-restart helper enable 命令用来关闭 OSPF 的 GR Helper 能力。

【命令】

```
graceful-restart helper enable [ planned-only ]
undo graceful-restart helper enable
```

【缺省情况】

OSPF 的 GR Helper 能力处于开启状态。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```


【参数】

planned-only: 表示只支持计划重启。如果未指定本参数，表示计划重启和非计划重启（即异常重启）都支持。

【使用指导】

参数 **planned-only** 只有在 IETF 标准 GR Helper 的时候使用。

【举例】

```
# 使能 OSPF 进程 1 的 GR Helper 能力。  
<Sysname> system-view  
[Sysname] ospf 1  
[Sysname-ospf-1] graceful-restart helper enable
```

1.1.46 graceful-restart helper strict-lsa-checking

graceful-restart helper strict-lsa-checking 命令用来使能 GR Helper 严格 LSA 检查能力。

undo graceful-restart helper strict-lsa-checking 命令用来关闭 GR Helper 严格 LSA 检查能力。

【命令】

```
graceful-restart helper strict-lsa-checking  
undo graceful-restart helper strict-lsa-checking
```

【缺省情况】

OSPF 协议的 GR Helper 严格 LSA 检查能力处于关闭状态。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

当检查到 GR Helper 设备的 LSA 发生变化时候，Helper 设备退出 GR Helper 模式。

【举例】

```
# 使能 OSPF 进程 1 的 GR Helper 严格 LSA 检查能力。  
<Sysname> system-view  
[Sysname] ospf 1  
[Sysname-ospf-1] graceful-restart helper strict-lsa-checking
```

1.1.47 graceful-restart interval (OSPF view)

graceful-restart interval 命令用来配置 OSPF 协议的 GR 重启间隔时间。

undo graceful-restart interval 命令用来恢复缺省情况。

【命令】

```
graceful-restart interval interval  
undo graceful-restart interval
```

【缺省情况】

OSPF 协议的 GR 重启间隔时间为 120 秒。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval：指定 OSPF 协议的 GR 重启间隔时间（期望重启时间），取值范围为 40～1800，单位为秒。

【使用指导】

OSPF 协议的 GR 重启间隔时间不能小于 OSPF 所有接口中邻居失效时间的最大值，否则可能会造成 OSPF 协议的 GR 重启失败。

【举例】

```
# 配置 OSPF 进程 1 的 GR 重启间隔时间为 100 秒。  
<Sysname> system-view  
[Sysname] ospf 1  
[Sysname-ospf-1] graceful-restart interval 100
```

【相关命令】

- **ospf timer dead**

1.1.48 host-advertise

host-advertise 命令用来配置并发布一条主机路由。

undo host-advertise 命令用来删除一条主机路由。

【命令】

```
host-advertise ip-address cost-value  
undo host-advertise ip-address
```

【缺省情况】

OSPF 不发布主机路由。

【视图】

OSPF 区域视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: 主机 IP 地址。

cost-value: 主机路由的开销值，取值范围为 1～65535。

【举例】

配置发布一条路由 1.1.1.1，并设置其开销为 100。

```
<Sysname> system-view
```

```
[Sysname] ospf 100
```

```
[Sysname-ospf-100] area 0
```

```
[Sysname-ospf-100-area-0.0.0.0] host-advertise 1.1.1.1 100
```

1.1.49 hostname

hostname 命令用来使能 OSPF 动态主机名映射功能。

undo hostname 命令用来关闭 OSPF 动态主机名映射功能。

【命令】

hostname [*host-name*]

undo hostname

【缺省情况】

OSPF 动态主机名映射功能处于关闭状态。

【视图】

OSPF 视图

【缺省用户角色】

network-admin

context-admin

【参数】

host-name: 配置与当前 OSPF 进程的 Router ID 对应的主机名称，为 1～255 个字符的字符串，区分大小写。如果未指定本参数，当前 OSPF 进程的 Router ID 对应的主机名为设备名称。

【使用指导】

OSPF 使用 Type-10 LSA 或 Type-11 LSA 携带动态主机名属性信息，因此，使用该功能前，需要保证 OSPF 的 Opaque LSA 发布接收能力处于开启状态。

【举例】

使能 OSPF 进程 1 的动态主机名映射功能，并配置 Router ID 映射后的主机名称为 red。

```
<Sysname> system-view
```

```
[Sysname] ospf 1
```

```
[Sysname-ospf-1] hostname red
```

【相关命令】

- **display ospf hostname-table**

- **opaque-capability enable**

1.1.50 import-route (OSPF view)

import-route 命令用来配置引入外部路由信息。

undo import-route 命令用来取消引入外部路由信息。

【命令】

```
import-route { direct | static } [ cost cost-value | nssa-only | route-policy
route-policy-name | tag tag | type type ] *
import-route { ospf | rip } [ process-id | all-processes ] [ allow-direct | cost
cost-value | nssa-only | route-policy route-policy-name | tag tag | type type ]
*
undo import-route { direct ospf | rip } [ process-id | all-processes ] |
static }
```

【缺省情况】

不引入外部路由信息。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

direct: 引入直连路由。

ospf: 引入 OSPF 协议的路由。

rip: 引入 RIP 协议的路由。

static: 引入静态路由。

process-id: 路由协议进程号，取值范围为 1~65535，缺省值为 1。

all-processes: 引入指定路由协议所有进程的路由。

allow-direct: 在引入的路由中包含使能了该协议的接口网段路由。如果未指定本参数，在引入协议路由时不会包含使能了该协议的接口网段路由。当 **allow-direct** 与 **route-policy route-policy-name** 参数一起使用时，需要注意路由策略中配置的匹配规则不要与接口路由信息存在冲突，否则会导致 **allow-direct** 配置失效。例如，当配置 **allow-direct** 参数引入 OSPF 直连时，在路由策略中不要配置 **if-match route-type** 匹配条件，否则，**allow-direct** 参数失效。

cost cost-value: 路由开销值，取值范围为 0~16777214，缺省值为 1。

nssa-only: 设置 Type-7 LSA 的 P 比特位不置位，即在对端路由器上不能转为 Type-5 LSA。如果未指定本参数，Type-7 LSA 的 P 比特位被置位，即在对端路由器上可以转为 Type-5 LSA（如果本地路由器是 ABR，则会检查骨干区域是否存在 FULL 状态的邻居，当 FULL 状态的邻居存在时，产生的 Type-7 LSA 中 P 比特位不置位）。

route-policy route-policy-name: 配置只能引入符合指定路由策略的路由。
route-policy-name 为路由策略名称, 为 1~63 个字符的字符串, 区分大小写。

tag tag: 外部 LSA 中的标记, 取值范围为 0~4294967295, 缺省值为 1。

type type: 度量值类型, 取值范围为 1~2, 缺省值为 2。

【使用指导】

外部路由是指到达自治系统外部的路由, 有两类:

- 第一类外部路由 (Type1 External): 这类路由的可信程度较高, 并且和 OSPF 自身路由的开销具有可比性, 所以到第一类外部路由的开销等于本路由器到相应的 ASBR 的开销与 ASBR 到该路由目的地址的开销之和。
- 第二类外部路由 (Type2 External): 这类路由的可信度比较低, 所以 OSPF 协议认为从 ASBR 到自治系统之外的开销远远大于在自治系统之内到达 ASBR 的开销。所以计算路由开销时将主要考虑前者, 即到第二类外部路由的开销等于 ASBR 到该路由目的地址的开销。如果计算出开销值相等的两条路由, 再考虑本路由器到相应的 ASBR 的开销。

该命令只能引入路由表中状态为 active 的路由, 是否为 active 状态可以通过 **display ip routing-table protocol** 命令来查看。不能引入缺省路由。

import-route nssa-only 命令配置后, 引入的路由只在 NSSA 区域产生 Type-7 LSA, 不会在非 NSSA 区域产生 Type-5 LSA。

undo import-route { ospf | rip } all-processes 命令只能取消 **import-route { ospf | rip } all-processes** 命令的配置, 不能取消 **import-route { ospf | rip } process-id** 命令的配置。

【举例】

指定引入的进程号为 40 的 RIP 路由为 Type-2 外部路由, 路由标记为 33, 度量值为 50。

```
<Sysname> system-view
```

```
[Sysname] ospf 100
```

```
[Sysname-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

【相关命令】

- **default-route-advertise** (OSPF view)

1.1.51 ispf enable (OSPF view)

ispf enable 命令用来使能增量 SPF 计算功能。

undo ispf enable 命令用来关闭增量 SPF 计算功能。

【命令】

```
ispf enable
```

```
undo ispf enable
```

【缺省情况】

增量 SPF 计算功能处于使能状态。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

使能增量 SPF 计算功能后，当网络的拓扑结构发生变化影响到最短路径树的结构时，只将受影响的部分节点进行修正，而不重建整棵最短路径树。

【举例】

```
# 关闭 OSPF 进程 100 的增量 SPF 计算功能。  
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] undo ispf enable
```

1.1.52 log-peer-change

log-peer-change 命令用来打开邻居状态变化的输出开关。

undo log-peer-change 命令用来关闭邻居状态变化的输出开关。

【命令】

log-peer-change
undo log-peer-change

【缺省情况】

邻居状态变化的输出开关处于打开状态。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

打开邻接状态输出开关后，OSPF 邻居状态变化时会生成日志信息发送到设备的信息中心，通过设置信息中心的参数，最终决定日志信息的输出规则（即是否允许输出以及输出方向）。（有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。）

【举例】

```
# 关闭 OSPF 进程 100 的邻居状态变化的输出开关。  
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] undo log-peer-change
```

1.1.53 lsa-arrival-interval

lsa-arrival-interval 命令用来配置 OSPF LSA 重复到达的最小时间间隔。

undo lsa-arrival-interval 命令用来恢复缺省情况。

【命令】

```
lsa-arrival-interval interval
undo lsa-arrival-interval
```

【缺省情况】

OSPF LSA 重复到达的最小时间间隔为 1000 毫秒。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interval: OSPF LSA 重复到达的最小时间间隔，取值范围为 0~60000，单位为毫秒。

【使用指导】

如果在 *interval* 的时间间隔内又收到一条 LSA 类型、LS ID、生成路由器 ID 均相同的 LSA 则直接丢弃，这样就可以抑制网络频繁变化可能导致的带宽资源和路由器资源被过多占用的问题。

建议 *interval* 小于或等于 **lsa-generation-interval** 命令所配置的 *minimum-interval*。

【举例】

```
# 设置 OSPF LSA 重复到达的最小时间间隔为 200 毫秒。
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-arrival-interval 200
```

【相关命令】

- **lsa-generation-interval**

1.1.54 lsa-generation-interval

lsa-generation-interval 命令用来配置 OSPF LSA 重新生成的时间间隔。

undo lsa-generation-interval 命令用来恢复缺省情况。

【命令】

```
lsa-generation-interval      maximum-interval      [      minimum-interval
[ incremental-interval ] ]
undo lsa-generation-interval
```

【缺省情况】

OSPF LSA 重新生成的最大时间间隔为 5 秒，最小时间间隔为 50 毫秒，时间间隔惩罚增量为 200 毫秒。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

maximum-interval: OSPF LSA 重新生成的最大时间间隔，取值范围为 1~60，单位为秒。

minimum-interval: OSPF LSA 重新生成的最小时间间隔，取值范围为 10~60000，单位为毫秒。

incremental-interval: OSPF LSA 重新生成的时间间隔惩罚增量，取值范围为 10~60000，单位为毫秒。

【使用指导】

通过调节 LSA 重新生成的时间间隔，可以抑制网络频繁变化可能导致的占用过多带宽资源和路由器资源。在网络变化不频繁的情况下，将 LSA 重新生成时间间隔缩小到 *minimum-interval*，而在网络变化频繁的情况下可以进行相应惩罚，将等待时间按照配置的惩罚增量延长，最大不超过 *maximum-interval*。

minimum-interval 和 *incremental-interval* 配置值不允许大于 *maximum-interval* 配置值。

【举例】

```
# 设置 LSA 重新生成的最大时间间隔为 2 秒，最小时间间隔为 100 毫秒，惩罚增量为 100 毫秒。  
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] lsa-generation-interval 2 100 100
```

【相关命令】

- **lsa-arrival-interval**

1.1.155 lsdb-overflow-interval

lsdb-overflow-interval 命令用来配置 OSPF 尝试退出 overflow 状态的定时器时间间隔。

undo lsdb-overflow-interval 命令用来恢复缺省情况。

【命令】

```
lsdb-overflow-interval interval  
undo lsdb-overflow-interval
```

【缺省情况】

OSPF 尝试退出 overflow 状态的定时器时间间隔是 300 秒。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval: OSPF 尝试退出 **overflow** 状态的定时器时间间隔，取值范围为 0~2147483647，单位为秒。

【使用指导】

网络中出现过多 LSA，会占用大量系统资源。当设置的 LSDB 中 External LSA 的最大数量达到上限时，LSDB 会进入 **overflow** 状态，在 **overflow** 状态中，不再接收 External LSA，同时删除自己生成的 External LSA，对于已经收到的 External LSA 则不会删除。这样就可以减少 LSA 从而节省系统资源。

通过调整定时器间隔，可以调整 OSPF 退出 **overflow** 状态的时间。

配置为 0 秒表示不启动定时器，不退出 **overflow** 状态。

【举例】

```
# 配置 OSPF 尝试退出 overflow 的定时器间隔为 10 秒。
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-interval 10
```

1.1.56 lsdb-overflow-limit

lsdb-overflow-limit 命令用来配置 OSPF 的 LSDB 中 External LSA 的最大条目数。

undo lsdb-overflow-limit 命令用来恢复缺省情况。

【命令】

```
lsdb-overflow-limit number
undo lsdb-overflow-limit
```

【缺省情况】

不对 LSDB 中 External LSA 的最大条目数进行限制。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

number: LSDB 中 External LSA 的最大条目数，取值范围为 1~1000000。

【举例】

```
# 设置 LSDB 中 External LSA 的最大条目数为 400000。
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-limit 400000
```

1.1.57 maximum load-balancing (OSPF view)

maximum load-balancing 命令用来配置 OSPF 支持的等价路由的最大条数。

undo maximum load-balancing 命令用来恢复缺省情况。

【命令】

maximum load-balancing *number*

undo maximum load-balancing

【缺省情况】

设备各款型对于本节所描述的参数支持情况有所不同，详细差异信息如下

型号	说明
T5000-G20	16
T5000-G30	32
T1000-G20/T1000-G50/T1000-G60/T1000-G80	16
T1000-CN60/T1000-CN80	32

【视图】

OSPF 视图

【缺省用户角色】

network-admin

context-admin

【参数】

number：等价路由的最大条数，当 *number* 取值为 1 时，相当于不进行负载分担。

【使用指导】

本命令中 *number* 参数的取值范围和 **max-ecmp-num** 命令相关。通过 **max-ecmp-num** 命令配置系统支持的最大等价路由条数为 *m*，并重启设备后，*number* 参数的取值范围将修改为 1~*m*。

【举例】

配置 OSPF 支持的等价路由的最大条数为 2。

```
<Sysname> system-view
```

```
[Sysname] ospf 100
```

```
[Sysname-ospf-100] maximum load-balancing 2
```

1.1.58 network (OSPF area view)

network 命令用来配置 OSPF 区域所包含的网段并在指定网段的接口上使能 OSPF。

undo network 命令用来删除区域所包含的网段并关闭指定网段接口上的 OSPF 功能。

【命令】

network *ip-address wildcard-mask*

undo network *ip-address wildcard-mask*

【缺省情况】

接口不属于任何区域且 OSPF 功能处于关闭状态。

【视图】

OSPF 区域视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: 接口所在的网段地址。

wildcard-mask: IP 地址掩码的反码，相当于将 IP 地址的掩码取反（0 变 1，1 变 0）。其中，“1”表示忽略 IP 地址中对应的位，“0”表示必须保留此位。（例如：子网掩码 255.0.0.0，该掩码的通配符掩码为 0.255.255.255）。

【使用指导】

该命令可以在一个区域内配置一个或多个接口。在接口上运行 OSPF 协议，此接口的主 IP 地址必须在 **network** 命令指定的网段范围之内。如果此接口只有从 IP 地址在 **network** 命令指定的网段范围之内，接口不运行 OSPF 协议。

【举例】

指定运行 OSPF 协议的接口的主 IP 地址位于网段 131.108.20.0/24，接口所在的 OSPF 区域 ID 为 2。

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] network 131.108.20.0 0.0.0.255
```

【相关命令】

- **ospf**

1.1.59 non-stop-routing

non-stop-routing 命令用来使能 OSPF 协议的 NSR 功能。

undo non-stop-routing 命令用来关闭 OSPF 协议的 NSR 功能。

【命令】

non-stop-routing

undo non-stop-routing

【缺省情况】

OSPF 协议的 NSR 功能处于关闭状态。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

各个进程的 NSR 功能是相互独立的，只对本进程生效。如果存在多个 OSPF 进程，建议在各个进程下使能 OSPF NSR 功能。

OSPF NSR 特性与 OSPF GR 特性互斥，即 **non-stop-routing** 和 **graceful-restart** 命令互斥，不能同时配置。

【举例】

```
# 在 OSPF 进程 100 中使能 NSR 功能。  
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] non-stop-routing
```

1.1.60 nssa (OSPF area view)

nssa 命令用来配置一个区域为 NSSA 区域。

undo nssa 命令用来恢复缺省情况。

【命令】

```
nssa [ default-route-advertise [ cost cost-value | nssa-only | route-policy route-policy-name | type type ] * | no-import-route | no-summary | suppress-fa  
| [ [ [ translate-always ] [ translate-ignore-checking-backbone ] ] | translate-never ] | translator-stability-interval value ] *  
undo nssa
```

【缺省情况】

没有区域被配置为 NSSA 区域。

【视图】

OSPF 区域视图

【缺省用户角色】

network-admin
context-admin

【参数】

default-route-advertise: 该参数只用于 NSSA 区域的 ABR 或 ASBR，配置后，对于 ABR，不论本地是否存在缺省路由，都将生成一条 Type-7 LSA 向区域内发布缺省路由；对于 ASBR，只有当本地存在缺省路由时，才产生 Type-7 LSA 向区域内发布缺省路由。

cost cost-value: 该缺省路由的度量值，取值范围为 0~16777214。如果未指定本参数，缺省路由的度量值将取 **default cost** 命令配置的值。

nssa-only: 设置 Type-7 LSA 的 P 比特位不置位，即在对端路由器上不能转为 Type-5 LSA。缺省时，Type-7 LSA 的 P 比特位被置位，即在对端路由器上可以转为 Type-5 LSA（如果本地路由器

是 ABR，则会检查骨干区域是否存在 FULL 状态的邻居，当 FULL 状态的邻居存在时，产生的 Type-7 LSA 中 P 比特位不置位）。

route-policy route-policy-name: 路由策略名，为 1~63 个字符的字符串，区分大小写。只有当前路由器的路由表中存在缺省路由，并且有路由匹配 *route-policy-name* 指定的路由策略，才可以产生一个描述缺省路由的 Type-7 LSA 发布出去，指定的路由策略会影响 Type-7 LSA 中的值。

type type: 该 Type-7 LSA 的类型，取值范围为 1~2，如果未指定本参数，Type-7 LSA 的缺省类型将取 **default type** 命令配置的值。

no-import-route: 该参数用于禁止将 AS 外部路由以 Type-7 LSA 的形式引入到 NSSA 区域中，这个参数通常只用在既是 NSSA 区域的 ABR，也是 OSPF 自治系统的 ASBR 的路由器上，以保证所有外部路由信息能正确地进入 OSPF 路由域。

no-summary: 该参数只用于 NSSA 区域的 ABR，配置后，ABR 只通过 Type-3 LSA 向区域内发布一条缺省路由，不再向区域内发布任何其它 Type-3 LSA（这种区域又称为 Totally NSSA 区域）。

suppress-fa: 指定当 Type-7 LSA 转换为 Type-5 LSA 时，生成的 Type-5 LSA 中的 Forwarding Address 不生效。

translate-always: 指定 ABR 为 NSSA 区域的 Type-7 LSA 转换为 Type-5 LSA 的转换路由器。

translate-ignore-checking-backbone: 选举 NSSA 区域的转换路由器时，不检查骨干区域是否存在 FULL 状态的邻居。

translate-never: 指定 ABR 不能将 NSSA 区域的 Type-7 LSA 转换为 Type-5 LSA。

translator-stability-interval value: 当有新的设备成为 NSSA 区域的 Type-7 LSA 转换为 Type-5 LSA 的转换路由器后，原 Type-7 LSA 转换为 Type-5 LSA 的转换路由器保持转换能力的时间。*value* 为保持时间，取值范围为 0~900，单位为秒，缺省值为 0，即不保持。

【使用指导】

如果要将一个区域配置成 NSSA 区域，则该区域中的所有路由器都必须配置该命令。

当 NSSA 区域存在多个 ABR 时，如果在某个 ABR 上指定了 **translate-ignore-checking-backbone** 参数，则需要在 NSSA 区域的其他 ABR 上做相同的配置，否则可能会出现没有 ABR 被选举为 NSSA 区域的转换路由器，或者多个 ABR 被选举为 NSSA 区域的转换路由器的情况。

【举例】

将区域 1 配置成 NSSA 区域。

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] nssa
```

【相关命令】

- **default-cost** (OSPF area view)

1.1.61 opaque-capability enable

opaque-capability enable 命令用来使能 OSPF 的 Opaque LSA 发布接收能力。

undo opaque-capability 命令用来关闭 OSPF 的 Opaque LSA 发布接收能力。

【命令】

```
opaque-capability enable
undo opaque-capability
```

【缺省情况】

OSPF 的 Opaque LSA 发布接收能力处于开启状态。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

使能 OSPF 的 Opaque LSA 发布接收能力后，OSPF 可以发布接收 Type9 的 Opaque LSA，接收 Type10 和 Type11 的 Opaque LSA。

【举例】

```
# 关闭 OSPF 的 Opaque LSA 发布接收能力。
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo opaque-capability
```

1.1.62 ospf

ospf 命令用来启动 OSPF，并进入 OSPF 视图。

undo ospf 命令用来关闭 OSPF。

【命令】

```
ospf [ process-id | router-id { auto-select | router-id } | vpn-instance
vpn-instance-name ] *
undo ospf [ process-id ] [ router-id ]
```

【缺省情况】

系统没有运行 OSPF。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

process-id: OSPF 进程号，取值范围为 1~65535，缺省值为 1。

router-id: 指定 OSPF 进程使用的 Router ID。如果未指定本参数，则使用全局 Router ID。

auto-select: 自动获取 OSPF 进程的 Router ID。

router-id: 手工指定的 Router ID，点分十进制形式，取值范围为 0.0.0.1~255.255.255.255。

vpn-instance vpn-instance-name : 指定 OSPF 进程所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 OSPF 位于公网中。

【使用指导】

必须先启动 OSPF 进程才能配置相关参数。

通过指定不同的进程号，可以在一台路由器上运行多个 OSPF 进程。这种情况下，建议使用命令中的 **router-id** 为不同进程指定不同的 Router ID。

若指定了 **auto-select** 参数，OSPF 进程将根据如下规则自动获取 Router ID：

- OSPF 进程启动时，将选取第一个运行该进程的接口的主 IPv4 地址作为 Router ID；
- 设备重启时，OSPF 进程将会选取第一个运行本进程的接口主 IPv4 地址作为 Router ID；
- OSPF 进程重启时，将从运行了本进程的所有接口的主 IPv4 地址中重新获取 Router ID，具体规则如下：
 - 如果存在配置 IP 地址的 Loopback 接口，则选择 Loopback 接口地址中最大的作为 Router ID。
 - 否则，从其他接口的 IP 地址中选择最大的作为 Router ID(不考虑接口的 up/down 状态)。

对于 **undo ospf** 命令，如果不指定 **router-id** 参数，则表示关闭 OSPF 进程；如果指定了 **router-id** 参数，则表示将已生效的 Router ID 获取方式恢复为使用全局 Router ID，进程重启后生效，进程重启前仍使用已获取的 Router ID。

【举例】

启动 OSPF 进程 100 并配置 Router ID 为 10.10.10.1。

```
<Sysname> system-view
[Sysname] ospf 100 router-id 10.10.10.1
[Sysname-ospf-100]
```

1.1.63 ospf area

ospf area 命令用来在接口上使能 OSPF。

undo ospf area 命令用来在接口上关闭 OSPF。

【命令】

```
ospf process-id area area-id [ exclude-subip ]
undo ospf process-id area [ exclude-subip ]
```

【缺省情况】

接口上未使能 OSPF。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。

area-id: 区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其转换成 IP 地址格式）或者是 IP 地址格式。

exclude-subip: 不包含从 IP 地址。如果未指定本参数，则会包含从 IP 地址。

【使用指导】

接口配置优先，接口使能 OSPF 优于命令 **network** 的配置。

在接口上使能 OSPF 时，如果不存在进程和区域，则创建对应的进程和区域；在接口上关闭 OSPF 时，不删除已经创建的进程和区域。

【举例】

配置接口 GigabitEthernet1/0/2 使能 OSPF 进程 1，接口所在的 OSPF 区域 ID 为 2，不包含从 IP 地址。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/2
```

```
[Sysname-GigabitEthernet1/0/2] ospf 1 area 2 exclude-subip
```

【相关命令】

- **network**

1.1.64 ospf authentication-mode

ospf authentication-mode 命令用来设置接口对 OSPF 报文进行验证的验证模式及验证字。

undo ospf authentication-mode 命令用来删除接口下指定的验证模式。

【命令】

MD5/HMAC-MD5 验证模式：

```
ospf authentication-mode { hmac-md5 | md5 } key-id { cipher | plain } string
```

```
undo ospf authentication-mode { hmac-md5 | md5 } key-id
```

简单验证模式：

```
ospf authentication-mode simple { cipher | plain } string
```

```
undo ospf authentication-mode simple
```

keychain 验证模式：

```
ospf authentication-mode keychain keychain-name
```

```
undo ospf authentication-mode keychain
```

【缺省情况】

接口不对 OSPF 报文进行验证。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

hmac-md5: HMAC-MD5 验证模式。

md5: MD5 验证模式。

simple: 简单验证模式。

key-id: 验证字标识符，取值范围为 1~255。

cipher: 以密文方式设置密钥。

plain: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。简单验证模式下，明文密钥为 1~8 个字符的字符串；密文密钥为 33~41 个字符的字符串。MD5/HMAC-MD5 验证模式下，明文密钥为 1~16 个字符的字符串；密文密钥为 33~53 个字符的字符串。

keychain: 使用 keychain 验证方式。

keychain-name: keychain 名称，为 1~63 个字符的字符串，区分大小写。

【使用指导】

同一网段的接口的验证字口令必须相同，可指定使用 MD5/HMAC-MD5 验证或简单验证两种方式，但不能同时指定；使用 MD5/HMAC-MD5 验证方式时，可配置多条 MD5/HMAC-MD5 验证命令，但 **key-id** 是唯一的，同一 **key-id** 只能配置一个验证字。

修改接口的 OSPF MD5/HMAC-MD5 验证字的步骤如下：

- 首先在该接口配置新的 MD5/HMAC-MD5 验证字；此时若邻居设备尚未配置新的 MD5/HMAC-MD5 验证字，便会触发 MD5/HMAC-MD5 验证平滑迁移过程。在这个过程中，OSPF 会发送分别携带各个 MD5/HMAC-MD5 验证字的多份报文，使得已配置新验证字的邻居设备和尚未配置新验证字的邻居设备都能通过验证，保持邻居关系。
- 然后在各个邻居设备上也都配置相同的新 MD5/HMAC-MD5 验证字；当设备上收到所有邻居的携带新验证字的报文后，便会退出 MD5/HMAC-MD5 验证平滑迁移过程。
- 最后在本设备和所有邻居上都删除旧的 MD5/HMAC-MD5 验证字；建议接口下不要保留多个 MD5/HMAC-MD5 验证字，每次 MD5/HMAC-MD5 验证字修改完毕后，应当及时删除旧的验证字，这样可以防止与持有旧验证字的系统继续通信、减少被攻击的可能，还可以减少验证迁移过程对系统、带宽的消耗。

在使能了 OSPF 的接口下使用 **keychain** 验证方式时，报文的收、发过程如下：

- OSPF 在发送报文前，会先从 **keychain** 获取当前的有效发送 key，根据该 key 的标识符、认证算法和认证密钥进行报文验证，如果当前不存在有效发送 key，或者该 key 的标识符大于 255，OSPF 不会发送报文。
- OSPF 在收到报文后，会根据报文携带的 key 的标识符从本地 **keychain** 中查找具有相同标识符的 key，找到且该 key 为有效 key，则根据该 key 的认证算法和认证密钥对报文进行校验，校验成功后再对报文进行下一步处理。如果报文校验失败，或者根据报文中携带的 key 的标识符无法从 **keychain** 中获取到有效接收 key，则该报文将被丢弃。

对于 **keychain** 认证算法和 key 的标识符的范围，OSPF 的支持情况如下：

- OSPF 仅支持 MD5 和 HMAC-MD5 认证算法。
- OSPF 仅支持 keychain 中 *key-id* 的范围在 0~255 内的 key，如果接收报文的 *key-id* 不在这个范围内，则该报文将被丢弃。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 采用 MD5 明文验证模式,验证字标识符为 15,验证密钥为 123456。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf authentication-mode md5 15 plain 123456
# 配置接口 GigabitEthernet1/0/1 采用简单明文验证模式,验证密钥为 123456。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf authentication-mode simple plain 123456
```

【相关命令】

- **authentication-mode**

1.1.65 ospf bfd enable

ospf bfd enable 命令用来使能 OSPF 的 BFD 功能。

undo ospf bfd enable 命令用来关闭 OSPF 的 BFD 功能。

【命令】

```
ospf bfd enable [ echo ]
undo ospf bfd enable
```

【缺省情况】

OSPF 的 BFD 功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

echo: 通过 BFD echo 报文方式实现 BFD 功能。如果不指定本参数，表示通过 BFD 控制报文方式实现 BFD 功能。

【举例】

```
# 使能接口 GigabitEthernet1/0/1 的 OSPF BFD 功能。
<Sysname> system-view
[Sysname] ospf
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.255.255
[Sysname-ospf-1-area-0.0.0.0] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf bfd enable
```

1.1.66 ospf cost (Interface view)

ospf cost 命令用来配置接口运行 OSPF 协议所需的开销。

undo ospf cost 命令用来恢复缺省情况。

【命令】

ospf cost *cost-value*

undo ospf cost

【缺省情况】

接口按照当前的带宽自动计算接口运行 OSPF 协议所需的开销。对于 Loopback 接口，缺省值为 0。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

cost-value: 接口运行 OSPF 协议所需的开销，Loopback 接口的取值范围为 0~65535，其他接口的取值范围为 1~65535。

【使用指导】

本命令可用来手动设置接口的开销值，否则 OSPF 会按照当前的带宽自动计算接口运行 OSPF 协议所需的开销。

【举例】

指定接口 GigabitEthernet1/0/1 运行 OSPF 协议的开销为 65。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospf cost 65
```

【相关命令】

- **bandwidth-reference**

1.1.67 ospf database-filter

ospf database-filter 命令用来对接口出方向的 LSA 进行过滤。

undo ospf database-filter 命令用来恢复缺省情况。

【命令】

ospf database-filter { **all** | { **ase** [**acl** *ipv4-acl-number*] | **nssa** [**acl** *ipv4-acl-number*] | **summary** [**acl** *ipv4-acl-number*] } * }

undo ospf database-filter

【缺省情况】

不对接口出方向的 LSA 进行过滤。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

all: 对接口出方向的所有 LSA（除了 Grace LSA）进行过滤。

ase: 对接口出方向的 Type-5 LSA 进行过滤。

nssa: 对接口出方向的 Type-7 LSA 进行过滤。

summary: 对接口出方向的 Type-3 LSA 进行过滤。

acl ipv4-acl-number: 指定基本或高级 IPv4 ACL 编号用于过滤，*ipv4-acl-number* 的取值范围为 2000～3999。

【使用指导】

当配置的是高级 ACL（3000～3999）时，其使用规则如下：

- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard** 来过滤携带指定链路状态 ID 的 LSA。
- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard destination dest-addr dest-wildcard** 来过滤携带指定链路状态 ID 和掩码的 LSA。

其中，**source** 用来过滤 LSA 的链路状态 ID，**destination** 用来过滤 LSA 的掩码，配置的掩码应该是连续的（当配置的掩码不连续时该过滤掩码的规则不生效）。

如果在配置该命令前邻居路由器就已经收到了将要进行过滤的 LSA，那么配置该命令后，这些 LSA 仍存在于邻居路由器的 LSDB 中。

【举例】

配置在接口 GigabitEthernet1/0/1 上对出方向的所有 LSA 进行过滤。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospf database-filter all
```

根据编号为 2000、2100 和 2200 的 ACL 分别对接口 GigabitEthernet1/0/2 出方向的 Type-5、Type-7 和 Type-3 LSA 进行过滤。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/2
```

```
[Sysname-GigabitEthernet1/0/2] ospf database-filter ase acl 2000 nssa acl 2100 summary acl 2200
```

【相关命令】

- **database-filter peer** (OSPF view)

1.1.68 ospf dr-priority

ospf dr-priority 命令用来设置接口的 DR 优先级。

undo ospf dr-priority 命令用来恢复缺省情况。

【命令】

```
ospf dr-priority priority
undo ospf dr-priority
```

【缺省情况】

接口的 DR 优先级为 1。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

priority: 接口的 DR 优先级，取值范围为 0~255。

【使用指导】

接口的 DR 优先级决定了该接口在选举 DR/BDR 时所具有资格，数值越大，优先级越高。优先级高的在选举权发生冲突时被首先考虑。如果一台设备的优先级为 0，则它不会被选举为 DR 或 BDR。

【举例】

```
# 设置接口 GigabitEthernet1/0/1 在选举 DR 时的优先级为 8。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf dr-priority 8
```

1.1.69 ospf fast-reroute lfa-backup

ospf fast-reroute lfa-backup 命令用来使能接口参与 LFA（Loop Free Alternate）计算。
undo ospf fast-reroute lfa-backup 命令用来禁止接口参与 LFA 计算。

【命令】

```
ospf fast-reroute lfa-backup
undo ospf fast-reroute lfa-backup
```

【缺省情况】

接口参与 LFA 计算，能够被选为备份接口。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

接口使能 LFA 计算，使其有资格成为备份接口。去使能此配置后，则接口不会被选为备份接口。

【举例】

```
# 禁止接口 GigabitEthernet1/0/1 参与 LFA 计算。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo ospf fast-reroute lfa-backup
```

1.1.70 ospf mib-binding

ospf mib-binding 命令用来配置 OSPF 进程绑定公有 MIB。

undo ospf mib-binding 命令用来恢复缺省情况。

【命令】

```
ospf mib-binding process-id
undo ospf mib-binding
```

【缺省情况】

MIB 绑定在进程号最小的 OSPF 进程上。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。

【使用指导】

该命令用来配置 OSPF 进程绑定 MIB，用户可通过 RFC4750-OSPF.MIB 文件来读取被绑定的 OSPF 进程的相关信息。对于 Uniware 的私有 MIB，不管是否配置此命令，均可读取所有 OSPF 进程的相关信息。

如果指定的 *process-id* 不存在，配置 OSPF 进程绑定命令时将会提示 OSPF 进程不存在，无法完成配置。

如果配置了 OSPF 进程绑定 MIB，若删除 *process-id* 对应的 OSPF 进程，则同时删除 OSPF 进程绑定 MIB 配置，MIB 绑定到进程号最小的 OSPF 进程上。

【举例】

```
# 配置 OSPF 进程 100 绑定 MIB。
<Sysname> system-view
[Sysname] ospf mib-binding 100
```

1.1.71 ospf mtu-enable

ospf mtu-enable 命令用来配置 DD 报文中 MTU 域的值为发送该报文接口的 MTU 值。

undo ospf mtu-enable 命令用来恢复缺省情况。

【命令】

```
ospf mtu-enable
undo ospf mtu-enable
```

【缺省情况】

接口发送的 DD 报文中 MTU 域的值为 0。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

通过 Virtual-Template 或 Tunnel 建立虚连接后，不同厂商的设备接口发送的 DD 报文中 MTU 域的缺省值可能不同，为了保证一致，应该将接口发送的 DD 报文中 MTU 域的值恢复为缺省值 0。

当配置了该命令后，接收到 DD 报文时会检查报文中的 MTU 值是否大于接收接口的 MTU 值，如果大于则将报文丢弃。

【举例】

指定接口 GigabitEthernet1/0/1 在发送 DD 报文时，填写 MTU 值域。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf mtu-enable
```

1.1.72 ospf network-type

ospf network-type 命令用来配置 OSPF 接口的网络类型。

undo ospf network-type 命令用来恢复为缺省情况。

【命令】

```
ospf network-type { broadcast | nbma | p2mp [ unicast ] | p2p
[ peer-address-check ] }
undo ospf network-type
```

【缺省情况】

缺省情况下，OSPF 接口网络类型的缺省值为广播类型。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

broadcast: 配置接口的网络类型为广播类型。

nbma: 配置接口的网络类型为 NBMA 类型。

p2mp: 配置接口的网络类型为点到多点类型。

unicast: P2MP 类型支持单播发送报文，缺省情况下是组播方式发送报文。

p2p: 配置接口的网络类型为点到点类型。

peer-address-check: 配置建立邻接关系必须在同一网段的检查功能，即在接收 Hello 报文时，对端的 IP 地址与当前接口必须在同一网段。

【使用指导】

如果在广播网络上有不支持组播地址的路由器，可以将接口的网络类型改为 NBMA。

在 NBMA 网络中，如果任意两台路由器之间都有一条虚电路直接可达，或者说，这个网络是全连通的，那么可以把 OSPF 接口的网络类型配置为 NBMA；否则，需要把 OSPF 接口的网络类型配置为点到多点，这样，两台不能直接可达的路由器之间可以通过一台与两者都直接可达的路由器来交换路由信息。

接口的网络类型为 NBMA 或 P2MP（unicast）时，必须使用 **peer** 命令来配置邻接点。

如果一网段内只有两台路由器运行 OSPF 协议，也可以将接口的网络类型改为点到点。

接口的网络类型为 P2MP（unicast）时，OSPF 协议在该接口上发送的报文均为单播报文。

【举例】

将接口 GigabitEthernet1/0/1 设置为 NBMA 类型。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospf network-type nbma
```

【相关命令】

- **ospf dr-priority**

1.1.73 ospf prefix-suppression

ospf prefix-suppression 命令用来抑制接口进行前缀发布。

undo ospf prefix-suppression 命令用来恢复缺省情况。

【命令】

ospf prefix-suppression [disable]

undo ospf prefix-suppression

【缺省情况】

不抑制接口进行前缀发布。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

disable: 不抑制接口进行前缀发布。

【使用指导】

如果 OSPF 进程配置了抑制前缀发布，但某个接口不想进行抑制，此时可以配置本命令并指定 **disable** 参数。

接口配置不能抑制从地址对应的前缀。

具体内容请参见命令 **prefix-suppression** 中的使用指导。

【举例】

```
# 抑制接口 GigabitEthernet1/0/2 进行前缀发布。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ospf prefix-suppression
```

【相关命令】

- **prefix-suppression**

1.1.74 ospf primary-path-detect bfd

ospf primary-path-detect bfd 命令用来使能 OSPF 协议中主用链路的 BFD 检测功能。

undo ospf primary-path-detect bfd 命令用来关闭 OSPF 协议中主用链路的 BFD 检测功能。

【命令】

```
ospf primary-path-detect bfd { ctrl | echo }
undo ospf primary-path-detect bfd
```

【缺省情况】

OSPF 协议中主用链路的 BFD 检测功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ctrl: 配置通过工作于控制报文方式的 BFD 会话对主用链路进行检测。

echo: 配置通过工作于 echo 报文方式的 BFD 会话对主用链路进行检测。

【使用指导】

配置本功能后，OSPF 协议的快速重路由特性和 PIC 特性中的主用链路将使用 BFD 进行检测。

【举例】

在接口 GigabitEthernet1/0/1 上配置 OSPF 协议快速重路由特性中主用链路使能 BFD(Ctrl 方式)检测功能。

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] fast-reroute lfa
[Sysname-ospf-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf primary-path-detect bfd ctrl
```

在接口 GigabitEthernet1/0/2 上配置 OSPF 协议 PIC 特性中主用链路使能 BFD (Echo 方式) 检测功能。

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] pic additional-path-always
[Sysname-ospf-1] quit
[Sysname] bfd echo-source-ip 1.1.1.1
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ospf primary-path-detect bfd echo
```

1.1.75 ospf timer dead

ospf timer dead 命令用来设置 OSPF 的邻居失效时间。

undo ospf timer dead 命令用来恢复缺省情况。

【命令】

```
ospf timer dead seconds
undo ospf timer dead
```

【缺省情况】

P2P、Broadcast 类型接口的 OSPF 邻居失效的时间为 40 秒；P2MP、NBMA 类型接口的 OSPF 邻居失效的时间为 120 秒。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

seconds: OSPF 邻居失效的时间，取值范围为 1~2147483647，单位为秒。

【使用指导】

OSPF 邻居的失效时间是指：在该时间间隔内，若未收到邻居的 Hello 报文，就认为该邻居已失效。**dead seconds** 值至少应为 **hello seconds** 值的 4 倍，同一网段上的接口的 **dead seconds** 也必须相同。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 上的邻居失效时间为 60 秒。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf timer dead 60
```

【相关命令】

- **ospf timer hello**

1.1.76 ospf timer hello

ospf timer hello 命令用来配置接口发送 Hello 报文的时间间隔。

undo ospf timer hello 命令用来恢复缺省情况。

【命令】

```
ospf timer hello seconds
undo ospf timer hello
```

【缺省情况】

P2P、Broadcast 类型接口发送 Hello 报文的时间间隔为 10 秒；P2MP、NBMA 类型接口发送 Hello 报文的时间间隔为 30 秒。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

seconds: 接口发送 Hello 报文的时间间隔，取值范围为 1~65535，单位为秒。

【使用指导】

seconds 的值越小，发现网络拓扑改变的速度越快，对系统资源的开销也就越大。同一网段上的接口的 **seconds** 必须相同。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 发送 Hello 报文的时间间隔为 20 秒。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf timer hello 20
```

【相关命令】

- **ospf timer dead**

1.1.77 ospf timer poll

ospf timer poll 命令用来配置在 NBMA 接口上向状态为 down 的邻居路由器发送轮询 Hello 报文的时间间隔。

undo ospf timer poll 命令用来恢复缺省情况。

【命令】

```
ospf timer poll seconds
undo ospf timer poll
```

【缺省情况】

在 NBMA 接口上向状态为 down 的邻居路由器发送轮询 Hello 报文的时间间隔为 120 秒。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

seconds：向状态为 down 的邻居路由器发送轮询 Hello 报文的时间间隔，取值范围为 1～2147483647，单位为秒。

【使用指导】

在 NBMA 的网络上，当邻居失效后，将按轮询时间间隔定期地发送 Hello 报文。用户可配置轮询时间间隔以指定该接口在与相邻路由器构成邻居关系之前发送 Hello 报文的时间间隔。

发送轮询 Hello 报文的时间间隔至少应为发送 Hello 报文时间间隔的 4 倍。

【举例】

配置接口 GigabitEthernet1/0/1 上发送轮询 Hello 报文的时间间隔为 130 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf timer poll 130
```

【相关命令】

- **ospf timer hello**

1.1.78 ospf timer retransmit

ospf timer retransmit 命令用来配置接口重传 LSA 的时间间隔。

undo ospf timer retransmit 命令用来恢复缺省情况。

【命令】

```
ospf timer retransmit seconds
undo ospf timer retransmit
```

【缺省情况】

接口重传 LSA 的时间间隔为 5 秒。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

seconds：接口重传 LSA 的时间间隔，取值范围为 1～3600，单位为秒。

【使用指导】

当一台路由器向它的邻居发送一条 LSA 后，需要等到对方的确认报文。若在该重传 LSA 的时间间隔内未收到对方的确认报文，就会重传这条 LSA。

请合理配置接口重传 LSA 的时间间隔，避免引起不必要的重传。比如，对于低速链路，可以适当把这个时间间隔值设置大一点。

【举例】

指定接口 GigabitEthernet1/0/1 与邻接路由器之间传送 LSA 的重传间隔为 8 秒。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospf timer retransmit 8
```

1.1.79 ospf trans-delay

ospf trans-delay 命令用来配置接口对 LSA 的传输延迟时间。

undo ospf trans-delay 命令用来恢复缺省情况。

【命令】

ospf trans-delay *seconds*

undo ospf trans-delay

【缺省情况】

接口对 LSA 的传输延迟时间为 1 秒。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

seconds：接口对 LSA 的传输延迟时间，取值范围为 1～3600，单位为秒。

【使用指导】

LSA 在本路由器的 LSDB 中会随时间老化（LSA 的老化时间每秒钟加 1），但在网络的传输过程中却不会，所以有必要在发送之前在 LSA 的老化时间上增加一定的延迟时间。此配置对低速率的网络尤其重要。

【举例】

指定接口 GigabitEthernet1/0/1 上传送 LSA 的时延值为 3 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospf trans-delay 3
```

1.1.80 ospf ttl-security

ospf ttl-security 命令用来开启接口的 OSPF GTSM 功能。

undo ospf ttl-security 命令用来关闭接口的 OSPF GTSM 功能。

【命令】

```
ospf ttl-security [ hops hop-count | disable ]
undo ospf ttl-security
```

【缺省情况】

接口的 OSPF GTSM 功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

hops hop-count: 指定接口收到 OSPF 报文并进行安全检测时，允许接收到的报文所经过的路由器的最大跳数。*hop-count* 表示最大跳数，取值范围为 1~254，如果未指定本参数，对于 OSPF 普通邻居，缺省值为 1；对于 OSPF 虚连接邻居和伪连接邻居，缺省值为 255。

disable: 关闭接口的 GTSM 功能。

【使用指导】

开启 OSPF 报文的 GTSM 功能后，只会对来自 OSPF 普通邻居和虚连接邻居的报文进行安全检测，不会对来自 OSPF 伪连接邻居的报文进行安全检测。当设备在接口上收到 OSPF 报文时，会判断报文的 TTL 是否在 255-“*hop-count*”+1 到 255 之间。如果在，就上送报文；否则直接丢弃报文。从而使设备能够避免受到 CPU 利用（CPU-utilization）类型的攻击（如 CPU 过载），增强系统的安全性。

执行本命令后，设备会将发送报文的初始 TTL 设置为 255，这就要求本地设备和邻居设备上同时配置本特性，指定的 *hop-count* 值可以不同，只要能够通过安全检测即可。

在接口视图下配置的 **hops** 参数比在 OSPF 区域视图下配置的 **hops** 参数的优先级高。

OSPF 区域视图下未开启 GTSM 时, **undo ospf ttl-security** 命令用来关闭接口的 GTSM 功能。OSPF 区域视图下已开启 GTSM 时, **undo ospf ttl-security** 命令用来取消接口下的 GTSM 配置, 并使区域下的 GTSM 配置在接口上生效; **ospf ttl-security disable** 命令用来关闭接口的 GTSM 功能。

如果区域中配置了虚连接, 建议用户只在区域视图下开启 GTSM 功能, 当且仅当用户已经明确知道哪些接口是用来发送和接收虚连接的 OSPF 报文时, 可以在所有这些接口下开启 OSPF 的 GTSM 功能, 否则可能会导致虚连接两端的路由器丢弃接收到的 OSPF 报文。

【举例】

开启接口 GigabitEthernet1/0/1 的 GTSM 功能, 并指定最大跳数为 254。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospf ttl-security hops 254
```

在区域视图下开启 OSPF 报文的 GTSM 功能, 再在接口 GigabitEthernet1/0/1 下关闭 OSPF 报文的 GTSM 功能。

```
<Sysname> system-view
```

```
[Sysname] ospf 100
```

```
[Sysname-ospf-100] area 1
```

```
[Sysname-ospf-100-area-0.0.0.1] ttl-security
```

```
[Sysname-ospf-100-area-0.0.0.1] quit
```

```
[Sysname-ospf-100] quit
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospf ttl-security disable
```

【相关命令】

- **ttl-security** (OSPF area view)

1.1.81 peer (OSPF view)

peer 命令用来配置 NBMA 网络或 P2MP 单播网络的邻居。

undo peer 命令用来删除指定的 NBMA 网络或 P2MP 单播网络的邻居。

【命令】

```
peer ip-address [ cost cost-value | dr-priority priority ]
```

```
undo peer ip-address
```

【缺省情况】

未配置邻居。

【视图】

OSPF 视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: 邻居的 IP 地址。

cost cost-value: 邻居的开销值，取值范围为 1~65535。

dr-priority priority: 邻居的优先级，取值范围为 0~255，缺省值为 1。

【使用指导】

NBMA 网络或 P2MP 单播网络采用单播形式发送协议报文，必须手工指定邻居。

本命令设置的开销值仅用于 P2MP 链路上建立的邻居，如果没有配置开销值，去往该邻居的花费等于接口的开销值。

本命令设置的优先级仅用于表示路由器是否主动向该邻居发送 Hello 报文，并不用于实际的 DR 选举，**ospf dr-priority** 命令设置的优先级用于实际的 DR 选举。

【举例】

```
# 指定邻居的 IP 地址为 1.1.1.1。  
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] peer 1.1.1.1
```

【相关命令】

- **ospf dr-priority**

1.1.82 pic (OSPF view)

pic 命令用来使能前缀无关收敛功能。

undo pic 命令用来关闭前缀无关收敛功能。

【命令】

```
pic [ additional-path-always ]  
undo pic
```

【缺省情况】

前缀无关收敛功能处于使能状态。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

additional-path-always: 支持非直连的次优路由作为备份。

【使用指导】

PIC (Prefix Independent Convergence, 前缀无关收敛)，即收敛时间与前缀数量无关，加快收敛速度。传统的路由计算快速收敛都与前缀数量相关，收敛时间与前缀数量成正比。OSPF 只实现区域间路由以及外部路由的前缀无关收敛。

OSPF 快速重路由功能和 PIC 同时配置时，OSPF 快速重路由功能生效。

【举例】

使能 OSPF 协议的 PIC 支持非直连次优路由做备份功能。

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] pic additional-path-always
```

1.1.83 preference (OSPF view)

preference 命令用来配置 OSPF 协议的路由优先级。

undo preference 命令用来取消 OSPF 协议的路由优先级的配置。

【命令】

```
preference [ ase ] { preference | route-policy route-policy-name } *
undo preference [ ase ]
```

【缺省情况】

对于自治系统内部路由，OSPF 协议的路由优先级为 10；对于自治系统外部路由，OSPF 协议的路由优先级为 150。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

ase: 配置 OSPF 协议对自治系统外部路由的优先级。如果未指定该参数，则配置的是 OSPF 协议对自治系统内部路由的优先级。

preference: OSPF 协议的路由优先级，取值范围为 1~255。优先级的值越小，其实际的优先程度越高。

route-policy *route-policy-name*: 应用路由策略，对特定的路由设置优先级。
route-policy-name 是路由策略名称，为 1~63 个字符的字符串，区分大小写。

【使用指导】

由于路由器上可能同时运行多个动态路由协议，就存在各个路由协议之间路由信息共享和选择的问题，所以为每一种路由协议指定了一个缺省的优先级。在不同的路由协议发现去往同一目的地的多条路由时，优先级高的协议发现的路由将被选中以转发 IP 报文。

配置了 **route-policy** 参数后，如果 **route-policy** 中对某些匹配的路由优先级进行了修改，则这些匹配的路由取 **route-policy** 修改的优先级，其它路由的优先级均取 **preference** 命令所设的值。

【举例】

配置 OSPF 协议对自治系统外部路由的优先级为 200。

```
<Sysname> system-view
```

```

[Sysname] ospf 100
[Sysname-ospf-100] preference ase 200
# 配置 OSPF 协议对自治系统内部路由的优先级，匹配路由策略 pre 的路由优先级为 100，未匹配
的路由优先级为 150。
<Sysname> system-view
[Sysname] ip prefix-list test index 10 permit 100.1.1.0 24
[Sysname] route-policy pre permit node 10
[Sysname-route-policy-pre-10] if-match ip address prefix-list test
[Sysname-route-policy-pre-10] apply preference 100
[Sysname-route-policy-pre-10] quit
[Sysname] ospf 100
[Sysname-ospf-100] preference route-policy pre 150

```

1.1.84 prefix-priority (OSPF view)

prefix-priority 命令用来使能 OSPF 的前缀按优先权快速收敛功能。

undo prefix-priority 命令用来关闭 OSPF 的前缀按优先权快速收敛功能。

【命令】

```

prefix-priority route-policy route-policy-name
undo prefix-priority

```

【缺省情况】

OSPF 的前缀按优先权快速收敛功能处于关闭状态。

【视图】

OSPF 视图

【缺省用户角色】

```

network-admin
context-admin

```

【参数】

route-policy *route-policy-name*: 应用路由策略，对特定的路由前缀设置优先权。
route-policy-name 是路由策略名称，为 1~63 个字符的字符串，区分大小写。

【使用指导】

通过策略指定优先权，不同前缀按优先权顺序下发，由高到低分为 4 个优先权（Critical、High、Medium 和 Low），如果一条路由符合多个收敛优先权的匹配规则，则这些收敛优先权中最高者当选为路由的收敛优先权。

OSPF 路由的 32 位主机路由为 Medium 优先权，其它为 Low 优先权。

【举例】

```

# 配置通过路由策略 pre 修改特定路由前缀的优先权为 Medium。
<Sysname> system-view
[Sysname] ip prefix-list test index 10 permit 100.1.1.0 24
[Sysname] route-policy pre permit node 10
[Sysname-route-policy-pre-10] if-match ip address prefix-list test

```

```
[Sysname-route-policy-pre-10] apply prefix-priority medium
[Sysname-route-policy-pre-10] quit
[Sysname] ospf 100
[Sysname-ospf-100] prefix-priority route-policy pre
```

1.1.85 prefix-suppression

prefix-suppression 命令用来抑制 OSPF 进程进行前缀发布。

undo prefix-suppression 命令用来恢复缺省情况。

【命令】

```
prefix-suppression
undo prefix-suppression
```

【缺省情况】

不抑制 OSPF 进程进行前缀发布。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

OSPF 使能网段时会将接口上匹配该网段的所有网段路由与主机路由都通过 LSA 发布,但有时候主机路由或网段路由是不希望被发布的。通过前缀抑制配置,可以减少 LSA 中携带不必要的前缀,即不发布某些网段路由和主机路由,从而提高网络安全性,加快路由收敛。

如果需要抑制前缀发布,建议整个 OSPF 网络都配置本命令。

全局配置不能抑制从地址、LoopBack 接口以及处于抑制状态的接口对应的前缀。如果想对 LoopBack 接口或处于抑制状态的接口进行抑制,可以通过配置接口前缀抑制 (**ospf prefix-suppression** 命令) 来实现。

当使能前缀抑制时,具体情况如下:

- P2P 或 P2MP 类型网络: Type-1 LSA 中不发布接口的主地址,即 Type-1 LSA 中链路类型为 3 的 Stub 链路被抑制,不生成接口路由,但其他路由信息可以正常计算,不会影响流量转发。
- 广播类型或者 NBMA 网络: DR 发布的 Type-2 LSA 的掩码字段会填成 32 位,即不生成网段路由,但其他路由信息可以正常计算,不会影响流量转发。另外,如果没有邻居,发布的 Type-1 LSA 中也不发布接口的主地址,即 Type-1 LSA 中链路类型为 3 的 Stub 链路被抑制。

【举例】

抑制 OSPF 进程 1 的前缀发布。

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] prefix-suppression
```

【相关命令】

- **ospf prefix-suppression**

1.1.86 reset ospf event-log

reset ospf event-log 命令用于清除 OSPF 的日志信息。

【命令】

```
reset ospf [ process-id ] event-log [ lsa-flush | peer [ slot slot-number |  
spf ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果未指定本参数，则清除所有 OSPF 进程的日志信息。

lsa-flush: LSA 老化日志信息个数。

peer: 清除邻居状态变化的日志信息。

slot slot-number: 清除指定成员设备上 OSPF 邻居状态变化的日志信息，**slot-number** 表示设备在 IRF 中的成员编号。如果未指定本参数，将清除主进程所在成员设备上 OSPF 邻居状态变化的日志信息。

spf: 清除路由计算的日志信息。

【使用指导】

如果未指定日志类型，则所有日志信息都被清除。

【举例】

清除所有 OSPF 进程路由计算的日志信息。

```
<Sysname> reset ospf event-log spf
```

【相关命令】

- **display ospf event-log**

1.1.87 reset ospf event-log hello

reset ospf event-log hello 命令用于清除 OSPF 接收或发送 Hello 报文的日志信息。

【命令】

```
reset ospf [ process-id ] event-log hello { received [ abnormal | dropped ] |  
sent [ abnormal | failed ] } [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: 清除指定 OSPF 进程接收或发送 Hello 报文的日志信息, *process-id* 表示 OSPF 进程号, 取值范围为 1~65535。如果未指定本参数, 则清除所有 OSPF 进程的日志信息。

received: 清除接收 Hello 报文的日志信息。

sent: 清除发送 Hello 报文的日志信息。

abnormal: 清除发送或者接收异常 Hello 报文的日志信息。异常 Hello 报文指的是发送或接收到的 Hello 报文的时间间隔大于或等于 1.5 倍 Hello 定时器的报文。

dropped: 清除丢弃接收到的 Hello 报文的日志信息个数。

failed: 清除发送失败的 Hello 报文的日志信息。

slot slot-number: 清除指定成员设备接收或发送 Hello 报文的日志信息, *slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数, 将清除主进程所在成员设备接收或发送 Hello 报文的日志信息。

【举例】

清除所有 OSPF 进程发送 Hello 报文的日志信息。

```
<Sysname> reset ospf event-log hello sent
```

【相关命令】

- **display ospf event-log hello**

1.1.88 reset ospf process

reset ospf process 命令用来重启 OSPF 进程。

【命令】

```
reset ospf [ process-id ] process [ graceful-restart ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: OSPF 进程号, 取值范围为 1~65535。如果不指定该参数, 则重启所有的 OSPF 进程。

graceful-restart: 以 GR 方式重启 OSPF 进程。

【使用指导】

使用 **reset ospf process** 命令重启 OSPF, 可以获得如下结果:

- 可以立即清除无效的 LSA, 而不必等到 LSA 超时。
- 如果改变了 Router ID, 该命令的执行会导致新的 Router ID 生效。
- 方便重新选举 DR、BDR。

- 重启前的 OSPF 配置不会丢失。

执行该命令后，系统提示用户确认是否重启 OSPF 协议。

【举例】

重启所有 OSPF 进程。

```
<Sysname> reset ospf process
```

```
Reset OSPF process? [Y/N]:y
```

1.1.89 reset ospf redistribution

reset ospf redistribution 命令用来重新向 OSPF 引入外部路由。

【命令】

reset ospf [*process-id*] redistribution

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: OSPF 进程号，取值范围为 1~65535。如果不指定本参数，则所有 OSPF 进程都将重新引入外部路由。

【举例】

重新向 OSPF 引入外部路由。

```
<Sysname> reset ospf redistribution
```

1.1.90 reset ospf statistics

reset ospf statistics 命令用来清除 OSPF 的统计信息。

【命令】

reset ospf [*process-id*] statistics

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: OSPF 进程号，取值范围为 1~65535，清除指定 OSPF 进程的统计信息。

【举例】

清除所有 OSPF 进程的统计信息。

```
<Sysname> reset ospf statistics
```

【相关命令】

- **display ospf statistics**

1.1.91 rfc1583 compatible

rfc1583 compatible 命令用来开启兼容 RFC 1583 的路由选择优先规则的功能。

undo rfc1583 compatible 命令用来关闭兼容 RFC 1583 的路由选择优先规则的功能。

【命令】

```
rfc1583 compatible
undo rfc1583 compatible
```

【缺省情况】

兼容 RFC 1583 的路由选择优先规则的功能处于开启状态。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

当有多条路径可以到达同一个外部路由时，在选择最优路由的问题上，RFC 2328 中定义的选路规则与 RFC 1583 的有所不同，进行此配置可以兼容 RFC 1583 中定义的规则。

具体的选路规则如下：

- (1) 当 RFC 2328 兼容 RFC 1583 时，所有到达 ASBR 的路由优先级相同。当 RFC 2328 不兼容 RFC 1583 时，非骨干区的区域内路由优先级最高，区域间路由与骨干区区域内路由优先级相同，优选非骨干区的区域内路由，尽量减少骨干区的负担；
- (2) 若存在多条优先级相同的路由时，按开销值优选，优选开销值小的路由；
- (3) 若存在多条开销值相同路由时，按路由来源区域的区域 ID 选择，优选区域 ID 大的路由。

为了避免路由环路，同一路由域内的路由器建议统一配置相同规则。

【举例】

关闭兼容 RFC 1583 的路由选择规则的功能。

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo rfc1583 compatible
```

1.1.92 router id

router id 命令用来配置全局 Router ID。

undo router id 命令用来恢复缺省情况。

【命令】

```
router id router-id  
undo router id
```

【缺省情况】

未配置全局 Router ID。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

router-id: IPv4 地址形式的 Router ID。

【使用指导】

一些动态路由协议要求使用 Router ID，如果在启动这些路由协议时没有指定 Router ID，则缺省使用全局路由器 ID。

如果配置了全局路由器 ID，则使用配置的值作为 Router ID。如果没有配置全局路由器 ID，则按照下面的规则进行选择：

- (1) 如果存在配置 IP 地址的 Loopback 接口，则选择 Loopback 接口地址中最大的作为 Router ID。
- (2) 如果没有配置 IP 地址的 Loopback 接口，则从其他接口的 IP 地址中选择最大的作为 Router ID（不考虑接口的 up/down 状态）。

存在主备的情况下，系统将备份命令行配置的 Router ID 或从接口地址中选择出来的 Router ID。主备倒换后，系统将检查从地址中选出的 Router ID 的有效性，如果无效将重新进行选择。

当且仅当被选为 Router ID 的接口 IP 地址被删除或被修改时，才触发重新选择过程，其他情况不触发重新选择的过程。例如，以下情况不会触发 Router ID 重新选择的过程：

- 接口 down。
- 已经选取了一个非 Loopback 接口地址后又配置了一个 Loopback 接口地址。
- 配置一个更大的接口地址。

Router ID 改变之后，各协议需要通过手工执行 **reset** 命令才会获取新的 Router ID。

【举例】

```
# 配置全局 Router ID 为 1.1.1.1。  
<Sysname> system-view  
[Sysname] router id 1.1.1.1
```

1.1.93 silent-interface (OSPF view)

silent-interface 命令用来禁止接口收发 OSPF 报文。

undo silent-interface 命令用来取消禁止接口收发 OSPF 报文的配置。

【命令】

```
silent-interface { interface-type interface-number | all }  
undo silent-interface { interface-type interface-number | all }
```

【缺省情况】

允许接口收发 OSPF 报文。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface-type interface-number: 接口类型和接口号，禁止指定 OSPF 接口收发 OSPF 报文。

all: 禁止所有 OSPF 接口收发 OSPF 报文。

【使用指导】

如果要使 OSPF 路由信息不被某一网络中的路由器获得，可使用本命令禁止在此接口上收发 OSPF 报文。

【举例】

```
# 禁止接口 GigabitEthernet1/0/1 收发 OSPF 报文。  
<Sysname> system-view  
[Sysname] ospf 100  
[Sysname-ospf-100] silent-interface gigabitethernet 1/0/1
```

1.1.94 snmp trap rate-limit

snmp trap rate-limit 命令用来配置 OSPF 在指定时间间隔内允许输出的告警信息条数。

undo snmp trap rate-limit 命令用来恢复缺省情况。

【命令】

```
snmp trap rate-limit interval trap-interval count trap-number  
undo snmp trap rate-limit
```

【缺省情况】

OSPF 在 10 秒内允许输出 7 条告警信息。

【视图】

OSPF 视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval trap-interval: 指定允许输出告警信息的时间间隔, 取值范围为 2~60, 单位为秒。
count trap-number: 在指定时间间隔内允许输出的告警信息条数, 取值范围为 0~300, 为 0 时表示不输出告警信息。

【举例】

配置 OSPF 在 5 秒内允许输出 10 条告警信息。

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] snmp trap rate-limit interval 5 count 10
```

1.1.95 snmp-agent trap enable ospf

snmp-agent trap enable ospf 命令用来开启 OSPF 的告警功能。

undo snmp-agent trap enable ospf 命令用来关闭 OSPF 的告警功能。

【命令】

```
snmp-agent trap enable ospf [ authentication-failure | bad-packet |
config-error | grhelper-status-change | grrestarter-status-change |
if-state-change | lsa-maxage | lsa-originate | lsdb-approaching-overflow |
lsdb-overflow | neighbor-state-change | nssatranslator-status-change |
retransmit | virt-authentication-failure | virt-bad-packet |
virt-config-error | virt-retransmit | virtgrhelper-status-change |
virtif-state-change | virtneighbor-state-change ] *
undo snmp-agent trap enable ospf [ authentication-failure | bad-packet |
config-error | grhelper-status-change | grrestarter-status-change |
if-state-change | lsa-maxage | lsa-originate | lsdb-approaching-overflow |
lsdb-overflow | neighbor-state-change | nssatranslator-status-change |
retransmit | virt-authentication-failure | virt-bad-packet |
virt-config-error | virt-retransmit | virtgrhelper-status-change |
virtif-state-change | virtneighbor-state-change ] *
```

【缺省情况】

OSPF 的告警功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

authentication-failure: 接口认证失败。

bad-packet: 接收了错误报文。

config-error: 接口配置错误。

grhelper-status-change: 邻居 GR Helper 状态变化。
grrestarter-status-change: GR Restarter 状态变化。
if-state-change: 接口状态变化。
lsa-maxage: LSA 的 max age。
lsa-originate: 本地生成 LSA。
lsdb-approaching-overflow: LSDB 接近溢出。
lsdb-overflow: LSDB 溢出。
neighbor-state-change: 邻居状态变化。
nssatranslator-status-change: NSSA 转换路由器状态变化。
retransmit: 接口接收和转发报文。
virt-authentication-failure: 虚接口认证失败。
virt-bad-packet: 虚接口接收错误报文。
virt-config-error: 虚接口配置错误。
virt-retransmit: 虚接口接收和转发报文。
virtgrhelper-status-change: 虚接口邻居 GR Helper 状态变化。
virtif-state-change: 虚接口状态变化。
virtneighbor-state-change: 虚接口邻居状态变化。

【举例】

```
# 关闭 OSPF 的告警功能。
<Sysname> system-view
[Sysname] undo snmp-agent trap enable ospf
```

1.1.96 spf-schedule-interval (OSPF view)

spf-schedule-interval 命令用来配置 OSPF 路由计算的时间间隔。
undo spf-schedule-interval 命令用来恢复缺省情况。

【命令】

```
spf-schedule-interval { maximum-interval [ minimum-interval
[ incremental-interval ] ] | millisecond interval }
undo spf-schedule-interval
```

【缺省情况】

OSPF 路由计算的最大时间间隔为 5 秒，最小时间间隔为 50 毫秒，时间间隔惩罚增量为 200 毫秒。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

maximum-interval: OSPF 路由计算的最大时间间隔, 取值范围为 1~60, 单位为秒。

minimum-interval: OSPF 路由计算的最小时间间隔, 取值范围为 10~60000, 单位为毫秒。

incremental-interval: OSPF 路由计算的时间间隔惩罚增量, 取值范围为 10~60000, 单位为毫秒。

millisecond interval: OSPF 路由计算采用固定的时间间隔, 取值范围为 0~10000, 单位为毫秒。

【使用指导】

根据本地维护的 LSDB, 运行 OSPF 协议的路由器通过 SPF 算法计算出以自己为根的最短路径树, 并根据这一最短路径树决定到目的网络的下一跳。通过调节 SPF 的计算间隔, 可以抑制网络频繁变化可能导致的占用过多带宽资源和路由器资源。

执行 **spf-schedule-interval maximum-interval [minimum-interval [incremental-interval]]** 命令后, 在网络变化不频繁的情况下将连续路由计算的时间间隔缩小到 **minimum-interval**, 而在网络变化频繁的情况下可以进行相应惩罚, 将等待时间按照配置的惩罚增量延长, 最大不超过 **maximum-interval**。

minimum-interval 和 **incremental-interval** 配置值不允许大于 **maximum-interval** 配置值。

在某些特定的组网环境下 (例如对路由收敛速度要求较高的环境), 可以使用 **spf-schedule-interval millisecond interval** 命令来加快路由计算的频率, 从而加速路由收敛。

【举例】

设置 OSPF 路由计算最大时间间隔为 10 秒, 最小时间间隔为 500 毫秒, 惩罚增量为 300 毫秒。

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] spf-schedule-interval 10 500 300
```

1.1.97 stub (OSPF area view)

stub 命令用来配置一个区域为 Stub 区域。

undo stub 命令用来恢复缺省情况。

【命令】

```
stub [ default-route-advertise-always | no-summary ] *
undo stub
```

【缺省情况】

没有区域被设置为 Stub 区域。

【视图】

OSPF 区域视图

【缺省用户角色】

network-admin

context-admin

【参数】

default-route-advertise-always: 该参数只用于 Stub 区域的 ABR，配置后，ABR 向 Stub 区域内发布缺省路由的 Type-3 LSA 时不检查骨干区域是否存在 FULL 状态的邻居。如果未指定本参数，ABR 向 Stub 区域内发布缺省路由的 Type-3 LSA 时需要检查骨干区域是否存在 FULL 状态的邻居，如果不存在 FULL 状态的邻居，则 ABR 不会向 Stub 区域内发布缺省路由的 Type-3 LSA。

no-summary: 该参数只用于 Stub 区域的 ABR，配置后，ABR 只向 Stub 区域内发布一条缺省路由的 Type-3 LSA，不生成任何其它 Type-3 LSA（这种区域又称为 Totally Stub 区域）。

【使用指导】

如果要将一个区域配置成 Stub 区域，则该区域中的所有路由器都必须配置此属性。

多次执行本命令，最后一次执行的命令生效。

【举例】

```
# 将 OSPF 区域 1 设置为 Stub 区域。
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
```

【相关命令】

- **default-cost** (OSPF area view)

1.1.98 stub-router (OSPF view)

stub-router 命令用来配置当前路由器为 Stub 路由器。

undo stub-router 命令用来恢复缺省情况。

【命令】

```
stub-router [ external-lsa [ max-metric-value ] | include-stub | on-startup
| summary-lsa [ max-metric-value ] ] *
undo stub-router
```

【缺省情况】

当前路由器没有被配置为 Stub 路由器。

【视图】

OSPF 视图

【缺省用户角色】

network-admin

context-admin

【参数】

external-lsa max-metric-value: 路由器发布的外部 LSA 链路度量值。*max-metric-value* 表示链路度量值，取值范围为 1~16777215，缺省值为 16711680。

include-stub: 路由器发布的 Router-LSA 中, 链路类型为 3 的 Stub 链路度量值将设置为最大值 65535。

on-startup seconds: 在路由器重启期间, 路由器作为 Stub 路由器。*seconds* 表示超时时间, 取值范围为 5~86400, 单位为秒。

summary-lsa max-metric-value: 路由器发布的 3 类 LSA 链路度量值。*max-metric-value* 表示链路度量值, 取值范围为 1~16777215, 缺省值为 16711680。

【使用指导】

通过将当前路由器配置为 Stub 路由器, 在该路由器发布的 Router-LSA 中, 当链路类型取值为 3 表示连接到 Stub 网络时, 链路度量值不变; 当链路类型为 1、2、4 分别表示通过 P2P 链路、与另一路由器相连、连接到传送网络、虚连接时, 链路度量值将设置为最大值 65535。这样其邻居计算出这条路由的开销就会很大, 如果邻居上有到这个目的地址开销更小的路由, 则数据不会通过这个 Stub 路由器转发。

【举例】

配置当前路由器为 Stub 路由器。

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] stub-router
```

1.1.99 transmit-pacing

transmit-pacing 命令用来配置接口发送 LSU 报文的时间间隔和一次发送 LSU 报文的最大个数。

undo transmit-pacing 命令用来恢复缺省情况。

【命令】

```
transmit-pacing interval interval count count
undo transmit-pacing
```

【缺省情况】

接口发送 LSU 报文的时间间隔为 20 毫秒, 一次最多发送 3 个 LSU 报文。

【视图】

OSPF 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interval *interval*: 接口发送 LSU 报文的时间间隔, *interval* 的取值范围为 10~1000, 单位为毫秒。当路由器上使能 OSPF 功能的接口数比较多时, 建议增大该值, 以控制路由器每秒钟发送 LSU 报文的总数。当 OSPF LSDB 规模较大或者路由更新比较频繁时, 建议不要将 *interval* 配置为 0, 否则可能会影响网络稳定性。

count *count*: 接口一次发送 LSU 报文的最大个数, *count* 的取值范围为 1~200。当路由器上使能 OSPF 功能的接口数比较多时, 建议减小该值, 以控制路由器每秒钟发送 LSU 报文的总数。

【举例】

配置 OSPF 进程 1 的所有接口发送 LSU 报文的时间间隔为 30 毫秒，一次最多发送 10 个 LSU 报文。

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] transmit-pacing interval 30 count 10
```

1.1.100 ttl-security

ttl-security 命令用来开启区域的 OSPF GTSM 功能。

undo ttl-security 命令用来关闭区域的 OSPF GTSM 功能。

【命令】

```
ttl-security [ hops hop-count ]
undo ttl-security
```

【缺省情况】

区域的 OSPF GTSM 功能处于关闭状态。

【视图】

OSPF 区域视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

hops hop-count: 指定接口收到 OSPF 报文并进行安全检测时，允许接收的报文所经过的路由器的最大跳数。*hop-count* 表示最大跳数，取值范围为 1~254，如果未指定本参数，对于 OSPF 普通邻居，缺省值为 1；对于 OSPF 虚连接邻居和伪连接邻居，缺省值为 255。

【使用指导】

在 OSPF 区域视图下开启 GTSM 功能后，该区域中所有使能 OSPF 的接口都会生效，并且只会对来自 OSPF 普通邻居和虚连接邻居的报文进行安全检测，不会对来自 OSPF 伪连接邻居的报文进行安全检测。当设备从某个接口上收到一个 OSPF 报文时，会判断报文的 TTL 是否在 255-“*hop-count*”+1 到 255 之间。如果在，就上送报文；否则直接丢弃报文。从而使设备能够避免受到 CPU 利用（CPU-utilization）类型的攻击（如 CPU 过载），增强系统的安全性。

执行本命令后，设备会将发送报文的初始 TTL 设置为 255，这就要求本地设备和邻居设备上同时配置本特性，指定的 *hop-count* 值可以不同，只要能够通过安全检测即可。

在接口视图下配置的 **hops** 参数的优先级高于在 OSPF 区域视图下配置的 **hops** 参数。

如果区域中配置了虚连接，建议用户指定 **hops** 参数，配置时需要考虑虚连接发送的 OSPF 报文所经过的路由器的最大跳数。同时建议用户只在区域视图下开启 GTSM 功能，当且仅当用户已经明确知道了哪些接口是用来发送和接收虚连接的 OSPF 报文时，可以在所有这些接口下开启 OSPF 的 GTSM 功能，否则可能会导致虚连接两端的路由器丢弃接收到的 OSPF 报文。

【举例】

```
# 配置在 OSPF 区域视图下开启 GTSM 功能。
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] ttl-security
```

【相关命令】

- **ospf ttl-security**

1.1.101 vlink-peer (OSPF area view)

vlink-peer 命令用来创建并配置一条虚连接。

undo vlink-peer 命令用来删除一条已有的虚连接。

【命令】

```
vlink-peer router-id [ dead seconds | hello seconds | { { hmac-md5 | md5 }  
key-id { cipher | plain } string | keychain keychain-name | simple { cipher |  
plain } string } | retransmit seconds | trans-delay seconds ] *  
undo vlink-peer router-id [ dead | hello | { hmac-md5 | md5 } key-id |  
retransmit | simple | trans-delay ] *
```

【缺省情况】

不存在虚链接。

【视图】

OSPF 区域视图

【缺省用户角色】

network-admin
context-admin

【参数】

router-id: 虚连接邻居的路由器 ID。

dead seconds: 失效时间间隔，取值范围为 1~32768，单位为秒，缺省值为 40。该值必须和与其建立虚连接路由器的 **dead seconds** 值相等，并至少为 **hello seconds** 值的 4 倍。

hello seconds: 接口发送 Hello 报文的时间间隔，取值范围为 1~8192，单位为秒，缺省值为 10。该值必须和与其建立虚连接路由器上的 **hello seconds** 值相等。

hmac-md5: HMAC-MD5 验证模式。

md5: MD5 验证模式。

simple: 简单验证模式。

key-id: MD5/HMAC-MD5 验证字标识符，取值范围为 1~255。

cipher: 以密文方式设置密钥。

plain: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。简单验证模式下，明文密钥为 1~8 个字符的字符串；密文密钥为 33~41 个字符的字符串。MD5/HMAC-MD5 验证模式下，明文密钥为 1~16 个字符的字符串；密文密钥为 33~53 个字符的字符串。

keychain: 使用 keychain 验证方式。

keychain-name: keychain 名称，为 1~63 个字符的字符串，区分大小写。

retransmit seconds: 接口重传 LSA 报文的时间间隔，取值范围为 1~3600，单位为秒，缺省值为 5。

trans-delay seconds: 接口延迟发送 LSA 报文的时间间隔，取值范围为 1~3600，单位为秒，缺省值为 1。

【使用指导】

根据 RFC 2328 的规定，OSPF 的所有非骨干区域必须是和骨干区域保持连通的，可以使用 **vlink-peer** 命令建立逻辑上的连通性。

各参数取值规则如下：

- **hello** 值越小，发现网络变化的速度越快，消耗的网络资源也就越多。
- 不能将 **retransmit** 值设置的太小，否则将会引起不必要的重传。网络速度相对较慢的时候应把该值设的更大一些。
- 设置 **trans-delay** 值时必须考虑接口的发送延迟。

虚连接可指定使用 MD5/HMAC-MD5 验证或简单验证两种方式，但不能同时指定；使用 MD5/HMAC-MD5 验证方式时，可配置多条 MD5/HMAC-MD5 验证命令，但 **key-id** 是唯一的，同一 **key-id** 只能配置一个验证字。

修改虚连接的 OSPF MD5/HMAC-MD5 验证字的步骤如下：

- 首先为该虚连接配置新的 MD5/HMAC-MD5 验证字；此时若邻居设备尚未配置新的 MD5/HMAC-MD5 验证字，便会触发 MD5/HMAC-MD5 验证平滑迁移过程。在这个过程中，OSPF 会发送分别携带各个 MD5/HMAC-MD5 验证字的多份报文，使得无论邻居设备上是否配置了新验证字都能验证通过，保持邻居关系。
- 然后在邻居设备上也都配置相同的新 MD5/HMAC-MD5 验证字；当本设备上收到邻居的携带新验证字的报文后，便会退出 MD5/HMAC-MD5 验证平滑迁移过程。
- 最后在本设备和邻居上都删除旧的 MD5/HMAC-MD5 验证字；建议不要为虚连接保留多个 MD5/HMAC-MD5 验证字，每次 MD5/HMAC-MD5 验证字修改完毕后，应当及时删除旧的验证字，这样可以防止与持有旧验证字的系统继续通信、减少被攻击的可能，还可以减少验证迁移过程对系统、带宽的消耗。

在 OSPF 虚连接使用 keychain 验证方式时，报文的收、发过程如下：

- OSPF 虚连接在发送报文前，会先从 keychain 获取当前的有效发送 key，然后发送报文。如果当前不存在有效发送 key，OSPF 虚连接不会发送报文。
- OSPF 虚连接在收到报文后，会根据报文携带的 key 的标识符从 keychain 中获取有效接收 key，根据该 key 的认证算法和认证密钥对报文进行校验，校验成功后再对报文进行下一步处理。如果报文校验失败，或者根据报文中携带的 key 的标识符无法从 keychain 中获取到有效接收 key，则该报文将被丢弃。

对于 keychain 认证算法和 key 的标识符的范围，OSPF 的支持情况如下：

- OSPF 仅支持 MD5 和 HMAC-MD5 认证算法。

- OSPF 仅支持标识符取值范围为 0~255 的 key。

【举例】

配置虚连接，对端路由器 Router ID 为 1.1.1.1。

```
<Sysname> system-view
```

```
[Sysname] ospf 100
```

```
[Sysname-ospf-100] area 2
```

```
[Sysname-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

【相关命令】

- **authentication-mode**
- **display ospf vlink**

目 录

1 策略路由.....	1-1
1.1 策略路由配置命令.....	1-1
1.1.1 apply access-vpn.....	1-1
1.1.2 apply continue.....	1-2
1.1.3 apply default-next-hop	1-2
1.1.4 apply default-output-interface	1-3
1.1.5 apply ip-df	1-4
1.1.6 apply loadshare	1-5
1.1.7 apply next-hop	1-7
1.1.8 apply output-interface	1-8
1.1.9 apply precedence	1-9
1.1.10 apply remark-vpn	1-9
1.1.11 display ip policy-based-route	1-10
1.1.12 display ip policy-based-route interface	1-11
1.1.13 display ip policy-based-route local	1-13
1.1.14 display ip policy-based-route setup	1-14
1.1.15 if-match acl.....	1-15
1.1.16 if-match app-group	1-16
1.1.17 if-match object-group	1-17
1.1.18 if-match packet-length.....	1-17
1.1.19 ip local policy-based-route	1-18
1.1.20 ip policy-based-route	1-19
1.1.21 policy-based-route.....	1-20
1.1.22 reset ip policy-based-route statistics.....	1-20

1 策略路由

1.1 策略路由配置命令

1.1.1 apply access-vpn

apply access-vpn 命令用来设置报文在公网或指定 VPN 实例中进行转发。

undo apply access-vpn 命令用来取消报文在公网或指定 VPN 实例中进行转发的设置。

【命令】

apply access-vpn { **public** | **vpn-instance** *vpn-instance-name*<1-4> }

undo apply access-vpn { **public** | **vpn-instance** [*vpn-instance-name*<1-4>] }

【缺省情况】

设备根据路由表在公网或 VPN 内转发报文。

【视图】

策略节点视图

【缺省用户角色】

network-admin

context-admin

【参数】

public: 设置报文在公网中进行转发。

vpn-instance: 设置报文在指定 VPN 实例中进行转发。

vpn-instance-name<1-4>: 指定 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。指定的 VPN 实例必须已经存在。<1-4> 表示前面的参数最多可以输入 4 次。

【使用指导】

本命令用于在某些特殊组网中在不同网络间转发报文，例如将公网接收到的报文发送到某个 VPN 中，或者在 VPN 之间转发报文。

用户可通过重复执行本命令来指定公网和 VPN 实例。设备将根据配置顺序查找公网或第一个可用的 VPN 实例中的转发表进行转发。

执行 **undo apply access-vpn vpn-instance** [*vpn-instance-name*<1-4>] 命令时，如果仅指定了 **vpn-instance** 关键字，那么节点上的所有 VPN 实例配置会被删除。

当节点上所有的 VPN 实例配置和公网配置均被删除后，设备恢复缺省转发方式，根据路由表在公网或 VPN 内转发报文。

【举例】

在策略节点中设置报文在名为 vpn1、vpn2 的 VPN 实例中进行转发（VPN 实例 vpn1、vpn2 已存在）。

```

<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-pbr-policy1-10] apply access-vpn vpn-instance vpn1 vpn2
# 在策略节点中设置报文在公网中进行转发。
<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-pbr-policy1-10] apply access-vpn public

```

【相关命令】

- **apply remark-vpn**

1.1.2 apply continue

apply continue 命令用来设置匹配成功的当前节点指定转发路径失败后，继续进行后续节点的处理。

undo apply continue 命令用来恢复缺省情况。

【命令】

```

apply continue
undo apply continue

```

【缺省情况】

匹配成功的当前节点指定转发路径失败后，不再进行下一节点的匹配。

【视图】

策略节点视图

【缺省用户角色】

```

network-admin
context-admin

```

【使用指导】

本命令仅在策略节点的匹配模式为 **permit** 时生效。

在配置了该命令后，如果当前节点中未配置影响报文转发路径的 **apply** 子句(**apply access-vpn**、**apply next-hop**、**apply output-interface**、**apply default-next-hop** 和 **apply default-output-interface**)，或者配置了这些子句中的一个或多个，但配置的子句都失效(下一跳不可达、出接口 down 或者报文在指定 VPN 内转发失败)时，会进行下一节点的处理。

【举例】

设置匹配成功的当前节点转发失败后继续进行后续节点的处理。

```

<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply continue

```

1.1.3 apply default-next-hop

apply default-next-hop 命令用来设置指导报文转发的缺省下一跳。

undo apply default-next-hop 命令用来取消指导报文转发的缺省下一跳的设置。

【命令】

```
apply default-next-hop [ vpn-instance vpn-instance-name | inbound-vpn ]
{ ip-address [ direct ] [ track track-entry-number ] }&<1-4>
undo apply default-next-hop [ [ vpn-instance vpn-instance-name |
inbound-vpn ] ip-address&<1-4> ]
```

【缺省情况】

未设置指导报文转发的缺省下一跳。

【视图】

策略节点视图

【缺省用户角色】

network-admin
context-admin

【参数】

vpn-instance vpn-instance-name: 缺省下一跳所在的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。指定的 VPN 实例必须已经存在。

inbound-vpn: 报文入接口所在的 VPN 实例。

ip-address: 缺省下一跳的 IP 地址。如果未指定 **vpn-instance** 或 **inbound-vpn** 参数，表示指定的是公网下一跳。

direct: 指定当前缺省下一跳生效的条件为直连下一跳。

track track-entry-number: 指定 Track 项的序号，*track-entry-number* 取值范围为 1~1024。

&<1-4>: 表示前面的参数最多可以输入 4 次。

【使用指导】

用户可以同时配置多个缺省下一跳（通过一次或多次配置本命令实现），起到主备或负载分担的作用。

配置 **undo** 命令时，如果指定了缺省下一跳 IP 地址，将取消已配置的该缺省下一跳；如果未指定缺省下一跳 IP 地址，将取消已配置的所有缺省下一跳。

【举例】

```
# 设置指导报文转发的缺省直连下一跳为 1.1.1.1。
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-next-hop 1.1.1.1 direct
```

【相关命令】

- **apply loadshare**

1.1.4 apply default-output-interface

apply default-output-interface 命令用来设置指导报文转发的缺省出接口。

undo apply default-output-interface 命令用来取消指导报文转发的缺省出接口的设置。

【命令】

```
apply default-output-interface { interface-type interface-number [ track  
track-entry-number ] }<1-4>  
undo    apply    default-output-interface    [    {    interface-type  
interface-number }<1-4> ]
```

【缺省情况】

未设置指导报文转发的缺省出接口。

【视图】

策略节点视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface-type interface-number: 指定接口类型和接口编号。

track track-entry-number: 指定 Track 项的序号, *track-entry-number* 取值范围为 1~1024。

<1-4>: 表示前面的参数最多可以输入 4 次

【使用指导】

用户可以同时配置多个缺省出接口（通过一次或多次配置本命令实现），起到主备或负载分担的作用。

指定缺省出接口类型需配置为 P2P（Point-to-Point，点到点）接口，对于非 P2P 接口（广播类型的接口和 NBMA 类型的接口），比如以太网接口、Virtual-Template 接口，由于有多个可能的下一跳，可能会造成报文转发不成功的现象。NBMA（Non Broadcast MultiAccess，非广播多路访问）指全连通、非广播、多点可达的网络，这种网络采用单播方式发送报文。

配置 **undo** 命令时，如果指定了接口，将取消已配置的该缺省出接口；如果未指定接口，将取消已配置的所有缺省出接口。

【举例】

```
# 设置报文的缺省出接口为 GigabitEthernet1/0/1。  
<Sysname> system-view  
[Sysname] policy-based-route aa permit node 11  
[Sysname-pbr-aa-11] apply default-output-interface gigabitethernet 1/0/1
```

【相关命令】

- **apply loadshare**

1.1.5 apply ip-df

apply ip-df 命令用来设置 IP 报文头中的 DF（Don't Fragment，不分片）标志。

undo apply ip-df 命令用来恢复缺省情况。

【命令】

```
apply ip-df df-value  
undo apply ip-df
```

【缺省情况】

未设置 IP 报文头中的 DF 标志。

【视图】

策略节点视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

df-value：设置 IP 报文头中的 DF 标志，取值 0 或 1。

【使用指导】

报文中 DF 标志位置为 0，表示可以对报文进行分片处理。

报文中 DF 标志位置为 1，表示不可对报文进行分片处理。

【举例】

```
# 将报文 IP 首部的 DF 标志位置为 0。  
<Sysname> system-view  
[Sysname] policy-based-route aa permit node 11  
[Sysname-pbr-aa-11] apply ip-df 0
```

1.1.6 apply loadshare

apply loadshare 命令用来设置多个下一跳（缺省下一跳、缺省出接口、下一跳和出接口）工作在负载分担模式。

undo apply loadshare 命令用来恢复缺省情况。

【命令】

```
apply loadshare { default-next-hop | default-output-interface | next-hop |  
output-interface }  
undo apply loadshare { default-next-hop | default-output-interface |  
next-hop | output-interface }
```

【缺省情况】

多个下一跳（缺省下一跳、缺省出接口、下一跳和出接口）工作在主备模式。

【视图】

策略节点视图

【缺省用户角色】

```
network-admin  
context-admin
```


【参数】

default-next-hop: 设置指导报文转发的多个缺省下一跳工作在负载分担模式。

default-output-interface: 设置指导报文转发的多个缺省出接口工作在负载分担模式。

next-hop: 设置指导报文转发的多个下一跳工作在负载分担模式。

output-interface: 设置指导报文转发的多个出接口工作在负载分担模式。

【使用指导】

多个出接口（缺省下一跳、缺省出接口、下一跳和出接口）的工作模式有两种：主备模式、负载分担模式。以多个出接口为例：

- 主备模式：按照配置顺序，以第一个配置出的接口作为主用出接口，指导报文转发。当主用出接口失效时，按配置顺序选择后续的第一个有效的出接口指导报文转发。
- 负载分担模式：出接口的负载分担方式，如果不匹配快速转发表，则按照配置顺序逐包轮流选择有效的出接口指导报文转发；如果匹配快速转发表，则按照配置顺序逐流轮流选择有效的出接口指导报文转发。下一跳的负载分担模式会按照下一跳的权重指导报文转发。缺省情况下，多个下一跳会按照缺省的权重值平均分配带宽，多个下一跳的转发流量的比例是相同的。

缺省下一跳和缺省出接口的情况请参考多个出接口。

【举例】

设置多个下一跳工作在负载分担模式。

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply next-hop 1.1.1.1 2.2.2.2
[Sysname-pbr-aa-11] apply loadshare next-hop
```

设置多个出接口工作在负载分担模式。

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply output-interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
[Sysname-pbr-aa-11] apply loadshare output-interface
```

设置多个缺省下一跳工作在负载分担模式。

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-next-hop 1.1.1.1 2.2.2.2
[Sysname-pbr-aa-11] apply loadshare default-next-hop
```

设置多个缺省出接口工作在负载分担模式。

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply default-output-interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
[Sysname-pbr-aa-11] apply loadshare default-output-interface
```

【相关命令】

- **apply default-next-hop**
- **apply default-output-interface**
- **apply next-hop**

- **apply output-interface**

1.1.7 apply next-hop

apply next-hop 命令用来设置报文转发的下一跳。

undo apply next-hop 命令用来取消报文转发下一跳的设置。

【命令】

```
apply next-hop [ vpn-instance vpn-instance-name | inbound-vpn ] { ip-address
[ direct ] [ track track-entry-number ] [ weight weight-value ] }&<1-4>
undo apply next-hop [ [ vpn-instance vpn-instance-name | inbound-vpn ]
ip-address&<1-4> ]
```

【缺省情况】

未设置报文转发的下一跳。

【视图】

策略节点视图

【缺省用户角色】

network-admin

context-admin

【参数】

vpn-instance *vpn-instance-name*: 下一跳所在的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。指定的 VPN 实例必须已经存在。

inbound-vpn: 报文入接口所在的 VPN 实例。

ip-address: 下一跳 IP 地址。如果未指定 **vpn-instance** 或 **inbound-vpn** 参数，表示指定的是公网下一跳。

direct: 指定当前下一跳生效的条件为直连下一跳。

track *track-entry-number*: 指定 Track 项的序号，*track-entry-number* 取值范围为 1~1024。

weight *weight-value*: 指定下一跳负载分担的权重。设备根据权重确定该下一跳转发流量的比例。例如，三个下一跳配置的负载分担权重分别为 1、1 和 2，则它们的负载分担的比例分别为 1/4、1/4 和 1/2。*weight-value* 取值范围为 1~100，缺省值为 10。

&<1-4>: 表示前面的参数最多可以输入 4 次。

【使用指导】

用户可以同时配置多个下一跳（通过一次或多次配置本命令实现），起到主备或负载分担的作用。

配置 **undo** 命令时，如果指定了下一跳 IP 地址，将取消已配置的该下一跳；如果未指定下一跳 IP 地址，将取消已配置的所有下一跳。

【举例】

设置报文的直连下一跳为 1.1.1.1。

```
<Sysname> system-view
```

```
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply next-hop 1.1.1.1 direct
```

【相关命令】

- **apply loadshare**

1.1.8 apply output-interface

apply output-interface 命令用来设置指导报文转发的出接口。

undo apply output-interface 命令用来取消指导报文转发的出接口的设置。

【命令】

```
apply output-interface { interface-type interface-number [ track
track-entry-number ] }&<1-4>
undo apply output-interface [ { interface-type interface-number }&<1-4> ]
```

【缺省情况】

未设置指导报文转发的出接口。

【视图】

策略节点视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface-type interface-number: 指定接口类型和接口编号。

track track-entry-number: 指定 Track 项的序号, *track-entry-number* 取值范围为 1~1024。

&<1-4>: 表示前面的参数最多可以输入 4 次。

【使用指导】

用户可以同时配置多个出接口（通过一次或多次配置本命令实现），起到主备或负载分担的作用。

指定出接口类型需配置为 P2P 接口，对于非 P2P 接口（广播类型的接口和 NBMA 类型的接口），比如以太网接口、Virtual-Template 接口，由于有多个可能的下一跳，可能会造成报文转发不成功的现象。

配置 **undo** 命令时，如果指定了接口，将取消已配置的该出接口；如果未指定接口，将取消已配置的所有出接口。

【举例】

```
# 对已经匹配的 IP 报文指定出接口为 GigabitEthernet1/0/1。
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] apply output-interface gigabitethernet 1/0/1
```

【相关命令】

- **apply loadshare**

1.1.9 apply precedence

apply precedence 命令用来设置 IP 报文的优先级。

undo apply precedence 命令用来恢复缺省情况。

【命令】

apply precedence { *type* | *value* }

undo apply precedence

【缺省情况】

未设置 IP 报文的优先级。

【视图】

策略节点视图

【缺省用户角色】

network-admin

context-admin

【参数】

type: IP 报文的优先级类型。

value: IP报文的优先级值，IP报文共有 8（0~7）个优先级，每个数值对应一个优先级类型。在输入参数的时候可以输入数值，也可以输入优先级类型。对应关系如 [表 1-1](#) 所示。

表1-1 IP 优先级值与优先级类型对应表

优先级值	优先级类型
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

【举例】

设置 IP 报文的优先级为 5（critical）。

```
<Sysname> system-view
```

```
[Sysname] policy-based-route aa permit node 11
```

```
[Sysname-pbr-aa-11] apply precedence critical
```

1.1.10 apply remark-vpn

apply remark-vpn 命令用来重标记报文所属的 VPN。

undo apply remark-vpn 命令用来恢复缺省情况。

【命令】

```
apply remark-vpn
undo apply remark-vpn
```

【缺省情况】

未重标记报文所属的 VPN。

【视图】

策略节点视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

一般情况下，配置 **apply access-vpn** 命令后，设备仅在指定的 VPN 实例内转发报文，但不会重标记报文所属的 VPN，后续业务模块学到的还是报文中之前的 VPN 实例。如果需要重标记报文所属的 VPN 信息，则需要配置本命令。

本命令必须和 **apply access-vpn** 命令同时使用。只有配置了 **apply access-vpn** 命令成功指导报文转发时，本命令才能重标记报文所属的 VPN 信息，标记的 VPN 例是生效的 **apply access-vpn** 命令配置的 VPN 实例。

【举例】

```
# 重标记匹配 ACL 3000 的报文所属的 VPN 实例为 vpn1。
<Sysname> system-view
[Sysname] policy-based-route aaa permit node 10
[Sysname-pbr-aaa-10] if-match acl 3000
[Sysname-pbr-aaa-10] apply access-vpn vpn-instance vpn1
[Sysname-pbr-aaa-10] apply remark-vpn
```

【相关命令】

- **apply access-vpn**

1.1.11 display ip policy-based-route

display ip policy-based-route 命令用来显示已经配置的策略。

【命令】

```
display ip policy-based-route [ policy policy-name ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

context-admin
context-operator

【参数】

policy *policy-name*: 显示指定的策略。*policy-name* 表示策略名，唯一标识一个策略，为1~19个字符的字符串，区分大小写。如果未指定本参数，则显示所有已经配置的策略。

【举例】

显示所有已经配置的策略。
<Sysname> display ip policy-based-route
Policy name: aaa
node 1 permit:
if-match acl 2000
apply next-hop 1.1.1.1

表1-2 display ip policy-based-route 命令显示信息描述表

字段	描述
Policy name	策略名
node 1 permit	节点1的匹配模式为允许
if-match acl	满足ACL的报文被匹配
apply next-hop	为匹配的报文指定下一跳

【相关命令】

- **policy-based-route**

1.1.12 display ip policy-based-route interface

display ip policy-based-route interface 命令用来显示接口下转发策略路由的配置信息和统计信息。

【命令】

display ip policy-based-route interface *interface-type interface-number*
[**slot slot-number**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-type interface-number: 用来指定接口的类型和编号。

slot slot-number: 显示指定成员设备上的信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示主设备上的信息。

【举例】

显示接口 GigabitEthernet1/0/1 下转发策略路由的配置信息和统计信息。

```
<Sysname> display ip policy-based-route interface gigabitethernet 1/0/1
```

```
Policy based routing information for interface GigabitEthernet1/0/1(failed):
```

```
Policy name: aaa
```

```
node 0 deny:
```

```
Matched: 0
```

```
node 1 permit:
```

```
if-match acl 3999
```

```
Matched: 0
```

```
node 2 permit:
```

```
if-match acl 2000
```

```
apply next-hop 2.2.2.2
```

```
Matched: 0
```

```
node 5 permit:
```

```
if-match acl 3101
```

```
apply next-hop 1.1.1.1
```

```
apply output-interface GigabitEthernet1/0/2 track 1 (down)
```

```
apply output-interface GigabitEthernet1/0/3 track 2 (inactive)
```

```
Matched: 0
```

```
Total matched: 0
```

```
<Sysname> display ip policy-based-route interface gigabitethernet 1/0/1
```

```
Policy based routing information for interface GigabitEthernet1/0/1:
```

```
Policy name: aaa
```

```
node 0 deny(not support):
```

```
Matched: 0
```

```
node 1 permit:
```

```
if-match acl 3999
```

```
Matched: 0
```

```
node 2 permit(no resource):
```

```
if-match acl 2000
```

```
apply next-hop 2.2.2.2
```

```
apply output-interface GigabitEthernet1/0/2 track 1 (down)
```

```
apply output-interface GigabitEthernet1/0/3 track 2 (inactive)
```

```
Matched: 0
```

```
node 5 permit:
```

```
if-match acl 3101
```

```
apply next-hop 1.1.1.1
```

```
Matched: 0 (no statistics resource)
```

```
Total matched: 0
```

表1-3 display ip policy-based-route interface 命令显示信息描述表

字段	描述
Policy based routing information for interface XXXX(failed)	接口下转发策略路由的配置信息和统计信息（failed表示策略下发驱动失败。只有在接口上删除转发策略路由，再重新创建转发策略路由，显示信息才能刷新）  说明 对于设备上的全局口（如 VLAN 接口）和物理口，只有指定 slot 后，才会显示括号内的信息。
Policy name	策略名
node 0 deny(not support) node 2 permit(no resource)	节点的匹配模式为允许（permit）/拒绝（deny）（not support表示设备不支持该节点设置的规则；no resource表示设备的ACL等资源不足，为该节点分配ACL等资源失败）  说明 对于设备上的全局口（如 VLAN 接口）和物理口，只有指定 slot 后，才会显示括号内的信息。
if-match acl	满足ACL的报文被匹配
apply next-hop	为匹配的报文指定下一跳
apply output-interface track 1 (down)	为匹配的报文指定出接口。括号中显示接口的状态：up、down、inactive。接口不在位时，显示inactive；接口网络层down时，显示down
Matched: 0 (no statistics resource)	节点匹配成功的次数（no statistics resource表示统计资源不足）  说明 对于设备上的全局口（如 VLAN 接口）和物理口，只有指定 slot 后，才会显示括号内的信息。
Total matched	策略所有节点匹配成功的次数

【相关命令】

- **reset ip policy-based-route statistics**

1.1.13 display ip policy-based-route local

display ip policy-based-route local 命令用来显示本地策略路由的配置信息和统计信息。

【命令】

display ip policy-based-route local [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin

context-operator

【参数】

slot slot-number：显示指定成员设备上本地策略路由的配置信息和统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示主设备上本地策略路由的配置信息和统计信息。

【举例】

```
# 显示本地策略路由的配置信息和统计信息。
<Sysname> display ip policy-based-route local
Policy based routing information for local:
Policy name: aaa
  node 0 deny:
    Matched: 0
  node 1 permit:
    if-match acl 3999
    Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 2.2.2.2
    Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1.1.1.1
    Matched: 0
Total matched: 0
```

表1-4 display ip policy-based-route local 命令显示信息描述表

字段	描述
Policy based routing information for local	本地策略路由的配置信息和统计信息
Policy name	策略名
node 0 deny/node 2 permit	节点的匹配模式为允许（permit）/拒绝（deny）
if-match acl	满足ACL的报文被匹配
apply next-hop	为匹配的报文指定下一跳
Matched: 0	节点匹配成功的次数
Total matched	策略所有节点匹配成功的次数

【相关命令】

- **reset ip policy-based-route statistics**

1.1.14 display ip policy-based-route setup

display ip policy-based-route setup 命令用来显示已经应用的策略路由信息。

【命令】

display ip policy-based-route setup

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示已经应用的策略路由信息。

```
<Sysname> display ip policy-based-route setup
Policy Name          Interface Name
aaa                  GigabitEthernet1/0/1
```

表1-5 display ip policy-based-route setup 命令显示信息描述表

字段	描述
Policy Name	策略名
Interface Name	应用策略的接口

【相关命令】

- **ip policy-based-route**

1.1.15 if-match acl

if-match acl 命令用来设置 ACL 匹配规则。
undo if-match acl 命令用来恢复缺省情况。

【命令】

if-match acl { *acl-number* | **name** *acl-name* }
undo if-match acl

【缺省情况】

未设置 ACL 匹配规则。

【视图】

策略节点视图

【缺省用户角色】

network-admin
context-admin

【参数】

acl-number: 访问控制列表号，取值范围为 2000～3999。其中：

- 基本 ACL，**acl-number** 取值范围为 2000～2999；
- 高级 ACL，**acl-number** 取值范围为 3000～3999。

name acl-name: 指定 ACL 的名称。**acl-name** 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 **all**。只有指定基本 ACL 或高级 ACL 的 **acl-name** 才生效。

【举例】

设置满足 ACL 2011 的报文被匹配。

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl 2011
```

设置满足 ACL 名称为 aaa 的报文被匹配。

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match acl name aaa
```

1.1.16 if-match app-group

if-match app-group 命令用来设置应用组匹配规则。

undo if-match app-group 命令用来删除应用组匹配规则。

【命令】

```
if-match app-group app-group-name<1-6>
undo if-match app-group [ app-group-name<1-6> ]
```

【缺省情况】

未设置应用组匹配规则。

【视图】

策略节点视图

【缺省用户角色】

network-admin
context-admin

【参数】

app-group-name: 应用组名，为 1～63 个字符的字符串，不区分大小写，可以为数字、字母、连字符和下划线，不允许为“Invalid”、“other”或系统预定义应用组的名称。

<1-6>: 表示前面的参数最多可以输入 6 次。

【使用指导】

应用组匹配规则只对转发策略路由生效，对本地策略路由不生效。

执行 **undo** 命令时，如果指定了参数，则表示删除和参数对应的应用组匹配规则；如果未指定任何参数，则表示删除所有的应用组匹配规则。

【举例】

```
# 设置应用组匹配规则 test。
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match app-group test
```

1.1.17 if-match object-group

if-match object-group 命令用来设置服务对象组匹配规则。

undo if-match object-group 命令用来删除服务对象组匹配规则。

【命令】

```
if-match object-group service object-group-name&<1-6>
undo if-match object-group service [object-group-name&<1-6> ]
```

【缺省情况】

未设置服务对象组匹配规则。

【视图】

策略节点视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

service *object-group-name*: 服务对象组名，为 1~31 个字符的字符串，不区分大小写。

&<1-6>: 表示前面的参数最多可以输入 6 次。

【使用指导】

执行 **undo** 命令时，如果指定了参数，则表示删除和参数对应的服务对象组匹配规则；如果未指定任何参数，则表示删除所有的服务对象组匹配规则。

【举例】

```
# 设置服务对象组匹配规则 test。
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match object-group service test
```

1.1.18 if-match packet-length

if-match packet-length 命令用来设置 IP 报文长度匹配规则。

undo if-match packet-length 命令用来恢复缺省情况。

【命令】

```
if-match packet-length min-len max-len
undo if-match packet-length
```

【缺省情况】

未设置 IP 报文长度匹配规则。

【视图】

策略节点视图

【缺省用户角色】

network-admin

context-admin

【参数】

min-len: 最短 IP 报文长度, 取值范围为 1~65535, 单位为字节。

max-len: 最长 IP 报文长度, 取值范围为 1~65535, 单位为字节。*max-len* 应该不小于 *min-len*。

【使用指导】

IP 报文长度是指从 IP 报文头开始到报文末尾的总长度, IP 报文长度匹配含边界值, 如指定 *min-len* 为 100, *max-len* 为 200, 则报文长度为 100 与 200 的报文都是匹配报文。

【举例】

```
# 设置 IP 报文长度在 100~200 字节之间的报文被匹配。
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-pbr-aa-11] if-match packet-length 100 200
```

1.1.19 ip local policy-based-route

ip local policy-based-route 命令用来对本地报文应用策略。

undo ip local policy-based-route 命令用来恢复缺省情况。

【命令】

ip local policy-based-route *policy-name*

undo ip local policy-based-route

【缺省情况】

未对本地报文应用策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: 策略名, 唯一标识一个策略, 为 1~19 个字符的字符串, 区分大小写。该策略必须已经存在。

【使用指导】

对本地报文只能应用一个策略，应用新的策略前必须删除本地原来已经应用的策略。

对本地报文应用的策略将对本地产生的所有报文（除了本地发送给自己的报文）进行匹配。若无特殊需求，建议用户不要配置本地策略路由。

【举例】

对本地报文应用策略 **aaa**。

```
<Sysname> system-view
```

```
[Sysname] ip local policy-based-route aaa
```

【相关命令】

- **display ip policy-based-route setup**
- **policy-based-route**

1.1.20 ip policy-based-route

ip policy-based-route 命令用来对接口转发的报文应用策略。

undo ip policy-based-route 命令用来恢复缺省情况。

【命令】

```
ip policy-based-route policy-name
```

```
undo ip policy-based-route
```

【缺省情况】

未对接口转发的报文应用策略。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy-name: 策略名，唯一标识一个策略，为 1~19 个字符的字符串，区分大小写。该策略必须已经存在。

【举例】

对接口 GigabitEthernet1/0/1 转发的报文应用策略 **aaa**。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ip policy-based-route aaa
```

【相关命令】

- **display ip policy-based-route setup**
- **policy-based-route**

1.1.21 policy-based-route

policy-based-route 命令用来创建策略节点，并进入策略节点视图。如果指定的策略节点已创建，则该命令直接用来进入该策略节点的视图。

undo policy-based-route 命令用来删除已创建的策略或策略节点。

【命令】

```
policy-based-route policy-name [ deny | permit ] node node-number  
undo policy-based-route policy-name [ deny | node node-number | permit ]
```

【缺省情况】

不存在策略节点。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 策略名，唯一标识一个策略，为 1~19 个字符的字符串，区分大小写。

deny: 指定策略节点的匹配模式为拒绝模式。

permit: 指定策略节点的匹配模式为允许模式。缺省匹配模式为 **permit**。

node node-number: 策略节点编号。节点编号越小优先级越高，先对优先级高的节点进行匹配操作。

【使用指导】

删除策略之前，必须先取消该策略在所有接口或者本地上的应用，否则删除失败。

配置 **undo** 命令时，如果指定了策略节点，将删除指定的节点；如果指定了节点模式，将按模式删除策略内所有与该模式匹配的所有节点；如果两者都未指定，将删除整个策略。

【举例】

```
# 创建一个策略 policy1，其节点序列号为 10，匹配模式为 permit，并进入策略节点视图。  
<Sysname> system-view  
[Sysname] policy-based-route policy1 permit node 10  
[Sysname-pbr-policy1-10]
```

【相关命令】

- **display ip policy-based-route**

1.1.22 reset ip policy-based-route statistics

reset ip policy-based-route statistics 命令用来清除策略路由的统计信息。

【命令】

```
reset ip policy-based-route statistics [ policy policy-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy *policy-name*: 清除指定策略的统计信息。*policy-name* 表示策略名，唯一标识一个策略，为 1~19 个字符的字符串，区分大小写。如果未指定本参数，则清除所有策略路由的统计信息。

【举例】

清除所有配置策略的统计信息。

```
<Sysname> reset ip policy-based-route statistics
```

【相关命令】

- **display ip policy-based-route interface**
- **display ip policy-based-route local**

目 录

1 IPv6 静态路由	1-1
1.1 IPv6 静态路由配置命令	1-1
1.1.1 delete ipv6 static-routes all	1-1
1.1.2 display ipv6 route-static nib	1-1
1.1.3 display ipv6 route-static routing-table	1-4
1.1.4 ipv6 route-static	1-6
1.1.5 ipv6 route-static default-preference	1-9

1 IPv6 静态路由

1.1 IPv6静态路由配置命令

1.1.1 delete ipv6 static-routes all

delete ipv6 static-routes all 命令用来删除所有 IPv6 静态路由。

【命令】

delete ipv6 [vpn-instance vpn-instance-name] static-routes all

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

vpn-instance vpn-instance-name：删除指定 VPN 的所有 IPv6 静态路由。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果不指定该参数，则删除公网实例下的所有 IPv6 静态路由。

【使用指导】

使用本命令删除 IPv6 静态路由时，系统会提示确认，确认后会删除所配置的所有 IPv6 静态路由。

【举例】

```
# 删除所有 IPv6 静态路由。
<Sysname> system-view
[Sysname] delete ipv6 static-routes all
This will erase all IPv6 static routes and their configurations, you must reconfigure all static routes.
Are you sure?[Y/N]:y
```

【相关命令】

- **ipv6 route-static**

1.1.2 display ipv6 route-static nib

display ipv6 route-static nib 命令用来显示 IPv6 静态路由下一跳信息。

【命令】

display ipv6 route-static nib [nib-id] [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

nib-id: 路由邻居 ID 值，取值范围为十六进制数 1~ffffff。
verbose: 显示详细信息。如果未指定本参数，则显示概要信息。

【举例】

```
# 显示 IPv6 静态路由邻居信息与下一跳信息。
<Sysname> display ipv6 route-static nib
Total number of nexthop(s): 35

      NibID: 0x21000000      Sequence: 0
      Type: 0x41             Flushed: Yes
UserKey0: 0x0                VrfNthp: 0
UserKey1: 0x0                Nexthop: 2::3
      IFIndex: 0x0           LocalAddr: ::
      TopoNthp: Invalid

      NibID: 0x21000001      Sequence: 1
      Type: 0x41             Flushed: Yes
UserKey0: 0x0                VrfNthp: 0
UserKey1: 0x0                Nexthop: 3::4
      IFIndex: 0x0           LocalAddr: ::
      TopoNthp: Invalid

.....（省略部分显示信息）
```

表1-1 display ipv6 route-static nib 命令显示信息描述表

字段	描述
Total number of nexthop(s)	总的NIB个数
NibID	NIB ID号
Sequence	NIB序列号
Type	NIB类型
Flushed	是否下刷FIB
UserKey0	NIB协议保留数据1
UserKey1	NIB协议保留数据2
VrfNthp	下一跳所在VPN索引，显示为0表示公网
Nexthop	下一跳信息

字段	描述
IFIndex	接口索引
LocalAddr	本地接口地址
TopoNthp	(暂不支持)下一跳所在拓扑索引, 显示为0表示公网拓扑(目前IPv6不支持子拓扑, 显示为Invalid)

显示 IPv6 静态路由邻居与下一跳的详细信息。

```
<Sysname> display ipv6 route-static nib verbose
```

```
Total number of nexthop(s): 35
```

```

      NibID: 0x21000000      Sequence: 0
      Type: 0x41             Flushed: Yes
      UserKey0: 0x0          VrfNthp: 0
      UserKey1: 0x0          Nexthop: 2::3
      IFIndex: 0x0           LocalAddr: ::
      TopoNthp: Invalid
      RefCnt: 1              FlushRefCnt: 0
      Flag: 0x12             Version: 1
1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 2::3
RelyDepth: 2                RealNexthop: ::
Interface: NULL0            LocalAddr: ::
TunnelCnt: 0                Vrf: default-vrf
TunnelID: N/A               Topology:
Weight: 0

```

```

      NibID: 0x21000001      Sequence: 1
      Type: 0x41             Flushed: Yes
      UserKey0: 0x0          VrfNthp: 0
      UserKey1: 0x0          Nexthop: 3::4
      IFIndex: 0x0           LocalAddr: ::
      TopoNthp: Invalid
      RefCnt: 1              FlushRefCnt: 0
      Flag: 0x12             Version: 1
1 nexthop(s):
PrefixIndex: 0              OrigNexthop: 3::4
RelyDepth: 1                RealNexthop: ::
Interface: GE1/0/1          LocalAddr: ::
TunnelCnt: 0                Vrf: default-vrf
TunnelID: N/A               Topology:
Weight: 0

```

..... (省略部分显示信息)

表1-2 display ipv6 route-static nib verbose 命令显示信息描述表

字段	描述
x nexthop(s)	下一跳具体值（前面数值表示下一跳个数）
PrefixIndex	等价时下一跳序号
Vrf	VPN实例名，显示为default-vrf表示公网
OrigNexthop	原始下一跳
RealNexthop	真实下一跳
Interface	出接口
localAddr	本地接口地址
RelyDepth	迭代深度
TunnelCnt	（暂不支持）迭代到隧道的个数
TunnelID	（暂不支持）迭代到隧道的ID
Topology	（暂不支持）拓扑名称，显示为base表示公网拓扑（目前IPv6不支持子拓扑，显示为空）
Weight	等价路由各路由的权重，取值为0表示不是等价路由
RefCnt	下一跳信息的引用计数
FlushRefCnt	下一跳信息的下刷引用计数
Flag	下一跳信息的标志位
Version	下一跳信息的版本号

1.1.3 display ipv6 route-static routing-table

display ipv6 route-static routing-table 命令用来显示 IPv6 静态路由表信息。

【命令】

display ipv6 route-static routing-table [vpn-instance vpn-instance-name]
[ipv6-address prefix-length]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

vpn-instance *vpn-instance-name*: 显示指定 VPN 的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示公网的信息。

ipv6-address: 目的 IPv6 地址。

prefix-length: 前缀长度，取值范围为 0~128。

【举例】

显示 IPv6 静态路由表信息。

```
<Sysname> display ipv6 route-static routing-table
```

```
Total number of routes: 5
```

```
Status: * - valid
```

```
*Destination: 1::1/128
```

```
      NibID: 0x21000000      NextHop: 2::2
MainNibID: N/A      BkNextHop: N/A
      BkNibID: N/A      Interface: GigabitEthernet1/0/1
      TableID: 0xa      BkInterface: N/A
      Flag: 0x80d0a      BfdSrcIp: N/A
      DbIndex: 0x3      BfdIfIndex: 0x0
      Type: Normal      BfdVrfIndex: 0
TrackIndex: 0xffffffff      Label: NULL
Preference: 60      vrfIndexDst: 0
      BfdMode: N/A      vrfIndexNH: 0
Permanent: 0      Tag: 0
```

```
*Destination: 1::1234/128
```

```
      NibID: 0x21000000      NextHop: 2::2
MainNibID: N/A      BkNextHop: N/A
      BkNibID: N/A      Interface: NULL0
      TableID: 0xa      BkInterface: N/A
      Flag: 0x80d0a      BfdSrcIp: N/A
      DbIndex: 0x1      BfdIfIndex: 0x0
      Type: Normal      BfdVrfIndex: 0
TrackIndex: 0xffffffff      Label: NULL
Preference: 60      vrfIndexDst: 0
      BfdMode: N/A      vrfIndexNH: 0
Permanent: 0      Tag: 0
```

.....（省略部分显示信息）

表1-3 display ipv6 route-static routing-table 命令显示信息描述表

字段	描述
Total number of routes	总的路由条数
Destination	目的地址/掩码

字段	描述
NibID	下一跳信息ID
MainNibID	FRR静态路由主下一跳信息ID
BkNibID	FRR静态路由备下一跳信息ID
NextHop	此路由的下一跳地址
BkNextHop	此路由的备份下一跳地址
Interface	出接口，即到该目的网段的数据包将从此接口发出
BkInterface	备份出接口
TableID	路由所在的表ID
Flag	路由标志位
DbIndex	路由所在DB的DB索引
Type	路由类型：Normal，普通类型的静态路由
BfdSrcIpf	BFD非直连会话源地址
BfdIfIndex	BFD使用的接口索引
BfdVrfIndex	BFD所在VPN索引，显示为0表示公网
BfdMode	BFD模式： • N/A：未配置 BFD 会话 • Ctrl：控制报文方式的 BFD 会话 • Echo：echo 报文方式的 BFD 会话
TrackIndex	NQA Track索引
Label	标签
Preference	路由优先级
vrfIndexDst	目的所在VPN，显示为0表示公网
vrfIndexNH	下一跳所在VPN，显示为0表示公网
Permanent	永久静态路由标志（1表示永久静态路由）
Tag	路由标记

1.1.4 ipv6 route-static

ipv6 route-static 命令用来配置 IPv6 静态路由。

undo ipv6 route-static 命令用来删除指定的 IPv6 静态路由。

【命令】

```

ipv6 route-static ipv6-address prefix-length { interface-type
interface-number [ next-hop-address ] [ bfd { control-packet | echo-packet }
[ bfd-source ipv6-address ] | permanent ] | [ vpn-instance

```

```

d-vpn-instance-name ] next-hop-address [ bfd control-packet bfd-source
ipv6-address | permanent ] } [ preference preference ] [ tag tag-value ]
[ description text ]

undo ipv6 route-static ipv6-address prefix-length [ interface-type
interface-number [ next-hop-address ] | [ vpn-instance d-vpn-instance-name ]
next-hop-address ] [ preference preference ]

ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address
prefix-length { interface-type interface-number [ next-hop-address ] [ bfd
{ control-packet | echo-packet } [ bfd-source ipv6-address ] | permanent ] |
next-hop-address [ public ] [ bfd control-packet bfd-source ipv6-address |
permanent ] | vpn-instance d-vpn-instance-name next-hop-address [ bfd
control-packet bfd-source ipv6-address | permanent ] } [ preference
preference ] [ tag tag-value ] [ description text ]

undo ipv6 route-static vpn-instance s-vpn-instance-name ipv6-address
prefix-length [ interface-type interface-number [ next-hop-address ] |
next-hop-address [ public ] | vpn-instance d-vpn-instance-name
next-hop-address ] [ preference preference ]

```

【缺省情况】

未配置 IPv6 静态路由。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address prefix-length: IPv6 地址及前缀长度。

interface-type interface-number: 路由出接口的类型和编号。对于接口类型为非 P2P 接口（包括 NBMA 类型接口或广播类型接口），必须指定下一跳地址。

next-hop-address: 下一跳 IPv6 地址。

bfd: 使能 BFD（Bidirectional Forwarding Detection，双向转发检测）功能，对静态路由下一跳的可达性进行快速检测。

control-packet: 通过 BFD 控制报文方式实现 BFD 功能。

bfd-source ipv6-address: BFD 源 IPv6 地址。

echo-packet: 通过 BFD echo 报文方式实现 BFD 功能。

permanent: 指定为永久 IPv6 静态路由。即使在出接口 down 时，配置的永久 IPv6 静态路由仍然保持 active 状态。

public: 指定静态路由下一跳处于公网实例。

vpn-instance d-vpn-instance-name: 指定目的 VPN。*d-vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果指定目的 VPN，IPv6 静态路由将根据配置的下一跳 IPv6 地址在目的 VPN 中查找出接口。

preference preference: 路由的优先级，取值范围为 1~255，缺省值为 60。

tag tag-value: 静态路由 Tag 值，用于标识该条静态路由，以便在路由策略中根据 Tag 对路由进行灵活的控制。*tag-value* 的取值范围为 1~4294967295，缺省值为 0。关于路由策略的详细信息，请参见“三层技术-IP 路由配置指导”中的“路由策略”。

description text: 静态路由描述信息。*text* 为 1~60 个字符的字符串，除“?”外，可以包含空格等特殊字符。

vpn-instance s-vpn-instance-name: 指定源 VPN。*s-vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。每个 VPN 都有自己的路由表，配置的 IPv6 静态路由将被加入指定 VPN 的路由表。

【使用指导】

如果配置的 IPv6 静态路由指定目的地址为::/0 (前缀长度为 0)，则表示配置了一条 IPv6 缺省路由。如果报文的目的地址无法匹配路由表中的任何一项，设备将选择 IPv6 缺省路由来转发 IPv6 报文。在配置静态路由时，可以指定出接口 (*interface-type interface-number*)，也可指定下一跳地址 (*next-hop-address*)，具体采用哪种方法，需要根据实际情况而定：

- 如果出接口类型为广播或者 NBMA 类型，必须指定下一跳地址。
- 如果出接口类型为点到点类型，配置时可以只指定出接口，不指定下一跳地址。这样，即使对端地址发生了变化也无须改变配置。

配置 IPv6 静态路由与 BFD 联动时，需要注意的是：

- 对于直连下一跳，当指定的出接口类型为非 P2P 接口时，建议用户通过 **bfd-source** 命令指定 BFD 源 IPv6 地址，该地址必须为出接口的 IPv6 地址，且与下一跳 IPv6 地址处在同一网段。如果下一跳 IPv6 地址指定的是链路本地地址，本参数也必须是链路本地地址。
- 对于直连下一跳或者非直连下一跳，如果要指定 BFD 源 IPv6 地址，那么下一跳 IPv6 地址和 BFD 源 IPv6 地址必须成对配置，即本端指定的下一跳 IPv6 地址是对端的 BFD 源 IPv6 地址，本端指定的 BFD 源 IPv6 地址是对端的下一跳 IPv6 地址。

配置 IPv6 静态路由时需要注意的是：

- 路由振荡时，使能 BFD 检测功能可能会加剧振荡，需谨慎使用。关于 BFD 的详细介绍，请参考“可靠性配置指导”中的“BFD”。
- 配置 BFD echo 报文方式时，下一跳 IPv6 地址必须为全球单播地址。

【举例】

配置 IPv6 静态路由，该路由的目的地址为 1:1:2::/64，下一跳地址为 1:1:3::1。

```
<Sysname> system-view
```

```
[Sysname] ipv6 route-static 1:1:2:: 64 1:1:3::1
```

【相关命令】

- **display ipv6 routing-table protocol** (三层技术-IP 路由命令参考/IP 路由基础)

1.1.5 ipv6 route-static default-preference

ipv6 route-static default-preference 命令用来配置 IPv6 静态路由的缺省优先级。

undo ipv6 route-static default-preference 命令用来恢复缺省情况。

【命令】

ipv6 route-static default-preference *default-preference*

undo ipv6 route-static default-preference

【缺省情况】

IPv6 静态路由的缺省优先级为 60。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

default-preference: IPv6 静态路由缺省优先级的值，取值范围为 1~255。

【使用指导】

如果在配置 IPv6 静态路由时没有指定优先级，就会使用缺省优先级。

重新配置缺省优先级后，新设置的缺省优先级仅对新增的 IPv6 静态路由有效。

【举例】

配置 IPv6 静态路由的缺省优先级为 120。

```
<Sysname> system-view
```

```
[Sysname] ipv6 route-static default-preference 120
```

【相关命令】

- **display ipv6 routing-table protocol**（三层技术-IP 路由命令参考/IP 路由基础）

目 录

1 RIPng	1-1
1.1 RIPng配置命令	1-1
1.1.1 checkzero	1-1
1.1.2 default cost	1-1
1.1.3 display ripng	1-2
1.1.4 display ripng database	1-4
1.1.5 display ripng graceful-restart	1-4
1.1.6 display ripng interface	1-5
1.1.7 display ripng neighbor	1-7
1.1.8 display ripng non-stop-routing	1-8
1.1.9 display ripng route	1-9
1.1.10 fast-reroute	1-11
1.1.11 filter-policy export	1-12
1.1.12 filter-policy import	1-13
1.1.13 graceful-restart	1-14
1.1.14 graceful-restart interval	1-14
1.1.15 import-route	1-15
1.1.16 maximum load-balancing	1-16
1.1.17 non-stop-routing	1-17
1.1.18 output-delay	1-18
1.1.19 preference	1-18
1.1.20 reset ripng process	1-19
1.1.21 reset ripng statistics	1-20
1.1.22 ripng	1-20
1.1.23 ripng default-route	1-21
1.1.24 ripng enable	1-22
1.1.25 ripng metricin	1-22
1.1.26 ripng metricout	1-23
1.1.27 ripng output-delay	1-24
1.1.28 ripng poison-reverse	1-24
1.1.29 ripng primary-path-detect bfd echo	1-25
1.1.30 ripng split-horizon	1-26
1.1.31 ripng summary-address	1-26

1.1.32 timer triggered	1-27
1.1.33 timers	1-28

1 RIPng

1.1 RIPng配置命令

1.1.1 checkzero

checkzero 命令用来使能 RIPng 报文的零域检查功能。

undo checkzero 命令用来关闭零域检查功能。

【命令】

checkzero
undo checkzero

【缺省情况】

RIPng 报文的零域检查功能处于使能状态。

【视图】

RIPng 视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

RIPng 报文头部中的一些字段必须配置为 0，也称为零域。使能 RIPng 报文的零域检查后，如果报文头部零域中的值不为零，这些报文将被丢弃，不做处理。

【举例】

```
# 关闭进程号为 100 的 RIPng 进程对 RIPng 报文的零域检查功能。  
<Sysname> system-view  
[Sysname] ripng 100  
[Sysname-ripng-100] undo checkzero
```

1.1.2 default cost

default cost 命令用来配置引入路由的缺省度量值。

undo default cost 命令用来恢复缺省情况。

【命令】

default cost *cost-value*
undo default cost

【缺省情况】

引入路由的缺省度量值为 0。

【视图】

RIPng 视图

【缺省用户角色】

network-admin

context-admin

【参数】

cost-value: 引入路由的缺省度量值，取值范围为 0~16。

【使用指导】

当使用 **import-route** 命令从其它协议引入路由时，如果不指定具体的度量值，则引入路由的度量值为 **default cost** 所指定的值。

【举例】

```
# 配置引入路由的缺省度量值为 2。
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] default cost 2
```

【相关命令】

- **import-route**

1.1.3 display ripng

display ripng 命令用来显示指定 RIPng 进程的当前运行状态及配置信息。

【命令】

display ripng [*process-id*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

process-id: RIPng 进程号，取值范围为 1~65535。如果未指定本参数，则显示所有已配置的 RIPng 进程的信息。

【举例】

```
# 显示所有已配置的 RIPng 进程的当前运行状态及配置信息。
<Sysname> display ripng
Public VPN-instance name:
```

```

RIPng process: 1
  Preference: 100
    Routing policy: abc
  Fast-reroute:
    Routing policy: abc
  Checkzero: Enabled
  Default cost: 0
  Maximum number of load balanced routes: 6
  Update time : 30 secs Timeout time : 180 secs
  Suppress time : 120 secs Garbage-collect time : 120 secs
  Update output delay: 20(ms) Output count: 3
  Graceful-restart interval: 60 secs
  Triggered Interval : 5 50 200
  Number of periodic updates sent: 256
  Number of triggered updates sent: 0

```

表1-1 display ripng 命令显示信息描述表

字段	描述
Public VPN-instance name	RIPng进程运行在公网实例下
Private VPN-instance name	RIPng进程应用于指定VPN实例
RIPng process	RIPng进程号
Preference	RIPng路由优先级
Routing policy	路由策略
Fast-reroute	RIPng快速重路由
Checkzero	RIPng报文头部的零域检查功能：Enabled表示使能，Disabled表示未使能
Default cost	引入路由的缺省度量值
Maximum number of load balanced routes	等价路由的最大数目
Update time	Update定时器的值，单位为秒
Timeout time	Timeout定时器的值，单位为秒
Suppress time	Suppress定时器的值，单位为秒
Garbage-collect time	Garbage-collect定时器的值，单位为秒
Update output delay	接口发送RIPng报文的时间间隔，单位为毫秒
Output count	接口一次发送RIPng报文的最大个数
Graceful-restart interval	GR重启间隔时间，单位为秒
Triggered Interval	发送触发更新的时间间隔
Number of periodic updates sent	定时发送的RIPng更新报文的统计数量
Number of triggered updates sent	触发发送的RIPng更新报文的统计数量

1.1.4 display ripng database

display ripng database 命令用来显示指定 RIPng 进程发布数据库的所有激活路由。

【命令】

display ripng process-id database [ipv6-address prefix-length]

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

process-id: RIPng 进程号，取值范围为 1~65535。
ipv6-address prefix-length: 显示指定 IPv6 地址的激活路由信息。*ipv6-address* 表示 IPv6 地址；*prefix-length* 表示 IPv6 地址前缀长度，取值范围为 0~128。

【举例】

显示进程号为 1 的 RIPng 进程发布数据库中的激活路由。

```
<Sysname> display ripng 1 database
  1::/64,
    cost 0, RIPng-interface
  10::/32,
    cost 0, imported
  2::2/128,
    via FE80::20C:29FF:FE7A:E3E4, cost 1
```

表1-2 display ripng database 命令显示信息描述表

字段	描述
cost	度量值
RIPng-interface	从使能RIPng协议的接口学来的路由
imported	表示该条路由是从其它路由协议引入的
via	下一跳IPv6地址

1.1.5 display ripng graceful-restart

display ripng graceful-restart 命令用来显示 RIPng 进程的 GR 状态信息。

【命令】

display ripng [process-id] graceful-restart

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: RIPng 进程号，取值范围为 1~65535。

【举例】

显示 RIPng 1 进程的 GR 状态信息。
<Sysname> display ripng 1 graceful-restart
RIPng process: 1
Graceful Restart capability : Enabled
Current GR state : Normal
Graceful Restart period : 60 seconds
Graceful Restart remaining time: 0 seconds

表1-3 display ripng graceful-restart 命令显示信息描述表

字段	描述
RIPng process	RIPng进程号
Graceful Restart capability	GR使能状态 - Enabled: 使能了 GR 能力 - Disabled: 关闭了 GR 能力
Current GR state	当前GR所处状态 - Under GR: 进程正在 GR - Normal: 普通状态
Graceful Restart period	GR间隔
Graceful Restart remaining time	GR结束剩余时间

1.1.6 display ripng interface

display ripng interface 命令用来显示指定 RIPng 进程的接口信息。

【命令】

display ripng process-id interface [interface-type interface-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: RIPng 进程号，取值范围为 1~65535。
interface-type interface-number: 接口类型和编号。如果未指定本参数，则显示指定 RIPng 进程的所有接口信息。

【举例】

```
# 显示 RIPng 进程 1 的接口信息。
<Sysname> display ripng 1 interface
Total: 1

Interface: GigabitEthernet1/0/2
  Link-local address: FE80::20C:29FF:FEC8:B4DD
  Split-horizon: On           Poison-reverse: Off
  MetricIn: 0                 MetricOut: 1
  Default route: Off
  Update output delay: 20 (ms) Output count: 3
  Primary path detection mode: BFD echo
  Summary address:
    1::/16
```

表1-4 display ripng interface 命令显示信息描述表

字段	意义
Total	运行RIPng协议的接口总数
Interface	运行RIPng协议的接口的名称
Link-local address	运行RIPng协议的接口的链路本地地址
Split-horizon	是否使能了水平分割（On表示使能，Off表示关闭）
Poison-reverse	是否使能了毒性逆转（On表示使能，Off表示关闭）
MetricIn/MetricOut	接收/发送路由时添加的附加度量值

字段	意义
Default route	是否配置了发布缺省路由以及发布缺省路由的模式/取消发布缺省路由/缺省路由处于Garbage-collect时间: - 配置了发布缺省路由: 此时从接口发布缺省路由的模式有两种 Only/Originate。Only 表示从接口只发布缺省路由, Originate 表示同时发布缺省路由和其他 RIPng 路由。处于这种状态时, 路由器相应的显示: Default route: Only, 或者 Default route: Originate - 取消发布缺省路由: 表示当前没有配置发布缺省路由或者是取消发布默认路由后 Garbage-collect 已经超时, 此时接口不发送 RIPng 的缺省路由。处于这种状态时, 路由器显示: Default route: Off - 缺省路由正处于 Garbage-collect 时间: 取消发布缺省路由配置后, 缺省路由会进入 garbage-collection 状态, 此时从接口发送 metric 为 16 的缺省路由。处于这种状态时, 路由器显示: Default route: In garbage-collection status (xs)
Update output delay	接口发送RIPng报文的时间间隔, 单位为毫秒
Output count	接口一次发送RIPng报文的最大个数
Default route cost	RIPng接口下配置发布缺省路由的cost值
Primary path detection mode	主链路检测方式: BFD echo: BFD echo报文检测方式
Summary address	在接口配置的聚合的IPv6地址以及被聚合的路由的IPv6前缀

1.1.7 display ripng neighbor

display ripng neighbor 命令用来显示 RIPng 进程的邻居信息。

【命令】

display ripng process-id neighbor [interface-type interface-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: RIPng 进程号, 取值范围为 1~65535。

interface-type interface-number: 接口类型和编号。如果未指定本参数, 将显示 RIPng 的所有邻居信息。

【举例】

显示 RIPng 进程 1 的邻居信息。

```
<Sysname> display ripng 1 neighbor
```

```
Neighbor Address: FE80::230:FF:FE00:0
Interface   : GigabitEthernet1/0/1
Version     : RIPng version 1      Last update: 00h00m27s
Bad packets: 0                      Bad routes : 0
```

表1-5 display ripng neighbor 命令显示信息描述表

字段	描述
Neighbor Address	邻居接口的链路本地地址
Interface	邻居接口名称
Version	收到邻居RIPng报文的版本
Last update	上次收到邻居更新报文距离现在时间

1.1.8 display ripng non-stop-routing

display ripng non-stop-routing 命令用来显示 RIPng 进程的 NSR 状态信息。

【命令】

display ripng [process-id] non-stop-routing

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

process-id: RIPng 进程号，取值范围为 1~65535。

【举例】

```
# 显示 RIPng 1 进程的 NSR 状态信息。
<Sysname> display ripng 1 non-stop-routing
RIPng process: 1
Nonstop Routing capability: Enabled
Current NSR state          : Finish
```

表1-6 display ripng non-stop-routing 命令显示信息描述表

字段	描述
RIPng process	RIPng进程号
Nonstop Routing capability	NSR使能状态: - Enabled: 使能 NSR - Disabled: 不使能 NSR

字段	描述
Current NSR state	当前NSR所处状态: • Initialization: 初始准备 • Smooth: 数据平滑 • Advertising: 发布路由 • Redistribution: 路由引入处理 • Finish: 完成

1.1.9 display ripng route

display ripng route 命令用来显示指定 RIPng 进程的路由信息。

【命令】

display ripng process-id route [*ipv6-address prefix-length* [**verbose**] | **peer** *ipv6-address* | **statistics**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: RIPng 进程号，取值范围为 1~65535。

ipv6-address prefix-length: 显示指定 IPv6 地址的路由信息。*ipv6-address* 表示 IPv6 地址；*prefix-length* 表示 IPv6 地址前缀长度，取值范围为 0~128。

verbose: 显示当前 RIPng 路由表中的指定前缀路由的所有路由信息。如果未指定本参数，则只显示指定 IPv6 目的地址和前缀的最优 RIPng 路由。

peer ipv6-address: 显示从指定邻居学到的所有路由信息。

statistics: 显示路由的统计信息。路由的统计信息包括路由总数目，各个邻居的路由数目。

【举例】

显示进程号为 1 的 RIPng 进程的路由信息。

```
<Sysname> display ripng 1 route
Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
              O - Optimal, F - Flush to RIB
-----

Peer FE80::20C:29FF:FED4:7171 on GigabitEthernet1/0/2
Destination 4::4/128,
via FE80::20C:29FF:FED4:7171, cost 1, tag 0, AOF, 5 secs
```

```

Local route
Destination 3::3/128,
    via ::, cost 0, tag 0, DOF
Destination 6::/64,
    via ::, cost 0, tag 0, DOF
# 显示进程号为 1 的 RIPng 进程中指定地址 3::3/128 的所有路由信息。
<Sysname> display ripng 1 route 3::3 128 verbose
    Route Flags: A - Aging, S - Suppressed, G - Garbage-collect, D - Direct
                  O - Optimal, F - Flush to RIB
-----
Peer FE80::4283:59FF:FE97:205 on GigabitEthernet1/0/2
Destination 3::3/128,
    via FE80::4283:59FF:FE97:205, cost 1, tag 0, AOF, 28 secs

```

表1-7 display ripng route 命令显示信息描述表

字段	描述
A - Aging	此路由项处于老化状态
S - Suppressed	此路由项处于抑制状态
G - Garbage-collect	此路由项处于Garbage-collect状态
D - Direct	此路由项是RIPng生成的直连路由
Local route	RIPng本地生成的直连路由
O - Optimal	此路由项处于最优路由状态
F - Flush to RIB	此路由项已经被下刷到RIB
Peer	与接口相连的邻居
Destination	目的IPv6地址
via	下一跳IPv6地址
cost	度量值
tag	路由标签
secs	此路由项处于某种状态的时间

显示进程号为 1 的 RIPng 进程路由信息的统计计数。

```

<Sysname> display ripng 1 route statistics
Peer                               Optimal/Aging    Garbage
FE80::20C:29FF:FED4:7171          1/2              0
Local                              2/0              0
total                              3/2              0

```

表1-8 display ripng route statistics 命令显示信息描述表

字段	描述
Peer	RIPng邻居IPv6地址
Optimal	路由信息中处于最优路由状态的路由条数

字段	描述
Aging	路由信息中处于老化状态的路由条数
Garbage	路由信息中处于Garbage-collection状态的路由条数
Local	RIPng本地生成的直连路由条数的总和
total	从所有RIPng邻居学习到的路由条数的总和

1.1.10 fast-reroute

fast-reroute 命令用来配置 RIPng 快速重路由功能。

undo fast-reroute 命令用来关闭 RIPng 快速重路由功能。

【命令】

fast-reroute route-policy route-policy-name

undo fast-reroute

【缺省情况】

RIPng 快速重路由功能处于关闭状态。

【视图】

RIPng 视图

【缺省用户角色】

network-admin

context-admin

【参数】

route-policy route-policy-name：为通过策略的路由指定备份下一跳。
route-policy-name 为路由策略名，为 1~63 个字符的字符串，区分大小写。

【使用指导】

RIPng 快速重路由功能只适合在主链路三层接口 **up**，主链路由双通变为单通或者不通的情况下使用。在主链路三层接口 **down** 的情况下，本功能不可用。单通现象，即一条链路上的两端，有且只有一端可以收到另一端发来的报文，此链路称为单向链路。

RIPng 快速重路由功能仅对非迭代 RIPng 路由（即从直连邻居学到 RIPng 路由）有效。

等价路由不支持快速重路由功能。

【举例】

配置对通过策略 **frr** 的路由指定备份下一跳信息。

```
<Sysname> system-view
```

```
[Sysname] ipv6 prefix-list abc index 10 permit 100:: 64
```

```
[Sysname] route-policy frr permit node 10
```

```
[Sysname-route-policy-frr-10] if-match ipv6 address prefix-list abc
```

```
[Sysname-route-policy-frr-10] apply ipv6 fast-reroute backup-interface gigabitethernet 1/0/1 backup-nexthop FE80::8
```

```
[Sysname-route-policy-frr-10] quit
[Sysname] ripng 100
[Sysname-ripng-100] fast-reroute route-policy frr
```

1.1.11 filter-policy export

filter-policy export 命令用来配置 RIPng 对发布的路由信息进行过滤。

undo filter-policy export 命令用来取消 RIPng 对发布的路由信息进行过滤。

【命令】

```
filter-policy { ipv6-acl-number | prefix-list prefix-list-name } export
[ protocol [ process-id ] ]
undo filter-policy export [ protocol [ process-id ] ]
```

【缺省情况】

RIPng 不对发布的路由信息进行过滤。

【视图】

RIPng 视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-acl-number: 指定的基本或高级 IPv6 ACL 编号，用于对发布的路由信息进行过滤，取值范围为 2000～3999。

prefix-list prefix-list-name: 指定用于过滤发布路由信息的 IPv6 地址前缀列表名称。
prefix-list-name 为 1～63 个字符的字符串。

protocol: 被过滤路由信息的路由协议。

process-id: 被过滤路由信息的路由协议的进程号，取值范围为 1～65535。仅当路由协议为 ripng、ospfv3、isisv6 时需要指定进程号，若未指定，缺省进程号为 1。

【使用指导】

如果指定 *protocol* 参数，则只对从指定路由协议引入的路由信息进行过滤；否则将对所有要发布的路由信息进行过滤。

当配置的是高级 ACL（3000～3999）时，其使用规则如下：

- 使用命令 **rule [rule-id] { deny | permit } ipv6 source sour sour-prefix** 来过滤指定目的地址的路由。
- 使用命令 **rule [rule-id] { deny | permit } ipv6 source sour sour-prefix destination dest dest-prefix** 来过滤指定目的地址和前缀的路由。

其中，**source** 用来过滤路由目的地址，**destination** 用来过滤路由前缀，配置的前缀应该是连续的（当配置的前缀不连续时该过滤前缀的条件不生效）。

【举例】

用地址前缀列表过滤发布的 RIPng 更新报文。


```

<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100:1:: 32
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy prefix-list abc export
# 用编号为 3000 的 IPv6 高级 ACL 对发布的路由进行过滤，只允许 2001::1/128 通过。
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy 3000 export

```

1.1.12 filter-policy import

filter-policy import 命令用来配置 RIPng 对接收的路由信息进行过滤。

undo filter-policy import 命令用来恢复缺省情况。

【命令】

```

filter-policy { ipv6-acl-number | prefix-list prefix-list-name } import
undo filter-policy import

```

【缺省情况】

RIPng 不对接收的路由信息进行过滤。

【视图】

RIPng 视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-acl-number: 用于过滤接收的路由信息的 IPv6 ACL 编号，取值范围为 2000～3999。

prefix-list *prefix-list-name*: 指定用于过滤接收路由信息的 IPv6 地址前缀列表名称。
prefix-list-name 为 1～63 个字符的字符串。

【使用指导】

当配置的是高级 ACL（3000～3999）时，其使用规则如下：

- 使用命令 **rule [*rule-id*] { deny | permit } ipv6 source *sour* *sour-prefix*** 来过滤指定目的地址的路由。
- 使用命令 **rule [*rule-id*] { deny | permit } ipv6 source *sour* *sour-prefix* destination *dest* *dest-prefix*** 来过滤指定目的地址和前缀的路由。

其中，**source** 用来过滤路由目的地址，**destination** 用来过滤路由前缀，配置的前缀应该是连续的（当配置的前缀不连续时该过滤前缀的条件不生效）。

【举例】

```
# 用地址前缀列表过滤收到的 RIPng 更新报文。
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100:1:: 32
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy prefix-list abc import
# 使用编号为 3000 的 IPv6 高级 ACL 对接收的路由进行过滤，只允许 2001::1/128 通过。
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy 3000 import
```

1.1.13 graceful-restart

graceful-restart 命令用来使能 RIPng 协议的 GR 能力。

undo graceful-restart 命令用来关闭 RIPng 协议的 GR 能力。

【命令】

```
graceful-restart
undo graceful-restart
```

【缺省情况】

RIPng 协议的 GR 能力处于关闭状态。

【视图】

RIPng 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

RIPng GR 特性与 RIPng NSR 特性互斥，即 **graceful-restart** 和 **non-stop-routing** 命令互斥，不能同时配置。

【举例】

```
# 使能 RIPng 进程 1 的 GR 能力。
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] graceful-restart
```

1.1.14 graceful-restart interval

graceful-restart interval 命令用来配置 RIPng 协议的 GR 重启间隔时间。

undo graceful-restart interval 命令用来恢复缺省情况。

【命令】

```
graceful-restart interval interval  
undo graceful-restart interval
```

【缺省情况】

RIPng 协议的 GR 重启间隔时间为 60 秒。

【视图】

RIPng 视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval: 指定 RIPng 协议的 GR 重启间隔时间（期望重启时间），取值范围为 5~360，单位为秒。

【举例】

```
# 配置 RIPng 进程 1 平滑重启间隔时间为 200 秒。  
<Sysname> system-view  
[Sysname] ripng 1  
[Sysname-ripng-1] graceful-restart interval 200
```

1.1.15 import-route

import-route 命令用来从其它路由协议引入路由。

undo import-route 命令用来取消引入的外部路由信息。

【命令】

```
import-route { direct | static } [ cost cost-value | route-policy  
route-policy-name ] *  
undo import-route { direct | static }  
import-route { ospfv3 | ripng } [ process-id ] [ allow-direct | cost cost-value  
| route-policy route-policy-name ] *  
undo import-route { ospfv3 | ripng } [ process-id ]
```

【缺省情况】

RIPng 不引入其它路由。

【视图】

RIPng 视图

【缺省用户角色】

network-admin
context-admin

【参数】

direct: 引入直连路由。

ospfv3: 引入 OSPFv3 协议的路由。

ripng: 引入其他 RIPng 进程的路由。

static: 引入静态路由。

process-id: OSPFv3 或 RIPng 路由协议的进程号，取值范围为 1~65535，缺省值为 1。

allow-direct: 在引入的路由中包含使能了该协议的接口网段路由。如果未指定本参数，在引入协议路由时不会包含使能了该协议的接口网段路由。当 **allow-direct** 与 **route-policy route-policy-name** 参数一起使用时，需要注意路由策略中配置的匹配规则不要与接口路由信息存在冲突，否则会导致 **allow-direct** 配置失效。例如，当配置 **allow-direct** 参数引入 OSPFv3 直连时，在路由策略中不要配置 **if-match route-type** 匹配条件，否则，**allow-direct** 参数失效。

cost cost-value: 所要引入路由的度量值，取值范围为 0~16。如果没有指定度量值，则使用缺省度量值 0。

route-policy route-policy-name: 路由策略名称，*route-policy-name* 为 1~63 个字符的字符串，区分大小写。

【使用指导】

只能引入路由表中状态为 **active** 的路由，是否为 **active** 状态可以通过 **display ipv6 routing-table protocol** 命令来查看。

【举例】

```
# 引入 Ripng 协议（进程号 7）的路由信息，并将其度量值设置为 7。
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route ripng 7 cost 7
```

1.1.16 maximum load-balancing

maximum load-balancing 命令用来配置 RIPng 最大等价路由条数。

undo maximum load-balancing 命令用来恢复缺省情况。

【命令】

```
maximum load-balancing number
undo maximum load-balancing
```

【缺省情况】

RIPng 支持的等价路由的最大条数与系统支持最大等价路由的条数相同。

【视图】

RIPng 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

number：等价路由的最大条数，当 **number** 取值为 1 时，相当于不进行负载分担。

设备各款型中本参数的取值范围有所不同，详细差异信息如下：

型号	参数	取值范围
T5000-G20	等价路由的 最大条数	1~16
T5000-G30		1~32
T1000-G20/T1000-G50/T1000-G60/T1000-G80		1~16
T1000-CN60/T1000-CN80		1~32

【举例】

配置 RIPng 最大等价路由条数为 2。

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] maximum load-balancing 2
```

1.1.17 non-stop-routing

non-stop-routing 命令用来使能 RIPng 协议的 NSR 功能。

undo non-stop-routing 命令用来关闭 RIPng 协议的 NSR 功能。

【命令】

```
non-stop-routing
undo non-stop-routing
```

【缺省情况】

RIPng 协议的 NSR 功能处于关闭状态。

【视图】

RIPng 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

各个进程的 NSR 功能是相互独立的，只对本进程生效。如果存在多个 RIPng 进程，建议在各个进程下使能 RIPng NSR 功能。

RIPng NSR 特性与 RIPng GR 特性互斥，即 **non-stop-routing** 和 **graceful-restart** 命令互斥，不能同时配置。

【举例】

配置 RIPng 进程 1 使能 NSR 功能。

```
<Sysname> system-view
[Sysname] ripng 1
```

```
[Sysname-ripng-1] non-stop-routing
```

1.1.18 output-delay

output-delay 用来配置 RIPng 报文的发送速率。

undo output-delay 命令用来恢复缺省情况。

【命令】

```
output-delay time count count
```

```
undo output-delay
```

【缺省情况】

发送 RIPng 报文的时间间隔为 20 毫秒，一次最多发送 3 个 RIPng 报文。

【视图】

RIPng 视图

【缺省用户角色】

network-admin

context-admin

【参数】

time: 发送 RIPng 报文的时间间隔，取值范围为 10~100，单位为毫秒。

count: 一次发送 RIPng 报文的最大个数，取值范围为 1~30。

【使用指导】

如果全局和接口都进行了配置，以接口的配置为准。

【举例】

配置 RIPng 进程 1 发送 RIPng 报文的时间间隔为 60 毫秒，一次最多发送 10 个 RIPng 报文。

```
<Sysname> system-view
```

```
[Sysname] ripng 1
```

```
[Sysname-ripng-1] output-delay 60 count 10
```

【相关命令】

- **ripng output-delay**

1.1.19 preference

preference 命令用来配置 RIPng 路由的优先级。

undo preference 命令用来恢复缺省情况。

【命令】

```
preference { preference | route-policy route-policy-name } *
```

```
undo preference
```

【缺省情况】

RIPng 路由优先级的值为 100。

【视图】

RIPng 视图

【缺省用户角色】

network-admin

context-admin

【参数】

preference: RIPng 路由优先级的值，取值范围为 1~255。取值越小，优先级越高。

route-policy route-policy-name: 路由策略名称，*route-policy-name* 为 1~63 个字符的字符串，区分大小写。对满足特定条件的路由设置优先级。

【使用指导】

通过指定 **route-policy** 参数，可应用路由策略对特定的路由设置优先级：

- 如果在路由策略中已经设置了匹配路由的优先级，则匹配路由取路由策略设置的优先级，其它路由取 **preference** 命令所设优先级。
- 如果在路由策略中没有设置匹配路由的优先级，则所有路由都取 **preference** 命令所设优先级。

【举例】

```
# 配置 RIPng 路由的优先级为 120。
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] preference 120
```

1.1.20 reset ripng process

reset ripng process 命令用来重启指定 RIPng 进程。

【命令】

reset ripng process-id process

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: RIPng 进程号，取值范围为 1~65535。

【使用指导】

执行该命令后，系统提示用户确认是否重启 RIPng 协议。

【举例】

```
# 重启进程号为 100 的 RIPng 进程。
<Sysname> reset ripng 100 process
```

Reset RIPng process? [Y/N]:y

1.1.21 reset ripng statistics

reset ripng statistics 命令用来清除 RIPng 进程的统计信息。

【命令】

reset ripng process-id statistics

【视图】

用户视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: RIPng 进程号，取值范围为 1～65535。

【举例】

清除进程号为 100 的 RIPng 进程的统计信息。
<Sysname> reset ripng 100 statistics

1.1.22 ripng

ripng 命令用来启动 RIPng，并进入 RIPng 视图。

undo ripng 命令用来关闭 RIPng。

【命令】

ripng [*process-id*] [**vpn-instance** *vpn-instance-name*]
undo ripng [*process-id*]

【缺省情况】

系统没有运行 RIPng。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

process-id: RIPng 进程号，取值范围为 1～65535，缺省值为 1。

vpn-instance vpn-instance-name: 指定 RIPng 所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示 RIPng 位于公网中。

【使用指导】

必须先创建 RIPng 进程, 才能配置 RIPng 的各种全局性参数, 而配置与接口相关的参数时, 可以不受这个限制。

停止运行 RIPng 进程后, 原来配置的接口参数也同时失效。

【举例】

创建 RIPng 进程 100 并进入其视图。

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100]
```

1.1.23 ripng default-route

ripng default-route 命令用来以指定度量值向 RIPng 邻居发布一条缺省路由。

undo ripng default-route 命令用来禁止发布 RIPng 缺省路由和转发 IPv6 缺省路由。

【命令】

```
ripng default-route { only | originate } [ cost cost-value | route-policy
route-policy-name ] *
undo ripng default-route
```

【缺省情况】

RIPng 进程不发布缺省路由。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

only: 只发布 IPv6 缺省路由 (::/0), 抑制其它路由的发布。

originate: 发布 IPv6 缺省路由 (::/0), 但不影响其它路由的发布。

cost-value: 发布缺省路由的度量值, 取值范围为 1~15, 缺省值为 1。

route-policy route-policy-name: 路由策略名称, *route-policy-name* 为 1~63 个字符的字符串, 区分大小写。只有当前路由器的路由表中有路由匹配 *route-policy-name* 指定的路由策略时, 才发送缺省路由。

【使用指导】

通过该命令的设置, 生成的 RIPng 缺省路由将强制通过指定接口的路由更新报文发布出去。该 IPv6 缺省路由的发布不考虑其是否已经存在于 IPv6 路由表中。

配置发布缺省路由的 RIPng 接口不接收来自 RIPng 邻居的缺省路由。

【举例】

在接口 GigabitEthernet1/0/1 上配置 RIPng 只将缺省路由以更新报文的形式从接口发布。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng default-route only
```

在接口 GigabitEthernet1/0/1 上配置 RIPng 将缺省路由同其它路由一起以更新报文的形式从接口发布。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng default-route originate
```

1.1.24 ripng enable

ripng enable 命令用来在接口上使能 RIPng 功能。

undo ripng enable 命令用来在接口上关闭 RIPng 功能。

【命令】

```
ripng process-id enable
undo ripng enable
```

【缺省情况】

接口上的 RIPng 功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

process-id: RIPng 进程号，取值范围为 1~65535。

【举例】

在接口 GigabitEthernet1/0/1 上使能 RIPng 100。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng 100 enable
```

1.1.25 ripng metricin

ripng metricin 命令用来配置接口接收 RIPng 路由时的附加度量值。

undo ripng metricin 命令用来恢复缺省情况。

【命令】

```
ripng metricin value
undo ripng metricin
```

【缺省情况】

接口接收 RIPng 路由时的附加度量值为 0。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

value: 接收附加度量值，取值范围为 0～16。

【举例】

指定接口 GigabitEthernet1/0/1 在接收 RIPng 路由时的附加度量值为 12。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ripng metricin 12
```

1.1.26 ripng metricout

ripng metricout 命令用来配置接口发送 RIPng 路由时的附加度量值。

undo ripng metricout 命令用来恢复缺省情况。

【命令】

ripng metricout *value*

undo ripng metricout

【缺省情况】

接口发送 RIPng 路由时的附加度量值为 1。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

value: 发送附加度量值，取值范围为 1～16。

【举例】

设置接口 GigabitEthernet1/0/1 发送 RIPng 路由时添加的附加度量值为 12。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ripng metricout 12
```

1.1.27 ripng output-delay

ripng output-delay 命令用来配置接口下 RIPng 报文的发送速率。

undo ripng output-delay 命令用来恢复缺省情况。

【命令】

```
ripng output-delay time count count
undo ripng output-delay
```

【缺省情况】

RIPng 报文的发包速率由进程全局的配置决定。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

time: 接口发送 RIP 报文的时间间隔，取值范围为 10~100，单位为毫秒。

count: 接口一次发送 RIPng 报文的最大个数，取值范围为 1~30。

【使用指导】

如果全局和接口都进行了配置，以接口的配置为准。

【举例】

在接口 GigabitEthernet1/0/1 配置发送 RIPng 报文的时间间隔为 30 毫秒，一次最多发送 6 个 RIPng 报文。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng output-delay 30 count 6
```

【相关命令】

- **output-delay**

1.1.28 ripng poison-reverse

ripng poison-reverse 命令用来使能毒性逆转功能。

undo ripng poison-reverse 命令用来关闭毒性逆转功能。

【命令】

```
ripng poison-reverse
undo ripng poison-reverse
```

【缺省情况】

毒性逆转功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【举例】

在接口 GigabitEthernet1/0/1 上配置对 RIPng 更新报文进行毒性逆转。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng poison-reverse
```

1.1.29 ripng primary-path-detect bfd echo

ripng primary-path-detect bfd echo 命令用来使能 RIPng 协议中主用链路的 BFD（Echo 方式）检测功能。

undo ripng primary-path-detect bfd 命令用来关闭 RIPng 协议中主用链路的 BFD（Echo 方式）检测功能。

【命令】

ripng primary-path-detect bfd echo

undo ripng primary-path-detect bfd

【缺省情况】

RIPng 协议中主用链路的 BFD（Echo 方式）检测功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

echo：配置通过工作于 echo 报文方式的 BFD 会话对主用链路进行检测。

【使用指导】

配置本功能后，RIPng 协议的快速重路由特性中的主用链路将使用 BFD 进行检测。

【举例】

在接口 GigabitEthernet1/0/1 上配置 RIPng 协议快速重路由特性中主用链路使能 BFD（Echo 方式）检测功能。

```
<Sysname> system-view
[Sysname] ripng 1
[Sysname-ripng-1] fast-reroute route-policy frr
[Sysname-ripng-1] quit
[Sysname] bfd echo-source-ipv6 1::1
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng primary-path-detect bfd echo
```

1.1.30 ripng split-horizon

ripng split-horizon 命令用来使能水平分割功能。

undo ripng split-horizon 命令用来关闭水平分割。

【命令】

```
ripng split-horizon
undo ripng split-horizon
```

【缺省情况】

水平分割功能处于使能状态。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

通常情况下，为了防止路由环路的出现，水平分割都是必要的，因此，建议不要关闭水平分割。只是在某些特殊情况下，为保证协议的正确执行，需要关闭水平分割。在关闭水平分割时一定要确认是否必要。

如果同时使能了水平分割和毒性逆转，则只有毒性逆转功能生效。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上配置水平分割。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ripng split-horizon
```

1.1.31 ripng summary-address

ripng summary-address 命令用来配置 RIPng 在接口发布聚合的 IPv6 地址，并指定被聚合的路由的 IPv6 前缀。

undo ripng summary-address 命令用来禁止 RIPng 路由器发布聚合的 IPv6 地址。

【命令】

```
ripng summary-address ipv6-address prefix-length
undo ripng summary-address ipv6-address prefix-length
```

【缺省情况】

未配置 RIPng 在接口发布聚合的 IPv6 地址。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address: 聚合路由的目的 IPv6 地址。

prefix-length: 聚合路由的目的 IPv6 地址前缀长度，取值范围为 0~128。它指定地址中有多少连续的位组成 IPv6 网络前缀，即 IPv6 地址中的网络地址部分。

【使用指导】

如果一条路由的前缀和前缀长度与定义的 IPv6 前缀匹配，则这个自定义的 IPv6 前缀将取代原来的路由被发布出去。这样，多条路由将由一条路由所代替，而且，这条路由的度量值是原多条路由中最低的。

【举例】

在接口 GigabitEthernet1/0/1 上配置 IPv6 地址 2001:200::3EFF:FE11:6770，前缀长度为 64 位。通过 RIPng 聚合为 IPv6 地址前缀 2001:200::/35。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 address 2001:200::3EFF:FE11:6770/64
[Sysname-GigabitEthernet1/0/1] ripng summary-address 2001:200:: 35
```

1.1.32 timer triggered

timer triggered 命令用来配置触发更新的时间间隔。

undo timer triggered 命令用来恢复缺省情况。

【命令】

```
timer          triggered          maximum-interval          [ minimum-interval
[ incremental-interval ] ]
undo timer triggered
```

【缺省情况】

发送触发更新的最大时间间隔为 5 秒，最小间隔为 50 毫秒，增量惩罚间隔为 200 毫秒。

【视图】

RIPng 视图

【缺省用户角色】

network-admin

context-admin

【参数】

maximum-interval: 触发更新的最大间隔时间。取值范围为 1~5，单位为秒。

minimum-interval: 触发更新的最小间隔时间。取值范围为 10~5000，单位为毫秒。

incremental-interval: 触发更新间隔的增加时间。取值范围为 100~1000，单位为毫秒。

【使用指导】

本命令在网络变化不频繁的情况下将触发更新的时间间隔缩小到 *minimum-interval*，而在网络变化频繁的情况下可以进行相应惩罚，将时间间隔按照配置的惩罚增量延长，最大不超过 *maximum-interval*。

minimum-interval 和 *incremental-interval* 配置值不允许大于 *maximum-interval* 配置值。

【举例】

配置发送触发更新的最大时间间隔为 2 秒，最小时间间隔为 100 毫秒，惩罚增量为 100 毫秒。

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] timer triggered 2 100 100
```

1.1.33 timers

timers 命令用来配置 RIPng 定时器的值。

undo timers 命令用来恢复 RIPng 定时器的缺省值。

【命令】

```
timers { garbage-collect garbage-collect-value | suppress suppress-value |  
timeout timeout-value | update update-value } *  
undo timers { garbage-collect | suppress | timeout | update } *
```

【缺省情况】

Garbage-collect 定时器的值为 120 秒，Suppress 定时器的值为 120 秒，Timeout 定时器的值为 180 秒，Update 定时器的值为 30 秒。

【视图】

RIPng 视图

【缺省用户角色】

network-admin
context-admin

【参数】

garbage-collect-value: Garbage-collect 定时器的值，取值范围为 1~86400，单位为秒。

suppress-value: Suppress 定时器的值，取值范围为 0~86400，单位为秒。

timeout-value: Timeout 定时器的值，取值范围为 1~86400，单位为秒。

update-value: Update 定时器的值，取值范围为 1~86400，单位为秒。

【使用指导】

RIPng 受四个定时器的控制，分别是 Update、Timeout、Suppress 和 Garbage-collect，其中：

- Update 定时器，定义了发送更新报文的时间间隔。

- **Timeout** 定时器，定义了路由老化时间。如果在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16。
- **Suppress** 定时器，定义了 RIPng 路由处于抑制状态的时间段长度。当一条路由的度量值变为 16 时，该路由将进入被抑制状态。在被抑制状态，只有来自同一邻居，且度量值小于 16 的路由更新才会被路由器接收，取代不可达路由。
- **Garbage-collect** 定时器，定义了一条路由从度量值变为 16 开始，直到它从路由表里被删除所经过的时间。在 **Garbage-collect** 时间内，RIPng 以 16 作为度量值向外发送这条路由的更新，如果 **Garbage-collect** 超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除。

通常情况下，无需改变各定时器的缺省值，该命令须谨慎使用。

各个定时器的值在网络中所有的路由器上必须保持一致。

【举例】

分别设置 RIPng 进程 1 各定时器的值：其中，Update 定时器的值为 5 秒、Timeout 定时器的值为 15 秒、Suppress 定时器的值为 15 秒、Garbage-collect 定时器的值为 30 秒。

```
<Sysname> system-view
```

```
[Sysname] ripng 1
```

```
[Sysname-ripng-1] timers update 5 timeout 15 suppress 15 garbage-collect 30
```

目 录

1 OSPFv3	1-1
1.1 OSPFv3 配置命令	1-1
1.1.1 abr-summary (OSPFv3 area view)	1-1
1.1.2 area	1-2
1.1.3 asbr-summary (OSPFv3 view)	1-2
1.1.4 bandwidth-reference (OSPFv3 view)	1-3
1.1.5 default tag	1-4
1.1.6 default-cost (OSPFv3 area view)	1-5
1.1.7 default-route-advertise (OSPFv3 view)	1-6
1.1.8 display ospfv3	1-7
1.1.9 display ospfv3 abr-asbr	1-14
1.1.10 display ospfv3 abr-summary	1-15
1.1.11 display ospfv3 asbr-summary	1-17
1.1.12 display ospfv3 event-log	1-19
1.1.13 display ospfv3 graceful-restart	1-22
1.1.14 display ospfv3 interface	1-27
1.1.15 display ospfv3 lsdb	1-30
1.1.16 display ospfv3 nexthop	1-34
1.1.17 display ospfv3 non-stop-routing	1-35
1.1.18 display ospfv3 peer	1-36
1.1.19 display ospfv3 request-queue	1-39
1.1.20 display ospfv3 retrans-queue	1-41
1.1.21 display ospfv3 routing	1-42
1.1.22 display ospfv3 spf-tree	1-44
1.1.23 display ospfv3 statistics	1-48
1.1.24 display ospfv3 vlink	1-52
1.1.25 event-log	1-54
1.1.26 fast-reroute (OSPFv3 view)	1-54
1.1.27 filter (OSPFv3 area view)	1-55
1.1.28 filter-policy export (OSPFv3 view)	1-56
1.1.29 filter-policy import (OSPFv3 view)	1-57
1.1.30 graceful-restart enable	1-59
1.1.31 graceful-restart helper enable	1-60

1.1.32 graceful-restart helper strict-lsa-checking	1-60
1.1.33 graceful-restart interval.....	1-61
1.1.34 import-route (OSPFv3 view)	1-62
1.1.35 log-peer-change	1-63
1.1.36 lsa-generation-interval.....	1-64
1.1.37 maximum load-balancing (OSPFv3 view)	1-65
1.1.38 non-stop-routing	1-66
1.1.39 nssa (OSPFv3 area view)	1-66
1.1.40 ospfv3	1-68
1.1.41 ospfv3 area	1-69
1.1.42 ospfv3 bfd enable.....	1-69
1.1.43 ospfv3 cost	1-70
1.1.44 ospfv3 dr-priority	1-71
1.1.45 ospfv3 fast-reroute lfa-backup exclude.....	1-71
1.1.46 ospfv3 mib-binding	1-72
1.1.47 ospfv3 mtu-ignore	1-73
1.1.48 ospfv3 network-type	1-73
1.1.49 ospfv3 peer	1-74
1.1.50 ospfv3 prefix-suppression	1-75
1.1.51 ospfv3 primary-path-detect bfd	1-76
1.1.52 ospfv3 timer dead	1-77
1.1.53 ospfv3 timer hello.....	1-77
1.1.54 ospfv3 timer poll	1-78
1.1.55 ospfv3 timer retransmit.....	1-79
1.1.56 ospfv3 trans-delay.....	1-80
1.1.57 preference	1-81
1.1.58 prefix-suppression.....	1-81
1.1.59 reset ospfv3 event-log	1-82
1.1.60 reset ospfv3 process.....	1-83
1.1.61 reset ospfv3 redistribution	1-84
1.1.62 reset ospfv3 statistics.....	1-84
1.1.63 router-id	1-84
1.1.64 silent-interface (OSPFv3 view)	1-85
1.1.65 snmp context-name	1-86
1.1.66 snmp trap rate-limit.....	1-87
1.1.67 snmp-agent trap enable ospfv3	1-87

1.1.68 spf-schedule-interval.....	1-89
1.1.69 stub (OSPFv3 area view).....	1-89
1.1.70 stub-router.....	1-90
1.1.71 transmit-pacing.....	1-91
1.1.72 vlink-peer (OSPFv3 area view).....	1-92

1 OSPFv3

1.1 OSPFv3配置命令

1.1.1 abr-summary (OSPFv3 area view)

abr-summary 命令用来配置 ABR 路由聚合。

undo abr-summary 命令用来取消 ABR 对指定网段的路由聚合。

【命令】

```
abr-summary ipv6-address prefix-length [ not-advertise ] [ cost cost-value ]  
undo abr-summary ipv6-address prefix-length
```

【缺省情况】

ABR 不对路由进行聚合。

【视图】

OSPFv3 区域视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address: 聚合路由的目的 IPv6 地址。

prefix-length: 聚合路由的目的 IPv6 地址前缀长度，取值范围为 0~128。它指定地址中有多少连续的位组成 IPv6 网络前缀，即 IPv6 地址中的网络地址部分。

not-advertise: 不通告聚合的 IPv6 路由。如果未指定本参数，则通告聚合的 IPv6 路由。

cost cost-value: 聚合路由的开销值，取值范围为 1~16777215，缺省值为所有被聚合的路由中最大的开销值。

【使用指导】

本命令只适用于 ABR，用来对当前区域进行路由聚合。对于落入该聚合网段的路由，ABR 向其它区域只发送一条聚合后的路由。一个区域可配置多条聚合网段，这样 OSPFv3 可对多个网段进行聚合。

当配置了 **undo abr-summary** 命令后，原来被聚合的路由将重新被发布。

【举例】

将 OSPFv3 区域 1 中两条路由 2000:1:1:1::/64、2000:1:1:2::/64 的路由聚合成一条前缀 2000:1:1::/48 向其它区域发送。

```
<Sysname> system-view  
[Sysname] ospfv3 1  
[Sysname-ospfv3-1] area 1  
[Sysname-ospfv3-1-area-0.0.0.1] abr-summary 2000:1:1:: 48
```

1.1.2 area

area 命令用来创建 OSPFv3 区域，并进入区域视图。

undo area 命令用来删除指定的 OSPFv3 区域。

【命令】

area *area-id*

undo area *area-id*

【缺省情况】

不存在 OSPFv3 区域。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

area-id: 区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其处理成 IPv4 地址格式）或 IPv4 地址格式。

【举例】

进入 OSPFv3 区域 0 视图。

```
<Sysname> system-view
```

```
[Sysname] ospfv3 1
```

```
[Sysname-ospfv3-1] area 0
```

```
[Sysname-ospfv3-1-area-0.0.0.0]
```

1.1.3 asbr-summary (OSPFv3 view)

asbr-summary 命令用来配置 ASBR 路由聚合。

undo asbr-summary 命令用来取消 ASBR 对指定网段的路由聚合。

【命令】

asbr-summary *ipv6-address prefix-length* [**cost** *cost-value* | **not-advertise** | **nssa-only** | **tag** *tag*] *

undo asbr-summary *ipv6-address prefix-length*

【缺省情况】

ASBR 不对引入的路由进行聚合。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address: 聚合路由的目的 IPv6 地址。

prefix-length: 聚合路由的目的 IPv6 地址前缀长度，取值范围为 0~128。它指定地址中有多少连续的位组成 IPv6 网络前缀，即 IPv6 地址中的网络地址部分。

cost cost-value: 聚合路由的开销，取值范围为 1~16777214。如果未指定本参数，**cost-value** 取所有被聚合的路由中最大的开销值作为聚合路由的开销；如果是 Type-7 LSA 转化成的 Type-5 LSA 描述的路由匹配聚合、且是 Type2 外部路由，则 **cost-value** 取所有被聚合的路由中最大的开销值加 1 作为聚合路由的开销。

not-advertise: 不通告聚合路由。如果未指定本参数，将通告聚合路由。

nssa-only: 设置 Type-7 LSA 的 P 比特位为不置位，即在对端路由器上不能转为 Type-5 LSA。缺省时，Type-7 LSA 的 P 比特位被置位，即在对端路由器上可以转为 Type-5 LSA（如果本地路由器是 ABR，则会检查骨干区域是否存在 FULL 状态的邻居，当 FULL 状态的邻居存在时，产生的 Type-7 LSA 中 P 比特位不置位）。

tag tag: 聚合路由的标记，取值范围为 0~4294967295。

【使用指导】

如果本地路由器是 ASBR，对引入的聚合地址范围内的 Type-5 LSA 描述的路由进行聚合；当配置了 NSSA 区域时，对引入的聚合地址范围内的 Type-7 LSA 描述的路由进行聚合。

如果本地路由器同时是 ASBR 和 ABR，并且是 NSSA 区域的转换路由器，则对由 Type-7 LSA 转化成的 Type-5 LSA 描述的路由进行聚合处理；如果不是 NSSA 区域的转换路由器，则不进行聚合处理。

配置 **asbr-summary** 命令后，对处于聚合地址范围内的外部路由，本地路由器只向邻居路由器发布一条聚合后的路由；配置 **undo asbr-summary** 命令后，原来被聚合的外部路由将重新被发布。

【举例】

```
# 配置 OSPFv3 进程 1 对引入的路由进行聚合，聚合路由为 2000::/16，开销值为 100，标记为 2。
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] asbr-summary 2000:: 16 cost 100 tag 2
```

1.1.4 bandwidth-reference (OSPFv3 view)

bandwidth-reference 命令用来配置计算链路开销时所依据的带宽参考值。

undo bandwidth-reference 命令用来恢复缺省情况。

【命令】

```
bandwidth-reference value
undo bandwidth-reference
```

【缺省情况】

计算链路开销时所依据的带宽参考值为 100Mbps。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

value: 计算链路开销时所依据的带宽参考值，取值范围为 1~4294967，单位为 Mbps。

【使用指导】

OSPFv3 有两种方式来配置接口的开销值，第一种方法是在接口视图下直接配置开销值；第二种方法是配置接口的带宽参考值，OSPFv3 根据带宽参考值自动计算接口的开销值，计算公式为：接口开销=带宽参考值÷接口带宽，当计算出来的开销值大于 65535，开销取最大值 65535；当计算出来的开销值小于 1 时，开销取最小值 1。

如果没有在接口视图下显式的配置此接口的开销值，OSPFv3 会根据该接口的带宽自动计算其开销值。

【举例】

配置计算链路开销时所依据的带宽参考值为 1000Mbps。

```
<Sysname> system-view
```

```
[Sysname] ospfv3 1
```

```
[Sysname-ospfv3-1] bandwidth-reference 1000
```

1.1.5 default tag

default tag 命令用来配置引入外部路由的全局标记。

undo default tag 命令用来恢复缺省情况。

【命令】

default tag tag

undo default tag

【缺省情况】

引入外部路由的全局标记为 1。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

tag: 外部路由的全局标记，取值范围为 0~4294967295。

【使用指导】

如果在配置 **default-route-advertise**、**import-route** 和 **route-tag** 命令时没有指定标记，则缺省使用本命令配置的全局标记。

【举例】

配置 OSPFv3 引入外部路由的标记为 2。

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default tag 2
```

【相关命令】

- **default-route-advertise** (OSPFv3 view)
- **import-route**

1.1.6 default-cost (OSPFv3 area view)

default-cost 命令用来配置发送到 Stub 区域或 NSSA 区域的缺省路由的开销。

undo default-cost 命令用来恢复缺省情况。

【命令】

```
default-cost cost
undo default-cost
```

【缺省情况】

发送到 Stub 区域或 NSSA 区域的缺省路由的开销为 1。

【视图】

OSPFv3 区域视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

cost：发送到 Stub 区域或 NSSA 区域的缺省路由的开销，取值范围为 0~16777214。

【使用指导】

该命令只有在 Stub 区域的 ABR 或 NSSA 区域的 ABR/ASBR 上配置才能生效。

【举例】

将 OSPFv3 区域 1 设置为 Stub 区域，使发送到该 Stub 区域的缺省路由开销为 60。

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
[Sysname-ospfv3-1-area-0.0.0.1] default-cost 60
```

【相关命令】

- **nssa** (OSPFv3 area view)
- **stub** (OSPFv3 area view)

1.1.7 default-route-advertise (OSPFv3 view)

default-route-advertise 命令用来将缺省路由引入到 OSPFv3 路由区域。

undo default-route-advertise 命令用来恢复缺省情况。

【命令】

```
default-route-advertise [ [ always | permit-calculate-other ] | cost  
cost-value | route-policy route-policy-name | tag tag | type type ] *  
undo default-route-advertise
```

【缺省情况】

未引入缺省路由。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

always: 如果当前路由器的路由表中没有缺省路由，使用此参数可产生一个描述缺省路由的 AS-external-LSA 发布出去。如果没有指定该关键字，仅当本地路由器的路由表中存在缺省路由时，才可以产生一个描述缺省路由的 AS-external-LSA 发布出去。

permit-calculate-other: 当路由器产生并发布了一个描述缺省路由的 AS-external-LSA 时，指定此参数的路由器仍然会计算来自于其他路由器的缺省路由，未指定此参数的路由器不再计算来自其他路由器的缺省路由。当路由器没有产生一个描述缺省路由的 AS-external-LSA 时，无论是否指定此参数，路由器都会计算来自其他路由器的缺省路由。

cost *cost-value*: 该缺省路由的度量值，取值范围为 0~16777214，缺省值为 1。

route-policy *route-policy-name*: 路由策略名，为 1~63 个字符的字符串，区分大小写。只有当前路由器的路由表中存在缺省路由，并且有路由匹配 *route-policy-name* 指定的路由策略，才可以产生一个描述缺省路由的 AS-external-LSA 发布出去，指定的路由策略会影响 AS-external-LSA 中的值。如果同时指定 **always** 参数，不论当前路由器的路由表中是否有缺省路由，只要有路由匹配指定的路由策略，就将产生一个描述缺省路由的 AS-external-LSA 发布出去，指定的路由策略会影响 AS-external-LSA 中的值。

tag *tag*: 外部路由的标记，取值范围为 0~4294967295。如果未指定本参数，将根据 **default tag** 命令的配置进行取值。

type *type*: 该 AS-external-LSA 的类型，取值范围为 1~2，缺省值为 2。

【使用指导】

使用 **import-route** 命令不能引入缺省路由，如果要引入缺省路由，必须使用本命令。当本地路由器的路由表中没有缺省路由时，要产生一个描述缺省路由的 AS-external-LSA 应使用 **always** 关键字。

【举例】

将产生的缺省路由引入到 OSPFv3 自治系统中（本地路由器没有缺省路由）。

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default-route-advertise always
```

【相关命令】

- **import-route** (OSPFv3 area view)

1.1.8 display ospfv3

display ospfv3 命令用来显示 OSPFv3 的进程信息。

【命令】

display ospfv3 [*process-id*] [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程的概要信息。

verbose: 显示 OSPFv3 进程的详细信息。如果未指定本参数，将显示 OSPFv3 进程的概要信息。

【举例】

显示所有 OSPFv3 进程的详细信息。

```
<Sysname> display ospfv3 verbose
```

```
OSPFv3 Process 1 with Router ID 1.1.1.1
```

```
RouterID: 1.1.1.1          Router type:  ABR  ASBR  NSSA
Route tag: 0
Route tag check: Disabled
Multi-VPN-Instance: Disabled
Type value of extended community attributes:
  Domain ID : 0x0005
  Route type: 0x0306
```

Router ID : 0x0107
Domain-id: 0.0.0.0
DN-bit check: Enabled
DN-bit set: Enabled
Originating router-LSAs with maximum metric
 Condition: On startup for 600 seconds, State: Inactive
 Advertise summary-LSAs with metric 16711680
 Advertise external-LSAs with metric 16711680
 Advertise intra-area-prefix-LSAs with maximum metric
SPF-schedule-interval: 5 50 200
LSA generation interval: 5
LSA arrival interval: 1000
Transmit pacing: Interval: 20 Count: 3
Default ASE parameters: Tag: 1
Route preference: 10
ASE route preference: 150
FRR backup mode: LFA
SPF calculation count: 0
External LSA count: 0
LSA originated count: 0
LSA received count: 0
SNMP trap rate limit interval: 10 Count: 7
Area count: 2 Stub area count: 0 NSSA area count: 1
ExChange/Loading neighbors: 0
Max equal cost paths: 32
Up interfaces: 1
Full neighbors: 1
Normal areas with up interfaces: 1
Calculation trigger type: Full
Current calculation type: SPF calculation
Current calculation phase: Calculation area topology
Redistribute timer: Off
Redistribute schedule type: RIB
Redistribute route count: 0
Process reset state: N/A
Current reset type: N/A
Next reset type: N/A
Reset prepare message replied: -/-/-/-
Reset process message replied: -/-/-/-
Reset phase of module:
 M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.0
Area flag: Normal
SPF scheduled count: 0
ExChange/Loading neighbors: 0
LSA count: 0
Keychain authentication: Enabled (chris)

Up interfaces: 0
 MTU: 1440
 Default cost: 1
 Created by Vlink
 Process reset state: N/A
 Current reset type: N/A
 Reset prepare message replied: -/-/-/-
 Reset process message replied: -/-/-/-
 Reset phase of module:
 M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.2
 Area flag: Normal
 SPF scheduled count: 0
 ExChange/Loading neighbors: 0
 LSA count: 0
 Up interfaces: 1
 MTU: 1500
 Default cost: 1
 Process reset state: N/A
 Current reset type: N/A
 Reset prepare message replied: -/-/-/-
 Reset process message replied: -/-/-/-
 Reset phase of module:
 M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

Area: 0.0.0.3
 Area flag: NSSA
 7/5 translator state: Disabled
 7/5 translate stability timer interval: 0
 SPF Scheduled Count: 0
 ExChange/Loading neighbors: 0
 LSA Count: 0
 Up interfaces: 0
 MTU: 1440
 Default cost: 1
 Process reset flag: N/A
 Current reset type: N/A
 Reset prepare message replied: -/-/-/-
 Reset process message replied: -/-/-/-
 Reset phase of module:
 M-N/A, P-N/A, S-N/A, C-N/A, R-N/A

表1-1 display ospfv3 verbose 命令显示信息描述表

字段	描述
OSPFv3 Process 1 with Router ID 1.1.1.1	OSPFv3进程是1， Router ID是1.1.1.1
RouterID	本路由器的Router ID

字段	描述
Router type	路由器类型，取值为： - ABR 表示区域边界路由器 - ASBR 表示自治系统边界路由器 - NSSA 表示支持 NSSA 区域 为空表示非上面三种情况
Route tag	当前进程引入外部路由的缺省标记
Route tag check	当前进程是否使能检查OSPFv3 LSA的标记
Multi-VPN-Instance	当前进程对多VPN实例的支持情况： - Multi-VPN-Instance: Disabled 表示不支持多 VPN 实例 - Multi-VPN-instance: Enabled 表示支持多 VPN 实例
Type value of extended community attributes	OSPFv3扩展团体属性的类型编码
Domain-id	OSPFv3域标识符
DN-bit check	当前进程是否使能检查OSPFv3 LSA的DN位
DN-bit set	当前进程是否使能设置OSPFv3 LSA的DN位
Originating router-LSAs with maximum metric/Originating router-LSAs with R-bit clear	Router LSA中使用最大开销值发布/Router LSA中清除R-bit
Condition	Stub路由器的状态： - Always 代表始终生效 - On startup for XXX seconds 代表重启后生效时间
State	Stub路由器是否生效： - Active 表示生效 - Inactive 表示不生效
Advertise summary-LSAs with metric	Summary LSA发布使用的开销值
Advertise external-LSAs with metric	外部LSA发布使用的开销值
Advertise intra-area-prefix-LSAs with maximum metric	Intra-area-prefix-LSA发布使用的开销值
SPF-schedule-interval	进行SPF计算的时间间隔
LSA generation interval	LSA生成时间间隔
LSA arrival interval	LSA重复到达的最小时间间隔
Transmit pacing	接口发送LSU报文的速率，其中： - Interval 表示接口发送 LSU 报文的时间间隔 - Count 表示接口一次发送 LSU 报文的最大个数
Default ASE parameters	引入外部路由的缺省参数值，其中Tag代表路由标记
Route preference	内部路由优先级
ASE route preference	外部路由优先级

字段	描述
FRR backup mode	指定快速重路由的备份下一跳地址的方式： - LFA: 为所有路由通过 LFA (Loop Free Alternate) 算法选取备份下一跳信息。如果显示为 LFA ABR-only, 则表示只有到 ABR 设备的路由才能够通过 LFA 算法被选取为备份路径。 - route-policy <i>route-policy-name</i>: 为通过策略的路由指定备份下一跳, <i>route-policy-name</i> 为路由策略名
SPF calculation count	OSPFv3进程的路由计算总数
External LSA count	外部LSA数目, 其中: - Count: LSA 数目 - checksum Sum: 校验和
LSA originated count	产生的LSA数目
LSA received count	接收的LSA数目
SNMP trap rate limit interval: 10 Count: 7	OSPFv3在10内秒允许输出7条告警信息
Area count	区域总数目
Stub area count	Stub区域数目
NSSA area count	NSSA区域数目
ExChange/Loading neighbors	处于ExChange/Loading状态的邻居数
Calculation trigger type	触发路由计算的类型, 具体如下: - Full: 触发全部路由计算 - Area topology change: 区域拓扑改变触发路由计算 - Intra router change: 增量的区域内路由器路由变化 - ASBR change: 增量的 ASBR 路由变化 - Full IP prefix: 触发全部 IP 前缀计算 - Full intra AS: 触发全部 AS 内部前缀计算 - Inc intra AS: 触发增量 AS 内部前缀计算 - Full inter AS: 触发全部 AS 外部前缀计算 - Inc inter AS: 触发增量 AS 外部前缀计算 - Nextthop calculation: 触发下一跳计算 - N/A: 未触发计算

字段	描述
Current calculation type	当前路由计算的类型，具体如下： • SPF calculation: 进行区域 SPF 计算 • Intra router calculation: 区域内路由器路由计算 • ASBR calculation: 区域间 ASBR 路由计算 • Inc intra router: 增量区域内路由器路由计算 • Inc ASBR calculation: 增量区域间 ASBR 路由计算 • Full intra AS: 进行全部 AS 内部前缀计算 • Inc intra AS: 进行增量 AS 内部前缀计算 • Full inter AS: 进行全部 AS 外部前缀计算 • Inc inter AS: 进行增量 AS 外部前缀计算 • N/A: 未触发计算
Current calculation phase	当前路由计算调度运行到的阶段，具体如下： • Calculation area topology: 计算区域拓扑 • Calculation router: 计算路由器路由 • Calculation intra AS: 计算 AS 内部路由 • Calculation ASBR: 计算 ASBR 路由 • Calculation inter AS: 计算 AS 外部路由 • Calculation end: 计算收尾阶段 • N/A: 未触发计算
Redistribute timer	引入路由定时器，其中： • Off: 关闭 • On: 开启
Redistribute schedule type	引入路由调度类型，其中： • RIB: 触发遍历 RIB 表进行引入 • Self: 触发遍历自身引入表进行引入 N/A: 未触发引入
Redistribute route count	引入路由计数
Process reset state	进程重启状态标志，具体如下： • N/A: 进程未重启 • Under reset: 进程正在重启 • Under RIB smooth: 进程正在同步 RIB 路由
Current reset type	当前进程重启类型，具体如下： • N/A: 进程未重启 • GR quit: GR 异常退出进行普通重启 • Delete: 删除 OSPFv3 进程 • Undo router-id: 删除 Router-id • Set router-id: 设置 Router-id

字段	描述
Next reset type	即将调度进程重启类型，具体如下： • N/A: 进程未重启 • GR quit: GR 异常退出进行普通重启 • Delete: 删除 OSPFv3 进程 • Undo router-id: 删除 Router-id • Set router-id: 设置 Router-id
Reset prepare message replied	响应准备重启消息的模块，具体如下： • P 代表邻居维护模块 • S 代表 LSDB 同步模块 • C 代表路由计算模块 • R 代表路由引入模块
Reset process message replied	响应进程重启消息的模块，具体如下： • P 代表邻居维护模块 • S 代表 LSDB 同步模块 • C 代表路由计算模块 • R 代表路由引入模块
Reset phase of module	各模块所处重启阶段。其中M代表主控制模块，P代表邻居维护模块，S代表LSDB同步模块，其阶段有： • N/A: 未重启 • Delete ASE: 删除所有 ASE LSA • Delete area LSA: 删除区域相关 LSA • Delete area IF: 删除区域下接口 • C 代表路由计算模块，其阶段有： • N/A: 未重启 • Delete topology: 删除区域拓扑 • Delete router: 删除路由器路由 • Delete intra AS: 删除 AS 内部路由 • Delete inter AS: 删除 AS 外部路由 • Delete ASBR: 删除 ASBR 路由 • R 代表路由引入模块，其阶段有： • N/A: 未重启 • Delete import: 删除引入路由
Area	区域信息
Area flag	区域类型
SPF scheduled count	OSPF区域的路由计算总数
LSA count	LSA数目，其中： • Count: LSA 数目 • checksum Sum: 校验和

字段	描述
Keychain authentication: Enabled (test)	OSPFv3区域采用keychain验证模式，keychain名称为test
MTU	区域的MTU值
Default cost	路由的缺省开销值
Created by Vlink	区域由Vlink创建
7/5 translator state	Type-7 LSA转换为Type-5 LSA的转换者状态，取值为： - Enabled: 表示本设备是通过命令指定的 Type-7 LSA 转换为 Type-5 LSA 的转换者 - Elected: 表示本设备是通过选举指定的 Type-7 LSA 转换为 Type-5 LSA 的转换者 - Disabled: 表示本设备不是 Type-7 LSA 转换为 Type-5 LSA 的转换者
7/5 translate stability timer interval	Type-7 LSA转换为Type-5 LSA转换稳定定时器的超时时间间隔，单位为秒

1.1.9 display ospfv3 abr-asbr

display ospfv3 abr-asbr 命令用来显示到 OSPFv3 的区域边界路由器和自治系统边界路由器的路由信息。

【命令】

display ospfv3 [process-id] abr-asbr

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程下到区域边界路由器和自治系统边界路由器的路由信息。

【举例】

显示所有 OSPFv3 进程的 ABR 和 ASBR 路由。

```
<Sysname> display ospfv3 abr-asbr
```

```
OSPFv3 Process 1 with Router ID 1.1.1.1
```

```
Destination : 1.1.1.2
Area        : 0.0.0.0
```

```
Rtr Type : ABR
Path Type: Intra
```

```

Interface      : GE2/0/2
NextHop        : FE80:1:1::1
BkNextHop      : FE80:1:2::2
Cost           : 1

Destination    : 1.1.1.3
Area           : 0.0.0.0
Interface      : GE2/0/3
NextHop        : FE80:2:1::1
BkNextHop      : FE80:1:2::4
Cost           : 1

Rtr Type       : ASBR
Path Type      : Intra
BkInterface    : GE2/0/4

```

表1-2 display ospfv3 abr-asbr 命令显示信息描述表

字段	描述
OSPFv3 Process 1 with Router ID 1.1.1.1	OSPFv3进程是1，Router ID是1.1.1.1
Destination	ABR或ASBR的路由器ID
Rtr Type	路由器类型，包括ABR和ASBR
Area	下一跳地址所在的区域ID
Path Type	到ABR或ASBR的路由类型，取值为： • Intra 表示区域内路由 • Inter 表示区域间路由
Interface	路由出接口
BkInterface	备份出接口
NextHop	下一跳地址
BkNextHop	备份下一跳地址
Cost	从本路由器到达ABR或ASBR的开销

1.1.10 display ospfv3 abr-summary

display ospfv3 abr-summary 命令用来显示 OSPFv3 的 ABR 聚合信息。

【命令】

```
display ospfv3 [ process-id ] [ area area-id ] abr-summary [ ipv6-address
prefix-length ] [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin

```

context-operator

【参数】

process-id: 当前的聚合配置所在进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程的 ABR 聚合信息。

area area-id: 显示位于指定区域的 ABR 聚合信息。如果未指定本参数，将显示所有区域的 ABR 聚合信息。**area-id** 为区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其处理成 IPv4 地址格式）或 IPv4 地址格式。

ipv6-address prefix-length: 显示指定 IPv6 地址的 ABR 聚合信息。**ipv6-address** 表示 IPv6 地址前缀；**prefix-length** 表示 IPv6 地址前缀长度，取值范围为 0~128。如果未指定本参数，将显示所有 ABR 聚合信息。

verbose: 显示 ABR 聚合详细信息。如果未指定本参数，将显示 ABR 聚合的概要信息。

【举例】

显示 OSPFv3 进程 1 的 ABR 聚合信息。
<Sysname> display ospfv3 1 abr-summary

```
OSPFv3 Process 1 with Router ID 2.2.2.2

          Area: 1.1.1.1
Total summary addresses: 1

Prefix      : 1000:4::/32
Status      : Advertise
NULL0       : Active
Cost        : 1 (Configured)
Routes count: 2
```

表1-3 display ospfv3 abr-summary 命令显示信息描述表

字段	描述
Area	聚合路由所在的区域
Total summary addresses	聚合路由的路由数
Prefix	聚合路由的地址前缀
Status	聚合路由的状态： - Advertise: 已发布 - Not-advertise: 未发布
NULL0	NULL0路由： - Active: 激活 - Inactive: 未激活
Cost	聚合路由的开销 - Configured: 配置的聚合开销 - Not Configured: 未配置聚合开销
Routes count	被聚合的路由数

显示 OSPFv3 进程 1 的 ABR 聚合详细信息。

<Sysname> display ospfv3 1 abr-summary verbose

OSPFv3 Process 1 with Router ID 2.2.2.2

Area: 1.1.1.1

Total summary addresses: 1

Prefix : 1000:4::/32

Status : Advertise

NULL0 : Active

Cost : 1 (Configured)

Routes count: 2

Destination	Metric
1000:4:10:3::/96	1
1000:4:11:3::/96	1

表1-4 display ospfv3 abr-summary verbose 命令显示信息描述表

字段	描述
Destination	被聚合路由的目的地址
Metric	路由的开销值

1.1.11 display ospfv3 asbr-summary

display ospfv3 asbr-summary 命令用来显示 OSPFv3 的 ASBR 聚合信息。

【命令】

display ospfv3 [*process-id*] **asbr-summary** [*ipv6-address prefix-length*]
[**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: 当前的聚合配置所在进程号，取值范围为 1～65535。如果未指定本参数，将显示所有 OSPFv3 进程的 ASBR 聚合信息。

ipv6-address prefix-length: 显示指定 IPv6 地址的 ASBR 聚合信息。*ipv6-address* 表示 IPv6 地址前缀; *prefix-length* 表示 IPv6 地址前缀长度, 取值范围为 0~128。如果未指定本参数, 将显示所有 ASBR 聚合信息。

verbose: 显示 ASBR 聚合详细信息。如果未指定本参数, 将显示 ASBR 聚合的概要信息。

【举例】

显示 OSPFv3 进程 1 的 ASBR 聚合信息。

<Sysname> display ospfv3 1 asbr-summary

```

      OSPFv3 Process 1 with Router ID 2.2.2.2

Total summary addresses: 1

Prefix       : 1000:4::/32
Status       : Advertise
NULL0        : Active
Cost         : 1 (Configured)
Tag          : (Not configured)
Nssa-only    : (Not configured)
Routes count: 2
```

表1-5 display ospfv3 asbr-summary 命令显示信息描述表

字段	描述
Total summary addresses	聚合路由的路由数
Prefix	聚合路由的地址前缀和前缀长度
Status	聚合路由的状态： - Advertise: 已发布 - Not-advertise: 未发布
NULL0	NULL0路由： - Active: 激活 - Inactive: 未激活
Cost	聚合路由的开销： - Configured: 配置的聚合开销 - Not configured: 未配置聚合开销
Tag	聚合路由的标记： - Configured: 配置的聚合标记 - Not configured: 未配置聚合标记
Nssa-only	是否配置Nssa-only： - Configured: 配置了 Nssa-only - Not configured: 未配置 Nssa-only
Routes count	被聚合的路由数

```
# 显示 OSPFv3 进程 1 的 ASBR 聚合详细信息。
<Sysname> display ospfv3 1 asbr-summary verbose

OSPFv3 Process 1 with Router ID 2.2.2.2

Total summary addresses: 1
```

```
Prefix      : 1000:4::/32
Status      : Advertise
NULL0       : Active
Cost        : 1 (Configured)
Tag         : (Not configured)
Nssa-only   : (Not configured)
Routes count: 2
Destination                                Protocol Process Type Metric
1000:4:10:3::/96                           Static    0         2     1
1000:4:11:3::/96                           Static    0         2     1
```

表1-6 display ospfv3 asbr-summary verbose 命令显示信息描述表

字段	描述
Destination	被聚合路由的前缀和前缀长度
Protocol	被聚合路由的协议类型
Process	被聚合路由的协议进程ID
Type	被聚合路由的类型
Metric	被聚合路由的开销

1.1.12 display ospfv3 event-log

display ospfv3 event-log 命令用来显示 OSPFv3 的日志信息。

【命令】

```
display ospfv3 [ process-id ] event-log { lsa-flush | peer | spf }
```

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有进程的日志信息。

lsa-flush: LSA 老化的日志信息。

peer: 邻居的日志信息。

spf: 路由计算的日志信息。

【使用指导】

路由计算的日志信息是指更新到 IPv6 路由表的路由计数信息。

邻居的日志信息包括 OSPFv3 邻居状态倒退到 DOWN, 以及收到 BadLSReq、SeqNumberMismatch 和 1-Way 事件导致邻居状态倒退的信息。

【举例】

显示 OSPFv3 进程 1 的 LSA 老化日志信息。

<Sysname>display ospfv3 1 event-log lsa-flush

```
OSPFv3 Process 1 with Router ID 1.3.3.3

2014-09-02 07:55:25 Received MaxAge LSA from 1.1.1.1
Type: 3   LS ID: 0.0.0.2           AdvRtr: 1.1.1.1           Seq#: 80000001

2014-09-02 07:55:22 Flushed MaxAge LSA by itself
Type: 3   LS ID: 0.0.0.2           AdvRtr: 1.3.3.3           Seq#: 80000001

2014-09-02 07:55:07 Flushed MaxAge LSA by itself
Type: 3   LS ID: 0.0.0.40          AdvRtr: 1.3.3.3           Seq#: 80000001

2014-09-02 07:55:07 Flushed MaxAge LSA by itself
Type: 3   LS ID: 0.0.0.39          AdvRtr: 1.3.3.3           Seq#: 80000001
```

表1-7 display ospfv3 event-log lsa-flush 命令显示信息描述表

字段	描述
Received MaxAge LSA from X.X.X.X	从Router ID为X.X.X.X的源收到MaxAge LSA
Flushed MaxAge LSA by itself	自身发起的老化, 洪泛MaxAge LSA
Type	LSA类型
LS ID	LSA链路状态ID
AdvRtr	发布LSA的路由器, 用Router ID表示
Seq#	LSA序列号

显示 OSPFv3 进程 1 的路由计算的日志信息。

<Sysname>display ospfv3 1 event-log spf

```
OSPFv3 Process 1 with Router ID 1.3.3.3

Date       Time       Duration  Intra  Inter  External Reason
2014-09-02 07:55:30 0.258827 0       0       0       Intra-area LSA
2014-09-02 07:55:30 0.679    0       0       0       Intra-area LSA
```


2014-09-02 07:55:30	0.51576	0	0	0	Intra-area LSA
2014-09-02 07:55:30	0.372	0	0	0	Intra-area LSA
2014-09-02 07:55:25	4.948353	0	0	0	Intra-area LSA
2014-09-02 07:55:25	0.5288	0	0	0	Area 0 full neighbor
2014-09-02 07:55:21	1.66013	0	0	0	Intra-area LSA
2014-09-02 07:55:20	0.450905	0	0	0	Intra-area LSA
2014-09-02 07:55:15	0.253688	0	0	0	Interface state change
2014-09-02 07:55:15	0.5693	0	0	0	Intra-area LSA

表1-8 display ospfv3 event-log spf 命令显示信息描述表

字段	描述
Date	路由计算开始的日期，单位为YYYY-MM-DD，其中YYYY为年，MM为月，DD为日
Time	路由计算开始的时间，单位为hh:mm:ss，其中hh为小时，mm为分钟，ss为秒
Duration	路由计算持续时间，单位为秒
Intra	区域内路由变化的个数
Inter	区域间路由变化的个数
External	外部路由变化的个数
Reason	路由计算的原因： • Intra-area LSA: 区域内 LSA 变化 • Inter-area LSA: 区域间 LSA 变化 • External LSA: 外部 LSA 变化 • Configuration: 配置变化 • Area 0 full neighbor: 区域 0 FULL 邻居个数变化 • Area 0 up interface: 区域 0 UP 接口个数变化 • AS number: AS 号变化 • ABR summarization: ABR 聚合变化 • GR end: GR 结束 • Routing policy: 路由策略变化 • Intra-area tunnel: 区域内隧道变化 • Others: 除上述原因之外的其他原因

显示 OSPFv3 进程 1 的邻居的日志信息。

<Sysname> display ospfv3 1 event-log peer

OSPFv3 Process 1 with Router ID 1.1.1.1

Date	Time	Router ID	Reason	InstID	Interface
2014-09-02	16:39:13	1.3.3.3	IntPhyChange	0	GE1/0/1
2014-09-02	16:36:46	1.3.3.3	IntPhyChange	0	GE1/0/1
2014-09-02	16:34:49	1.3.3.3	BFDDown	0	GE1/0/1
2014-09-02	10:08:45	1.3.3.3	DeadExpired	0	GE1/0/2
2014-09-02	10:08:39	1.3.3.3	DeadExpired	0	VLINK1

表1-9 display ospfv3 event-log peer 命令显示信息描述表

字段	描述
Date	邻居状态变化的日期，单位为YYYY-MM-DD，其中YYYY为年，MM为月，DD为日
Time	邻居状态变化的时间，单位为hh:mm:ss，其中hh为小时，mm为分钟，ss为秒
Router ID	邻居的Router ID
Reason	邻居状态变化的原因： • ResetConnect: 内存不足，邻居关系中断 • IntChange: 接口参数改变 • ResetOspfv3: 重启 OSPFv3 进程 • UndoOspfv3: 删除 OSPFv3 进程 • UndoArea: 删除 OSPFv3 区域 • UndoInt: 接口去使能 • IntLogChange: 接口逻辑属性变化 • IntPhyChange: 接口物理属性变化 • DeadExpired: Dead Timer 超时 • Retrans: 重传过多 • BFDDown: BFD Down • SilentInt: 配置抑制接口 • ConfStubArea: 配置 Stub 区域参数 • ConfNssaArea: 配置 NSSA 区域参数 • VlinkDown: 虚连接 Down • BadLSReq: 收到 BadLSReq 事件 • SeqMismatch: 收到 SeqNumberMismatch 事件 • 1-Way: 收到 1-Way 事件
InstID	接口所属的实例ID
Interface	接口名称

1.1.13 display ospfv3 graceful-restart

display ospfv3 graceful-restart 命令用来显示 OSPFv3 进程的 GR 状态信息。

【命令】

display ospfv3 [*process-id*] **graceful-restart** [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程的 GR 状态信息。

verbose: 显示 GR 详细状态信息。如果未指定本参数，将显示 OSPFv3 进程的 GR 状态概要信息。

【举例】

显示所有 OSPFv3 进程的 GR 状态信息（Restarter）。

<Sysname> display ospfv3 graceful-restart

```
OSPFv3 Process 1 with Router ID 3.3.3.3

Graceful-restart capability      : Enable
Graceful-restart support        : Planned and un-planned, Partial
Helper capability                : Enable
Helper support                  : Planned and un-planned
Current GR state                : Normal
Graceful-restart period         : 120 seconds
Number of neighbors under helper: 0
Number of restarting neighbors  : 0
Last exit reason:
  Restarter: None
  Helper   : None
```

表1-10 display ospfv3 graceful-restart 命令显示信息描述表

字段	描述
OSPFv3 Process 1 with Router ID 3.3.3.3	OSPFv3进程是1， Router ID是3.3.3.3的GR状态信息
Graceful-restart capability	是否使能OSPFv3协议的GR能力 - Enable: 使能 - Disable: 未使能
Graceful-restart support	进程GR支持模式（GR使能时才显示）： - Planned and un-planned: 支持计划和计划外 GR - Planned only: 只支持计划性 GR - Partial: 支持接口级 GR - Global: 不支持接口级 GR，支持全局 GR
Helper capability	是否使能OSPFv3协议的GR Helper能力 - Enable: 使能 - Disable: 未使能

字段	描述
Helper support	显示Helper的支持模式（Helper使能时才显示）： - Strict LSA check: Helper 端支持严格的 LSA 检查 - Planned and un-planned: 支持作为计划和非计划 GR 的 Helper - Planned only: 只支持作为计划 GR 的 Helper
Current GR state	当前GR的状态，其状态有如下几种： - Normal: 表示正处在非 GR 的正常状态 - Under GR: 表示正在 GR 过程中，自身作为 Restarter - Under Helper: 表示正在 GR 过程中，自身作为 Helper
Graceful-restart period	GR重启间隔时间
Number of neighbors under helper	处于GR Helper模式的邻居个数
Number of restarting neighbors	处于GR Restarter模式的邻居个数
Last exit reason	上次退出原因，其中： - Restarter: 表示退出 Restarter 的原因 - None: 无 - Completed: GR 完成 - Interval timer is fired: GR 定时器超时 - Interface state change: 接口状态变化 - Received 1-way hello: 收到邻居的 1-way Hello 报文 - Reset neighbor: 邻居发生 Reset 操作 - DR or BDR change: DR 或 BDR 发生变化 - Helper: 表示退出 Helper 的原因 - None: 无 - Completed: GR 完成 - Received 1-way hello: 收到邻居的 1-way Hello 报文 - Grace Period timer is fired: GR 定时器超时 - Lsa check failed: LSA 检查未通过 - Reset neighbor: 邻居发生 Reset 操作 - Received MAXAGE gracelsa but neighbor is not full: 收到到达老化时间的 Grace LSA，但邻居状态未达到 FULL 状态

显示 OSPFv3 进程的 GR 详细状态信息（Restarter）。

```
<Sysname> display ospfv3 graceful-restart verbose
```

```
OSPFv3 Process 1 with Router ID 3.3.3.3
```

```
Graceful-restart capability      : Enable
Graceful-restart support        : Planned and un-planned, Partial
Helper capability                : Enable
Helper support                   : Planned and un-planned
```

Current GR state : Normal
Graceful-restart period : 120 seconds
Number of neighbors under helper: 0
Number of restarting neighbors : 0
Last exit reason:
Restarter: None
Helper : None

Area: 0.0.0.0
Area flag: Normal
Area up interface count: 1

Virtual-link Neighbor-ID: 100.1.1.1, Neighbor-state: Full
Restarter state: Normal State: P-2-P Type: Virtual
Interface: 6696 (GigabitEthernet1/0/2), Instance-ID: 0
Local IPv6 address: 200:1:FFFF::1
Remote IPv6 address: 201:FFFF::2
Transit area: 0.0.0.1
Last exit reason:
Restarter: None
Helper : None

Neighbor	GR state	Last helper exit reason
100.1.1.1	Normal	None

Area: 0.0.0.1
Area flag: Transit
Area up interface count: 3

Interface: 5506 (GigabitEthernet1/0/3), Instance-ID: 0
Restarter state: Normal State: DR Type: Broadcast
Last exit reason:
Restarter: None
Helper : None
Neighbor count of this interface: 0
Number of neighbors under helper: 0

Interface: 6696 (GigabitEthernet1/0/2), Instance-ID: 0
Restarter state: Normal State: DR Type: Broadcast
Last exit reason:
Restarter: None
Helper : None
Neighbor count of this interface: 1
Number of neighbors under helper: 0

Neighbor	GR state	Last helper exit reason
100.1.1.1	Normal	None

Sham-link Neighbor-ID: 100.1.1.1, Neighbor-state: Full
Restarter state: Normal State: P-2-P Type: Sham

```

Interface-ID: 2147483649, Instance-ID: 0
Source      : 8000:88::FFFF
Destination : 7000:77::FFFF
Last exit reason:
  Restarter: None
  Helper   : None
Neighbor    GR state    Last helper exit reason
100.1.1.1   Normal      None

```

```

Area: 0.0.0.5
Area flag: NSSANoSummaryNoImportRoute
7/5 translator state: Disabled
7/5 translate stability timer interval: 0
Area up interface count: 0

```

表1-11 display ospfv3 graceful-restart 命令显示信息描述表

字段	描述
Area	区域信息
Area flag	区域类型： • Normal: 普通区域 • Transit: 传输区 • Stub: Stub 区域 • StubNoSummary: 完全 Stub 区域 • NSSA: NSSA 区域 • NSSANoSummary: 完全 NSSA 区域 • NSSANoSummaryNoImportRoute: 完全 NSSA 区域，配置了 no-import-route 参数
7/5 translator state	Type-7 LSA转换为Type-5 LSA的转换者状态，取值为： • Enabled: 表示通过命令指定 Type-7 LSA 转换为 Type-5 LSA 的转换者 • Elected: 表示通过选举指定 Type-7 LSA 转换为 Type-5 LSA 的转换者 • Disabled: 表示不是 Type-7 LSA 转换为 Type-5 LSA 的转换者
7/5 translate stability timer interval	Type-7 LSA转换为Type-5 LSA转换稳定定时器的超时时间，单位为秒
Area up interface count	区域下up的接口计数
Interface	区域内的普通接口，以及虚连接所属的出接口
Instance-ID	接口实例ID
Restarter state	作为Restarter的状态
State	接口状态
Type	接口的网络类型

字段	描述
Neighbor count of this interface	接口下的邻居个数
Neighbor	邻居Router ID
GR state	邻居的GR状态： • Normal: 普通状态 • Under GR: 进程正在 GR • Under Helper: 进程正在作为 GR Helper
Last helper exit reason	上一次作为该邻居Helper退出的原因
Virtual-link Neighbor-ID	虚连接的邻居Router ID
Neighbor-State	虚连接和邻居的状态, 包括Down、Init、2-Way、ExStart、Exchange、Loading和Full
Local IPv6 address	本地IPv6地址
Remote IPv6 address	对端IPv6地址
Transit area	传输区域ID

1.1.14 display ospfv3 interface

display ospfv3 interface 命令用来显示 OSPFv3 的接口信息。

【命令】

display ospfv3 [*process-id*] **interface** [*interface-type interface-number* | **verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号, 取值范围为 1~65535。

interface-type interface-number: 接口类型和接口编号。显示指定接口的详细信息。

verbose: 显示所有接口的详细信息。

【使用指导】

如果未指定 OSPFv3 进程号, 将显示所有 OSPFv3 进程的接口概要信息。

如果未指定接口或参数 **verbose**, 将显示所有接口的概要信息。

【举例】

显示运行 OSPFv3 的接口 GigabitEthernet1/0/1 的信息。
<Sysname> display ospfv3 interface gigabitethernet 1/0/1

```

      OSPFv3 Process 1 with Router ID 1.1.1.1

Area: 0.0.0.0
-----
GigabitEthernet1/0/1 is up, line protocol is up
  Interface ID 3          Instance ID 0
  IPv6 prefixes
    FE80::200:12FF:FE34:1 (Link-Local address)
    2001::1
  Cost: 1          State: BDR          Type: Broadcast      MTU: 1500
  Priority: 1
  Designated router: 2.2.2.2
  Backup designated router: 1.1.1.1
  Timers: Hello 10, Dead 40, Poll 40, Retransmit 5, Transmit delay 1
  FRR backup: Enabled
  Neighbor count is 1, Adjacent neighbor count is 1
  Primary path detection mode: BFD echo
  Exchanging/Loading neighbors: 0
  Wait timer: Off,  LsAck timer: Off
  Prefix-suppression is enabled
```

表1-12 display ospfv3 interface 命令显示信息描述表

字段	描述
Area	接口所属的区域ID
Interface ID	接口ID
Instance ID	实例ID
IPv6 prefixes	IPv6前缀
Cost	接口开销
State	根据OSPFv3接口状态机确定的当前接口状态，取值为： - Down：表示在接口上没有发送和接收任何路由协议的报文 - Waiting：表示接口开始发送和接收 Hello 报文，并试图去识别网络上的 DR 和 BDR - P-2-P：表示接口将每隔 HelloInterval 的时间间隔发送 Hello 报文，并尝试和接口链路另一端相连的路由器建立邻接关系 - DR：表示路由器是所连网络的指定路由器 - BDR：表示路由器是所连网络的备份指定路由器 - DROther：表示路由器既不是所连网络的指定路由器，也不是所连网络的备份指定路由器

字段	描述
Type	接口的网络类型，取值为： • PTP：表示网络类型为点对点 • PTMP：表示网络类型为点对多点 • Broadcast：表示网络类型为广播 • NBMA：表示网络类型为 NBMA
MTU	接口MTU的值
Priority	接口的DR优先级
Designated router	本链路上的DR
Backup designated router	本链路上的BDR
Timers	配置的OSPFv3定时器，分别定义如下： • Hello：表示接口发送 Hello 报文的时间间隔，单位为秒 • Dead：表示邻居的失效时间，单位为秒 • Poll：表示 NBMA 网络上发送轮询 Hello 报文的时间间隔，单位为秒 • Retransmit：表示接口重传 LSA 的时间间隔，单位为秒
Transmit Delay	接口对LSA的传输延迟时间，单位为秒
FRR backup	是否使能接口参与LFA（Loop Free Alternate）计算： • Enabled：使能 • Disabled：关闭
Neighbor count	接口的邻居数目
Primary path detection mode	主链路检测方式： • BFD ctrl：BFD 控制报文检测方式 • BFD echo：BFD echo 报文检测方式
Adjacent neighbor count	接口的邻接数目
Keychain authentication: Enabled (test)	OSPFv3接口采用keychain验证模式，keychain名称为test
Exchanging/Loading neighbors	处于Exchanging或Loading状态的邻居个数
Wait timer	等待定时器，其中： • Off：关闭 • On：开启
LsAck timer	报文确认定时器，其中： • Off：关闭 • On：开启
Prefix-suppression is enabled	接口处于前缀抑制

1.1.15 display ospfv3 lsdb

display ospfv3 lsdb 命令用来显示 OSPFv3 的链路状态数据库信息。

【命令】

```
display ospfv3 [ process-id ] lsdb [ { external | grace | inter-prefix |  
inter-router | intra-prefix | link | network | nssa | router | unknown [ type ] }  
[ link-state-id ] [ originate-router router-id | self-originate ] |  
statistics | total | verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程的链路状态数据库信息。

external: 显示链路状态数据库中 Type-5 LSA（AS External LSA）的信息。

grace: 显示链路状态数据库中 Type-11 LSA（Grace LSA）的信息。

inter-prefix: 显示链路状态数据库中 Type-3 LSA（Inter-Area-Prefix LSA）的信息。

inter-router: 显示链路状态数据库中 Type-4 LSA（Inter-Area-Router LSA）的信息。

intra-prefix: 显示链路状态数据库中 Type-9 LSA（Intra-Area-Prefix LSA）的信息。

link: 显示链路状态数据库中 Type-8 LSA（Link LSA）的信息。

network: 显示链路状态数据库中 Type-2 LSA（Network LSA）的信息。

nssa: 显示链路状态数据库中 Type-7 LSA（NSSA LSA）的信息。

router: 显示链路状态数据库中 Type-1 LSA（Router LSA）的信息。

unknown: 显示链路状态数据库中未知类型 LSA 的信息。

type: LSA 类型，取值范围为十六进制数 0~ffff。如果未指定本参数，将显示所有未知类型 LSA 的信息。

link-state-id: 链路状态 ID，IPv4 地址形式。

originate-router router-id: 发布该 LSA 的路由器的 Router ID。

self-originate: 显示本地路由器自己产生的 LSA 的链路状态数据库信息。

statistics: 显示链路状态数据库中 LSA 的统计信息。

total: 显示链路状态数据库中各种 LSA 的总数。

verbose: 显示详细信息。如果未指定本参数，将显示概要信息。

【举例】

显示 OSPFv3 的链路状态数据库信息。

<Sysname> display ospfv3 lsdB

OSPFv3 Process 1 with Router ID 1.1.1.1

Link-LSA (Interface GigabitEthernet1/0/1)

Link state ID	Origin router	Age	SeqNumber	Checksum	Prefix
0.15.0.8	2.2.2.2	0691	0x80000041	0x8315	1
0.0.0.3	1.1.1.1	0623	0x80000001	0x0fee	1

Router-LSA (Area 0.0.0.1)

Link state ID	Origin router	Age	SeqNumber	Checksum	Link
0.0.0.0	1.1.1.1	0013	0x80000068	0x5d5f	2
0.0.0.0	2.2.2.2	0024	0x800000ea	0x1e22	0

Network-LSA (Area 0.0.0.1)

Link state ID	Origin router	Age	SeqNumber	Checksum
0.15.0.8	2.2.2.2	0019	0x80000007	0x599e

Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link state ID	Origin router	Age	SeqNumber	Checksum	Prefix	Reference
0.0.0.2	2.2.2.2	3600	0x80000002	0x2eed	2	Network-LSA
0.0.0.1	2.2.2.2	0018	0x80000001	0x1478	1	Network-LSA

表1-13 display ospfv3 lsdB 命令显示信息描述表

字段	描述
Link state ID	链路状态ID
Origin router	产生LSA的路由器
Age	LSA老化时间
SeqNumber	LSA序列号
Checksum	LSA校验和
Prefix	前缀数目
Link	链路数目
Reference	引用的LSA类型

显示 OSPFv3 链路状态数据库中 Link-LSA 的信息。

<Sysname> display ospfv3 lsdB link

OSPFv3 Process 1 with Router ID 1.1.1.1

Link-LSA (Interface GigabitEthernet1/0/1)

```

LS age          : 833
LS type         : Link-LSA
Link state ID   : 0.15.0.8
Originating router: 2.2.2.2
LS seq number   : 0x80000041
Checksum        : 0x8315
Length          : 56
Priority         : 1
Options         : 0x000013 (-|R|-|x|E|V6)
Link-Local address: fe80::200:5eff:fe00:100
Number of prefixes: 1
    Prefix      : 1001::/64
    Prefix options: 0 (-|-|x|-|-)

```

表1-14 display ospfv3 lsdB link 命令显示信息描述表

字段	描述
LS age	LSA老化时间
LS type	LSA类型
Link state ID	链路状态ID
Originating router	产生LSA的路由器
LS seq number	LSA序列号
Checksum	LSA校验和
Length	LSA长度
Priority	路由器优先级
Options	选项
Link-Local address	链路本地地址
Number of prefixes	前缀的数目
Prefix	地址前缀
Prefix options	前缀选项

显示 OSPFv3 链路状态数据库中 LSA 的统计信息。

```
<System> display ospfv3 lsdB statistics
```

```

                OSPFv3 Process 1 with Router ID 1.1.1.1
-----
Area ID      Router Network IntePre  InteRou IntraPre NSSA
0.0.0.1      2      0      0      0      2      0
0.0.0.3      1      0      0      0      1      1
Total        3      0      0      0      3      1
-----

                Link  Grace  ASE
Total          4      0      0

```

表1-15 display ospfv3 lsdB statistics 命令显示信息描述表

字段	描述
Area ID	区域ID，显示该区域各类LSA的总数
Router	Type-1 LSA的数目
Network	Type-2 LSA的数目
IntePre	Type-3 LSA的数目
InteRou	Type-4 LSA的数目
IntraPre	Type-9 LSA的数目
NSSA	Type-7 LSA的数目
Link	Type-8 LSA的数目
Grace	Type-11 LSA的数目
ASE	Type-5 LSA的数目
Total	不同区域相同类型LSA的总数

显示 OSPFv3 的链路状态数据库的详细信息。

<Sysname> display ospfv3 lsdB verbose

OSPFv3 Process 1 with Router ID 1.1.1.1

Link-LSA (Interface GigabitEthernet1/0/1)

Link state ID	Origin router	Age	SeqNumber	Checksum	Prefix
0.15.0.8	2.2.2.2	0691	0x80000041	0x8315	1
	SendCnt: 0	RxmtCnt: 0		Status: Stale	
0.0.0.3	1.1.1.1	0623	0x80000001	0x0fee	1
	SendCnt: 0	RxmtCnt: 0		Status: Stale	

Router-LSA (Area 0.0.0.1)

Link state ID	Origin router	Age	SeqNumber	Checksum	Link
0.0.0.0	1.1.1.1	0013	0x80000068	0x5d5f	2
	SendCnt: 0	RxmtCnt: 0		Status: Stale	
0.0.0.0	2.2.2.2	0024	0x800000ea	0x1e22	0
	SendCnt: 0	RxmtCnt: 0		Status: Stale	

Network-LSA (Area 0.0.0.1)

Link state ID	Origin router	Age	SeqNumber	Checksum
0.15.0.8	2.2.2.2	0019	0x80000007	0x599e
	SendCnt: 0	RxmtCnt: 0		Status: Stale

Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link state ID	Origin router	Age	SeqNumber	Checksum	Prefix	Reference
0.0.0.2	2.2.2.2	3600	0x80000002	0x2eed	2	Network-LSA
	SendCnt: 0	RxmtCnt: 0	Status: Stale			
0.0.0.1	2.2.2.2	0018	0x80000001	0x1478	1	Network-LSA
	SendCnt: 0	RxmtCnt: 0	Status: Stale			

表1-16 display ospfv3 lsdb verbose 命令显示信息描述表

字段	描述
SendCnt	待发送该LSA的接口数目
RxmtCnt	该LSA在重传列表中的数目
Status	LSA所处的状态： • Normal: 正常状态 • Delayed: 延迟生成的 LSA • Maxage routed: Maxage 的 LSA 且已经经过拓扑前缀处理 • Self originated: 收到自己产生的 LSA • Stale: GR 过程中收到自己产生的 LSA

1.1.16 display ospfv3 nexthop

display ospfv3 nexthop 命令用来显示 OSPFv3 的路由下一跳信息。

【命令】

display ospfv3 [*process-id*] nexthop

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程的下一跳信息。

【举例】

显示 OSPFv3 进程 1 的路由下一跳信息。

```
<Sysname> display ospfv3 1 nexthop
```

```
OSPFv3 Process 1 with Router ID 1.1.1.1
```

```
Nexthop : FE80::20C:29FF:FED7:F308
```

```
Interface: GE1/0/2
```

```

RefCount: 4                               Status   : Valid
NbrID    : 1.1.1.1                       NbrIntID : 21

NextHop   : FE80::20C:29FF:FED7:F312      Interface: GE1/0/3
RefCount: 3                               Status   : Valid
NbrID    : 1.1.1.1                       NbrIntID : 38

```

表1-17 display ospfv3 nexthop 命令显示信息描述表

字段	描述
NextHop	下一跳地址
Interface	出接口名
RefCount	下一跳引用计数
Status	该下一跳的状态： - Valid: 有效 - Invalid: 无效
NbrID	邻居路由器ID
NbrIntID	邻居的接口ID

1.1.17 display ospfv3 non-stop-routing

display ospfv3 non-stop-routing 命令用来显示 OSPFv3 进程的 NSR 状态信息。

【命令】

display ospfv3 [*process-id*] non-stop-routing

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程的 NSR 状态信息。

【举例】

```

# 显示所有 OSPFv3 进程的 NSR 状态信息。
<Sysname> display ospfv3 non-stop-routing

```

OSPFv3 Process 1 with Router ID 3.3.3.3

Nonstop Routing capability: Enabled
Upgrade phase : Normal

表1-18 display ospfv3 non-stop-routing 命令显示信息描述表

字段	描述
Nonstop Routing capability	是否使能OSPFv3协议的NSR能力 • Enabled: 使能 • Disabled: 未使能
Upgrade phase	NSR的各个阶段，有如下几种： • Normal: 普通状态 • Preparation: 准备阶段 • Smooth: 数据平滑阶段 • Precalculation: 路由计算预处理阶段 • Calculation: 路由计算阶段 • Redistribution: 路由引入阶段

1.1.18 display ospfv3 peer

display ospfv3 peer 命令用来显示 OSPFv3 的邻居信息。

【命令】

display ospfv3 [*process-id*] [**area** *area-id*] **peer** [[*interface-type* *interface-number*] [**verbose**] | *peer-router-id* | **statistics**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果不指定本参数，则显示所有 OSPFv3 进程的邻居信息。

area area-id: 显示位于指定区域的邻居信息。**area-id** 为区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其处理成 IPv4 地址格式）或 IPv4 地址格式。如果不指定本参数，则显示所有区域的邻居信息。

interface-type interface-number: 接口类型和接口编号。

verbose: 显示邻居的详细信息。

peer-router-id: 显示指定邻居的信息。

statistics: 显示 OSPFv3 邻居的统计信息。

【使用指导】

如果接口参数、邻居 Router ID 参数都不输入，则显示所有接口的邻居信息。

【举例】

显示 OSPFv3 进程 1 的邻居信息。

<Sysname> display ospfv3 1 peer gigabitethernet 1/0/1

```
OSPFv3 Process 1 with Router ID 1.1.1.1

Area: 0.0.0.1
-----
Router ID      Pri State          Dead-Time InstID Interface
2.2.2.2        1  Full/DR          00:00:33  0      GE1/0/1
```

表1-19 display ospfv3 peer 命令显示信息描述表

字段	描述
Router ID	邻居ID
Pri	邻居路由器优先级
State	邻居状态
Dead-Time	邻居路由器的失效时间
InstID	实例ID
Interface	和邻居相连的接口

显示接口上的 OSPFv3 进程 1 的邻居详细信息。

<Sysname> display ospfv3 1 peer gigabitethernet 1/0/2 verbose

```
OSPFv3 Process 1 with Router ID 1.1.1.1

Area 0.0.0.1 interface GE1/0/2's neighbors
Router ID: 2.2.2.2      Address: FE80::200:5EFF:FE00:100
  State: Full  Mode: Nbr is master  Priority: 1
  DR: 2.2.2.2  BDR: None  MTU: 1500
  Options is 0x000013 (-|R|-|x|E|V6)
  Dead timer due in 00:00:38
  Neighbor is up for 00:19:07
  Neighbor state change count: 120
  Database Summary List 0
  Link State Request List 0
  Link State Retransmission List 3
  Neighbor interface ID: 8037
  GR state: Normal
  Grace period: 0      Grace period timer: Off
  DD Rxmt Timer: Off   LS Rxmt Timer: On
```

表1-20 display ospfv3 peer verbose 命令显示信息描述表

字段	描述
Router ID	邻居的Router ID
Address	接口链路本地地址
State	邻居状态
Mode	路由器在数据库同步阶段，路由器与邻居协商的主从关系，取值为： • Nbr is master: 邻居路由器为主路由器 • Nbr is slave: 邻居路由器为从路由器
Priority	邻居路由器优先级
DR	接口所属网段的DR
BDR	接口所属网段的BDR
MTU	接口MTU的值
Options	邻居的LSA选项，各选项含义如下： • DC: 支持按需链路 • R: 是否为活跃路由器 • N: 是否支持 NSSA 外部 LSA • x: 保留 • E: AS 外部 LSA 的接受能力 • V6: 是否参与 IPv6 路由计算
Dead timer due in hh:mm:ss	Dead定时器距离超时的剩余时间，单位为hh:mm:ss，其中hh为小时，mm为分钟，ss为秒。Dead定时器超时后，认为该邻居已失效
Neighbor is up for hh:mm:ss	邻居关系建立的时长，单位为hh:mm:ss，其中hh为小时，mm为分钟，ss为秒
Neighbor state change count	邻居状态发生改变的次数
Database Summary List	需要DD报文发送的LSA个数
Link State Request List	链路状态请求列表中LSA个数
Link State Retransmission List	链路状态重传列表中LSA个数
Neighbor interface ID	邻居的接口ID
GR state	GR状态，取值为： • Normal: 普通状态 • Doing GR: 正在作为 GR Restarter • Complete GR: GR 完成 • Helper: 正在作为 GR Helper
Grace period	发送Grace LSA的间隔
Grace period timer	发送Grace LSA的间隔定时器，其中： • Off: 关闭 • On: 开启

字段	描述
DD Rxmt Timer	DD报文重传定时器，其中： - Off: 关闭 - On: 开启
LS Rxmt Timer	LSU报文重传定时器，其中： - Off: 关闭 - On: 开启

显示所有 OSPFv3 邻居的统计信息。

<Sysname> display ospfv3 peer statistics

```

OSPFv3 Process 1 with Router ID 1.1.1.1
-----
Area ID      Down Attempt Init 2-Way ExStart Exchange Loading Full Total
0.0.0.0      0   0       0   0     0       0       0     1   1
Total        0   0       0   0     0       0       0     1   1

```

表1-21 display ospfv3 peer statistics 命令显示信息描述表

字段	描述
Area ID	区域标识
Down	该状态为OSPFv3建立邻居关系的初始化状态，表示OSPFv3路由器在一定时间之内没有收到从某一邻居路由器发送来的信息
Attempt	该状态仅对NBMA网络上的邻居有效，表示最近没有从邻居收到信息，但仍需作出进一步的尝试，用以与邻居联系
Init	此状态表示OSPFv3路由器已经接收到邻居路由器发送来的Hello数据包，但该Hello数据包内没有包含自己的Router ID，还没有建立起双方的双向通信
2-Way	此状态表示OSPFv3路由器与邻居路由器的双向通信已经建立。DR及BDR的选择是在这个状态（或更高的状态）完成的
ExStart	在此状态，路由器要确定邻居双方的主从关系并决定初始的DD报文的序列号
Exchange	在此状态，OSPFv3路由器向其邻居路由器发送DD报文来交换链路状态信息
Loading	在此状态，OSPFv3路由器向邻居路由器发送LSR报文，请求最新的链路状态信息
Full	在此状态，建立起邻居关系的路由器之间已经完成了数据库同步的工作，它们的链路状态数据库已经一致
Total	所有区域中处于相同状态的邻居数目的总和

1.1.19 display ospfv3 request-queue

display ospfv3 request-queue 命令用来显示 OSPFv3 请求列表的信息。

【命令】

display ospfv3 [*process-id*] [*area area-id*] **request-queue** [*interface-type*
interface-number] [*neighbor-id*]

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程的请求列表信息。

area area-id: 显示位于指定区域的信息。**area-id** 为区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其处理成 IPv4 地址格式）或 IPv4 地址格式。如果未指定本参数，将显示所有 OSPFv3 区域的请求列表信息。

interface-type interface-number: 接口类型和编号。如果未指定本参数，将显示所有接口的请求列表信息。

neighbor-id: 邻居路由器的 Router ID。如果未指定本参数，将显示所有邻居路由器的请求列表信息。

【举例】

显示 OSPFv3 请求列表的信息。
<Sysname> display ospfv3 request-queue

```
OSPFv3 Process 1 with Router ID 1.1.1.1

Area: 0.0.0.0
Interface GigabitEthernet1/0/1
-----
Nbr-ID 1.3.3.3 Request List
Type   LinkState ID   AdvRouter   SeqNum      Age    CkSum
0x4005 0.0.34.127     1.3.3.3     0x80000001  0027   0x274d
0x4005 0.0.34.128     1.3.3.3     0x80000001  0027   0x2d45
0x4005 0.0.34.129     1.3.3.3     0x80000001  0027   0x333d
0x4005 0.0.34.130     1.3.3.3     0x80000001  0027   0x3935
```

表1-22 display ospfv3 request-queue 命令显示信息描述表

字段	描述
Area	区域ID
Interface	接口类型和序号

字段	描述
Nbr-ID	邻居ID
Request List	请求列表信息
Type	LSA类型
LinkState ID	链路状态标示符
AdvRouter	通告路由器
SeqNum	LSA序列号
Age	LSA老化时间
CkSum	校验和

1.1.20 display ospfv3 retrans-queue

display ospfv3 retrans-queue 命令用来显示 OSPFv3 重传列表的信息。

【命令】

display ospfv3 [*process-id*] [**area** *area-id*] **retrans-queue** [*interface-type* *interface-number*] [*neighbor-id*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程的重传列表信息。

area area-id: 显示位于指定区域的信息。**area-id** 为区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其处理成 IPv4 地址格式）或 IPv4 地址格式。如果未指定本参数，将显示所有 OSPFv3 区域的重传列表信息。

interface-type interface-number: 接口类型和编号。如果未指定本参数，将显示所有接口的重传列表信息。

neighbor-id: 邻居路由器的 Router ID。如果未指定本参数，将显示所有邻居路由器的重传列表信息。

【举例】

显示 OSPFv3 重传列表的信息。

```
<Sysname> display ospfv3 retrans-queue
```

OSPFv3 Process 1 with Router ID 1.1.1.1

Area: 0.0.0.0

Interface GigabitEthernet1/0/1

Nbr-ID 1.2.2.2 Retransmit List

Type	LinkState ID	AdvRouter	SeqNum	Age	CkSum
0x2009	0.0.0.0	1.3.3.3	0x80000001	3600	0x49fb

表1-23 display ospfv3 retrans-queue 命令显示信息描述表

字段	描述
Area	区域ID
Interface	接口类型和序号
Nbr-ID	邻居ID
Retransmit List	重传列表信息
Type	LSA类型
LinkState ID	链路状态标示符
AdvRouter	通告路由器
SeqNum	LSA序列号
Age	LSA老化时间
CkSum	校验和

1.1.21 display ospfv3 routing

display ospfv3 routing 命令用来显示 OSPFv3 路由表的信息。

【命令】

display ospfv3 [*process-id*] **routing** [*ipv6-address prefix-length*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1～65535。如果未指定本参数，将显示所有 OSPFv3 进程的路由表信息。

ipv6-address prefix-length: 显示指定 IPv6 地址的 OSPFv3 路由表的信息。*ipv6-address* 表示 IPv6 地址前缀; *prefix-length* 表示 IPv6 地址前缀长度, 取值范围为 0~128。

【举例】

显示 OSPFv3 路由表的信息。

<Sysname> display ospfv3 routing

```

                                OSPFv3 Process 1 with Router ID 9.9.9.9
-----
I  - Intra area route,  E1 - Type 1 external route,  N1 - Type 1 NSSA route
IA - Inter area route,  E2 - Type 2 external route,  N2 - Type 2 NSSA route
*  - Selected route

*Destination: 1::/64
Type           : IA                      Area           : 0.0.0.1
AdvRouter      : 2.2.2.2                  Preference     : 10
NibID          : 0x230000003              Cost           : 2
Interface      : GE1/0/1                  BkInterface    : GE1/0/2
Nexthop        : FE80::6AC7:45FF:FE5C:206
BkNexthop      : N/A

*Destination: 23::/64
Type           : I                       Area           : 0.0.0.1
AdvRouter      : 3.3.3.3                  Preference     : 10
NibID          : 0x230000001              Cost           : 1
Interface      : GE1/0/1                  BkInterface    : GE1/0/2
Nexthop        : ::
BkNexthop      : N/A

*Destination: 8::/64
Type           : E2                      Tag            : 1
AdvRouter      : 1.1.1.1                  Preference     : 150
NibID          : 0x230000004              Cost           : 1
Interface      : GE1/0/1                  BkInterface    : GE1/0/2
Nexthop        : FE80::6AC7:45FF:FE5C:206
BkNexthop      : N/A

Total: 3
Intra area: 3          Inter area: 0          ASE: 0          NSSA: 0
```

表1-24 display ospfv3 routing 命令显示信息描述表

字段	描述
Destination	目的网段
Type	路由类型
Area	区域ID
AdvRouter	发布LSA的路由器, 用Router ID表示

字段	描述
Preference	路由优先级
NibID	路由下一跳信息的ID值
Cost	路由开销值
Interface	出接口
BkInterface	备份下一跳出接口
Nexthop	下一跳地址
BkNexthop	备份下一跳地址
Interface	出接口
AdvRouter	发布路由器
Area	区域ID
Tag	外部路由标记
Preference	路由优先级
Total	路由总数目
Intra area	区域内路由数目
Inter area	区域间路由数目
ASE	5类外部路由数目
NSSA	7类外部路由数目

1.1.22 display ospfv3 spf-tree

display ospfv3 spf-tree 命令用来显示 OSPFv3 区域的最短路径树信息。

【命令】

display ospfv3 [*process-id*] [*area area-id*] **spf-tree** [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程下区域的最短路径树信息。

area area-id: 显示指定区域的最短路径树信息。如果未指定本参数，将显示所有区域的最短路径树信息。*area-id* 为区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其处理成 IPv4 地址格式）或 IPv4 地址格式。

verbose: 显示 OSPFv3 区域的最短路径树的详细信息。如果未指定本参数，将显示 OSPFv3 区域的最短路径树的概要信息。

【举例】

显示 OSPFv3 进程 1 下区域 0 的最短路径树信息。

```
<Sysname> display ospfv3 1 area 0 spf-tree

      OSPFv3 Process 1 with Router ID 1.1.1.1

Flags: S-Node is on SPF tree      R-Node is directly reachable
      I-Node or Link is init      D-Node or Link is to be deleted
      P-Neighbor is parent        A-Node is in candidate list
      C-Neighbor is child         H-Nexthop changed
      N-Link is a new path        V-Link is involved

      Area: 0.0.0.0  Shortest Path Tree

SPFNode      Type  Flag      SPFLink      Type  Cost  Flag
>1.1.1.1      Router S R
                                -->2.2.2.2      RT2RT  1    C
                                -->2.2.2.2      RT2RT  1    P
```

表1-25 display ospfv3 spf-tree 命令显示信息描述表

字段	描述
SPFNode	SPF节点，以宣告路由器ID作为标识，其中，Type为节点类型： • Network: 网络节点 • Router: 路由器节点 • Flag 为节点标志： • I: 节点处于初始化状态 • T: 节点在候选列表上 • S: 节点在 SPF 树上 • R: 该节点与根节点直连 • D: 该节点将被删除

字段	描述
SPFLink	SPF链路，以宣告路由器ID作为标识，其中，Type为链路类型： • RT2RT：表示路由器到路由器链路 • NET2RT：表示网络到路由器链路 • RT2NET：表示路由器到网络链路 • Cost 为链路花费，Flag 为链路标志： • I：链路处于初始化状态 • P：目的节点是父节点 • C：目的节点是子节点 • D：链路将要被删除 • H：下一跳发生改变 • V：目的节点删除或者是新增节点时，链路的目的节点不在 SPF 树上或处于删除状态 • N：新增链路，并且源节点和目的节点都在 SPF 树上 • L：链路在区域变化列表中

显示 OSPFv3 进程 1 下区域 0 的最短路径树详细信息。

```
<Sysname> display ospfv3 1 area 0 spf-tree verbose
```

```
OSPFv3 Process 1 with Router ID 1.1.1.1
```

```
Flags: S-Node is on SPF tree      R-Node is directly reachable
      I-Node or Link is init      D-Node or Link is to be deleted
      P-Neighbor is parent        A-Node is in candidate list
      C-Neighbor is child         H-Nexthop changed
      N-Link is a new path        V-Link is involved
```

```
Area: 0.0.0.0 Shortest Path Tree
```

```
>SPFNode[0]
```

```
AdvID       : 1.1.1.1           LSID       : 0.0.0.0
NodeType     : Router           Distance    : 1
NodeFlag     : S R
Nexthop count: 1
-->NbrID     : 1.1.1.1           NbrIntID   : 21
Interface    : GE1/0/2          NhFlag     : Valid
BkInterface  : GE1/0/3          RefCount   : 4
Nexthop      : FE80::20C:29FF:FED7:F308
BkNexthop    : FE80::4
SPFLink count: 1
-->AdvID     : 1.1.1.1           LSID       : 0.0.0.0
IntID        : 232              NbrIntID   : 465
NbrID        : 2.2.2.2          LinkType    : RT2RT
LinkCost     : 1                LinkNewCost : 1
LinkFlag     : C                NexthopCnt  : 0
ParentLink count: 1
```

```

-->AdvID      : 1.1.1.1          LsID        : 0.0.0.0
    IntID      : 215              NbrIntID     : 466
    NbrID      : 2.2.2.2          LinkType    : RT2RT
    LinkCost   : 1                LinkNewCost : 1
    LinkFlag   : P                NexthopCnt  : 0

```

表1-26 display ospfv3 spf-tree verbose 命令显示信息描述表

字段	描述
SPFNode	SPF节点
AdvID	通告路由器ID
LsID	链路状态ID
NodeType	节点类型
Distance	到根节点的开销
NodeFlag	节点标志
Nexthop count	下一跳计数
NbrID	邻居路由器ID
NbrIntID	邻居的接口ID
Interface	出接口
NhFlag	下一跳标志： Valid: 有效 Invalid: 无效
BkInterface	备份下一跳出接口
RefCount	下一跳的引用计数
Nexthop	下一跳地址
BkNexthop	备份下一跳地址
SPFLink count	SPF链路计数
IntID	接口ID
LinkType	链路类型： - RT2RT: 表示路由器到路由器链路 - NET2RT: 表示网络到路由器链路 - RT2NET: 表示路由器到网络链路
LinkCost	当前链路花费
LinkNewCost	新的链路花费

字段	描述
LinkFlag	链路标志： • I: 链路处于初始化状态 • P: 目的节点是父节点 • C: 目的节点是子节点 • D: 链路将要被删除 • H: 下一跳发生改变 • V: 目的节点删除或者是新增节点时，链路的目的节点不在 SPF 树上或处于删除状态 • N: 新增链路，并且源节点和目的节点都在 SPF 树上 • L: 链路在区域变化列表中
NexthopCnt	下一跳个数
ParentLink count	父链路计数

1.1.23 display ospfv3 statistics

display ospfv3 statistics 命令用来显示 OSPFv3 的统计信息。

【命令】

display ospfv3 [*process-id*] **statistics** [**error** | **packet** [*interface-type* *interface-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程的统计信息。

error: 显示错误统计信息。如果未指定本参数，将显示 OSPFv3 进程的报文、LSA 和路由的统计信息。

packet: 显示 OSPFv3 的报文统计信息。

interface-type interface-number: 接口类型和编号。显示指定接口的统计信息。如果未指定本参数，将显示所有接口的统计信息。

【举例】

显示 OSPFv3 的统计信息。

```
<Sysname> display ospfv3 statistics
```

OSPFv3 Process 1 with Router ID 1.1.1.1

Packet Statistics

Type	Recv	Send
Hello	1746	1284
DB Description	505	941
Ls Req	252	136
Ls Upd	851	1553
Ls Ack	416	450

Local Originated LSAs Statistics

Type	Count
Router-LSA	192
Network-LSA	0
Inter-Area-Prefix-LSA	0
Inter-Area-Router-LSA	0
AS-external-LSA	0
NSSA-LSA	0
Link-LSA	10
Intra-Area-Prefix-LSA	112
Grace-LSA	0
Unknown-LSA	0
Total	314

Routes Statistics

Type	Count
Intra Area	0
Inter Area	0
ASE	0
NSSA	0

表1-27 display ospfv3 statistics 命令显示信息描述表

字段	描述
Packet Statistics	收发报文统计
Hello	Hello报文
DB Description	数据库描述报文
Ls Req	链路状态请求报文
Ls Upd	链路状态更新报文
Ls Ack	链路状态确认报文
Local Originated LSAs Statistics	生成的LSA统计
Router-LSA	Type-1 LSA的数目

字段	描述
Network-LSA	Type-2 LSA的数目
Inter-Area-Prefix-LSA	Type-3 LSA的数目
Inter-Area-Router-LSA	Type-4 LSA的数目
AS-external-LSA	Type-5 LSA的数目
NSSA-LSA	Type-7 LSA的数目
Link-LSA	Type-8 LSA的数目
Intra-Area-Prefix-LSA	Type-9 LSA的数目
Grace-LSA	Type-11 LSA的数目
Unknown-LSA	Unknown-LSA数目
Total	总数目
Routes Statistics	路由计数
Intra Area	区域内路由
Inter Area	区域间路由
ASE	5类外部路由
NSSA	7类外部路由

显示 OSPFv3 进程的统计错误信息。

```
<sysname> display ospfv3 statistics error
```

OSPFv3 Process 1 with Router ID 1.1.1.1

```

0      : Transmit error          0      : Neighbor state low
0      : Packet too small        0      : Bad version
0      : Bad checksum            0      : Unknown neighbor
0      : Bad area ID            0      : Bad packet
0      : Packet dest error       0      : Inactive area packet
0      : Router ID confusion     0      : Bad virtual link
0      : HELLO: Hello-time mismatch 0      : HELLO: Dead-time mismatch
0      : HELLO: Ebit option mismatch 0      : DD: Ebit option mismatch
0      : DD: Unknown LSA type    0      : DD: MTU option mismatch
0      : REQ: Empty request      0      : REQ: Bad request
0      : UPD: LSA checksum bad   0      : UPD: Unknown LSA type
0      : UPD: Less recent LSA    0      : UPD: LSA length bad
0      : UPD: LSA AdvRtr id bad  0      : ACK: Bad ack packet
0      : ACK: Invalid ack       0      : Interface down
0      : Multicast incapable     0      : Authentication failure
0      : AuthSeqNumber error

```

表1-28 display ospfv3 statistics error 命令显示信息描述表

字段	描述
Transmit error	发送出错的OSPFv3报文数
Neighbor state low	在低邻居状态收到的OSPFv3报文数
Packet too small	报文长度太小的OSPFv3报文数
Bad version	错误版本号的OSPFv3报文数
Bad checksum	校验和出错的OSPFv3报文数
Unknown neighbor	未知的邻居发来的OSPFv3报文数
Bad area ID	非法的区域ID的OSPFv3报文数
Bad packet	非法的OSPFv3报文数
Packet dest error	目的地址错误的OSPFv3报文数
Inactive area packet	非活动区域中接收到的报文数
Router ID confusion	含有重复路由器ID的OSPFv3报文数
Bad virtual link	错误的虚链路的OSPFv3报文数
HELLO: Hello-time mismatch	Hello定时器不匹配的Hello报文数
HELLO: Dead-time mismatch	Dead定时器不匹配的Hello报文数
HELLO: Ebit option mismatch	Option字段E位不匹配的Hello报文数
DD: Ebit option mismatch	Option字段E位不匹配的DD报文数
DD: Unknown LSA type	DD报文中含有未知类型LSA的数目
DD: MTU option mismatch	MTU不匹配的DD报文数
REQ: Empty request	不含有任何请求信息的LSR报文数
REQ: Bad request	请求错误LSA的LSR报文数
UPD: LSA checksum bad	LSU报文中含有错误校验和LSA的数目
UPD: Unknown LSA type	LSU报文中含有未知类型LSA的数目
UPD: Less recent LSA	LSU报文中含有不是最新LSA的数目
UPD: LSA length bad	LSU报文中含有错误长度LSA的数目
UPD: LSA AdvRtr id bad	LSU报文中含有错误宣告路由器LSA的数目
ACK: Bad ack packet	对LSU报文错误确认的ack报文数
ACK: Invalid ack	LSAck报文中无效确认ack的数目
Interface down	接口down计数
Multicast incapable	加入组播组出错计数
Authentication failure	接收到的报文验证失败
AuthSeqNumber error	接收到的报文验证序列号错误

显示 OSPFv3 进程和接口的报文统计信息。
<Sysname> display ospfv3 statistics packet

```
OSPFv3 Process 1 with Router ID 1.1.1.1

      Hello      DD      LSR      LSU      ACK      Total
Input : 8727      128      28      1584     929     11396
Output: 8757      159      86      987     1513     11502

Area: 0.0.0.0

Area: 0.0.0.1
Interface: GigabitEthernet1/0/1
      DD      LSR      LSU      ACK      Total
Input : 16       0       45       7       68
Output: 17       1       7       44      69
Interface: GigabitEthernet1/0/2
      DD      LSR      LSU      ACK      Total
Input : 41       13      720      719     1493
Output: 54       41      750      713     1558
```

表1-29 display ospfv3 statistics packet 命令显示信息描述表

字段	描述
Hello	Hello报文
DD	数据库描述报文
LSR	链路状态请求报文
LSU	链路状态更新报文
ACK	链路状态确认报文
Total	报文总数
Input	接收报文数
Output	发送报文数
Area	区域ID
Interface	接口名称

1.1.24 display ospfv3 vlink

display ospfv3 vlink 命令用来显示 OSPFv3 的虚连接信息。

【命令】

display ospfv3 [process-id] vlink

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，将显示所有 OSPFv3 进程的虚连接信息。

【举例】

显示 OSPFv3 的虚连接信息。

<Sysname> display ospfv3 vlink

OSPFv3 Process 1 with Router ID 1.1.1.1

Virtual-link Neighbor-ID: 12.2.2.2, Neighbor-state: Full
Interface: 2348 (GigabitEthernet1/0/2), Instance-ID: 0
Local IPv6 address: 3:3333::12
Remote IPv6 address: 2:2222::12
Cost: 1 State: P-2-P Type: Virtual
Transit area: 0.0.0.1
Timers: Hello 10, Dead 40, Retransmit 5, Transmit delay 1

表1-30 display ospfv3 vlink 命令显示信息描述表

字段	描述
Virtual-link Neighbor-ID	通过虚连接相连的邻居路由器的Router ID
Neighbor-state	邻居状态，包括Down、Init、2-Way、ExStart、Exchange、Loading和Full
Interface	此虚连接的本端接口的端口号和名称
Instance-ID	实例ID
Local IPv6 address	本地IPv6地址
Remote IPv6 address	对端IPv6地址
Cost	接口的路由开销
State	接口状态
Type	类型：虚连接
Transit area	传输区域ID（如果当前接口为虚连接，则显示）
Timers	OSPFv3定时器，分别定义如下： • Hello：表示接口发送 Hello 报文的时间间隔，单位为秒 • Dead：表示邻居的失效时间，单位为秒 • Retransmit：表示接口重传 LSA 时间间隔，单位为秒
Transmit delay	接口对LSA的传输延迟时间，单位为秒

字段	描述
Keychain authentication: Enabled (test)	OSPFv3虚连接采用keychain验证模式，keychain名称为test

1.1.25 event-log

event-log 命令用来配置保存 OSPFv3 的日志信息的最大个数。

undo event-log 命令用来取消保存 OSPFv3 的日志信息的最大个数的配置。

【命令】

event-log { lsa-flush | peer | spf } size count

undo event-log { lsa-flush | peer | spf } size

【缺省情况】

保存的路由计算、邻居和 LSA 老化的日志信息个数均为 10 个。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

lsa-flush: LSA 老化日志信息个数。

peer: 邻居日志信息个数。

spf: SPF 日志信息个数。

count: 日志信息个数，取值范围为 0~65535。

【举例】

配置保存 OSPFv3 进程 100 的路由计算日志信息的最大个数为 50。

```
<Sysname> system-view
```

```
[Sysname] ospfv3 100
```

```
[Sysname-ospfv3-100] event-log spf size 50
```

1.1.26 fast-reroute (OSPFv3 view)

fast-reroute 命令用来配置 OSPFv3 快速重路由功能。

undo fast-reroute 命令用来关闭 OSPFv3 快速重路由功能。

【命令】

fast-reroute { lfa [abr-only] | route-policy route-policy-name }

undo fast-reroute

【缺省情况】

OSPFv3 快速重路由功能处于关闭状态。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

lfa: 为所有路由通过 LFA（Loop Free Alternate）算法选取备份下一跳信息。

abr-only: 仅选取到 ABR 设备的路由作为备份下一跳。

route-policy route-policy-name: 为通过策略的路由指定备份下一跳，*route-policy-name* 为路由策略名，为 1~63 个字符的字符串，区分大小写。

【使用指导】

OSPFv3 快速重路由功能（通过 LFA 算法选取备份下一跳信息）使能后，不能配置 **vlink-peer** 命令。

【举例】

使能 OSPFv3 进程 1 的快速重路由功能，为所有路由通过 LFA 算法选取备份下一跳信息。

```
<Sysname> system-view
```

```
[Sysname] ospfv3 1
```

```
[Sysname-ospfv3-1] fast-reroute lfa
```

1.1.27 filter (OSPFv3 area view)

filter 命令用来配置对 Inter-Area-Prefix-LSA 进行过滤。

undo filter 命令用来取消对 Inter-Area-Prefix-LSA 进行过滤。

【命令】

```
filter { ipv6-acl-number | prefix-list prefix-list-name | route-policy route-policy-name } { export | import }
```

```
undo filter { export | import }
```

【缺省情况】

不对 Inter-Area-Prefix-LSA 进行过滤。

【视图】

OSPFv3 区域视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-acl-number: 指定的基本或高级 IPv6 ACL 编号，对进出本区域的 Inter-Area-Prefix-LSA 进行过滤，取值范围为 2000~3999。

prefix-list-name: 指定的 IPv6 地址前缀列表, 对进出本区域的 Inter-Area-Prefix-LSA 进行过滤, 为 1~63 个字符的字符串, 区分大小写。

route-policy-name: 指定的路由策略, 对进出本区域的 Inter-Area-Prefix-LSA 进行过滤, 为 1~63 个字符的字符串, 区分大小写。

export: 对 ABR 向其它区域发布的 Inter-Area-Prefix-LSA 进行过滤。

import: 对 ABR 向本区域发布的 Inter-Area-Prefix-LSA 进行过滤。

【使用指导】

此命令只在 ABR 路由器上有效, 对区域内部路由器无效。

【举例】

根据 IPv6 地址前缀列表 my-prefix-list 和编号为 2000 的 IPv6 基本 ACL 分别对进出 OSPFv3 区域 1 的 Inter-Area-Prefix-LSA 进行过滤。

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] filter prefix-list my-prefix-list import
[Sysname-ospfv3-1-area-0.0.0.1] filter 2000 export
```

1.1.28 filter-policy export (OSPFv3 view)

filter-policy export 命令用来配置对引入的路由信息进行过滤。

undo filter-policy export 命令用来取消对引入的路由信息进行过滤。

【命令】

```
filter-policy { ipv6-acl-number | prefix-list prefix-list-name } export
[ direct | { ospfv3 | ripng } [ process-id ] | static ]
undo filter-policy export [ direct | { ospfv3 | ripng } [ process-id ] |
static ]
```

【缺省情况】

不对引入的路由信息进行过滤。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-acl-number: 用于过滤路由信息目的地址的基本或高级 IPv6 ACL 编号, 取值范围为 2000~3999。

prefix-list-name: 用于过滤路由信息目的地址的 IPv6 地址前缀列表的名称, 为 1~63 个字符的字符串, 区分大小写。

direct: 对引入的直连路由进行过滤。

ospfv3: 对引入的 OSPFv3 路由进行过滤。

ripng: 对引入的 RIP 路由进行过滤。

process-id: 路由协议进程号，取值范围为 1~65535，缺省值为 1。

static: 对引入的静态路由进行过滤。

【使用指导】

当配置的是高级 ACL（3000~3999）时，其使用规则如下：

- 使用命令 **rule [rule-id] { deny | permit } ipv6 source sour-addr sour-prefix** 来过滤指定目的地址的路由。
- 使用命令 **rule [rule-id] { deny | permit } ipv6 source sour-addr sour-prefix destination dest-addr dest-prefix** 来过滤指定目的地址和掩码的路由。

其中，**source** 用来过滤路由目的地址，**destination** 用来过滤路由前缀，配置的前缀应该是连续的（当配置的前缀不连续时该过滤前缀的条件不生效）。

filter-policy export 命令只对本设备使用 **import-route** 引入的路由起作用。如果没有配置 **import-route** 命令来引入其它外部路由（包括不同进程的 OSPFv3 路由），则 **filter-policy export** 命令无效。

如果没有指定路由协议，将对引入的任何一个协议产生的路由都要进行过滤。

【举例】

```
# 根据 IPv6 地址前缀列表 abc 对引入的路由信息进行过滤。
<Sysname> system-view
[Sysname] ipv6 prefix-list abc permit 2002:1:: 64
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy prefix-list abc export
# 使用编号为 3000 的 IPv6 高级 ACL 对引入的路由进行过滤，只允许 2001::1/128 通过。
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 3000 export
```

1.1.29 filter-policy import (OSPFv3 view)

filter-policy import 命令用来过滤通过接收到的 LSA 计算出来的路由信息。

undo filter-policy import 命令用来恢复缺省情况。

【命令】

```
filter-policy { ipv6-acl-number [ gateway prefix-list-name ] | prefix-list  
prefix-list-name [ gateway prefix-list-name ] | gateway prefix-list-name |  
route-policy route-policy-name } import  
undo filter-policy import
```

【缺省情况】

不对通过接收到的 LSA 计算出来的路由信息进行过滤。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-acl-number: 用于过滤路由信息目的地址的基本或高级 IPv6 ACL 编号, 取值范围为 2000~3999。

gateway prefix-list-name: 指定的 IPv6 地址前缀列表, 基于要加入到路由表的路由信息的下一跳进行过滤。**prefix-list-name** 为 1~63 个字符的字符串, 区分大小写。如果未指定本参数, 则不会基于要加入到路由表的路由信息的下一跳进行过滤。

prefix-list prefix-list-name: 指定的地址前缀列表, 基于目的地址对接收的路由信息进行过滤。**prefix-list-name** 为 1~63 个字符的字符串, 区分大小写。

route-policy route-policy-name: 指定路由策略名, 基于路由策略对接收的路由信息进行过滤。**route-policy-name** 为 1~63 个字符的字符串, 区分大小写。

【使用指导】

当配置的是高级 ACL (3000~3999) 或者指定的路由策略中配置的是高级 ACL 时, 其使用规则如下:

- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-prefix** 来过滤指定目的地址的路由。
- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-prefix destination dest-addr dest-prefix** 来过滤指定目的地址和前缀的路由。

其中, **source** 用来过滤路由目的地址, **destination** 用来过滤路由前缀, 配置的前缀应该是连续的 (当配置的前缀不连续时该过滤前缀的条件不生效)。

filter-policy import 命令只对 OSPFv3 计算出来的路由进行过滤, 没有通过过滤的路由将不被加入路由表中, 从而不能指导报文转发。

【举例】

根据 IPv6 地址前缀列表 abc 对接收的路由信息进行过滤。

```
<Sysname> system-view
```

```
[Sysname] ipv6 prefix-list abc permit 2002:1:: 64
```

```
[Sysname] ospfv3
```

```
[Sysname-ospfv3-1] filter-policy prefix-list abc import
```

使用编号为 3000 的 IPv6 高级 ACL 对接收的路由进行过滤, 只允许 2001::1/128 通过。

```
<Sysname> system-view
```

```
[Sysname] acl ipv6 advanced 3000
```

```
[Sysname-acl-ipv6-adv-3000] rule 10 permit ipv6 source 2001::1 128 destination  
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 128
```

```
[Sysname-acl-ipv6-adv-3000] rule 100 deny ipv6
```

```
[Sysname-acl-ipv6-adv-3000] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 3000 import
```

1.1.30 graceful-restart enable

graceful-restart enable 命令用来使能 OSPFv3 协议的 GR 能力。

undo graceful-restart enable 命令用来关闭 OSPFv3 协议的 GR 能力。

【命令】

```
graceful-restart enable [ global | planned-only ] *
undo graceful-restart enable
```

【缺省情况】

OSPFv3 的 GR 能力处于关闭状态。

【视图】

OSPFv3 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

global: 全局 GR，必须保证所有的 GR Helper 都存在，整个 GR 才会完成，如果有一个 GR Helper 失效（比如，接口 down），则整个 GR 失败。如果未指定本参数，表示支持接口级 GR，即只要有一个 GR Helper 存在，则整个 GR 会完成。

planned-only: 表示只支持计划重启。如果未指定本参数，表示计划重启和非计划重启都支持。

【使用指导】

GR 包括计划重启和非计划重启：

- 计划重启指的是手动通过命令执行重启或主备倒换，在进行重启或主备倒换前 GR Restarter 会先发送 Grace-LSA。
- 非计划 GR 指的是由于设备故障等原因进行重启或主备倒换，在进行重启或主备倒换前 GR Restarter 不会事先发送 Grace-LSA。

graceful-restart enable 和 **non-stop-routing** 命令互斥，不能同时配置。

支持 OSPFv3 的 GR Restarter 能力的设备主备倒换后，为了实现设备转发业务的不中断，它必须完成下列两项任务：

- 重启过程 GR Restarter 转发表项保持稳定；
- 重启流程结束后重建所有邻居关系，重新获取完整的网络拓扑信息。

【举例】

使能 OSPFv3 进程 1 的 GR 能力。

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart enable
```

【相关命令】

- **graceful-restart helper enable**

1.1.31 graceful-restart helper enable

graceful-restart helper enable 命令用来使能 OSPFv3 的 GR Helper 能力。

undo graceful-restart helper enable 命令用来关闭 OSPFv3 的 GR Helper 能力。

【命令】

graceful-restart helper enable [planned-only]

undo graceful-restart helper enable

【缺省情况】

OSPFv3 的 GR Helper 能力处于开启状态。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

planned-only: 表示只支持计划重启。如果未指定本参数，表示计划重启和非计划重启（即异常重启）都支持。

【使用指导】

收到 Grace-LSA 后，如果支持 GR Helper 能力则进入 Helper 模式（此时该邻居称为 GR Helper）。在 GR Restarter 重新建立邻居的时候，GR Helper 帮助 GR Restarter 进行 LSDB 的同步。

【举例】

```
# 使能 OSPFv3 进程 1 的 GR Helper 能力。  
<Sysname> system-view  
[Sysname] ospfv3 1  
[Sysname-ospfv3-1] graceful-restart helper enable
```

【相关命令】

- **graceful-restart enable**

1.1.32 graceful-restart helper strict-lsa-checking

graceful-restart helper strict-lsa-checking 命令用来使能 GR Helper 严格 LSA 检查能力。

undo graceful-restart helper strict-lsa-checking 命令用来关闭 GR Helper 严格 LSA 检查能力。

【命令】

graceful-restart helper strict-lsa-checking

undo graceful-restart helper strict-lsa-checking

【缺省情况】

GR Helper 严格 LSA 检查能力处于关闭状态。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

使能 GR Helper 严格 LSA 检查能力，当检查到 GR Helper 设备的 LSA 发生变化时候，Helper 设备退出 GR Helper 模式。

【举例】

```
# 使能 OSPFv3 进程 1 的 GR Helper 严格 LSA 检查能力。  
<Sysname> system-view  
[Sysname] ospfv3 1  
[Sysname-ospfv3-1] graceful-restart helper strict-lsa-checking
```

【相关命令】

- **graceful-restart helper enable**

1.1.1.33 graceful-restart interval

graceful-restart interval 命令用来配置 OSPFv3 协议的 GR 重启间隔时间。

undo graceful-restart interval 命令用来恢复缺省情况。

【命令】

graceful-restart interval *interval*

undo graceful-restart interval

【缺省情况】

OSPFv3 协议的 GR 重启间隔时间为 120 秒。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval：指定 OSPFv3 协议的 GR 重启间隔时间（期望重启时间），取值范围为 40～1800，单位为秒。

【使用指导】

配置此命令的用户需要确保配置的 GR 重启间隔不小于 OSPFv3 所有接口的邻居失效时间的最大值，否则可能造成 GR 重启失败。

【举例】

```
# 配置 OSPFv3 进程 1 的 GR 重启间隔时间为 100 秒。
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] graceful-restart interval 100
```

【相关命令】

- **ospfv3 timer dead**

1.1.34 import-route (OSPFv3 view)

import-route 命令用来配置引入外部路由信息。

undo import-route 命令用来取消引入外部路由信息。

【命令】

```
import-route { direct | static } [ cost cost-value | nssa-only | route-policy route-policy-name | tag tag | type type ] *
undo import-route { direct | static }
import-route { ospfv3 | ripng } [ process-id | all-processes ]
undo import-route { ospfv3 | ripng } [ process-id | all-processes ]
```

【缺省情况】

不引入外部路由信息。

【视图】

OSPFv3 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

direct: 引入直连路由。

static: 引入静态路由。

ospfv3: 引入 OSPFv3 协议的路由。

ripng: 引入 RIPng 协议的路由。

process-id: 路由协议进程号，取值范围为 1~65535，缺省值为 1。

all-processes: 引入指定路由协议所有进程的路由。

allow-direct: 在引入的路由中包含使能了该协议的接口网段路由。如果未指定本参数，在引入协议路由时不会包含使能了该协议的接口网段路由。当 **allow-direct** 与 **route-policy route-policy-name** 参数一起使用时，需要注意路由策略中配置的匹配规则不要与接口路由信

息存在冲突，否则会导致 **allow-direct** 配置失效。例如，当配置 **allow-direct** 参数引入 OSPFv3 直连时，在路由策略中不要配置 **if-match route-type** 匹配条件，否则，**allow-direct** 参数失效。

cost cost-value: 路由开销值，取值范围为 0~16777214，缺省值为 1。

nssa-only: 设置 Type-7 LSA 的 P 比特位不置位，即在对端路由器上不能转为 Type-5 LSA。如果未指定本参数，Type-7 LSA 的 P 比特位被置位，即在对端路由器上可以转为 Type-5 LSA（如果本地路由器是 ABR，则会检查骨干区域是否存在 FULL 状态的邻居，当 FULL 状态的邻居存在时，产生的 Type-7 LSA 中 P 比特位不置位）。

route-policy route-policy-name: 配置只能引入符合指定路由策略的路由。
route-policy-name 为路由策略名称，为 1~63 个字符的字符串，区分大小写。

tag tag: 外部 LSA 中的标记，取值范围为 0~4294967295。如果未指定本参数，将根据 **default tag** 命令的配置进行取值。

type type: 度量值类型，取值范围为 1~2，缺省值为 2。

【使用指导】

外部路由是指到达自治系统外部的路由，有两类：

- 第一类外部路由（Type1 External）：这类路由的可信程度较高，并且和 OSPFv3 自身路由的开销具有可比性，所以到第一类外部路由的开销等于本路由器到相应的 ASBR 的开销与 ASBR 到该路由目的地址的开销之和。
- 第二类外部路由（Type2 External）：这类路由的可信度比较低，所以 OSPFv3 协议认为从 ASBR 到自治系统之外的开销远远大于在自治系统之内到达 ASBR 的开销。所以计算路由开销时将主要考虑前者，即到第二类外部路由的开销等于 ASBR 到该路由目的地址的开销。如果计算出开销值相等的两条路由，再考虑本路由器到相应的 ASBR 的开销。

该命令不能引入缺省路由。

import-route nssa-only 命令配置后，引入的路由只在 NSSA 区域产生 Type-7 LSA，不会在非 NSSA 区域产生 Type-5 LSA。

【举例】

指定引入进程号为 10 的 RIPng 路由为第二类路由，路由开销值为 50。

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] import-route ripng 10 type 2 cost 50
# OSPFv3 进程 100 引入 OSPFv3 进程 160 发现的路由。
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] import-route ospfv3 160
```

【相关命令】

- **default-route-advertise** (OSPFv3 view)

1.1.35 log-peer-change

log-peer-change 命令用来打开邻居状态变化的输出开关。

undo log-peer-change 命令用来关闭邻居状态变化的输出开关。

【命令】

```
log-peer-change
undo log-peer-change
```

【缺省情况】

邻居状态变化的输出开关处于打开状态。

【视图】

OSPFv3 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

打开邻居状态输出开关后，OSPFv3 邻居状态变化时会生成日志信息发送到设备的信息中心，通过设置信息中心的参数，最终决定日志信息的输出规则（即是否允许输出以及输出方向）。（有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。）

【举例】

关闭 OSPFv3 进程 100 的邻居状态变化的输出开关。

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] undo log-peer-change
```

1.1.36 lsa-generation-interval

lsa-generation-interval 命令用来配置 OSPFv3 LSA 重新生成的时间间隔。

undo lsa-generation-interval 命令用来恢复缺省情况。

【命令】

```
lsa-generation-interval      maximum-interval      [      minimum-interval
[ incremental-interval ] ]
undo lsa-generation-interval
```

【缺省情况】

OSPFv3 LSA 重新生成的最大时间间隔为 5 秒，最小时间间隔为 0 毫秒，时间间隔惩罚增量为 0 毫秒。

【视图】

OSPFv3 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

maximum-interval: OSPFv3 LSA 重新生成的最大时间间隔，取值范围为 1~60，单位为秒。

minimum-interval: OSPFv3 LSA 重新生成的最小时间间隔, 取值范围为 10~60000, 单位为毫秒。取值为 0 毫秒时表示不对 OSPFv3 LSA 重新生成的最小时间间隔进行限制。

incremental-interval: OSPFv3 LSA 重新生成的时间间隔惩罚增量, 取值范围为 10~60000, 单位为毫秒。

【使用指导】

通过调节 LSA 重新生成的时间间隔, 可以抑制网络频繁变化可能导致的带宽资源和路由器资源被过多占用的问题。在网络变化不频繁的情况下, 将 LSA 重新生成时间间隔缩小到 *minimum-interval*, 而在网络变化频繁的情况下可以进行相应惩罚, 将等待时间按照配置的惩罚增量延长, 最大不超过 *maximum-interval*。

minimum-interval 和 *incremental-interval* 配置值不允许大于 *maximum-interval* 配置值。

【举例】

```
# 设置 LSA 重新生成的最大时间间隔为 2 秒, 最小时间间隔为 100 毫秒, 惩罚增量为 100 毫秒。  
<Sysname> system-view  
[Sysname] ospfv3 100  
[Sysname-ospfv3-100] lsa-generation-interval 2 100 100
```

【相关命令】

- **lsa-arrival-interval**

1.1.37 maximum load-balancing (OSPFv3 view)

maximum load-balancing 命令用来配置 OSPFv3 支持的等价路由的最大条数。

undo maximum load-balancing 命令用来恢复缺省情况。

【命令】

maximum load-balancing *number*

undo maximum load-balancing

【缺省情况】

设备各款型对于本节所描述的参数支持情况有所不同, 详细差异信息如下:

型号	说明
T5000-G20	16
T5000-G30	32
T1000-G20/T1000-G50/T1000-G60/T1000-G80	16
T1000-CN60/T1000-CN80	32

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

number: 等价路由的最大条数，当 **number** 取值为 1 时，相当于不进行负载分担。

【举例】

配置 OSPFv3 支持的等价路由的最大条数为 2。

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] maximum load-balancing 2
```

1.1.38 non-stop-routing

non-stop-routing 命令用来使能 OSPFv3 协议的 NSR 能力。

undo non-stop-routing 命令用来关闭 OSPFv3 协议的 NSR 能力。

【命令】

```
non-stop-routing
undo non-stop-routing
```

【缺省情况】

OSPFv3 的 NSR 能力处于关闭状态。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

各个进程的 NSR 功能是相互独立的，只对本进程生效。如果存在多个 OSPFv3 进程，建议在各个进程下使能 OSPFv3 NSR 功能。

non-stop-routing 和 **graceful-restart enable** 命令互斥，不能同时配置。

【举例】

```
# 使能 OSPFv3 进程 100 的 NSR 能力。
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] non-stop-routing
```

1.1.39 nssa (OSPFv3 area view)

nssa 命令用来配置一个区域为 NSSA 区域。

undo nssa 命令用来恢复缺省情况。

【命令】

```
nssa [ default-route-advertise [ cost cost-value | nssa-only | route-policy  
route-policy-name | tag tag | type type ] * | no-import-route | no-summary |  
[ translate-always | translate-never ] | suppress-fa |  
translator-stability-interval value ] *  
undo nssa
```

【缺省情况】

没有区域被配置为 NSSA 区域。

【视图】

OSPFv3 区域视图

【缺省用户角色】

network-admin
context-admin

【参数】

default-route-advertise: 该参数只用于 NSSA 区域的 ABR 或 ASBR，配置后，对于 ABR，不论本地是否存在缺省路由，都将生成一条 Type-7 LSA 向区域内发布缺省路由；对于 ASBR，只有当本地存在缺省路由时，才产生 Type-7 LSA 向区域内发布缺省路由。

cost cost-value: 该缺省路由的度量值，取值范围为 0~16777214。如果未指定本参数，缺省路由的度量值将取 **default-cost** 命令配置的值。

nssa-only: 设置 Type-7 LSA 的 P 比特位不置位，即在对端路由器上不能转为 Type-5 LSA，对端路由器不能引入 Type-7 LSA 产生的外部路由。如果未指定本参数，Type-7 LSA 的 P 比特位被置位，即在对端路由器上可以转为 Type-5 LSA，对端路由器可以引入 Type-7 LSA 产生的外部路由（如果本地路由器是 ABR，则会检查骨干区域是否存在 FULL 状态的邻居，当 FULL 状态的邻居存在时，产生的 Type-7 LSA 中 P 比特位不置位）。

route-policy route-policy-name: 路由策略名，为 1~63 个字符的字符串，区分大小写。只有 **route-policy-name** 指定的路由策略匹配时，才可以产生一个描述缺省路由的 Type-7 LSA 发布出去，指定的路由策略会影响 Type-7 LSA 中的属性。

tag tag: 缺省路由的标识，取值范围为 0~4294967295。

type type: 该 NSSA LSA 的类型，取值范围为 1~2，缺省类型为 2。

no-import-route: 该参数用于禁止将 AS 外部路由以 Type-7 LSA 的形式引入到 NSSA 区域中，这个参数通常只用在既是 NSSA 区域的 ABR，也是 OSPFv3 自治系统的 ASBR 的路由器上，以保证所有外部路由信息能正确地进入 OSPFv3 路由域。

no-summary: 该参数只用于 NSSA 区域的 ABR，配置后，NSSA ABR 只通过 Type-3 LSA 向区域内发布一条缺省路由，不再向区域内发布任何其它 Type-3 LSA（这种区域又称为 Totally NSSA 区域）。

translate-always: 指定 ABR 为 NSSA 区域的 Type-7 LSA 转换为 Type-5 LSA 的转换路由器。

translate-never: 指定 ABR 不能将 NSSA 区域的 Type-7 LSA 转换为 Type-5 LSA。

suppress-fa: 指定当 Type-7 LSA 转换为 Type-5 LSA 时，生成的 Type-5 LSA 不携带 Forwarding Address。

translator-stability-interval value: 当有新的设备成为 NSSA 区域的 Type-7 LSA 转换为 Type-5 LSA 的转换路由器后, 原 Type-7 LSA 转换为 Type-5 LSA 的转换路由器保持转换能力的时间。**value** 为保持时间, 取值范围为 0~900, 单位为秒, 缺省值为 0, 即不保持。

【使用指导】

如果要将一个区域配置成 NSSA 区域, 则该区域中的所有路由器都必须配置本命令。

【举例】

```
# 将区域 1 配置成 NSSA 区域。
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] area 1
[Sysname-ospfv3-120-area-0.0.0.1] nssa
```

【相关命令】

- **default-cost** (OSPFv3 area view)

1.1.40 ospfv3

ospfv3 命令用来启动 OSPFv3 进程, 并进入 OSPFv3 视图。

undo ospfv3 命令用来关闭指定的 OSPFv3 进程。

【命令】

```
ospfv3 [ process-id | vpn-instance vpn-instance-name ] *
undo ospfv3 [ process-id ]
```

【缺省情况】

系统没有运行 OSPFv3 进程。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

process-id: OSPFv3 进程号, 取值范围为 1~65535, 缺省值为 1。

vpn-instance vpn-instance-name: 指定 OSPFv3 进程所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示 OSPFv3 位于公网中。

【使用指导】

只有在 OSPFv3 视图下配置了 Router ID, OSPFv3 进程才能正常运行, 否则只能看到该进程, 但无法生成 LSA。

【举例】

```
# 启动进程号为 120 的 OSPFv3 进程并配置路由器的 Router ID 为 1.1.1.1。
```



```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] router-id 1.1.1.1
```

【相关命令】

- **router-id**

1.1.41 ospfv3 area

ospfv3 area 命令用来在接口上使能 OSPFv3 功能，并指定其所属区域。

undo ospfv3 area 命令用来在指定接口上关闭 OSPFv3 功能。

【命令】

```
ospfv3 process-id area area-id [ instance instance-id ]
undo ospfv3 process-id area area-id [ instance instance-id ]
```

【缺省情况】

接口上的 OSPFv3 功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。

area-id: 区域的标识，可以是十进制整数（取值范围为 0~4294967295，系统会将其处理成 IPv4 地址格式）或 IPv4 地址格式。

instance-id: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【举例】

在接口 GigabitEthernet1/0/1 上启动 OSPFv3 实例 1 的运行，并使能到 Area 1 中。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 1 area 1 instance 1
```

1.1.42 ospfv3 bfd enable

ospfv3 bfd enable 命令用来在运行 OSPFv3 的接口下使能 BFD 功能。

undo ospfv3 bfd enable 命令用来在运行 OSPFv3 的接口下关闭 BFD 功能。

【命令】

```
ospfv3 bfd enable [ instance instance-id ]
undo ospfv3 bfd enable [ instance instance-id ]
```

【缺省情况】

运行 OSPFv3 的接口的 BFD 功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

instance-id: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

BFD（Bidirectional Forwarding Detection，双向转发检测）能够为 OSPFv3 邻居之间的链路提供快速检测功能。当邻居之间的链路出现故障时，加快 OSPFv3 协议的收敛速度。

OSPFv3 通过 BFD 控制报文实现 BFD 功能。

【举例】

```
# 使能接口 GigabitEthernet1/0/1 的 OSPFv3 实例 1 的 BFD 功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 bfd enable instance 1
```

1.1.43 ospfv3 cost

ospfv3 cost 命令用来配置运行不同 OSPFv3 实例的接口的开销值。

undo ospfv3 cost 命令用来取消运行不同 OSPFv3 实例的接口的开销值的配置。

【命令】

```
ospfv3 cost cost-value [ instance instance-id ]
undo ospfv3 cost [ instance instance-id ]
```

【缺省情况】

路由器接口按照带宽自动计算运行 OSPFv3 协议所需的开销；对于 VLAN 接口，缺省值为 1；对于 Loopback 接口，缺省值为 0。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

cost-value: 接口运行 OSPFv3 协议的路由开销，Loopback 接口的取值范围为 0~65535，其他接口的取值范围为 1~65535。

instance-id: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【举例】

```
# 指定运行 OSPFv3 实例 1 的接口 GigabitEthernet1/0/1 的开销为 33。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 cost 33 instance 1
```

1.1.44 ospfv3 dr-priority

ospfv3 dr-priority 命令用来配置运行不同 OSPFv3 实例的接口的 DR 优先级。

undo ospfv3 dr-priority 命令用来取消运行不同 OSPFv3 实例的接口的 DR 优先级的配置。

【命令】

```
ospfv3 dr-priority priority [ instance instance-id ]
undo ospfv3 dr-priority [ instance instance-id ]
```

【缺省情况】

接口的 DR 优先级为 1。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

priority: 接口的 DR 优先级，取值范围为 0~255。

instance instance-id: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

接口的 DR 优先级决定了该接口在选举 DR/BDR 时所具有资格，优先级高的在选举时被首先考虑。

【举例】

```
# 设置运行 OSPFv3 实例 1 的接口 GigabitEthernet1/0/1 在选举 DR/BDR 时的优先级为 8。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 dr-priority 8 instance 1
```

1.1.45 ospfv3 fast-reroute lfa-backup exclude

ospfv3 fast-reroute lfa-backup exclude 命令用来禁止接口参与 LFA（Loop Free Alternate）计算。

undo ospfv3 fast-reroute lfa-backup exclude 命令用来取消禁止接口参与 LFA 计算配置的配置。

【命令】

```
ospfv3 fast-reroute lfa-backup exclude [ instance instance-id ]
undo ospfv3 fast-reroute lfa-backup exclude [ instance instance-id ]
```

【缺省情况】

接口参与 LFA 计算。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

instance *instance-id*: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

接口缺省参与 LFA 计算，有资格成为备份接口。配置本功能后，接口不会被选为备份接口。

【举例】

```
# 禁止接口 GigabitEthernet1/0/1 参与 LFA 计算。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 fast-reroute lfa-backup exclude
```

1.1.46 ospfv3 mib-binding

ospfv3 mib-binding 命令用来配置 OSPFv3 进程绑定 MIB。

undo ospfv3 mib-binding 命令用来恢复缺省情况。

【命令】

ospfv3 mib-binding *process-id*

undo ospfv3 mib-binding

【缺省情况】

MIB 绑定在进程号最小的 OSPFv3 进程上。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。

【使用指导】

如果指定的 *process-id* 不存在，配置 OSPFv3 进程绑定命令时将会提示 OSPFv3 进程不存在，无法完成配置。

如果配置了 OSPFv3 进程绑定 MIB，若删除 *process-id* 对应的 OSPFv3 进程，则同时删除 OSPFv3 进程绑定 MIB 配置，MIB 绑定到进程号最小的 OSPFv3 进程上。

【举例】

```
# 配置 OSPFv3 进程 100 绑定 MIB。
<Sysname> system-view
[Sysname] ospfv3 mib-binding 100
```

1.1.47 ospfv3 mtu-ignore

ospfv3 mtu-ignore 命令用来配置接口在进行 DD 报文交换时忽略 MTU 检查。

undo ospfv3 mtu-ignore 命令用来取消接口在进行 DD 报文交换时忽略 MTU 检查的配置。

【命令】

```
ospfv3 mtu-ignore [ instance instance-id ]
undo ospfv3 mtu-ignore [ instance instance-id ]
```

【缺省情况】

接口在进行 DD 报文交换时执行 MTU 检查。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

instance *instance-id*: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

双方的接口 MTU 必须相同才能建立邻居关系。

【举例】

```
# 配置运行 OSPFv3 实例 1 的接口 GigabitEthernet1/0/1 在进行 DD 报文交换时忽略 MTU 检查。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 mtu-ignore instance 1
```

1.1.48 ospfv3 network-type

ospfv3 network-type 命令用来配置 OSPFv3 接口的网络类型。

undo ospfv3 network-type 命令用来取消 OSPFv3 接口的网络类型的配置。

【命令】

```
ospfv3 network-type { broadcast | nbma | p2mp [ unicast ] | p2p } [ instance instance-id ]
undo ospfv3 network-type [ instance instance-id ]
```

【缺省情况】

OSPFv3 接口网络类型的缺省值为广播类型。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

broadcast: 配置接口的网络类型为广播类型。

nbma: 配置接口的网络类型为 NBMA 类型。

p2mp: 配置接口的网络类型为点到多点类型。

unicast: P2MP 类型支持单播发送报文，缺省情况下是组播方式发送报文。

p2p: 配置接口的网络类型为点到点类型。

instance-id: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

如果在广播网络上有不支持组播地址的路由器，可以将接口的网络类型改为 NBMA。

在 NBMA 网络中，如果任意两台路由器之间都有一条虚电路直接可达，或者说，这个网络是全连通的，那么可以把 OSPFv3 接口的网路类型配置为 NBMA；否则，需要把 OSPFv3 接口的网络类型配置为点到多点，这样，两台不能直接可达的路由器之间可以通过一台与两者都直接可达的路由器来交换路由信息。

接口的网络类型为 NBMA 或 P2MP（unicast）时，必须使用 **peer** 命令来配置邻接点。

接口的网络类型为 P2MP（unicast）时，OSPFv3 协议在该接口上发送的报文均为单播报文。

【举例】

```
# 设置运行 OSPFv3 的接口 GigabitEthernet1/0/1 网络类型为 NBMA。
```

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospfv3 network-type nbma
```

【相关命令】

- **ospfv3 dr-priority**

1.1.49 ospfv3 peer

ospfv3 peer 命令用来指定邻居接口的链路本地地址，并指定该邻居是否有选举权。

undo ospfv3 peer 命令用来取消指定邻居接口的链路本地地址的配置。

【命令】

```
ospfv3 peer ipv6-address [ cost cost-value | dr-priority priority ] [ instance instance-id ]
```

```
undo ospfv3 peer ipv6-address [ instance instance-id ]
```

【缺省情况】

未指定邻居接口的链路本地地址。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address: 邻居的链路本地地址。

cost *cost-value*: 表示网络邻居的开销，取值范围为 1~65535。

dr-priority *priority*: 表示网络邻居的优先级，取值范围为 0~255，缺省值为 1。

instance *instance-id*: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

当路由器的接口类型为如下网络类型时，需要为其指定相邻路由器 IP 地址：

- NBMA 网络
- P2MP 网络（仅当接口选择单播形式发送报文时，需要此配置）

由于无法通过广播 Hello 报文的形式发现相邻路由器，必须手工指定相邻路由器的本地链路地址。

对于 NBMA 网络，可以指定该相邻路由器是否有选举权等。

【举例】

在运行 OSPFv3 协议的接口 GigabitEthernet1/0/1 上指定邻居的链路本地地址为 FE80::1111。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospfv3 peer fe80::1111
```

1.1.50 ospfv3 prefix-suppression

ospfv3 prefix-suppression 命令用来抑制接口进行前缀发布。

undo ospfv3 prefix-suppression 命令用来取消抑制接口进行前缀发布的配置。

【命令】

ospfv3 prefix-suppression [disable] [instance *instance-id*]

undo ospfv3 prefix-suppression [instance *instance-id*]

【缺省情况】

不抑制接口进行前缀发布。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

disable: 不抑制接口进行前缀发布。

instance *instance-id*: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

如果 OSPFv3 进程配置了抑制前缀发布，但某个接口不想进行抑制，此时可以配置本命令并指定 **disable** 参数。

【举例】

```
# 抑制接口 GigabitEthernet1/0/1 进行前缀发布。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 prefix-suppression
```

【相关命令】

prefix-suppression

1.1.51 ospfv3 primary-path-detect bfd

ospfv3 primary-path-detect bfd 命令用来使能 OSPFv3 协议中主用链路的 BFD 检测功能。

undo ospfv3 primary-path-detect bfd 命令用来关闭 OSPFv3 协议中主用链路的 BFD 检测功能。

【命令】

```
ospfv3 primary-path-detect bfd { ctrl | echo } [ instance instance-id ]
undo ospfv3 primary-path-detect bfd [ instance instance-id ]
```

【缺省情况】

OSPFv3 协议中主用链路的 BFD 检测功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ctrl: 配置通过工作于控制报文方式的 BFD 会话对主用链路进行检测。

echo: 配置通过工作于 echo 报文方式的 BFD 会话对主用链路进行检测。

instance *instance-id*: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

配置本功能后，OSPFv3 协议的快速重路由特性中的主用链路将使用 BFD 进行检测。

【举例】

在接口 GigabitEthernet1/0/1 上配置 OSPFv3 协议快速重路由特性中主用链路使能 BFD（Echo 方式）检测功能。


```

<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] fast-reroute lfa
[Sysname-ospfv3-1] quit
[Sysname] bfd echo-source-ipv6 1::1
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 primary-path-detect bfd echo

```

1.1.52 ospfv3 timer dead

ospfv3 timer dead 命令用来配置 OSPFv3 的邻居失效时间。

undo ospfv3 timer dead 命令用来取消 OSPFv3 的邻居失效时间的配置。

【命令】

```

ospfv3 timer dead seconds [ instance instance-id ]
undo ospfv3 timer dead [ instance instance-id ]

```

【缺省情况】

P2P、Broadcast 类型接口的 OSPFv3 邻居失效的时间为 40 秒；P2MP、NBMA 类型接口的 OSPFv3 邻居失效的时间为 120 秒。

【视图】

接口视图

【缺省用户角色】

```

network-admin
context-admin

```

【参数】

seconds: OSPFv3 邻居失效的时间，取值范围为 1~65535，单位为秒。

instance instance-id: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

OSPFv3 邻居的失效时间是指：在该时间间隔内，若未收到邻居的 Hello 报文，就认为该邻居已失效。**dead seconds** 值至少应为 **hello seconds** 值的 4 倍，同一网段上的接口的 **dead seconds** 也必须相同。

【举例】

配置接口 GigabitEthernet1/0/1 上的邻居失效时间为 60 秒。

```

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ospfv3 timer dead 60

```

【相关命令】

- **ospfv3 timer hello**

1.1.53 ospfv3 timer hello

ospfv3 timer hello 命令用来配置接口发送 Hello 报文的时间间隔。

undo ospfv3 timer hello 命令用来取消接口发送 Hello 报文的时间间隔的配置。

【命令】

```
ospfv3 timer hello seconds [ instance instance-id ]  
undo ospfv3 timer hello [ instance instance-id ]
```

【缺省情况】

P2P、Broadcast 类型接口发送 Hello 报文的时间间隔为 10 秒；P2MP、NBMA 类型接口发送 Hello 报文的时间间隔为 30 秒。

【视图】

接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

seconds: 接口发送 Hello 报文的时间间隔，取值范围为 1~65535，单位为秒。

instance instance-id: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

seconds 的值越小，发现网络拓扑改变的速度越快，对系统资源的开销也就越大。同一网段上的接口的 **seconds** 必须相同。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 发送 Hello 报文的时间间隔为 20 秒。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ospfv3 timer hello 20
```

【相关命令】

- **ospfv3 timer dead**

1.1.54 ospfv3 timer poll

ospfv3 timer poll 命令用来配置在 NBMA 接口上向状态为 down 的邻居路由器发送轮询 Hello 报文的时间间隔。

undo ospfv3 timer poll 命令用来取消在 NBMA 接口上向状态为 down 的邻居路由器发送轮询 Hello 报文的时间间隔的配置。

【命令】

```
ospfv3 timer poll seconds [ instance instance-id ]  
undo ospfv3 timer poll [ instance instance-id ]
```

【缺省情况】

在 NBMA 接口上向状态为 down 的邻居路由器发送轮询 Hello 报文的时间间隔为 120 秒。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

seconds: 向状态为 down 的邻居路由器发送轮询 Hello 报文的时间间隔，取值范围为 1～65535，单位为秒。

instance instance-id: 接口所属的实例 ID，取值范围为 0～255，缺省值为 0。

【使用指导】

在 NBMA 的网络上，当邻居失效后，将按轮询时间间隔定期地发送 Hello 报文。用户可配置轮询时间间隔以指定该接口在与相邻路由器构成邻居关系之前发送 Hello 报文的时间间隔。

发送轮询 Hello 报文的时间间隔至少应为发送 Hello 报文时间间隔的 4 倍。

【举例】

配置接口 GigabitEthernet1/0/1 发送轮询 Hello 报文的时间间隔为 120 秒。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospfv3 timer poll 120
```

【相关命令】

- **ospfv3 timer hello**

1.1.55 ospfv3 timer retransmit

ospfv3 timer retransmit 命令用来配置接口重传 LSA 的时间间隔。

undo ospfv3 timer retransmit 命令用来取消接口重传 LSA 的时间间隔的配置。

【命令】

ospfv3 timer retransmit seconds [instance instance-id]

undo ospfv3 timer retransmit [instance instance-id]

【缺省情况】

接口重传 LSA 的时间间隔为 5 秒。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

seconds: 接口重传 LSA 的时间间隔，取值范围为 1～3600，单位为秒。

instance *instance-id*: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

当一台路由器向它的邻居发送一条 LSA 后，需要等到对方的确认报文。若在该重传 LSA 的时间间隔内未收到对方的确认报文，就会重传这条 LSA。

相邻路由器重传 LSA 时间间隔的值不要设置得太小，否则将会引起不必要的重传。

【举例】

指定运行 OSPFv3 实例 1 的接口 GigabitEthernet1/0/1 重传 LSA 的时间间隔为 12 秒。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospfv3 timer retransmit 12 instance 1
```

1.1.56 ospfv3 trans-delay

ospfv3 trans-delay 命令用来配置接口对 LSA 的传输延迟时间。

undo ospfv3 trans-delay 命令用来取消接口对 LSA 的传输延迟时间的配置。

【命令】

ospfv3 trans-delay *seconds* [**instance** *instance-id*]

undo ospfv3 trans-delay [**instance** *instance-id*]

【缺省情况】

接口对 LSA 的传输延迟时间为 1 秒。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

seconds: 接口对 LSA 的传输延迟时间，取值范围为 1~3600，单位为秒。

instance *instance-id*: 接口所属的实例 ID，取值范围为 0~255，缺省值为 0。

【使用指导】

LSA 在本路由器的 LSDB 中会随时间老化（LSA 的老化时间每秒钟加 1），但在网络的传输过程中却不会，所以有必要在发送之前在 LSA 的老化时间上增加一定的延迟时间。此配置对低速率的网络尤其重要。

【举例】

指定运行 OSPFv3 实例 1 的接口 GigabitEthernet1/0/1 洪泛 LSA 的时延值为 3 秒。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ospfv3 trans-delay 3 instance 1
```

1.1.57 preference

preference 命令用来配置 OSPFv3 协议的路由优先级。

undo preference 命令用来取消 OSPFv3 协议的路由优先级的配置。

【命令】

```
preference [ ase ] { preference | route-policy route-policy-name } *  
undo preference [ ase ]
```

【缺省情况】

对于自治系统内部路由，OSPFv3 协议的路由优先级为 10；对于自治系统外部路由，OSPFv3 协议的路由优先级为 150。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin
context-admin

【参数】

ase: 配置 OSPFv3 协议对自治系统外部路由的优先级。如果未指定该参数，则配置的是 OSPFv3 协议对自治系统内部路由的优先级。

preference: OSPFv3 路由的优先级，取值范围为 1~255。优先级的值越小，其实际的优先程度越高。

route-policy route-policy-name: 应用路由策略，对特定的路由设置优先级。
route-policy-name 是路由策略名称，为 1~63 个字符的字符串，区分大小写。

【使用指导】

由于路由器上可能同时运行多个动态路由协议，就存在各个路由协议之间路由信息共享和选择的问题，所以为每一种路由协议指定了一个缺省的优先级。在不同的路由协议发现去往同一目的地的多条路由时，优先级高的协议发现的路由将被选中以转发 IPv6 报文。

【举例】

```
# 配置 OSPFv3 协议路由的优先级为 150。  
<Sysname> system-view  
[Sysname] ospfv3  
[Sysname-ospfv3-1] preference 150
```

1.1.58 prefix-suppression

prefix-suppression 命令用来抑制 OSPFv3 进程进行前缀发布。

undo prefix-suppression 命令用来恢复缺省情况。

【命令】

```
prefix-suppression  
undo prefix-suppression
```

【缺省情况】

不抑制 OSPFv3 进程进行前缀发布。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

接口使能 OSPFv3 后，会将接口下的所有网段路由都通过 LSA 发布，但有时候网段路由是不希望被发布的。通过前缀抑制配置，可以减少 LSA 中携带不必要的前缀，即不发布某些网段路由，从而提高网络安全性，加快路由收敛。

全局配置前缀抑制不能抑制 LoopBack 接口和处于 silent-interface 状态接口对应的前缀。如果想对 Loopback 接口或处于 silent-interface 状态接口进行抑制，可以通过接口下配置前缀抑制（**ospfv3 prefix-suppression** 命令）来实现。

当使能前缀抑制时，具体处理如下：

- Type-8 LSA 中不发布处于抑制的接口前缀信息。
- 对于广播网/NBMA 网络，DR 在生成 Type-9 LSA 引用 Type-2 LSA 时，不发布处于抑制的接口前缀信息。
- 对于 P2P/P2MP 网络，生成 Type-9 LSA 引用 Type-1 LSA 时，不发布处于抑制的接口前缀信息。

【举例】

抑制 OSPFv3 进程 100 的前缀发布。

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] prefix-suppression
```

【相关命令】

ospfv3 prefix-suppression

1.1.59 reset ospfv3 event-log

reset ospfv3 event-log 命令用于清除 OSPFv3 的日志信息。

【命令】

reset ospfv3 [*process-id*] event-log [*lsa-flush* | *peer* | *spf*]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，则清除所有 OSPFv3 进程的日志信息。

lsa-flush: 清除 LSA 老化日志信息。

peer: 清除邻居的日志信息。

spf: 清除路由计算的日志信息。

【使用指导】

如果未指定日志类型，则所有日志信息都被清除。

【举例】

清除所有 OSPFv3 进程路由计算的日志信息。

```
<Sysname> reset ospfv3 event-log spf
```

【相关命令】

- **display ospfv3 event-log**

1.1.60 reset ospfv3 process

reset ospfv3 process 命令用来重启 OSPFv3 进程。

【命令】

reset ospfv3 [process-id] process [graceful-restart]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，则重启所有 OSPFv3 进程。

graceful-restart: 以 GR 方式重启 OSPFv3 进程。

【使用指导】

使用 **reset ospfv3 process** 命令重启 OSPFv3，可以获得如下结果：

- 可以立即清除无效的 LSA，而不必等到 LSA 超时。
- 方便重新选举 DR、BDR。
- 重启前的 OSPFv3 配置不会丢失。

执行该命令后，系统提示用户确认是否重启 OSPFv3 协议。

【举例】

重启所有 OSPFv3 进程。

```
<Sysname> reset ospfv3 process
```

```
Reset OSPFv3 process? [Y/N]:y
```

1.1.61 reset ospfv3 redistribution

reset ospfv3 redistribution 命令用来重新向 OSPFv3 引入外部路由。

【命令】

reset ospfv3 [*process-id*] redistribution

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，所有 OSPFv3 进程都将重新引入外部路由。

【举例】

重新向 OSPFv3 引入外部路由。

<Sysname> reset ospfv3 redistribution

1.1.62 reset ospfv3 statistics

reset ospfv3 statistics 命令用来清除 OSPFv3 的统计信息。

【命令】

reset ospfv3 [*process-id*] statistics

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

process-id: OSPFv3 进程号，取值范围为 1~65535。如果未指定本参数，则清除所有 OSPFv3 进程的统计信息。

【举例】

清除所有 OSPFv3 进程的统计信息。

<Sysname> reset ospfv3 statistics

1.1.63 router-id

router-id 命令用来配置运行 OSPFv3 协议的路由器的 Router ID。

undo router-id 命令用来恢复缺省情况。

【命令】

```
router-id router-id  
undo router-id
```

【缺省情况】

运行 OSPFv3 协议的路由器没有 Router ID。

【视图】

OSPFv3 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

router-id: 路由器标识符，IPv4 地址格式。

【使用指导】

Router ID 是一台运行 OSPFv3 协议的路由器在自治系统中的唯一标识。如果用户没有指定路由器的 Router ID，则 OSPFv3 进程无法运行。

同一台设备上以及同一自治系统中不同的 OSPFv3 进程，必须为其指定不同的 Router ID。

【举例】

```
# 设置 OSPFv3 进程 1 的 Router ID 为 10.1.1.3。  
<Sysname> system-view  
[Sysname] ospfv3 1  
[Sysname-ospfv3-1] router-id 10.1.1.3
```

【相关命令】

- **ospfv3**

1.1.64 silent-interface (OSPFv3 view)

silent-interface 命令用来禁止接口收发 OSPFv3 报文。

undo silent-interface 命令用来取消禁止接口收发 OSPFv3 报文的配置。

【命令】

```
silent-interface { interface-type interface-number | all }  
undo silent-interface { interface-type interface-number | all }
```

【缺省情况】

允许接口收发 OSPFv3 报文。

【视图】

OSPFv3 视图

【缺省用户角色】

```
network-admin
```

context-admin

【参数】

interface-type interface-number: 接口类型和接口号，禁止指定 OSPFv3 接口收发 OSPFv3 报文。

all: 禁止所有 OSPFv3 接口收发 OSPFv3 报文。

【使用指导】

不同的进程可以对同一接口禁止收发 OSPFv3 报文,但 **silent-interface** 命令只对本进程已经使能的 OSPFv3 接口起作用,对其它进程的接口不起作用。

【举例】

禁止接口 GigabitEthernet1/0/1 在 OSPFv3 进程 100 和 200 中收发 OSPFv3 报文。

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] router-id 10.100.1.9
[Sysname-ospfv3-100] silent-interface gigabitethernet 1/0/1
[Sysname-ospfv3-100] quit
[Sysname] ospfv3 200
[Sysname-ospfv3-200] router-id 20.100.1.9
[Sysname-ospfv3-200] silent-interface gigabitethernet 1/0/1
```

1.1.65 snmp context-name

snmp context-name 命令用来创建一个管理 OSPFv3 的 SNMP 实体所使用的上下文名称。

undo snmp context-name 命令用来恢复缺省情况。

【命令】

snmp context-name context-name

undo snmp context-name

【缺省情况】

不存在管理 OSPFv3 的 SNMP 实体所使用的上下文名称。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

context-name: 管理 OSPFv3 的 SNMP 实体所使用的上下文名称,为 1~32 个字符的字符串,区分大小写。

【使用指导】

OSPFv3 使用 MIB (Management Information Base, 管理信息库) 为 NMS (Network Management System, 网络管理系统) 提供对 OSPFv3 实例的管理,但标准 OSPFv3 MIB 中定义的 MIB 为单实

例管理对象，无法对多个 OSPFv3 实例进行管理。因此，参考 RFC 4750 中对 OSPF 多实例的管理方法，为管理 OSPFv3 的 SNMP 实体定义一个上下文名称，以此来区分不同的 OSPFv3 实例，实现对多个 OSPFv3 实例进行管理。由于上下文名称只是 SNMPv3 独有的概念，对于 SNMPv1/v2c，会将团体名映射为上下文名称以对不同协议进行区分。

【举例】

```
# 配置管理 OSPFv3 进程 1 的 SNMP 实体所使用的上下文名称为 mib。  
<Sysname> system-view  
[Sysname] ospfv3 1  
[Sysname-ospfv3-1] snmp context-name mib
```

1.1.66 snmp trap rate-limit

snmp trap rate-limit 命令用来配置 OSPFv3 在指定时间间隔内允许输出的告警信息条数。
undo snmp trap rate-limit 命令用来恢复缺省情况。

【命令】

```
snmp trap rate-limit interval trap-interval count trap-number  
undo snmp trap rate-limit
```

【缺省情况】

OSPFv3 在 10 内秒允许输出 7 条告警信息。

【视图】

OSPFv3 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

interval trap-interval: 指定时间间隔，取值范围为 2~60，单位为秒。

count trap-number: 在指定时间间隔内允许输出的告警信息条数，取值范围为 0~300，为 0 时表示不输出告警信息。

【举例】

```
# 配置 OSPFv3 在 5 秒内允许输出 10 条告警信息。  
<Sysname> system-view  
[Sysname] ospfv3 100  
[Sysname-ospfv3-100] snmp trap rate-limit interval 5 count 10
```

1.1.67 snmp-agent trap enable ospfv3

snmp-agent trap enable ospfv3 命令用来开启 OSPFv3 的告警功能。
undo snmp-agent trap enable ospfv3 命令用来关闭 OSPFv3 的告警功能。

【命令】

```
snmp-agent trap enable ospfv3 [ grrestarter-status-change |  
grhelper-status-change | if-state-change | if-cfg-error | if-bad-pkt |  
neighbor-state-change | nssatranslator-status-change | virtif-bad-pkt |  
virtif-cfg-error | virtif-state-change | virtgrhelper-status-change |  
virtneighbor-state-change ] *  
  
undo snmp-agent trap enable ospfv3 [ grrestarter-status-change |  
grhelper-status-change | if-state-change | if-cfg-error | if-bad-pkt |  
neighbor-state-change | nssatranslator-status-change | virtif-bad-pkt |  
virtif-cfg-error | virtif-state-change | virtgrhelper-status-change |  
virtneighbor-state-change ] *
```

【缺省情况】

OSPFv3 的告警功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

grrestarter-status-change: GR Restarter 状态变化。

grhelper-status-change: 邻居 GR Helper 状态变化。

if-state-change: 接口状态变化。

if-cfg-error: 接口配置错误。

if-bad-pkt: 接口接收了错误报文。

neighbor-state-change: 邻居状态变化。

nssatranslator-status-change: NSSA 转换路由器状态变化。

virtif-bad-pkt: 虚接口接收错误报文。

virt-cfg-error: 虚接口配置错误。

virtif-state-change: 虚接口状态变化。

virtgrhelper-status-change: 虚接口邻居 GR Helper 状态变化。

virtneighbor-state-change: 虚接口邻居状态变化。

【举例】

关闭 OSPFv3 的告警功能。

<Sysname> system-view

[Sysname] undo snmp-agent trap enable ospfv3

1.1.68 spf-schedule-interval

spf-schedule-interval 命令用来配置 OSPFv3 路由计算的时间间隔。

undo spf-schedule-interval 命令用来恢复缺省情况。

【命令】

```
spf-schedule-interval          maximum-interval          [          minimum-interval  
[ incremental-interval ] ]  
undo spf-schedule-interval
```

【缺省情况】

OSPFv3 路由计算的最大时间间隔为 5 秒，最小时间间隔为 50 毫秒，时间间隔惩罚增量为 200 毫秒。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin
context-admin

【参数】

maximum-interval: OSPFv3 路由计算的最大时间间隔，取值范围为 1~60，单位为秒。

minimum-interval: OSPFv3 路由计算的最小时间间隔，取值范围为 10~60000，单位为毫秒。

incremental-interval: OSPFv3 路由计算的时间间隔惩罚增量，取值范围为 10~60000，单位为毫秒。

【使用指导】

根据本地维护的 LSDB，运行 OSPFv3 协议的路由器通过 SPF 算法计算出以自己为根的最短路径树，并根据这一最短路径树决定到目的网络的下一跳。通过调节 SPF 的计算间隔，可以抑制网络频繁变化可能导致的带宽资源和路由器资源被过多占用的问题。

本命令在网络变化不频繁的情况下将连续路由计算的时间间隔缩小到 *minimum-interval*，而在网络变化频繁的情况下可以进行相应惩罚，将等待时间按照配置的惩罚增量延长，最大不超过 *maximum-interval*。

minimum-interval 和 *incremental-interval* 配置值不允许大于 *maximum-interval* 配置值。

【举例】

```
# 设置 OSPFv3 路由计算最大时间间隔为 10 秒，最小时间间隔为 500 毫秒，惩罚增量为 300 毫秒。  
<Sysname> system-view  
[Sysname] ospfv3 100  
[Sysname-ospfv3-100] spf-schedule-interval 10 500 300
```

1.1.69 stub (OSPFv3 area view)

stub 命令用来配置一个区域为 Stub 区域。

undo stub 命令用来恢复缺省情况。

【命令】

```
stub [ default-route-advertise-always | no-summary ] *  
undo stub
```

【缺省情况】

没有区域被设置为 Stub 区域。

【视图】

OSPFv3 区域视图

【缺省用户角色】

network-admin
context-admin

【参数】

default-route-advertise-always: 该参数用于设置总是通告默认路由。

no-summary: 该参数只用于 Stub 区域的 ABR，配置后 ABR 只向区域内发布一条缺省路由的 Inter-Area-Prefix-LSA。这种既没有 AS-external-LSA，也没有其它 Inter-Area-Prefix-LSA、Inter-Area-Router-LSA 的 Stub 区域，又称为 Totally Stub 区域。

【使用指导】

如果需要在 ABR 上取消配置 no-summary 参数，可以通过重新执行 stub 命令覆盖之前配置即可。
如果要将一个区域配置成 Stub 区域，则该区域中的所有路由器都必须配置此属性。

【举例】

```
# 将 OSPFv3 区域 1 设置为 Stub 区域。  
<Sysname> system-view  
[Sysname] ospfv3 1  
[Sysname-ospfv3-1] area 1  
[Sysname-ospfv3-1-area-0.0.0.1] stub
```

【相关命令】

- **default-cost** (OSPFv3 area view)

1.1.1.70 stub-router

stub-router 命令用来配置当前路由器为 Stub 路由器。

undo stub-router 命令用来恢复缺省情况。

【命令】

```
stub-router r-bit [ include-stub | on-startup ] *  
stub-router max-metric [ external-lsa [ max-metric-value ] | summary-lsa  
[ max-metric-value ] | include-stub | on-startup ] *  
undo stub-router
```

【缺省情况】

当前路由器没有被配置为 Stub 路由器。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

r-bit: 路由器发布的 Type-1 LSA 中, options 域的 R-bit 将清除。

max-metric: 路由器发布的 Type-1 LSA 的链路度量值将设置为最大值 65535。

external-lsa max-metric-value: 路由器发布的外部 LSA 链路度量值。*max-metric-value* 表示链路度量值, 取值范围为 1~16777215, 缺省值为 16711680。

summary-lsa max-metric-value: 路由器发布的 Type-3 LSA 和 Type-4 LSA 链路度量值。*max-metric-value* 表示链路度量值, 取值范围为 1~16777215, 缺省值为 16711680。

include-stub: 路由器发布的引用 Type-1 LSA 的 Type-9 LSA 中, 链路度量值将设置为最大值 65535。

on-startup seconds: 在路由器重启期间, 路由器做为 Stub 路由器。*seconds* 表示超时时间, 取值范围为 5~86400, 单位为秒。

【使用指导】

将当前路由器配置为 Stub 路由器的功能, 可通过 R-bit 和 max-metric 两种模式来实现:

- **R-bit 模式**: 通过清除该路由器发布 Type-1 LSA 中 options 域的 R-bit, 使其他路由器不通过该路由器来转发数据。
- **max-metric 模式**: 该路由器发布的 Type-1 LSA 的链路度量值将设为最大值 65535, 这样其邻居计算出这条路由的开销就会很大, 如果邻居上有到这个目的地址开销更小的路由, 则数据不会通过这个 Stub 路由器转发。

【举例】

配置当前路由器为 Stub 路由器。

```
<Sysname> system-view
```

```
[Sysname] ospfv3 100
```

```
[Sysname-ospfv3-100] stub-router r-bit
```

1.1.71 transmit-pacing

transmit-pacing 用来配置接口发送 LSU 报文的时间间隔和一次发送 LSU 报文的最大个数。

undo transmit-pacing 命令用来恢复缺省情况。

【命令】

transmit-pacing interval *interval* count *count*

undo transmit-pacing

【缺省情况】

接口发送 LSU 报文的时间间隔为 20 毫秒，一次最多发送 3 个 LSU 报文。

【视图】

OSPFv3 视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval interval: 接口发送 LSU 报文的时间间隔，*interval* 的取值范围为 10~1000，单位为毫秒。当路由器上使能 OSPFv3 功能的接口数比较多时，建议增大该值，以控制路由器每秒钟发送 LSU 报文的总数。

count count: 接口一次发送 LSU 报文的最大个数，*count* 的取值范围为 1~200。当路由器上使能 OSPFv3 功能的接口数比较多时，建议减小该值，以控制路由器每秒钟发送 LSU 报文的总数。

【举例】

配置 OSPFv3 进程 1 的所有接口发送 LSU 报文的时间间隔为 30 毫秒，一次最多发送 10 个 LSU 报文。

```
<Sysname> system-view
```

```
[Sysname] ospfv3 1
```

```
[Sysname-ospfv3-1] transmit-pacing interval 30 count 10
```

1.1.72 vlink-peer (OSPFv3 area view)

vlink-peer 命令用来创建并配置一条虚连接。

undo vlink-peer 命令用来删除一条已有的虚连接。

【命令】

vlink-peer router-id [**dead seconds** | **hello seconds** | **instance instance-id** | **keychain keychain-name** | **retransmit seconds** | **trans-delay seconds**] *

undo vlink-peer router-id [**dead** | **hello** | **keychain** | **retransmit** | **trans-delay**] *

【缺省情况】

不存在虚连接。

【视图】

OSPFv3 区域视图

【缺省用户角色】

network-admin

context-admin

【参数】

router-id: 虚连接邻居的路由器 ID。

dead seconds: 失效时间间隔, 取值范围为 1~32768, 单位为秒, 缺省值为 40 秒。该值必须和与其建立虚连接路由器的 **dead seconds** 值相等, 并至少为 **hello seconds** 值的 4 倍。

hello seconds: 接口发送 Hello 报文的时间间隔, 取值范围为 1~8192, 单位为秒, 缺省值为 10 秒。该值必须和与其建立虚连接路由器上的 **hello seconds** 值相等。

instance instance-id: 设置虚连接的实例 ID, 取值范围为 0~255, 缺省值为 0。

keychain: 使用 keychain 验证模式。

keychain-name: keychain 名称, 为 1~63 个字符的字符串, 区分大小写。

retransmit seconds: 接口重传 LSA 报文的时间间隔, 取值范围为 1~3600, 单位为秒, 缺省值为 5。

trans-delay seconds: 接口延迟发送 LSA 报文的时间间隔, 取值范围为 1~3600, 单位为秒, 缺省值为 1。

【使用指导】

对于没有和骨干区域直接相连的非骨干区域, 或者不连续的骨干区域来说, 可以使用 **vlink-peer** 命令建立逻辑上的连通性。在某种程度上, 可以将虚连接看作一个普通的使能了 OSPFv3 的接口, 因为在其上配置的 **hello**、**dead**、**retransmit** 和 **trans-delay** 等参数的原理是类似的。

虚连接的两端必须是 ABR, **vlink-peer** 命令必须在两端同时配置才可生效。

各参数取值规则如下:

- **hello** 值越小, 发现网络变化的速度越快, 消耗的网络资源也就越多。
- 不能将 **retransmit** 值设置的太小, 否则将会引起不必要的重传。网络速度相对较慢的时候应把该值设的更大一些。
- 设置 **trans-delay** 值时必须考虑接口的发送延迟。

在 OSPFv3 虚连接下配置的验证模式, 其优先级高于在骨干区域下配置的验证模式。只有在 OSPFv3 虚连接下未配置验证模式时, 骨干区域下配置的验证模式才会对该虚连接生效。

在 OSPFv3 虚连接使用 keychain 验证模式时, 报文的收、发过程如下:

- OSPFv3 在发送报文前, 会先从 keychain 获取当前的有效发送 key, 然后发送报文。如果当前不存在有效发送 key, 则不会发送报文。
- OSPFv3 在收到报文后, 会根据报文携带的 key 的标识符从本地 keychain 中查找具有相同标识符的 key, 找到且该 key 为有效 key, 则根据该 key 的认证算法和认证密钥对报文进行校验, 校验成功后再对报文进行下一步处理。如果报文校验失败, 或者根据报文中携带的 key 的标识符无法从 keychain 中获取到有效接收 key, 则该报文将被丢弃。

对于 keychain 认证算法和 key 的标识符的范围, OSPFv3 的支持情况如下:

- OSPFv3 仅支持 HMAC-SHA-256 认证算法。
- OSPFv3 仅支持 keychain 中 **key-id** 的范围在 0~65535 的 key, 如果接收报文中的 **key-id** 不在这个范围内, 则该报文将被丢弃。

【举例】

创建一条到 10.10.0.3 的虚连接。

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] vlink-peer 10.10.0.3
```

【相关命令】

- `display ospfv3 vlink`

目 录

1 IPv6 策略路由	1-1
1.1 IPv6 策略路由配置命令	1-1
1.1.1 apply access-vpn	1-1
1.1.2 apply continue	1-2
1.1.3 apply default-next-hop	1-2
1.1.4 apply default-output-interface	1-3
1.1.5 apply loadshare	1-4
1.1.6 apply next-hop	1-6
1.1.7 apply output-interface	1-7
1.1.8 apply precedence	1-8
1.1.9 apply remark-vpn	1-9
1.1.10 display ipv6 policy-based-route	1-10
1.1.11 display ipv6 policy-based-route interface	1-11
1.1.12 display ipv6 policy-based-route local	1-13
1.1.13 display ipv6 policy-based-route setup	1-14
1.1.14 if-match acl	1-15
1.1.15 if-match packet-length	1-16
1.1.16 ipv6 local policy-based-route	1-16
1.1.17 ipv6 policy-based-route (interface view)	1-17
1.1.18 ipv6 policy-based-route (system view)	1-18
1.1.19 reset ipv6 policy-based-route statistics	1-19

1 IPv6 策略路由

1.1 IPv6策略路由配置命令

1.1.1 apply access-vpn

apply access-vpn 命令用来设置报文在公网或指定 VPN 实例中进行转发。

undo apply access-vpn 命令用来取消报文在公网或指定 VPN 实例中进行转发的设置。

【命令】

apply access-vpn { public | vpn-instance vpn-instance-name <1-4> }

undo apply access-vpn { public | vpn-instance [vpn-instance-name <1-4>] }

【缺省情况】

设备根据路由表在公网或 VPN 内转发报文。

【视图】

IPv6 策略节点视图

【缺省用户角色】

network-admin

context-admin

【参数】

public: 设置报文在公网中进行转发。

vpn-instance: 设置报文在指定 VPN 实例中进行转发。

vpn-instance-name <1-4>: 指定 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。指定的 VPN 实例必须已经存在。**<1-4>** 表示前面的参数最多可以输入 4 次。

【使用指导】

本命令用于在某些特殊组网中在不同网络间转发报文，例如将公网接收到的报文发送到某个 VPN 中，或者在 VPN 之间转发报文。

用户可通过重复执行本命令来指定公网和 VPN 实例。设备将根据配置顺序查找公网或第一个可用的 VPN 实例中的转发表进行转发。

执行 **undo apply access-vpn vpn-instance [vpn-instance-name <1-4>]** 命令时，如果仅指定了 **vpn-instance** 关键字，那么节点上的所有 VPN 实例配置会被删除。

当节点上所有的 VPN 实例配置和公网配置均被删除后，设备恢复缺省转发方式，根据路由表在公网或 VPN 内转发报文。

【举例】

在策略节点中设置报文在名为 vpn1、vpn2 的 VPN 实例中进行转发（VPN 实例 vpn1、vpn2 已存在）。

```

<Sysname> system-view
[Sysname] ipv6 policy-based-route policy1 permit node 10
[Sysname-pbr6-policy1-10] apply access-vpn vpn-instance vpn1 vpn2
# 在策略节点中设置报文在公网中进行转发。
<Sysname> system-view
[Sysname] ipv6 policy-based-route policy1 permit node 10
[Sysname-pbr6-policy1-10] apply access-vpn public

```

【相关命令】

- **apply remark-vpn**

1.1.2 apply continue

apply continue 命令用来设置匹配成功的当前节点指定转发路径失败后，继续进行后续节点的处理。

undo apply continue 命令用来恢复缺省情况。

【命令】

```

apply continue
undo apply continue

```

【缺省情况】

匹配成功的当前节点指定转发路径失败后，不再进行下一节点的匹配。

【视图】

IPv6 策略节点视图

【缺省用户角色】

```

network-admin
context-admin

```

【使用指导】

本命令仅在策略节点的匹配模式为 **permit** 时生效。

在配置了该命令后，如果当前节点中未配置影响报文转发路径的 **apply** 子句(**apply access-vpn**、**apply next-hop**、**apply output-interface**、**apply default-next-hop** 和 **apply default-output-interface**)，或者配置了这些子句中的一个或多个，但配置的子句都失效（下一跳不可达、出接口 down 或者报文在指定 VPN 内转发失败）时，会进行下一节点的处理。

【举例】

设置匹配成功的当前节点转发失败后继续进行后续节点的处理。

```

<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply continue

```

1.1.3 apply default-next-hop

apply default-next-hop 命令用来设置指导报文转发的缺省下一跳。

undo apply default-next-hop 命令用来取消指导报文转发的缺省下一跳的设置。

【命令】

```
apply default-next-hop [ vpn-instance vpn-instance-name | inbound-vpn ]
{ ipv6-address [ direct ] [ track track-entry-number ] }&<1-4>
undo apply default-next-hop [ [ vpn-instance vpn-instance-name |
inbound-vpn ] ipv6-address&<1-4> ]
```

【缺省情况】

未设置指导报文转发的缺省下一跳。

【视图】

IPv6 策略节点视图

【缺省用户角色】

network-admin
context-admin

【参数】

vpn-instance *vpn-instance-name*: 缺省下一跳所在的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。指定的 VPN 实例必须已经存在。

inbound-vpn: 报文入接口所在的 VPN 实例。

ipv6-address: 缺省下一跳的 IPv6 地址。如果未指定 **vpn-instance** 或 **inbound-vpn** 参数，表示指定的是公网下一跳。

direct: 指定当前缺省下一跳生效的条件为直连下一跳。

track track-entry-number: 指定 Track 项的序号，*track-entry-number* 取值范围为 1~1024。

&<1-4>: 表示前面的参数最多可以输入 4 次。

【使用指导】

用户可以同时配置多个缺省下一跳（通过一次或多次配置本命令实现），起到主备或负载分担的作用。

配置 **undo** 命令时，如果指定了缺省下一跳 IPv6 地址，将取消已配置的该缺省下一跳；如果未指定缺省下一跳 IPv6 地址，将取消已配置的所有缺省下一跳。

【举例】

```
# 设置指导报文转发的缺省直连下一跳为 1:1::1:1。
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-next-hop 1:1::1:1 direct
```

【相关命令】

- **apply loadshare**

1.1.4 apply default-output-interface

apply default-output-interface 命令用来设置指导报文转发的缺省出接口。

undo apply default-output-interface 命令用来取消指导报文转发的缺省出接口的设置。

【命令】

```
apply default-output-interface { interface-type interface-number [ track  
track-entry-number ] }<1-4>  
undo apply default-output-interface [ { interface-type  
interface-number }<1-4> ]
```

【缺省情况】

未设置指导报文转发的缺省出接口。

【视图】

IPv6 策略节点视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface-type interface-number: 指定接口类型和接口编号。

track track-entry-number: 指定 Track 项的序号, *track-entry-number* 取值范围为 1~1024。

<1-4>: 表示前面的参数最多可以输入 4 次。

【使用指导】

用户可以同时配置多个缺省出接口（通过一次或多次配置本命令实现），起到主备或负载分担的作用。

指定缺省出接口类型需配置为 P2P（Point-to-Point，点到点）接口，对于非 P2P 接口（广播类型的接口和 NBMA 类型的接口），比如以太网接口、Virtual-Template 接口，由于有多个可能的下一跳，可能会造成报文转发不成功的现象。NBMA（Non Broadcast MultiAccess，非广播多路访问）指全连通、非广播、多点可达的网络，这种网络采用单播方式发送报文。

配置 **undo** 命令时，如果指定了接口，将取消已配置的该缺省出接口；如果未指定接口，将取消已配置的所有缺省出接口。

【举例】

```
# 设置报文的缺省出接口为 GigabitEthernet1/0/1。  
<Sysname> system-view  
[Sysname] ipv6 policy-based-route aa permit node 11  
[Sysname-pbr6-aa-11] apply default-output-interface gigabitethernet 1/0/1
```

【相关命令】

- **apply loadshare**

1.1.5 apply loadshare

apply loadshare 命令用来设置多个下一跳（缺省下一跳、缺省出接口、下一跳和出接口）工作在负载分担模式。

undo apply loadshare 命令用来恢复缺省情况。

【命令】

```
apply loadshare { default-next-hop | default-output-interface | next-hop |  
output-interface }  
undo apply loadshare { default-next-hop | default-output-interface |  
next-hop | output-interface }
```

【缺省情况】

多个下一跳（缺省下一跳、缺省出接口、下一跳和出接口）工作在主备模式。

【视图】

IPv6 策略节点视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

default-next-hop: 设置指导报文转发的多个缺省下一跳工作在负载分担模式。

default-output-interface: 设置指导报文转发的多个缺省出接口工作在负载分担模式。

next-hop: 设置指导报文转发的多个下一跳工作在负载分担模式。

output-interface: 设置指导报文转发的多个出接口工作在负载分担模式。

【使用指导】

多个出接口（缺省下一跳、缺省出接口、下一跳和出接口）的工作模式有两种：主备模式、负载分担模式。以多个出接口为例：

- 主备模式：按照配置顺序，以第一个配置出的接口作为主用出接口，指导报文转发。当主用出接口失效时，按配置顺序选择后续的第一个有效的出接口指导报文转发。
- 负载分担模式：出接口的负载分担方式，如果不匹配快速转发表，则按照配置顺序逐包轮流选择有效的出接口指导报文转发；如果匹配快速转发表，则按照配置顺序逐流轮流选择有效的出接口指导报文转发。下一跳的负载分担模式会按照下一跳的权重指导报文转发。缺省情况下，多个下一跳会按照缺省的权重值平均分配带宽，多个下一跳的转发流量的比例是相同的。

缺省下一跳和缺省出接口的情况请参考多个出接口。

【举例】

设置多个下一跳工作在负载分担模式。

```
<Sysname> system-view  
[Sysname] ipv6 policy-based-route aa permit node 11  
[Sysname-pbr6-aa-11] apply next-hop 1::1 2::2  
[Sysname-pbr6-aa-11] apply loadshare next-hop
```

设置多个出接口工作在负载分担模式。

```
<Sysname> system-view  
[Sysname] ipv6 policy-based-route aa permit node 11  
[Sysname-pbr6-aa-11] apply output-interface gigabitethernet 1/0/1 gigabitethernet 1/0/2
```



```

[Sysname-pbr6-aa-11] apply loadshare output-interface
# 设置多个缺省下一跳工作在负载分担模式。
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-next-hop 1::1 2::2
[Sysname-pbr6-aa-11] apply loadshare default-next-hop
# 设置多个缺省出接口工作在负载分担模式。
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default-output-interface gigabitethernet 1/0/1 gigabitethernet
1/0/2
[Sysname-pbr6-aa-11] apply loadshare default-output-interface

```

【相关命令】

- **apply default-next-hop**
- **apply default-output-interface**
- **apply next-hop**
- **apply output-interface**

1.1.6 apply next-hop

apply next-hop 命令用来设置报文转发的下一跳。

undo apply next-hop 命令用来取消报文转发下一跳的设置。

【命令】

```

apply next-hop [ vpn-instance vpn-instance-name | inbound-vpn ]
{ ipv6-address [ direct ] [ track track-entry-number ] [ weight weight-value ] }
&<1-4>

undo apply next-hop [ [ vpn-instance vpn-instance-name | inbound-vpn ]
ipv6-address&<1-4> ]

```

【缺省情况】

未设置报文转发的下一跳。

【视图】

IPv6 策略节点视图

【缺省用户角色】

```

network-admin
context-admin

```

【参数】

vpn-instance *vpn-instance-name*: 下一跳所在的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。指定的 VPN 实例必须已经存在。

inbound-vpn: 报文入接口所在的 VPN 实例。

ipv6-address: 下一跳 IPv6 地址。如果未指定 **vpn-instance** 或 **inbound-vpn** 参数, 表示指定的是公网下一跳。

direct: 指定当前下一跳生效的条件为直连下一跳。

track track-entry-number: 指定 Track 项的序号, *track-entry-number* 取值范围为 1~1024。

weight weight-value: 指定下一跳负载分担的权重。设备根据权重确定该下一跳转发流量的比例。例如, 三个下一跳配置的负载分担权重分别为 1、1 和 2, 则它们的负载分担的比例分别为 1/4、1/4 和 1/2。*weight-value* 取值范围为 1~100, 缺省值为 10。

&<1-4>: 表示前面的参数最多可以输入 4 次。

【使用指导】

用户可以同时配置多个下一跳（通过一次或多次配置本命令实现），起到主备或负载分担的作用。

配置 **undo** 命令时, 如果指定了下一跳 IPv6 地址, 将取消已配置的该下一跳; 如果未指定下一跳 IPv6 地址, 将取消已配置的所有下一跳。

【举例】

```
# 设置报文转发的下一跳为 1::1。
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply next-hop 1::1
```

【相关命令】

- **apply loadshare**

1.1.7 apply output-interface

apply output-interface 命令用来设置指导报文转发的出接口。

undo apply output-interface 命令用来取消指导报文转发的出接口的设置。

【命令】

```
apply output-interface { interface-type interface-number [ track  
track-entry-number ] }&<1-4>
```

```
undo apply output-interface [ { interface-type interface-number }&<1-4> ]
```

【缺省情况】

未设置指导报文转发的出接口。

【视图】

IPv6 策略节点视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type interface-number: 指定接口类型和接口编号。

track track-entry-number: 指定 Track 项的序号, *track-entry-number* 取值范围为 1~1024。

&<1-4>: 表示前面的参数最多可以输入 4 次。

【使用指导】

用户可以同时配置多个出接口（通过一次或多次配置本命令实现），起到主备或负载分担的作用。指定出接口类型需配置为 P2P 接口，对于非 P2P 接口（广播类型的接口和 NBMA 类型的接口），比如以太网接口、Virtual-Template 接口，由于有多个可能的下一跳，可能会造成报文转发不成功的现象。

配置 **undo** 命令时，如果指定了接口，将取消已配置的该出接口；如果未指定接口，将取消已配置的所有出接口。

【举例】

```
# 对已经匹配的 IPv6 报文指定出接口为 GigabitEthernet1/0/1。
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply output-interface gigabitethernet 1/0/1
```

【相关命令】

- **apply loadshare**

1.1.8 apply precedence

apply precedence 命令用来设置 IPv6 报文的优先级。

undo apply precedence 命令用来恢复缺省情况。

【命令】

```
apply precedence { type | value }
undo apply precedence
```

【缺省情况】

未设置 IPv6 报文的优先级。

【视图】

IPv6 策略节点视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

type: IPv6 报文的优先级类型。

value: IPv6 报文的优先级值, IPv6 报文共有 8 (0~7) 个优先级, 每个数值对应一个优先级类型。在输入参数的时候可以输入数值, 也可以输入优先级类型。对应关系如 [表 1-1](#) 所示。

表1-1 IPv6 优先级值与优先级类型对应表

优先级值	优先级类型
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

【举例】

```
# 设置 IPv6 报文的优先级为 5（critical）。
<Sysname> system-view
[Sysname]ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply precedence critical
```

1.1.9 apply remark-vpn

apply remark-vpn 命令用来重标记报文所属的 VPN。

undo apply remark-vpn 命令用来恢复缺省情况。

【命令】

```
apply remark-vpn
undo apply remark-vpn
```

【缺省情况】

未重标记报文所属的 VPN。

【视图】

策略节点视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

一般情况下，配置 **apply access-vpn** 命令后，设备仅在指定的 VPN 实例内转发报文，但不会重标记报文所属的 VPN，后续业务模块学到的还是报文中之前的 VPN 实例。如果需要重标记报文所属的 VPN 信息，则需要配置本命令。

本命令必须和 **apply access-vpn** 命令同时使用。只有配置了 **apply access-vpn** 命令成功指导报文转发时，本命令才能重标记报文所属的 VPN 信息，标记的 VPN 实例是生效的 **apply access-vpn** 命令配置的 VPN 实例。

【举例】

```
# 重标记匹配 ACL 3000 的报文所属的 VPN 实例为 vpn1。
<Sysname> system-view
[Sysname] ipv6 policy-based-route aaa permit node 10
[Sysname-pbr6-aaa-10] if-match acl 3000
[Sysname-pbr6-aaa-10] apply access-vpn vpn-instance vpn1
[Sysname-pbr6-aaa-10] apply remark-vpn
```

【相关命令】

- **apply access-vpn**

1.1.10 display ipv6 policy-based-route

display ipv6 policy-based-route 命令用来显示已经配置的 IPv6 策略。

【命令】

```
display ipv6 policy-based-route [ policy policy-name ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

policy policy-name: 显示指定的 IPv6 策略。*policy-name* 表示策略名，唯一标识一个 IPv6 策略，为 1~19 个字符的字符串，区分大小写。如果未指定本参数，则显示所有已经配置的 IPv6 策略。

【举例】

```
# 显示所有已经配置的 IPv6 策略。
<Sysname> display ipv6 policy-based-route
Policy name: aaa
  node 1 permit:
    if-match acl 2000
    apply next-hop 1000::1
```

表1-2 display ipv6 policy-based-route 命令显示信息描述表

字段	描述
Policy name	策略名
node 1 permit	节点1的匹配模式为允许
if-match acl	满足ACL的报文被匹配
apply next-hop	为匹配的报文指定下一跳

【相关命令】

- **ipv6 policy-based-route** (system view)

1.1.11 display ipv6 policy-based-route interface

display ipv6 policy-based-route interface 命令用来显示接口下 IPv6 转发策略路由的配置信息和统计信息。

【命令】

display ipv6 policy-based-route interface *interface-type interface-number*
[**slot slot-number**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-type interface-number: 用来指定接口的类型和编号。

slot slot-number: 显示指定成员设备上 IPv6 转发策略路由的配置信息和统计信息。

slot-number 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示主设备上 IPv6 转发策略路由的配置信息和统计信息。

【举例】

显示接口 GigabitEthernet1/0/1 下 IPv6 转发策略路由的配置信息和统计信息。

```
<Sysname> display ipv6 policy-based-route interface gigabitethernet 1/0/1
Policy based routing information for interface GigabitEthernet1/0/1(failed):
Policy name: aaa
  node 0 deny:
    Matched: 0
  node 1 permit:
    if-match acl 3999
    Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 1000::1
    apply output-interface GigabitEthernet1/0/2 track 1 (down)
    apply output-interface GigabitEthernet1/0/3 track 2 (inactive)
    Matched: 0
  node 5 permit:
    if-match acl 3101
    apply next-hop 1000::1
```

```

    Matched: 0
Total matched: 0
<Sysname> display ipv6 policy-based-route interface gigabitethernet 1/0/1
Policy based routing information for interface GigabitEthernet1/0/1:
Policy name: aaa
    node 0 deny(not support):
        Matched: 0
    node 1 permit:
        if-match acl 3999
        Matched: 0
    node 2 permit(no resource):
        if-match acl 2000
        apply next-hop 1000::1
        apply output-interface GigabitEthernet1/0/2 track 1 (down)
        apply output-interface GigabitEthernet1/0/3 track 2 (inactive)
        Matched: 0
    node 5 permit:
        if-match acl 3101
        apply next-hop 1000::1
        Matched: 0 (no statistics resource)
Total matched: 0

```

表1-3 display ipv6 policy-based-route interface 命令显示信息描述表

字段	描述
Policy based routing information for interface XXXX (failed)	接口下IPv6转发策略路由的配置信息和统计信息(failed表示策略下发驱动失败。只有在接口上删除IPv6转发策略路由，再重新创建IPv6转发策略路由，显示信息才能刷新)  说明 对于设备上的全局口（如 VLAN 接口）和物理口，只有指定 slot 后，才会显示括号内的信息。
Policy name	策略名
node 0 deny(not support) node 2 permit(no resource)	节点的匹配模式为允许（permit）/拒绝（deny）（not support表示设备不支持该节点设置的规则；no resource表示设备的ACL等资源不足，为该节点分配ACL等资源失败）  说明 对于设备上的全局口（如 VLAN 接口）和物理口，只有指定 slot 后，才会显示括号内的信息。
if-match acl	满足ACL的报文被匹配
apply next-hop	为匹配的报文指定下一跳
apply output-interface track 1 (down)	为匹配的报文指定出接口。括号中显示接口的状态：up、down、inactive。接口不在位时，显示inactive；接口网络层down时，显示down

字段	描述
Matched: 0 (no statistics resource)	节点匹配成功的次数（no statistics resource表示统计资源不足）  说明 对于设备上的全局口（如 VLAN 接口）和物理口，只有指定 slot 后，才会显示括号内的信息。
Total matched	策略所有节点匹配成功的次数

【相关命令】

- **reset ipv6 policy-based-route statistics**

1.1.12 display ipv6 policy-based-route local

display ipv6 policy-based-route local 命令用来显示 IPv6 本地策略路由的配置信息和统计信息。

【命令】

display ipv6 policy-based-route local [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number：显示指定成员设备上 IPv6 本地策略路由的配置信息和统计信息。
slot-number 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示主设备上 IPv6 本地策略路由的配置信息和统计信息。

【举例】

```
# 显示 IPv6 本地策略路由的配置信息和统计信息。
<Sysname> display ipv6 policy-based-route local
Policy based routing information for local:
Policy name: aaa
  node 0 deny:
    Matched: 0
  node 1 permit:
    if-match acl 3999
    Matched: 0
  node 2 permit:
    if-match acl 2000
    apply next-hop 1::1
```



```

Matched: 0
node 5 permit:
  if-match acl 3101
  apply next-hop 2::2
Matched: 0
Total matched: 0

```

表1-4 display ipv6 policy-based-route local 命令显示信息描述表

字段	描述
Policy based routing information for local	IPv6本地策略路由的配置信息和统计信息
Policy name	策略名
node 0 deny/node 2 permit	节点的匹配模式为允许（permit）/拒绝（deny）
if-match acl	满足ACL的报文被匹配
apply next-hop	为匹配的报文指定下一跳
Matched: 0	节点匹配成功的次数
Total matched	策略所有节点匹配成功的次数

【相关命令】

- **reset ipv6 policy-based-route statistics**

1.1.13 display ipv6 policy-based-route setup

display ipv6 policy-based-route setup 命令用来显示已经应用的 IPv6 策略路由信息。

【命令】

display ipv6 policy-based-route setup

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【举例】

```

# 显示已经应用的 IPv6 策略路由信息。
<Sysname> display ipv6 policy-based-route setup
Policy Name      Interface Name
pr01             GigabitEthernet1/0/1

```

表1-5 display ipv6 policy-based-route setup 命令显示信息描述表

字段	描述
Policy name	策略名
Interface Name	应用策略的接口

【相关命令】

- **ipv6 policy-based-route (interface view)**

1.1.14 if-match acl

if-match acl 命令用来设置 ACL 匹配规则。

undo if-match acl 命令用来恢复缺省情况。

【命令】

```
if-match acl { ipv6-acl-number | name ipv6-acl-name }
undo if-match acl
```

【缺省情况】

未设置 ACL 匹配规则。

【视图】

IPv6 策略节点视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-acl-number: 访问控制列表号，取值范围为 2000～3999。其中：

- IPv6 基本 ACL，**ipv6-acl-number** 取值范围为 2000～2999；
- IPv6 高级 ACL，**ipv6-acl-number** 取值范围为 3000～3999。

name ipv6-acl-name: 指定 IPv6 ACL 的名称。**ipv6-acl-name** 表示 IPv6 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，IPv6 ACL 的名称不允许使用英文单词 **all**。只有指定 IPv6 基本 ACL 或 IPv6 高级 ACL 的 **acl-name** 才生效。

【举例】

设置满足 ACL 2000 的报文被匹配。

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 10
[Sysname-pbr6-aa-10] if-match acl 2000
```

设置满足 ACL 名称为 aaa 的报文被匹配。

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 10
[Sysname-pbr6-aa-10] if-match acl name aaa
```

1.1.15 if-match packet-length

if-match packet-length 命令用来设置 IPv6 报文长度匹配规则。

undo if-match packet-length 命令用来恢复缺省情况。

【命令】

```
if-match packet-length min-len max-len  
undo if-match packet-length
```

【缺省情况】

未设置 IPv6 报文长度匹配规则。

【视图】

IPv6 策略节点视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

min-len: 最短 IPv6 报文长度, 取值范围为 1~65535, 单位为字节。

max-len: 最长 IPv6 报文长度, 取值范围为 1~65535, 单位为字节。*max-len* 应该不小于 *min-len*。

【使用指导】

长度匹配含边界值, 如指定 *min-len* 为 100, *max-len* 为 200, 报文长度为 100 与 200 的报文都是匹配报文。

【举例】

```
# 设置报文长度在 100~200 字节之间的报文被匹配。  
<Sysname> system-view  
[Sysname] ipv6 policy-based-route aa permit node 11  
[Sysname-pbr6-aa-11] if-match packet-length 100 200
```

1.1.16 ipv6 local policy-based-route

ipv6 local policy-based-route 命令用来对本地报文应用 IPv6 策略。

undo ipv6 local policy-based-route 命令用来恢复缺省情况。

【命令】

```
ipv6 local policy-based-route policy-name  
undo ipv6 local policy-based-route
```

【缺省情况】

未对本地报文应用 IPv6 策略。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 策略名, 唯一标识一个 IPv6 策略, 为 1~19 个字符的字符串, 区分大小写。该 IPv6 策略必须已经存在。

【使用指导】

对本地报文只能应用一个 IPv6 策略。应用新的 IPv6 策略前必须删除本地原来已经应用的 IPv6 策略。
对本地报文应用的 IPv6 策略将对本地产生的所有 IPv6 报文（除了本地发送给自己的报文）进行匹配。若无特殊需求, 建议用户不要配置本地策略路由。

【举例】

```
# 对本地报文应用 IPv6 策略 aaa。  
<Sysname> system-view  
[Sysname] ipv6 local policy-based-route aaa
```

【相关命令】

- **display ipv6 policy-based-route setup**
- **ipv6 policy-based-route (system view)**

1.1.17 ipv6 policy-based-route (interface view)

ipv6 policy-based-route 命令用来对接口转发的报文应用 IPv6 策略。

undo ipv6 policy-based-route 命令用来恢复缺省情况。

【命令】

```
ipv6 policy-based-route policy-name  
undo ipv6 policy-based-route
```

【缺省情况】

未对接口转发的报文应用 IPv6 策略。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 策略名, 唯一标识一个 IPv6 策略, 为 1~19 个字符的字符串, 区分大小写。该 IPv6 策略必须已经存在。

【举例】

```
# 对接口 GigabitEthernet1/0/1 转发的报文应用 IPv6 策略 aaa。  
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 policy-based-route aaa
```

【相关命令】

- **display ipv6 policy-based-route setup**
- **ipv6 policy-based-route (system view)**

1.1.18 ipv6 policy-based-route (system view)

ipv6 policy-based-route 命令用来创建 IPv6 策略节点，并进入 IPv6 策略节点视图。如果指定的 IPv6 策略节点已创建，则该命令直接用来进入该 IPv6 策略节点的视图。

undo ipv6 policy-based-route 命令用来删除已创建的 IPv6 策略或 IPv6 策略节点。

【命令】

```
ipv6 policy-based-route policy-name [ deny | permit ] node node-number
undo ipv6 policy-based-route policy-name [ deny | node node-number | permit ]
```

【缺省情况】

不存在 IPv6 策略节点。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: 策略名，唯一标识一个 IPv6 策略，为 1~19 个字符的字符串，区分大小写。

deny: 指定节点的匹配模式为拒绝模式。

permit: 指定节点的匹配模式为允许模式。缺省匹配模式为 **permit**。

node node-number: IPv6 策略节点。节点编号越小优先级越高，先对优先级高的节点进行匹配操作。

【使用指导】

删除 IPv6 策略之前，必须先取消该 IPv6 策略在所有接口上的应用，否则删除失败。

配置 **undo** 命令时，如果指定了策略节点，将删除指定的节点；如果指定了节点模式，将按模式删除策略内所有与该模式匹配的所有节点；如果两者都未指定，将删除整个策略。

【举例】

配置一个 IPv6 策略 **aaa**，其节点序列号为 **10**，匹配模式为 **permit**，并进入 IPv6 策略节点视图。

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aaa permit node 10
[Sysname-pbr6-aaa-10]
```

【相关命令】

- **display ipv6 policy-based-route**

1.1.19 reset ipv6 policy-based-route statistics

reset ipv6 policy-based-route statistics 命令用来清除 IPv6 策略路由的统计信息。

【命令】

reset ipv6 policy-based-route statistics [*policy policy-name*]

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

policy *policy-name*: 清除指定 IPv6 策略的统计信息。*policy-name* 表示策略名，唯一标识一个 IPv6 策略，为 1~19 个字符的字符串，区分大小写。如果未指定本参数，则清除所有策略路由的统计信息。

【举例】

清除所有配置 IPv6 策略的统计信息。

```
<Sysname> reset ipv6 policy-based-route statistics
```

【相关命令】

- **display ipv6 policy-based-route interface**
- **display ipv6 policy-based-route local**

目 录

1 路由策略.....	1-1
1.1 路由策略公共配置命令.....	1-1
1.1.1 apply cost	1-1
1.1.2 apply cost-type.....	1-1
1.1.3 apply ip-precedence	1-2
1.1.4 apply preference.....	1-3
1.1.5 apply prefix-priority.....	1-3
1.1.6 apply tag.....	1-4
1.1.7 continue	1-5
1.1.8 description	1-5
1.1.9 display route tag-list	1-6
1.1.10 display route-policy.....	1-7
1.1.11 if-match cost	1-8
1.1.12 if-match interface	1-8
1.1.13 if-match route-type	1-9
1.1.14 if-match tag	1-10
1.1.15 if-match tag-list.....	1-11
1.1.16 route tag-list.....	1-11
1.1.17 route-policy.....	1-12
1.2 IPv4 路由策略配置命令	1-13
1.2.1 apply fast-reroute.....	1-13
1.2.2 apply ip-address next-hop	1-14
1.2.3 display ip prefix-list.....	1-15
1.2.4 if-match ip	1-16
1.2.5 ip prefix-list.....	1-17
1.2.6 reset ip prefix-list	1-18
1.3 IPv6 路由策略配置命令	1-19
1.3.1 apply ipv6 fast-reroute	1-19
1.3.2 apply ipv6 next-hop	1-20
1.3.3 display ipv6 prefix-list	1-21
1.3.4 if-match ipv6	1-22
1.3.5 ipv6 prefix-list.....	1-23
1.3.6 reset ipv6 prefix-list	1-24

1 路由策略

1.1 路由策略公共配置命令

1.1.1 apply cost

apply cost 命令用来配置路由信息的路由开销。

undo apply cost 命令用来恢复缺省情况。

【命令】

apply cost [+ | -] cost-value

undo apply cost

【缺省情况】

未配置路由信息的路由开销。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

+: 增加开销值。

-: 减少开销值。

cost-value: 指定路由信息的路由开销，取值范围为 0~4294967295。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。如果匹配 OSPF 外部路由，那么设置该路由的路由开销为 **120**。

```
<Sysname> system-view
```

```
[Sysname] route-policy policy1 permit node 10
```

```
[Sysname-route-policy-policy1-10] if-match route-type external-type1or2
```

```
[Sysname-route-policy-policy1-10] apply cost 120
```

1.1.2 apply cost-type

apply cost-type 命令用来配置路由信息的路由开销类型。

undo apply cost-type 命令用来恢复缺省情况。

【命令】

apply cost-type { type-1 | type-2 }

undo apply cost-type

【缺省情况】

未配置路由开销类型。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

type-1: OSPF 的外部 Type-1 路由。

type-2: OSPF 的外部 Type-2 路由。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。如果匹配标记域为 **8** 的路由，那么设置该路由的路由开销类型为 OSPF 的外部 Type-1 路由。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match tag 8
[Sysname-route-policy-policy1-10] apply cost-type type-1
```

1.1.3 apply ip-precedence

apply ip-precedence 命令用来配置路由的 IP 优先级。

undo apply ip-precedence 命令用来恢复缺省情况。

【命令】

apply ip-precedence { *value* | clear }

undo apply ip-precedence

【缺省情况】

未配置路由的 IP 优先级。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

value: 路由的 IP 优先级，取值范围是 0~7。

clear: 清除路由的 IP 优先级。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。如果匹配前缀列表号 **100** 的路由，那么配置路由的 IP 优先级为 **3**。

```
<Sysname> system-view
[Sysname] ip prefix-list 100 permit 192.168.10.1 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list 100
[Sysname-route-policy-policy1-10] apply ip-precedence 3
```

1.1.4 apply preference

apply preference 命令用来配置路由协议的优先级。

undo apply preference 命令用来恢复缺省情况。

【命令】

apply preference *preference*

undo apply preference

【缺省情况】

未配置路由协议的优先级。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

preference: 路由的优先级，取值范围为 1~255。

【使用指导】

如果路由协议已经用命令 **preference** 配置了优先级，再用 **apply preference** 命令修改路由协议的优先级，则这些匹配策略的路由采用 **apply preference** 命令修改的优先级，其它路由的优先级均采用 **preference** 命令所设的值。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 10，匹配模式为 **permit**。如果匹配 OSPF 外部路由，那么设置该路由协议的优先级为 90。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match route-type external-type1or2
[Sysname-route-policy-policy1-10] apply preference 90
```

1.1.5 apply prefix-priority

apply prefix-priority 命令用来配置路由的收敛优先级。

undo apply prefix-priority 命令用来恢复缺省情况。

【命令】

apply prefix-priority { **critical** | **high** | **medium** }

undo apply prefix-priority

【缺省情况】

未配置路由的收敛优先级，即路由的收敛优先级为低（Low）。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

critical: 路由的收敛优先级为关键。

high: 路由的收敛优先级为高。

medium: 路由的收敛优先级中。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。如果匹配已存在的地址前缀列表 **abc**，那么设置该路由的收敛优先级为关键。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list abc
[Sysname-route-policy-policy1-10] apply prefix-priority critical
```

1.1.6 apply tag

apply tag 命令用来配置 IGP 路由信息的标记。

undo apply tag 命令用来恢复缺省情况。

【命令】

apply tag *tag-value*

undo apply tag

【缺省情况】

未配置 IGP 路由信息的标记。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

tag-value: 指定路由信息的标记值，取值范围为 0～4294967295。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。配置 IGP 路由信息的标记为 **100**。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] apply tag 100
```

1.1.7 continue

continue 命令用来配置下一个执行节点。

undo continue 命令用来恢复缺省情况。

【命令】

```
continue [ node-number ]
undo continue
```

【缺省情况】

未配置下一个执行节点。

【视图】

路由策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

node-number：标识本命令会跳转到的节点索引，取值范围为 0～65535。

【使用指导】

下一个执行节点序列号必须大于当前节点序列号。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。定义 **continue** 子句，配置下一个执行节点序列号为 **20**。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] continue 20
```

1.1.8 description

description 命令用来配置当前策略节点的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

未配置策略节点的描述信息。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: 策略节点的描述信息，为 1~80 个字符的字符串，区分大小写。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**，描述信息为 **aa**。

```
<Sysname> system-view
```

```
[Sysname] route-policy policy1 permit node 10
```

```
[Sysname-route-policy-policy1-10] description aa
```

1.1.9 display route tag-list

display route tag-list 命令用来显示 IGP 路由标记列表信息。

【命令】

display route tag-list [*tag-list-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

tag-list-number: IGP 路由标记列表号，取值范围为 1~65535。如果未指定本参数，将显示所有 IGP 路由标记列表信息。

【举例】

显示列表号为 1 的 IGP 路由标记列表信息。

```
<Sysname> display route tag-list 1
```

```
Tag list 1
```

```
Index: 1           Mode: Permit  Tag value: 1 2 3
```

```
Index: 2           Mode: Permit  Tag value: 6 7 8
```

表1-1 display route tag-list 命令显示信息描述表

字段	描述
Tag list	IGP路由标记列表号
Index	IGP路由标记列表的表项编号
Mode	匹配模式，取值包括： • Permit: 表示允许 • Deny: 表示拒绝
Tag value	路由标记值

【相关命令】

- **route tag-list**

1.1.10 display route-policy

display route-policy 命令用来显示配置的路由策略信息。

【命令】

display route-policy [*name route-policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

name route-policy-name: 指定显示的路由策略名，为 1~63 个字符的字符串，区分大小写。如果未指定本参数，将显示所有已配置的路由策略信息。

【举例】

显示名为 policy1 的路由策略信息。

```
<Sysname> display route-policy name policy1
Route-policy: policy1
  Permit : 1
    Description: policy1
    if-match cost 10
    continue: next node 11
    apply preference 10
```

表1-2 display route-policy 命令显示信息描述表

字段	描述
Route-policy	路由策略名称
permit	匹配模式，有两种取值： - Permit: 表示允许 - Deny: 表示拒绝
Description	路由策略描述信息
if-match	if-match子句，配置的匹配条件
continue	continue字句，配置下一个执行节点
apply	apply子句，如满足匹配条件，则要执行的动作

1.1.11 if-match cost

if-match cost 命令用来配置路由信息的路由开销的匹配条件。

undo if-match cost 命令用来恢复缺省情况。

【命令】

```
if-match cost cost-value
undo if-match cost
```

【缺省情况】

未配置路由信息的路由开销的匹配条件。

【视图】

路由策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

cost-value: 路由开销，取值范围为 0~4294967295。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。定义一条 **if-match** 子句，允许路由开销为 **8** 的路由信息通过。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match cost 8
```

1.1.12 if-match interface

if-match interface 命令用来配置路由信息的出接口的匹配条件。

undo if-match interface 命令用来取消路由信息的出接口的匹配条件的配置。

【命令】

```
if-match interface { interface-type interface-number }&<1-16>  
undo if-match interface [ interface-type interface-number ]&<1-16>
```

【缺省情况】

未配置路由信息的出接口的匹配条件。

【视图】

路由策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface-type interface-number: 指定接口类型和编号。

&<1-16>: 表示前面的参数可以输入 1~16 次。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。定义一条 **if-match** 子句，匹配出接口为 **GigabitEthernet1/0/1** 的路由信息。

```
<Sysname> system-view  
[Sysname] route-policy policy1 permit node 10  
[Sysname-route-policy-policy1-10] if-match interface gigabitethernet 1/0/1
```

1.1.13 if-match route-type

if-match route-type 命令用来配置路由信息类型的匹配条件。

undo if-match route-type 命令用来取消路由信息类型的匹配条件的配置。

【命令】

```
if-match route-type { external-type1 | external-type1or2 | external-type2 |  
internal | nssa-external-type1 | nssa-external-type1or2 |  
nssa-external-type2 } *  
undo if-match route-type [ external-type1 | external-type1or2 |  
external-type2 | internal | nssa-external-type1 | nssa-external-type1or2 |  
nssa-external-type2 ] *
```

【缺省情况】

未配置路由信息的类型的匹配条件。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

external-type1: OSPF Type1 的外部路由。

external-type1or2: OSPF 外部路由。

external-type2: OSPF Type2 的外部路由。

internal: 内部路由（包括 OSPF 区域间和区域内路由）。

nssa-external-type1: OSPF NSSA Type1 的外部路由。

nssa-external-type1or2: OSPF NSSA 的外部路由。

nssa-external-type2: OSPF NSSA Type2 的外部路由。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。定义一条 **if-match** 子句，匹配 **internal** 类型的路由。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match route-type internal
```

1.1.14 if-match tag

if-match tag 命令用来配置 IGP 路由信息标记的匹配条件。

undo if-match tag 命令用来恢复缺省情况。

【命令】

if-match tag tag-value

undo if-match tag

【缺省情况】

未配置 IGP 路由信息标记的匹配条件。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

tag-value: 指定要求的标记值，取值范围为 0~4294967295。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。定义一条 **if-match** 子句，匹配标记为 **8** 的 IGP 路由信息。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match tag 8
```

1.1.15 if-match tag-list

if-match tag-list 命令用来配置 IGP 路由标记列表的匹配条件。

undo if-match tag-list 命令用来恢复缺省情况。

【命令】

```
if-match tag-list tag-list-number
undo if-match tag-list
```

【缺省情况】

未配置 IGP 路由标记列表的匹配条件。

【视图】

路由策略视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

tag-list-number: IGP 路由标记列表号，取值范围为 1~65535。

【使用指导】

通过指定匹配 IGP 路由标记列表，可在同一策略节点下匹配多个 IGP 路由标记。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 10，匹配模式为 **permit**。定义一条 **if-match** 子句，允许匹配路由标记列表号为 100 的 IGP 路由通过。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match tag-list 100
```

【相关命令】

- **route tag-list**

1.1.16 route tag-list

route tag-list 命令用来配置 IGP 路由标记列表。

undo route tag-list 命令用来删除指定的 IGP 路由标记列表或某个表项。

【命令】

```
route tag-list tag-list-number [ index index-number ] { deny | permit }
tag-value<1-32>
undo route tag-list tag-list-number [ index index-number [ { deny | permit }
tag-value<1-32> ] ]
```

【缺省情况】

不存在路由信息标记列表。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

tag-list-number: 路由标记列表号，取值范围为 1～65535。

index index-number: 路由标记列表中的表项编号，用来唯一标识一条表项，取值范围为 1～4294967295。每个路由标记列表可以包含多条表项，**index-number** 取值小的表项优先匹配。如果未指定本参数，表项编号值按照配置先后顺序依次递增，每次加 1，第一个表项编号值为 1；若当前表项编号已为最大值，则从未使用的表项编号中从小到大分配。

deny: 指定路由标记列表的匹配模式为拒绝模式。

permit: 指定路由标记列表的匹配模式为允许模式。

tag-value: 路由标记值，取值范围为 0～4294967295。&<1-32>表示前面的参数最多可以输入 32 次。

【使用指导】

重复执行本命令配置路由标记列表中的同一条表项时，配置后表项中的路由标记为多次配置结果的集合，且标记的个数不能超过 32。

【举例】

配置列表号为 1、表项编号为 10 的 IGP 路由标记列表表项，允许标记值为 100 的路由通过。

```
<Sysname> system-view
```

```
[Sysname] route tag-list 1 index 10 permit 100
```

【相关命令】

- **display route tag-list**
- **if-match tag-list**

1.1.17 route-policy

route-policy 命令用来创建路由策略，并进入该路由策略视图。如果指定的路由策略已经存在，则直接进入该路由策略视图。

undo route-policy 命令用来删除指定的路由策略。

【命令】

```
route-policy route-policy-name { deny | permit } node node-number
```

```
undo route-policy route-policy-name [ deny | permit ] [ node node-number ]
```

【缺省情况】

不存在路由策略。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

route-policy-name: 指定路由策略名，为 1~63 个字符的字符串，区分大小写。

deny: 指定所定义的路由策略节点的匹配模式为拒绝模式。当路由项满足该节点的所有 if-match 子句时被拒绝通过该节点的过滤，并且不会进行下一个节点的匹配；如果路由项不满足该节点的 if-match 子句，将进入下一个节点继续匹配。

permit: 指定所定义的路由策略节点的匹配模式为允许模式。当路由项满足该节点的所有 if-match 子句时被允许通过该节点的过滤并执行该节点的 apply 子句，如路由项不满足该节点的 if-match 子句，将继续匹配该路由策略的下一个节点。

node node-number: 标识路由策略中的一个节点索引，当该路由策略用于路由信息过滤时，node-number 小的节点先被匹配，取值范围为 0~65535。

【使用指导】

路由策略用于路由信息过滤。一个路由策略由若干节点组成，每一节点由一些 if-match 子句和 apply 子句组成。if-match 子句定义该节点的匹配规则，apply 子句定义通过该节点过滤后进行的动作。节点的 if-match 子句之间的过滤关系是“与”的关系，即必须满足该节点的所有 if-match 子句。路由策略节点之间的过滤关系是“或”的关系，即通过一个节点的过滤就意味着通过该路由策略的过滤。若没有通过任一节点的过滤，则表示没有通过该路由策略的过滤。

【举例】

创建一个名为 policy1 的路由策略，其节点序列号为 10，匹配模式为 permit，并进入路由策略视图。

```
<Sysname> system-view  
[Sysname] route-policy policy1 permit node 10  
[Sysname-route-policy-policy1-10]
```

【相关命令】

- **display route-policy**

1.2 IPv4路由策略配置命令

1.2.1 apply fast-reroute

apply fast-reroute 命令用来配置快速重路由备份。

undo apply fast-reroute 命令用来恢复缺省情况。

【命令】

```
apply fast-reroute { backup-interface interface-type interface-number  
[ backup-nexthop ip-address ] | backup-nexthop ip-address }  
undo apply fast-reroute
```

【缺省情况】

未配置快速重路由备份。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

backup-interface interface-type interface-number: 备份出接口。对于备份出接口为非 P2P 类型的接口时（包括 NBMA 类型接口或广播类型接口），必须同时指定其对应的备份下一跳地址。*interface-type interface-number* 为指定的接口类型和编号。

backup-nexthop ip-address: 备份下一跳地址。

【使用指导】

当网络中的链路或某台路由器发生故障时，需要通过故障链路或故障路由器传输才能到达目的地的报文将会丢失或产生路由环路，数据流量将会被中断，直到路由协议根据新的拓扑网络路由收敛完毕后，被中断的流量才能恢复正常的传输。

网络管理员可以为路由协议配置快速重路由功能，路由协议将通过路由策略为路由指定备份下一跳，当路由器探测到网络故障时，路由协议会使用事先指定好的备份下一跳替换失效下一跳，通过备份下一跳来指导报文的转发，从而大大缩短了流量中断时间。

网络管理员可以在路由策略中配置快速重路由功能的指定备份下一跳，为符合过滤条件的路由指定备份下一跳。

【举例】

创建一个名为 policy1 的路由策略，为到达目的地 100.1.1.0/24 的路由配置备份出接口为 GigabitEthernet1/0/1，备份下一跳地址为 193.1.1.8。

```
<Sysname> system-view
[Sysname] ip prefix-list abc index 10 permit 100.1.1.0 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list abc
[Sysname-route-policy-policy1-10] apply fast-reroute backup-interface gigabitethernet
1/0/1 backup-nexthop 193.1.1.8
```

1.2.2 apply ip-address next-hop

apply ip-address next-hop 命令用来配置 IPv4 路由信息的下一跳地址。

undo apply ip-address next-hop 命令用来恢复缺省情况。

【命令】

apply ip-address next-hop ip-address [public | vpn-instance vpn-instance-name]

undo apply ip-address next-hop

【缺省情况】

未配置 IPv4 路由信息的下一跳地址。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: 下一跳 IP 地址。

public: 指定公网。

vpn-instance vpn-instance-name: 指定 VPN 实例的信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

当引入路由时，使用本命令设置下一跳地址无效。

如果未指定参数 **public** 或 **vpn-instance vpn-instance-name**，则表示下一跳地址为公网地址。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。如果匹配前缀列表号 **100** 的路由，那么设置路由信息的下一跳地址为 **193.1.1.8**。

```
<Sysname> system-view
[Sysname] ip prefix-list 100 permit 192.168.10.1 24
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip address prefix-list 100
[Sysname-route-policy-policy1-10] apply ip-address next-hop 193.1.1.8
```

1.2.3 display ip prefix-list

display ip prefix-list 命令用来显示 IPv4 地址前缀列表的统计信息。

【命令】

display ip prefix-list [name prefix-list-name]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

name prefix-list-name: 指定显示的地址前缀列表名，为 1~63 个字符的字符串，区分大小写。如果未指定本参数，将显示所有已配置的地址前缀列表的统计信息。

【举例】

```
# 显示名为 abc 的地址前缀列表的统计信息。
<Sysname> display ip prefix-list name abc
Prefix-list: abc
Permitted 0
Denied 0
          index: 10          Deny   6.6.6.0/24          ge  26  le  28
```

表1-3 display ip prefix-list 命令显示信息描述表

字段	描述
Prefix-list	地址前缀列表的名称
Permitted	符合匹配条件的路由个数
Denied	不符合匹配条件的路由个数
index	地址前缀列表的内部序列号
deny	匹配模式，有两种取值： • Permit: 表示允许 • Deny: 表示拒绝
6.6.6.0/24	匹配的IP地址和掩码长度
ge	即greater-equal，匹配的IP地址掩码长度的下限值
le	即less-equal，匹配的IP地址掩码长度的上限值

【相关命令】

- ip prefix-list
- reset ip prefix-list

1.2.4 if-match ip

if-match ip 命令用来配置 IPv4 的路由信息的匹配条件。
undo if-match ip 命令用来取消 IPv4 的路由信息的匹配条件的配置。

【命令】

```
if-match ip { address | next-hop } { acl { ipv4-acl-number | name ipv4-acl-name }  
| prefix-list prefix-list-name }  
undo if-match ip { address | next-hop } [ acl | prefix-list ]
```

【缺省情况】

未配置 IPv4 的路由信息的匹配条件。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

address: 匹配 IPv4 路由信息的目的地址。

next-hop: 匹配下一跳地址。

acl ipv4-acl-number: 指定用于过滤的 ACL 号。对于 **address**, *ipv4-acl-number* 的取值范围为 2000~3999; 对于 **next-hop**, *ipv4-acl-number* 的取值范围为 2000~2999。

acl name ipv4-acl-name: 指定用于过滤的 ACL 名称, *ipv4-acl-name* 表示 ACL 的名称, 为 1~63 个字符的字符串, 不区分大小写, 必须以英文字母 a~z 或 A~Z 开头。为避免混淆, ACL 的名称不允许使用英文单词 all。

prefix-list prefix-list-name: 指定用于过滤的地址前缀列表名称, 为 1~63 个字符的字符串, 区分大小写。

【使用指导】

当配置的是高级 ACL 时, 其使用规则如下:

- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard** 来过滤指定 IPv4 地址的路由信息。
- 使用命令 **rule [rule-id] { deny | permit } ip destination dest-addr dest-wildcard** 来过滤指定掩码的路由信息, 配置的掩码应该是连续的 (当配置的掩码不连续时该过滤掩码的条件不生效)。当指定 **next-hop** 或 **route-source** 参数时, 不能使用本规则, 否则, 所有的报文都可与指定 ACL 中的规则相匹配, 导致路由信息匹配结果异常。

【举例】

创建一个名为 **policy1** 的路由策略, 其节点序列号为 10, 匹配模式为 **permit**。定义一个 **if-match** 子句, 允许下一跳地址匹配已存在的地址前缀列表 **p1** 的路由信息通过。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ip next-hop prefix-list p1
```

1.2.5 ip prefix-list

ip prefix-list 命令用来配置一个 IPv4 地址前缀列表或表项。

undo ip prefix-list 命令用来删除指定的 IPv4 地址前缀列表或其某个表项。

【命令】

```
ip prefix-list prefix-list-name [ index index-number ] { deny | permit }
ip-address mask-length [ greater-equal min-mask-length ] [ less-equal
max-mask-length ]
undo ip prefix-list prefix-list-name [ index index-number ]
```

【缺省情况】

不存在 IPv4 地址前缀列表。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

prefix-list-name: 指定 IPv4 地址前缀列表名，为 1~63 个字符的字符串，区分大小写。

index-number: 标识 IPv4 地址前缀列表中的一项，**index-number** 小的项先被匹配，取值范围为 1~65535。如果未指定本参数，该序号值按照配置先后顺序依次递增，每次加 10，第一个序号值为 10。

deny: 指定所定义的 IPv4 地址前缀列表项的匹配模式为拒绝模式。在该模式下，如果过滤的 IPv4 地址在定义的范围内，则不能通过过滤，并且不进行下一节点的匹配；否则，进行下一节点的匹配。

permit: 指定所定义的 IPv4 地址前缀列表项的匹配模式为允许模式。在该模式下，如果过滤的 IPv4 地址在定义的范围内，则通过过滤，不进行下一个节点的匹配；否则，进行下一节点的匹配。

ip-address mask-length: 指定 IPv4 地址前缀和前缀长度，**mask-length** 的取值范围为 0~32。

greater-equal min-mask-length, less-equal max-mask-length: 如果 IPv4 地址和前缀长度都已匹配，则使用该参数来指定地址前缀长度范围。**greater-equal** 表示大于等于，**less-equal** 表示小于等于。前缀长度范围可以表达为 **mask-length <= min-mask-length <= max-mask-length <= 32**。如果只指定 **min-mask-length** 时，则前缀长度范围为 [**min-mask-length**, 32]；如果只指定 **max-mask-length** 时，则前缀长度范围为 [**mask-length**, **max-mask-length**]；如果二者都指定，则前缀长度范围为 [**min-mask-length**, **max-mask-length**]。

【使用指导】

IPv4 地址前缀列表用于 IPv4 地址的过滤。一个 IPv4 地址前缀列表可以有若干条表项，每一表项指定一个地址前缀范围。表项之间的过滤关系是“或”的关系，即通过一条表项的过滤就意味着通过该 IPv4 地址前缀列表的过滤。若没有通过任一表项的过滤，则不能通过该 IPv4 地址前缀列表的过滤。

如果将 **ip-address mask-length** 指定为 0.0.0.0 0，则只匹配缺省路由。如果需要匹配所有路由，则应配置为 0.0.0.0 0 **less-equal 32**。

【举例】

定义一条名为 p1 的 IPv4 地址前缀列表，只允许 10.0.0.0/8 网段的，掩码长度为 17 或 18 的路由通过。

```
<Sysname> system-view
```

```
[Sysname] ip prefix-list p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18
```

【相关命令】

- **display ip prefix-list**
- **reset ip prefix-list**

1.2.6 reset ip prefix-list

reset ip prefix-list 命令用来清除 IPv4 地址前缀列表的统计信息。

【命令】

```
reset ip prefix-list [ prefix-list-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

prefix-list-name: 指定地址前缀列表的名称，为 1~63 个字符的字符串，区分大小写。如果未指定本参数，将清除所有的 IPv4 地址前缀列表的统计信息。

【举例】

清除 IPv4 地址前缀列表 abc 的统计信息。

```
<Sysname> reset ip prefix-list abc
```

【相关命令】

- **display ip prefix-list**
- **ip prefix-list**

1.3 IPv6路由策略配置命令

1.3.1 apply ipv6 fast-reroute

apply ipv6 fast-reroute 命令用来配置快速重路由备份。

undo apply ipv6 fast-reroute 命令用来恢复缺省情况。

【命令】

```
apply ipv6 fast-reroute { backup-interface interface-type interface-number  
[ backup-nexthop ipv6-address ] | backup-nexthop ipv6-address }  
undo apply ipv6 fast-reroute
```

【缺省情况】

未配置快速重路由备份。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

backup-interface interface-type interface-number: 备份出接口。对于备份出接口为非 P2P 类型的接口时（包括 NBMA 类型接口或广播类型接口），必须同时指定其对应的备份下一跳地址。*interface-type interface-number* 为指定的接口类型和编号。

backup-nexthop ipv6-address: 备份下一跳 IPv6 地址。

【使用指导】

当网络中的链路或某台路由器发生故障时，需要通过故障链路或故障路由器传输才能到达目的地的报文将会丢失或产生路由环路，数据流量将会被中断，直到路由协议根据新的拓扑网络路由收敛完毕后，被中断的流量才能恢复正常的传输。

网络管理员可以为路由协议配置快速重路由功能，路由协议将通过路由策略为路由指定备份下一跳，当路由器探测到网络故障时，路由协议会使用事先指定好的备份下一跳替换失效下一跳，通过备份下一跳来指导报文的转发，从而大大缩短了流量中断时间。

网络管理员可以在路由策略中配置快速重路由功能的指定备份下一跳，为符合过滤条件的路由指定备份下一跳。

【举例】

创建一个名为 policy1 的路由策略，为到达目的地 100::1/64 的路由配置备份下一跳地址为 1::1/64。

```
<Sysname> system-view
[Sysname] ipv6 prefix-list abc index 10 permit 100::1 64
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ipv6 address prefix-list abc
[Sysname-route-policy-policy1-10] apply ipv6 fast-reroute backup-nexthop 1::1
```

1.3.2 apply ipv6 next-hop

apply ipv6 next-hop 命令用来配置 IPv6 路由信息的下一跳地址。

undo apply ipv6 next-hop 命令用来恢复缺省情况。

【命令】

apply ipv6 next-hop ipv6-address

undo apply ipv6 next-hop

【缺省情况】

未配置 IPv6 路由信息的下一跳地址。

【视图】

路由策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address: 指定下一跳 IPv6 地址。

【使用指导】

引入路由时，使用 **apply ipv6 next-hop** 命令设置下一跳地址无效。

【举例】

```
# 创建一个名为 policy1 的路由策略，其节点序列号为 10，匹配模式为 permit。如果匹配前缀列表
# 号 100 的路由，那么设置路由信息的下一跳地址为 3ffe:506::1。
<Sysname> system-view
[Sysname] ipv6 prefix-list 100 permit 2::2 64
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ipv6 address prefix-list 100
[Sysname-route-policy-policy1-10] apply ipv6 next-hop 3ffe:506::1
```

1.3.3 display ipv6 prefix-list

display ipv6 prefix-list 命令用来显示 IPv6 地址前缀列表的统计信息。

【命令】

```
display ipv6 prefix-list [ name prefix-list-name ]
```

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

name prefix-list-name：指定 IPv6 地址前缀列表的名称，为 1~63 个字符的字符串，区分大小写。如果未指定本参数，将显示所有配置的 IPv6 地址前缀列表的统计信息。

【举例】

```
# 显示所有 IPv6 地址前缀列表的统计信息。
<Sysname> display ipv6 prefix-list
Prefix-list6: 666
  Permitted 0
  Denied 0
      index: 10          Permit 6::/64          ge 66 le 88
```

表1-4 display ipv6 prefix-list 命令显示信息描述表

字段	描述
Prefix-list6	IPv6地址前缀列表的名称
Permitted	符合匹配条件的路由个数
Denied	不符合匹配条件的路由个数
index	地址前缀列表的内部序列号

字段	描述
permit	匹配模式，有两种取值： • Permit: 表示允许 • Deny: 表示拒绝
6::/64	匹配的IPv6地址和前缀长度
ge	即greater-equal，匹配的IPv6前缀长度的下限值
le	即less-equal，匹配的IPv6前缀长度的上限值

【相关命令】

- **ipv6 prefix-list**
- **reset ipv6 prefix-list**

1.3.4 if-match ipv6

if-match ipv6 命令用来配置 IPv6 的路由信息的匹配条件。

undo if-match ipv6 命令用来取消 IPv6 的路由信息的匹配条件的配置。

【命令】

```

if-match ipv6 { address | next-hop | route-source } { acl { ipv6-acl-number |
name ipv6-acl-name } | prefix-list prefix-list-name }
undo if-match ipv6 { address | next-hop | route-source } [ acl | prefix-list ]

```

【缺省情况】

未配置 IPv6 的路由信息的匹配条件。

【视图】

路由策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

address: 匹配 IPv6 路由信息的目的地址。

next-hop: 匹配 IPv6 路由信息的下一跳。

route-source: 匹配 IPv6 路由信息的源地址。

acl *ipv6-acl-number*: 指定用于过滤的 IPv6 ACL 号。对于 **address**, *ipv6-acl-number* 的取值范围为 2000~3999; 对于 **next-hop** 和 **route-source**, *ipv6-acl-number* 的取值范围为 2000~2999。

acl name *ipv6-acl-name*: 指定用于过滤的 IPv6 ACL 名称, *ipv6-acl-name* 表示 ACL 的名称, 为 1~63 个字符的字符串, 不区分大小写, 必须以英文字母 a~z 或 A~Z 开头。为避免混淆, ACL 的名称不允许使用英文单词 all。

prefix-list prefix-list-name: 指定用于过滤的 IPv6 地址前缀列表的名称，为 1~63 个字符的字符串，区分大小写。

当配置的是高级 ACL 时，其使用规则如下：

- 使用命令 **rule [rule-id] { deny | permit } ip source sour-addr sour-wildcard** 来过滤指定 IPv6 地址的路由信息。
- 使用命令 **rule [rule-id] { deny | permit } ip destination dest-addr dest-wildcard** 来过滤指定 IPv6 地址前缀的路由信息，配置的 IPv6 地址前缀应该是连续的（当配置的 IPv6 地址前缀不连续时该过滤掩码的条件不生效）。当指定 **next-hop** 或 **route-source** 参数时，不能使用本规则，否则，所有的报文都可与指定 ACL 中的规则相匹配，导致路由信息匹配结果异常。

【举例】

创建一个名为 **policy1** 的路由策略，其节点序列号为 **10**，匹配模式为 **permit**。定义一条 **if-match** 子句，允许下一跳地址匹配已存在的 IPv6 地址前缀列表 **p1** 的路由信息通过。

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy-policy1-10] if-match ipv6 next-hop prefix-list p1
```

1.3.5 ipv6 prefix-list

ipv6 prefix-list 命令用来配置 IPv6 地址前缀列表或表项。

undo ipv6 prefix-list 命令用来删除指定的 IPv6 地址前缀列表或其中某个表项。

【命令】

```
ipv6 prefix-list prefix-list-name [ index index-number ] { deny | permit }  
ipv6-address { prefix-length [ greater-equal min-prefix-length ]  
[ less-equal max-prefix-length ] | inverse inverse-prefix-length }  
undo ipv6 prefix-list prefix-list-name [ index index-number ]
```

【缺省情况】

不存在 IPv6 地址前缀列表。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

prefix-list-name: 指定 IPv6 地址前缀列表名，为 1~63 个字符的字符串，区分大小写。

index-number: 标识 IPv6 地址前缀列表中的一项表项，**index-number** 小的表项先被匹配，取值范围为 1~65535。如果未指定本参数，该序号值按照配置先后顺序依次递增，每次加 10，第一个序号值为 10。

deny: 指定所定义的 IPv6 地址前缀列表表项的匹配模式为拒绝模式。在该模式下，如果过滤的 IPv6 地址在定义的范围外，则不能通过过滤，并且不进行下一节点的匹配；否则，进行下一节点的匹配。

permit: 指定所定义的 IPv6 地址前缀列表表项的匹配模式为允许模式。在该模式下, 如果过滤的 IPv6 地址在定义的范围内, 则通过过滤, 不进行下一个节点的匹配; 否则, 进行下一节点的匹配。

ipv6-address: 指定 IPv6 地址。

prefix-length: 指定前缀长度, 取值范围为 0~128。

greater-equal min-prefix-length, less-equal max-prefix-length: 如果 IPv6 地址和前缀长度都已匹配, 则使用该参数来指定地址前缀长度范围。**greater-equal** 表示大于等于, **less-equal** 表示小于等于。前缀长度范围可以表达为 **prefix-length <= min-prefix-length <= max-prefix-length <= 128**。如果只指定了 **min-prefix-length**, 则前缀范围为 **[min-prefix-length, 128]**; 如果只指定了 **max-prefix-length**, 则前缀范围为 **[prefix-length, max-prefix-length]**; 如果二者都指定, 则前缀范围为 **[min-prefix-length, max-prefix-length]**。

inverse inverse-prefix-length: 指定反向前缀长度, 即与指定的 IPv6 地址前缀从最低位开始需要匹配的位数。**inverse-prefix-length** 的取值范围为 1~128。

【使用指导】

IPv6 地址前缀列表用于 IPv6 地址过滤。一个 IPv6 地址前缀列表可包含多个表项, 一个表项指定一个地址前缀范围。表项之间的过滤关系是“或”, 即通过一个表项就可通过该 IPv6 地址前缀列表的过滤。没有通过任何一个表项的过滤就意味着没有通过该 IPv6 地址前缀列表的过滤。

如果将 **ipv6-address prefix-length** 指定为 **:: 0**, 则只匹配缺省路由。如果需要匹配所有路由, 则应配置为 **:: 0 less-equal 128**。

【举例】

配置一条 IPv6 地址前缀列表, 允许前缀长度在 32 位到 64 位之间的 IPv6 地址通过。

```
<Sysname> system-view
```

```
[Sysname] ipv6 prefix-list abc permit :: 0 greater-equal 32 less-equal 64
```

配置一条 IPv6 地址前缀列表, 拒绝地址前缀为 3FFE:D00::/32, 前缀长度大于等于 32 位的 IPv6 地址通过。

```
<Sysname> system-view
```

```
[Sysname] ipv6 prefix-list abc deny 3FFE:D00:: 32 less-equal 128
```

【相关命令】

- **display ipv6 prefix-list**
- **reset ipv6 prefix-list**

1.3.6 reset ipv6 prefix-list

reset ipv6 prefix-list 命令用来清除 IPv6 地址前缀列表的统计信息。

【命令】

```
reset ipv6 prefix-list [ prefix-list-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

prefix-list-name: 指定地址前缀列表的名称，为 1~63 个字符的字符串，区分大小写。如果未指定本参数，将清除所有的 IPv6 地址前缀列表的统计信息。

【举例】

清除指定 IPv6 地址前缀列表的统计信息。

```
<Sysname> reset ipv6 prefix-list abc
```

【相关命令】

- **display ipv6 prefix-list**
- **ipv6 prefix-list**



UNIS 入侵检测系统

ACL 命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《ACL 命令参考》主要介绍 ACL 和时间段的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下

格 式	意 义
	的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 ACL	1-1
1.1 ACL配置命令	1-1
1.1.1 accelerate	1-1
1.1.2 acl	1-1
1.1.3 acl copy	1-4
1.1.4 acl logging interval	1-5
1.1.5 acl trap interval	1-6
1.1.6 description	1-7
1.1.7 display acl	1-7
1.1.8 display acl accelerate	1-9
1.1.9 display packet-filter	1-10
1.1.10 display packet-filter statistics	1-11
1.1.11 display packet-filter verbose	1-13
1.1.12 packet-filter	1-14
1.1.13 reset acl counter	1-15
1.1.14 reset packet-filter statistics	1-16
1.1.15 rule (IPv4 advanced ACL view)	1-17
1.1.16 rule (IPv4 basic ACL view)	1-22
1.1.17 rule (IPv6 advanced ACL view)	1-24
1.1.18 rule (IPv6 basic ACL view)	1-30
1.1.19 rule (Layer 2 ACL view)	1-32
1.1.20 rule comment	1-33
1.1.21 step	1-34

1 ACL

1.1 ACL配置命令

1.1.1 accelerate

accelerate 命令用来开启 ACL 规则的加速匹配功能。

undo accelerate 命令用来恢复缺省情况。

【命令】

accelerate

undo accelerate

【缺省情况】

ACL 规则的加速匹配功能处于关闭状态。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图

IPv6 基本 ACL 视图/IPv6 高级 ACL 视图

二层 ACL 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

只有系统 ACL 资源充足时加速匹配功能才会生效。

开启本功能后，再去修改或添加新的规则，可能由于 ACL 资源不足，会导致新的规则加速失败，新规则匹配不生效，但是不影响之前加速成功的规则。

【举例】

开启 ACL 2000 的加速匹配功能。

```
<Sysname> system-view
```

```
[Sysname] acl basic 2000
```

```
[Sysname-acl-ipv4-basic-2000] accelerate
```

【相关命令】

- **display acl accelerate**

1.1.2 acl

acl 命令用来创建 ACL，并进入 ACL 视图。如果指定的 ACL 已存在，则直接进入 ACL 视图。

undo acl 命令用来删除指定或全部 ACL。

【命令】

```
acl [ ipv6 ] { name acl-name | number acl-number [ name acl-name ] [ match-order { auto | config } ] }  
undo acl [ ipv6 ] { all | name acl-name | number acl-number }  
acl [ ipv6 ] { advanced | basic } { acl-number | name acl-name } [ match-order { auto | config } ]  
acl mac { acl-number | name acl-name } [ match-order { auto | config } ]  
undo acl [ ipv6 ] { all | { advanced | basic } { acl-number | name acl-name } }  
undo acl mac { all | acl-number | name acl-name }
```

【缺省情况】

不存在 ACL。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6: 指定 ACL 类型为 IPv6 ACL。

basic: 指定创建基本 ACL。

advanced: 指定创建高级 ACL。

mac: 指定创建二层 ACL。

acl-number: 指定 ACL 的编号。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999: 表示基本 ACL。
- 3000～3999: 表示高级 ACL。
- 4000～4999: 表示二层 ACL。

name acl-name: 指定 ACL 的名称。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

match-order { auto | config }: 指定规则的匹配顺序，**auto** 表示按照自动排序（即“深度优先”原则）的顺序进行规则匹配，**config** 表示按照配置顺序进行规则匹配。缺省情况下，规则的匹配顺序为配置顺序。

all: 指定类型中全部 ACL。

【使用指导】

通过编号创建的 ACL，可以通过如下命令进入其视图：

- **acl [ipv6] number acl-number**;
- **acl { [ipv6] { advanced | basic } | mac } acl-number**。

通过 **acl [ipv6] number acl-number name acl-name** 命令指定编号和名称创建的 ACL，可以使用如下命令进入其视图：

- **acl [ipv6] name acl-name**，本命令仅支持进入已创建的基本或高级 ACL 视图；
- **acl [ipv6] number acl-number [name acl-name]**；
- **acl { [ipv6] { advanced | basic } | mac } name acl-name**。

通过 **acl { [ipv6] { advanced | basic } | mac } name acl-name** 命令指定名称创建的 ACL，可以使用如下命令进入其视图：

- **acl [ipv6] name acl-name**，本命令仅支持进入已创建的基本或高级 ACL 视图；
- **acl { [ipv6] { advanced | basic } | mac } name acl-name**。

当 ACL 内不存在任何规则时，用户可以使用本命令对该 ACL 的规则匹配顺序进行修改，否则不允许进行修改。

如果 ACL 规则的匹配项中包含了除 IP 五元组（源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议）、ICMP 报文或 ICMPv6 报文的报文类型和消息码信息、VPN 实例、日志操作和时间段之外的其它匹配项，则设备转发 ACL 匹配的这类报文时会启用慢转发流程。慢转发时设备会将报文上送控制平面，计算报文相应的表项信息。执行慢转发流程时，设备的转发能力将会有所降低。

【举例】

创建一个编号为 2000 的 IPv4 基本 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000]
```

创建一个 IPv4 基本 ACL，指定其名称为 flow，并进入其视图。

```
<Sysname> system-view
[Sysname] acl basic name flow
[Sysname-acl-ipv4-basic-flow]
```

创建一个编号为 3000 的 IPv4 高级 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000]
```

创建一个编号为 2000 的 IPv6 基本 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000]
```

创建一个 IPv6 基本 ACL，其名称为 flow，并进入其视图。

```
<Sysname> system-view
[Sysname] acl ipv6 basic name flow
[Sysname-acl-ipv6-basic-flow]
```

创建一个 IPv6 高级 ACL，其名称为 abc，并进入其视图。

```
<Sysname> system-view
[Sysname] acl ipv6 advanced name abc
[Sysname-acl-ipv6-adv-abc]
```

创建一个编号为 4000 的二层 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl mac 4000
```

```
[Sysname-acl-mac-4000]
# 创建一个二层 ACL，其名称为 flow，并进入其视图。
<Sysname> system-view
[Sysname] acl mac name flow
[Sysname-acl-mac-flow]
```

【相关命令】

- **display acl**

1.1.3 acl copy

acl copy 命令用来复制并生成一个新的 ACL。

【命令】

```
acl [ ipv6 | mac ] copy { source-acl-number | name source-acl-name } to
{ dest-acl-number | name dest-acl-name }
```

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

source-acl-number: 指定源 ACL 的编号，该 ACL 必须存在。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999: 表示基本 ACL。
- 3000～3999: 表示高级 ACL。
- 4000～4999: 表示二层 ACL。

name source-acl-name: 指定源 ACL 的名称，该 ACL 必须存在。**source-acl-name** 为 1～63 个字符的字符串，不区分大小写。

dest-acl-number: 指定目的 ACL 的编号，该 ACL 必须不存在。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999: 表示基本 ACL。
- 3000～3999: 表示高级 ACL。
- 4000～4999: 表示二层 ACL。

name dest-acl-name: 指定目的 ACL 的名称，该 ACL 必须不存在。**dest-acl-name** 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

【使用指导】

目的 ACL 的类型要与源 ACL 的类型相同。

除了 ACL 的编号或名称不同外，新生成的 ACL（即目的 ACL）的匹配顺序、规则匹配软件统计功能的开启情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 ACL 的相同。

【举例】

通过复制已存在的 IPv4 基本 ACL 2001，来生成一个新的编号为 2002 的同类型 ACL。

```
<Sysname> system-view
```

```
[Sysname] acl copy 2001 to 2002
```

通过复制已存在的 IPv4 基本 ACL test，来生成名为 paste 的同类型 ACL。

```
<Sysname> system-view
```

```
[Sysname] acl copy name test to name paste
```

1.1.4 acl logging interval

acl logging interval 命令用来配置报文过滤日志信息的生成与发送周期，同时开启报文的首包上送功能。

undo acl logging interval 命令用来恢复缺省情况。

【命令】

acl logging interval *interval*

undo acl logging interval

【缺省情况】

报文过滤日志信息的生成与发送周期为 0 分钟，即不记录报文过滤的日志。报文首包上送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval：报文过滤日志信息的生成与发送周期，取值范围为 0~1440，且必须为 5 的整数倍，0 表示不进行记录，单位为分钟。

【使用指导】

系统只支持对应用 IPv4 基本 ACL、IPv4 高级 ACL、IPv6 基本 ACL 或 IPv6 高级 ACL 进行报文过滤的报文过滤日志信息进行记录，且在上述 ACL 中配置规则时必须指定 **logging** 参数。

报文过滤日志的生成与发送周期起始于报文过滤中 ACL 匹配数据流的第一个数据包，报文过滤日志包括周期内被匹配的报文数量以及所使用的 ACL 规则。在一个周期内：

- 对于规则匹配数据流的第一个数据包，设备会立即生成报文过滤日志并发送到信息中心；
- 对于规则匹配数据流的其他数据包，设备将在周期结束后生成报文过滤日志并发送到信息中心。

有关信息中心的详细介绍请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

```
# 配置 IPv4 报文过滤日志的生成与发送周期为 10 分钟。  
<Sysname> system-view  
[Sysname] acl logging interval 10
```

【相关命令】

- **rule** (IPv4 advanced ACL view)
- **rule** (IPv4 basic ACL view)
- **rule** (IPv6 advanced ACL view)
- **rule** (IPv6 basic ACL view)

1.1.5 acl trap interval

acl trap interval 命令用来配置报文过滤告警信息的生成与发送周期。

undo acl trap interval 命令用来恢复缺省情况。

【命令】

```
acl trap interval interval  
undo acl trap interval
```

【缺省情况】

报文过滤告警信息的生成与发送周期为 0 分钟，即不记录报文过滤的告警信息。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

interval: 报文过滤告警信息的生成与发送周期，取值范围为 0~1440，且必须为 5 的整数倍，0 表示不进行记录，单位为分钟。

【使用指导】

系统只支持对应用 IPv4 基本 ACL、IPv4 高级 ACL、IPv6 基本 ACL 或 IPv6 高级 ACL 进行报文过滤的报文过滤告警信息进行记录，且在上述 ACL 中配置规则时必须指定 **logging** 参数。

报文过滤告警信息的生成与发送周期起始于报文过滤中 ACL 匹配数据流的第一个数据包，报文过滤告警信息包括周期内被匹配的报文数量以及所使用的 ACL 规则。在一个周期内：

- 对于规则匹配数据流的第一个数据包，设备会立即生成报文过滤告警信息并发送到 SNMP 模块；
- 对于规则匹配数据流的其他数据包，设备将在周期结束后生成报文过滤告警信息并发送到 SNMP 模块。

有关 SNMP 的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

【举例】

配置 IPv4 报文过滤告警信息的生成与发送周期为 10 分钟。

```
<Sysname> system-view
[Sysname] acl trap interval 10
```

【相关命令】

- **rule** (IPv4 advanced ACL view)
- **rule** (IPv4 basic ACL view)
- **rule** (IPv6 advanced ACL view)
- **rule** (IPv6 basic ACL view)

1.1.6 description

description 命令用来配置 ACL 的描述信息。

undo description 命令用来删除 ACL 的描述信息。

【命令】

```
description text
undo description
```

【缺省情况】

ACL 没有任何描述信息。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图
IPv6 基本 ACL 视图/IPv6 高级 ACL 视图
二层 ACL 视图

【缺省用户角色】

network-admin
context-admin

【参数】

text: 表示 ACL 的描述信息，为 1~127 个字符的字符串，区分大小写。

【举例】

为 IPv4 基本 ACL 2000 配置描述信息。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.
```

【相关命令】

- **display acl**

1.1.7 display acl

display acl 命令用来显示 ACL 的配置和运行情况。

【命令】

display acl [**ipv6** | **mac**] { **acl-number** | **all** | **name acl-name** }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

acl-number: 显示指定编号的 ACL 的配置和运行情况。**acl-number** 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999: 表示基本 ACL。
- 3000～3999: 表示高级 ACL。
- 4000～4999: 表示二层 ACL。

all: 显示指定类型中全部 ACL 的配置和运行情况。

name acl-name: 显示指定名称的 ACL 的配置和运行情况。**acl-name** 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

本命令将按照实际匹配顺序来排列 ACL 内的规则，即：当 ACL 的规则匹配顺序为配置顺序时，各规则将按照编号由小到大排列；当 ACL 的规则匹配顺序为自动排序时，各规则将按照“深度优先”原则由深到浅排列。

【举例】

显示所有 IPv4 ACL 的配置和运行情况。

```
<Sysname> display acl all
Basic IPv4 ACL 2001, 2 rules, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5
ACL accelerated
Rule insert-only enabled
  rule 5 permit source 1.1.1.1 0 (5 times matched)
  rule 5 comment This rule is used on GigabitEthernet1/0/1.
  rule 10 permit source object-group permit (5 times matched)
Advanced IPv4 ACL 3001, 1 rule,
ACL's step is 5
  rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 3.3.3.0 0.0.0.255 (Dynamic)
```

表1-1 display acl 命令显示信息描述表

字段	描述
Basic IPv4 ACL 2001	该ACL的类型和编号，ACL的类型包括： - Basic IPv4 ACL：表示 IPv4 基本 ACL - Advanced IPv4 ACL：表示 IPv4 高级 ACL - Basic IPv6 ACL：表示 IPv6 基本 ACL - Advanced IPv6 ACL：表示 IPv6 高级 ACL - MAC ACL：表示二层 ACL
2 rules	该ACL内包含的规则数量
match-order is auto	该ACL的规则匹配顺序为自动排序（匹配顺序为配置顺序时不显示本字段）
This is an IPv4 basic ACL.	该ACL的描述信息
ACL's step is 5	该ACL的规则编号的步长值为5
ACL accelerated	该ACL开启了加速功能
Rule insert-only enabled	该ACL开启了抢占ACL规则编号功能
rule 5 permit source 1.1.1.1 0	规则5的具体内容，源地址为具体地址
rule 10 permit source object-group permit	规则10的具体内容，源地址为对象组
5 times matched	该规则匹配的次数为5（仅统计软件ACL的匹配次数，当匹配次数为0时不显示本字段）
rule 5 comment This rule is used on GigabitEthernet1/0/1.	规则5的描述信息
Dynamic	该规则由应用模块动态添加

1.1.8 display acl accelerate

display acl accelerate 命令用来显示 ACL 的加速状态。

【命令】

```
display acl accelerate { summary [ ipv6 | mac ] | verbose [ ipv6 | mac ]
{ acl-number | name acl-name } slot slot-number }
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```


【参数】

summary: 显示 ACL 加速的概要信息。

verbose: 显示 ACL 加速的详细信息。

ipv6: 显示 IPv6 ACL 的加速状态。

mac: 显示二层 ACL 的加速状态。

acl-number: 显示指定编号的 ACL 的加速状态。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000~2999: 表示基本 ACL。
- 3000~3999: 表示高级 ACL。
- 4000~4999: 表示二层 ACL。

name acl-name: 显示指定名称的 ACL 的加速状态。*acl-name* 表示 ACL 的名称，为 1~63 个字符的字符串，不区分大小写。

slot slot-number: 显示指定成员设备的 ACL 加速信息，该设备必须为加速芯片所在成员设备，*slot-number* 表示设备在 IRF 中的成员编号。

【举例】

显示加速概要信息。

```
<Sysname> display acl accelerate summary
Basic IPv4 ACL 2000
```

表1-2 display acl accelerate verbose 命令显示信息描述表

字段	描述
failed	表示此规则加速失败，匹配不生效

1.1.9 display packet-filter

display packet-filter 命令用来显示 ACL 在报文过滤中的应用情况。

【命令】

display packet-filter zone-pair security [source source-zone-name destination destination-zone-name] [slot slot-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

zone-pair security [source source-zone-name destination destination-zone-name]: 显示指定安全域间实例上 ACL 在报文过滤中的应用情况。

source-zone-name: 表示安全域间实例源安全域的名称，为 1~31 个字符的字符串，不区分大小写。**destination-zone-name**: 表示安全域间实例目的安全域的名称，为 1~31 个字符的字符串，不区分大小写。

slot slot-number: 显示指定成员设备上 ACL 在报文过滤中的应用情况，**slot-number** 表示设备在 IRF 中的成员编号。若未指定本参数，将显示主用设备上 ACL 在报文过滤中的应用情况。

【举例】

显示安全域间实例源域 office 到目的域 library 上 ACL 在报文过滤中的应用情况。

```
<Sysname> display packet-filter zone-pair security source office destination library
Zone-pair: source office destination library
IPv4 ACL 2001
IPv4 ACL 2002
```

表1-3 display packet-filter 命令显示信息描述表

字段	描述
Zone-pair	ACL在指定安全域间实例上的应用情况
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv6 ACL 2002 (Failed)	IPv6基本ACL 2002应用失败

1.1.10 display packet-filter statistics

display packet-filter statistics 命令用来显示 ACL 在报文过滤中应用的统计信息。

【命令】

display packet-filter statistics zone-pair security source source-zone-name destination destination-zone-name [[ipv6] { acl-number | name acl-name }] [brief]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

zone-pair security source source-zone-name destination destination-zone-name: 显示指定安全域间实例上的统计信息。**source-zone-name**: 表示安全域间实例源安全域的名称，为 1~31 个字符的字符串，不区分大小写。

destination-zone-name: 表示安全域间实例目的安全域的名称，为 1~31 个字符的字符串，不区分大小写。

default: 显示报文过滤缺省动作的统计信息。

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

acl-number: 显示指定编号 ACL 在报文过滤中应用的统计信息。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000~2999: 表示基本 ACL。
- 3000~3999: 表示高级 ACL。
- 4000~4999: 表示二层 ACL。

name acl-name: 显示指定名称 ACL 在报文过滤中应用的统计信息。*acl-name* 表示 ACL 的名称，为 1~63 个字符的字符串，不区分大小写。

brief: 显示简要统计信息。

【使用指导】

如果未指定 **default**、*acl-number*、**name acl-name** 和 ACL 类型 (**ipv6**、**mac**) 参数，将显示全部 ACL 在报文过滤中应用的统计信息。

【举例】

显示安全域间实例源域 office 到目的域 library 上 IPv4 高级 ACL 3001 在报文过滤中应用的统计信息。

```
<Sysname> display packet-filter statistics zone-pair security source office destination library 3001
```

```
Zone-pair: source office destination library
```

```
IPv4 ACL 3001
```

```
rule 0 permit source 2.2.2.2 0
```

```
rule 5 permit source 1.1.1.1 0 counting (2 packets)
```

```
rule 10 permit vpn-instance test (Failed)
```

```
Totally 2 packets 256 bytes permitted, 0 packets 0 bytes denied
```

```
Totally 100% permitted, 0% denied
```

表1-4 display packet-filter statistics 命令显示信息描述表

字段	描述
Zone-pair	在指定安全域间实例上应用的统计信息
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv4 ACL 2002 (Failed)	IPv4基本ACL 2002应用失败
2 packets	该规则匹配了2个包（当匹配的包个数为0时不显示本字段）
No resource	该规则对应的统计资源不足。在显示统计信息时，若该规则的统计资源不足，便会显示本字段
rule 5 permit source 1.1.1.1 0 (Failed)	规则5应用失败
Totally 2 packets permitted, 0 packets denied	该ACL允许和拒绝符合条件报文的个数

字段	描述
Totally 100% permitted, 0% denied	该ACL允许符合条件报文的通过率和拒绝符合条件报文的丢弃率

【相关命令】

- **reset packet-filter statistics**

1.1.11 display packet-filter verbose

display packet-filter verbose 命令用来显示 ACL 在报文过滤中的详细应用情况。

【命令】

```
display packet-filter verbose zone-pair security source source-zone-name
destination destination-zone-name [ [ ipv6 ] { acl-number | name acl-name } ]
[ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface interface-type interface-number: 显示指定接口上 ACL 在报文过滤中的详细应用情况。*interface-type interface-number* 表示接口类型和接口编号。当接口类型为以太网接口时，不需要指定 **slot** 参数。

zone-pair security source source-zone-name destination destination-zone-name: 显示指定安全域间实例上 ACL 在报文过滤中的详细应用情况。*source-zone-name*: 表示安全域间实例源安全域的名称，为 1~31 个字符的字符串，不区分大小写。*destination-zone-name*: 表示安全域间实例目的安全域的名称，为 1~31 个字符的字符串，不区分大小写。

inbound: 显示入方向上 ACL 在报文过滤中的详细应用情况。

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

acl-number: 显示指定编号 ACL 在报文过滤中的详细应用情况。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000~2999: 表示基本 ACL。
- 3000~3999: 表示高级 ACL。
- 4000~4999: 表示二层 ACL。

name acl-name:显示指定名称 ACL 在报文过滤中的详细应用情况。*acl-name* 表示 ACL 的名称，为 1~63 个字符的字符串，不区分大小写。

slot slot-number: 显示指定成员设备上 ACL 在报文过滤中的详细应用情况，*slot-number* 表示设备在 IRF 中的成员编号。若未指定本参数，将显示主用设备上 ACL 在报文过滤中的详细应用情况。

【使用指导】

若未指定 *acl-number*、**name acl-name** 和 ACL 类型 (**ipv6**、**mac**) 参数，将显示全部 IPv4 ACL 在报文过滤中的详细应用情况。

【举例】

```
#显示安全域间实例源域 office 到目的域 library 上全部 ACL 在报文过滤中的详细应用情况。
<Sysname> display packet-filter verbose zone-pair security source office destination library
Zone-pair: source office destination library
  IPv4 ACL 2001
    rule 0 permit
    rule 5 permit source 1.1.1.1 0
    rule 10 permit vpn-instance test
```

表1-5 display packet-filter verbose 命令显示信息描述表

字段	描述
Zone-pair	ACL在指定安全域间实例上的详细应用情况
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv4 ACL 2002 (Failed)	IPv4基本ACL 2002应用失败
rule 5 permit source 1.1.1.1 0 (Failed)	规则5应用失败

1.1.12 packet-filter

packet-filter 命令用来在安全域间实例上应用 ACL 进行报文过滤。
undo packet-filter 命令用来取消在安全域间实例上应用 ACL 进行报文过滤。

【命令】

```
packet-filter [ ipv6 ] { acl-number | name acl-name }
undo packet-filter [ ipv6 ] { acl-number | name acl-name }
```

【缺省情况】

在安全域间实例上没有应用 ACL 进行报文过滤。

【视图】

安全域间实例视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6: 指定 ACL 类型为 IPv6 ACL。若未指定本参数，则表示 IPv4 ACL。

acl-number: 指定 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。

name acl-name: 指定 ACL 的名称。**acl-name** 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【举例】

应用 IPv4 基本 ACL 2002 对源安全域 office 到目的安全域 library 的安全域间实例收到的报文进行过滤。

```
<Sysname> system-view
```

```
[Sysname] zone-pair security source office destination library
```

```
[Sysname-zone-pair-security-office-library] packet-filter 2002
```

【相关命令】

- **display packet-filter**
- **display packet-filter statistics**
- **display packet-filter verbose**

1.1.13 reset acl counter

reset acl counter 命令用来清除 ACL 的统计信息。

【命令】

reset acl [ipv6 | mac] counter { acl-number | all | name acl-name }

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

acl-number: 清除指定编号 ACL 的统计信息。**acl-number** 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

all: 清除指定类型中全部 ACL 的统计信息。

name acl-name: 清除指定名称 ACL 的统计信息。**acl-name** 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【举例】

```
# 清除 IPv4 基本 ACL 2001 的统计信息。  
<Sysname> reset acl counter 2001
```

【相关命令】

- **display acl**

1.1.14 reset packet-filter statistics

reset packet-filter statistics 命令用来清除 ACL 在报文过滤中应用的统计信息。

【命令】

```
reset packet-filter statistics zone-pair security [ source source-zone-name  
destination destination-zone-name ] [ ipv6 ] { acl-number | name acl-name } ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

zone-pair security [**source** *source-zone-name* **destination** *destination-zone-name*]: 清除指定接口上的统计信息。*source-zone-name*: 表示安全域间实例源安全域的名称, 为 1~31 个字符的字符串, 不区分大小写。*destination-zone-name*: 表示安全域间实例目的安全域的名称, 为 1~31 个字符的字符串, 不区分大小写。

default: 清除缺省动作在报文过滤中应用的统计信息。

ipv6: 指定 ACL 类型为 IPv6 ACL。

mac: 指定 ACL 类型为二层 ACL。

acl-number: 清除指定编号 ACL 在报文过滤中应用的统计信息。*acl-number* 表示 ACL 的编号, 取值范围及其代表的 ACL 类型如下:

- 2000~2999: 表示基本 ACL。
- 3000~3999: 表示高级 ACL。
- 4000~4999: 表示二层 ACL。

name *acl-name*: 清除指定名称 ACL 在报文过滤中应用的统计信息。*acl-name* 表示 ACL 的名称, 为 1~63 个字符的字符串, 不区分大小写。

【使用指导】

如果未指定 **default**、*acl-number*、**name** *acl-name* 和 ACL 类型 (**ipv6**、**mac**) 参数, 将清除全部 ACL 在报文过滤中应用的统计信息。

【举例】

```
# 清除在源安全域 office 到目的安全域 library 的安全域间实例上 IPv4 基本 ACL 2001 在报文过滤中应用的统计信息。
```

```
<Sysname> reset packet-filter statistics zone-pair security source office destination  
library 2001
```

【相关命令】

- **display packet-filter statistics**
- **display packet-filter statistics sum**

1.1.15 rule (IPv4 advanced ACL view)

rule 命令用来为 IPv4 高级 ACL 创建一条规则。

undo rule 命令用来为 IPv4 高级 ACL 删除一条规则或删除规则中的部分内容。

【命令】

```
rule [ rule-id ] { deny | permit } protocol [ { { ack ack-value | fin fin-value |  
psh psh-value | rst rst-value | syn syn-value | urg urg-value } * | established }  
| counting | destination { object-group address-group-name | dest-address  
dest-wildcard | any } | destination-port { object-group port-group-name |  
operator port1 [ port2 ] } | { dscp dscp | { precedence precedence | tos tos } * }  
| fragment | icmp-type { icmp-type [ icmp-code ] | icmp-message } | logging |  
source { object-group address-group-name | source-address source-wildcard |  
any } | source-port { object-group port-group-name | operator port1 [ port2 ] }  
| time-range time-range-name | vpn-instance vpn-instance-name ] *
```

```
undo rule rule-id [ { { ack | fin | psh | rst | syn | urg } * | established } |  
counting | destination | destination-port | { dscp | { precedence | tos } * } |  
fragment | icmp-type | logging | source | source-port | time-range |  
vpn-instance ] *
```

```
undo rule [ rule-id ] { deny | permit } protocol [ { { ack ack-value | fin  
fin-value | psh psh-value | rst rst-value | syn syn-value | urg urg-value } * |  
established } | counting | destination { object-group address-group-name |  
dest-address dest-wildcard | any } | destination-port { object-group  
port-group-name | operator port1 [ port2 ] } | { dscp dscp | { precedence  
precedence | tos tos } * } | fragment | icmp-type { icmp-type [ icmp-code ] |  
icmp-message } | logging | source { object-group address-group-name |  
source-address source-wildcard | any } | source-port { object-group  
port-group-name | operator port1 [ port2 ] } | time-range time-range-name |  
vpn-instance vpn-instance-name ] *
```

【缺省情况】

IPv4 高级 ACL 内不存在任何规则。

【视图】

IPv4 高级 ACL 视图

【缺省用户角色】

network-admin
context-admin

【参数】

rule-id: 指定 IPv4 高级 ACL 规则的编号, 取值范围为 0~65534。若未指定本参数, 系统将从规则编号的起始值开始, 自动分配一个大于现有最大编号的步长最小倍数。譬如现有规则的最大编号为 28, 步长为 5, 那么自动分配的新编号将是 30。

deny: 表示拒绝符合条件的报文。

permit: 表示允许符合条件的报文。

protocol: 表示 IPv4 承载的协议类型, 可输入的形式如下:

- 数字: 取值范围为 0~255;
- 名称 (括号内为对应的数字): 可选取 **gre** (47)、**icmp** (1)、**igmp** (2)、**ip**、**ipinip** (4)、**ospf** (89)、**tcp** (6) 或 **udp** (17)。**ip** 表示所有协议类型。

protocol之后可配置如 [表 1-6](#) 所示的规则信息参数。

表1-6 规则信息参数

参数	类别	作用	说明
source { object-group <i>address-group-name</i> <i>source-address</i> <i>source-wildcard</i> any }	源地址信息	指定ACL规则的源地址信息	<i>address-group-name</i> : 源地址对象组的名称 <i>source-address</i> : 源IP地址 <i>source-wildcard</i> : 源IP地址的通配符掩码 (为0表示主机地址) any : 任意源IP地址
destination { object-group <i>address-group-name</i> <i>dest-address</i> <i>dest-wildcard</i> any }	目的地址信息	指定ACL规则的目的地址信息	<i>address-group-name</i> : 目的地址对象组的名称 <i>dest-address</i> : 目的IP地址 <i>dest-wildcard</i> : 目的IP地址的通配符掩码 (为0表示主机地址) any : 任意目的IP地址
counting	统计	开启规则匹配软件统计功能, 缺省为关闭	本参数用于开启本规则的匹配统计功能
precedence <i>precedence</i>	报文优先级	指定IP优先级	<i>precedence</i> 用数字表示时, 取值范围为0~7; 用字符表示时, 分别对应 routine 、 priority 、 immediate 、 flash 、 flash-override 、 critical 、 internet 、 network
tos <i>tos</i>	报文优先级	指定ToS优先级	<i>tos</i> 用数字表示时, 取值范围为0~15; 用字符表示时, 可以选取 max-reliability (2)、 max-throughput (4)、 min-delay (8)、 min-monetary-cost (1)、 normal (0)
dscp <i>dscp</i>	报文优先级	指定DSCP优先级	<i>dscp</i> 用数字表示时, 取值范围为0~63; 用字符表示时, 可以选取 af11 (10)、 af12 (12)、 af13 (14)、 af21 (18)、 af22 (20)、 af23 (22)、 af31 (26)、 af32 (28)、 af33 (30)、 af41 (34)、 af42 (36)、 af43 (38)、 cs1 (8)、 cs2 (16)、 cs3 (24)、 cs4 (32)、 cs5 (40)、 cs6 (48)、 cs7 (56)、 default (0)、 ef (46)。

参数	类别	作用	说明
fragment	分片信息	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定该参数，则表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效
logging	日志操作	表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数	该功能需要使用该ACL的模块支持日志记录功能，例如报文过滤
time-range <i>time-range-name</i>	时间段	指定本规则生效的时间段	<i>time-range-name</i> : 时间段的名称，为1~32个字符的字符串，不区分大小写。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL配置指导”中的“时间段”
vpn-instance <i>vpn-instance-name</i>	VPN实例	对指定VPN实例中的报文有效	<i>vpn-instance-name</i> : MPLS L3VPN的VPN实例名称，为1~31个字符的字符串，区分大小写 若未指定本参数，表示该规则对非VPN报文和VPN报文均有效

当`protocol`为**tcp**（6）或**udp**（17）时，用户还可配置如 [表 1-7](#) 所示的规则信息参数。

表1-7 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port { object-group <i>port-group-name</i> <i>operator port1</i> [<i>port2</i>] }	源端口	定义TCP/UDP报文的源端口信息	<i>port-group-name</i> : 端口对象组的名称 <i>operator</i> 为操作符，取值可以为 lt （小于）、 gt （大于）、 eq （等于）、 neq （不等于）或者 range （在范围内，包括边界值）。只有操作符 range 需要两个端口

参数	类别	作用	说明
destination-port { object-group <i>port-group-name</i> <i>operator port1</i> [<i>port2</i>] }	目的端口	定义TCP/UDP报文的目的端口信息	号做操作数，其它的只需要一个端口号做操作数 <i>port1</i> 、 <i>port2</i> : TCP或UDP的端口号，用数字表示时，取值范围为0~65535；用字符表示时，TCP端口号可以选取 chargen (19)、 bgp (179)、 cmd (514)、 daytime (13)、 discard (9)、 dns (53)、 domain (53)、 echo (7)、 exec (512)、 finger (79)、 ftp (21)、 ftp-data (20)、 gopher (70)、 hostname (101)、 irc (194)、 klogin (543)、 kshell (544)、 login (513)、 lpd (515)、 nnntp (119)、 pop2 (109)、 pop3 (110)、 smtp (25)、 sunrpc (111)、 tacacs (49)、 talk (517)、 telnet (23)、 time (37)、 uucp (540)、 whois (43)、 www (80)；UDP端口号可以选取 biff (512)、 bootpc (68)、 bootps (67)、 discard (9)、 dns (53)、 dnsix (90)、 echo (7)、 moblip-ag (434)、 moblip-mn (435)、 nameserver (42)、 netbios-dgm (138)、 netbios-ns (137)、 netbios-ssn (139)、 ntp (123)、 rip (520)、 snmp (161)、 snmptrap (162)、 sunrpc (111)、 syslog (514)、 tacacs-ds (65)、 talk (517)、 tftp (69)、 time (37)、 who (513)、 xdmcp (177)
{ ack <i>ack-value</i> fin <i>fin-value</i> psh <i>psh-value</i> rst <i>rst-value</i> syn <i>syn-value</i> urg <i>urg-value</i> } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各 <i>value</i> 的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 对于一条规则中各标志位的配置组合，处理方式为“或”，譬如：当配置为 ack 0 psh 1 时，匹配不携带ACK或携带PSH标志位的TCP报文
established	TCP连接建立标识	定义对TCP连接报文的处理规则	TCP协议特有的参数，表示匹配携带ACK或RST标志位的TCP连接报文

当*protocol*为**icmp** (1) 时，用户还可配置如 [表 1-8](#) 所示的规则信息参数。

表1-8 ICMP 特有的规则信息参数

参数	类别	作用	说明
icmp-type { <i>icmp-type</i> <i>icmp-code</i> <i>icmp-message</i> }	ICMP报文的 消息类型和消息码信息	指定本规则中 ICMP报文的 消息类型和消息码信息	<i>icmp-type</i> : ICMP消息类型，取值范围为0~255 <i>icmp-code</i> : ICMP消息码，取值范围为0~255 <i>icmp-message</i> : ICMP消息名称。可以输入的ICMP消息名称，及其与消息类型和消息码的对应关系如 表 1-9 所示

表1-9 ICMP 消息名称与消息类型和消息码的对应关系

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

创建的规则若与动态规则的内容完全相同，则会覆盖已有动态规则。

新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

display acl all 命令可以查看所有已存在的 IPv4 高级 ACL 规则和 IPv4 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule rule-id** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule [rule-id] { deny | permit }** 命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }** 命令时，必须输入已存在规则的完整形式。

【举例】

为 IPv4 高级 ACL 3000 创建规则如下：允许 129.9.0.0/16 网段内的主机与 202.38.160.0/24 网段内主机的 WWW 端口（端口号为 80）建立连接。

```
<Sysname> system-view
```

```

[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq 80
# 为 IPv4 高级 ACL 3001 创建规则如下：允许 IP 报文通过，但拒绝发往 192.168.1.0/24 网段的 ICMP
报文通过。
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] rule permit ip
# 为 IPv4 高级 ACL 3002 创建规则如下：在出、入双方向上都允许建立 FTP 连接并传输 FTP 数据。
<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data
# 为 IPv4 高级 ACL 3003 创建规则如下：在出、入双方向上都允许 SNMP 报文和 SNMP Trap 报文
通过。
<Sysname> system-view
[Sysname] acl advanced 3003
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap

```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.16 rule (IPv4 basic ACL view)

rule 命令用来为 IPv4 基本 ACL 创建一条规则。

undo rule 命令用来为 IPv4 基本 ACL 删除一条规则或删除规则中的部分内容。

【命令】

```

rule [ rule-id ] { deny | permit } [ counting | fragment | logging | source
{ object-group address-group-name | source-address source-wildcard | any } |
time-range time-range-name | vpn-instance vpn-instance-name ] *
undo rule rule-id [ counting | fragment | logging | source | time-range |
vpn-instance ] *
undo rule [ rule-id ] { deny | permit } [ counting | fragment | logging | source
{ object-group address-group-name | source-address source-wildcard | any } |
time-range time-range-name | vpn-instance vpn-instance-name ] *

```

【缺省情况】

IPv4 基本 ACL 内不存在任何规则。

【视图】

IPv4 基本 ACL 视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-id: 指定 IPv4 基本 ACL 规则的编号，取值范围为 0~65534。若未指定本参数，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny: 表示拒绝符合条件的报文。

permit: 表示允许符合条件的报文。

counting: 表示开启规则匹配软件统计功能，缺省为关闭。

fragment: 表示仅对非首片分片报文有效，而对非分片报文和首片分片报文无效。若未指定本参数，表示该规则对非分片报文和分片报文均有效。

logging: 表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数。该功能需要使用该 ACL 的模块支持日志记录功能，例如报文过滤。

source { object-group address-group-name | source-address source-wildcard | any }: 指定规则的源 IP 地址信息。**address-group-name** 表示源 IP 地址对象组的名称，**source-address** 表示报文的源 IP 地址，**source-wildcard** 表示源 IP 地址的通配符掩码（为 0 表示主机地址），**any** 表示任意源 IP 地址。

time-range time-range-name: 指定本规则生效的时间段。**time-range-name** 表示时间段的名称，为 1~32 个字符的字符串，不区分大小写。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL 配置指导”中的“时间段”。

vpn-instance vpn-instance-name: 表示对指定 VPN 实例中的报文有效。**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，表示该规则对非 VPN 报文和 VPN 报文均有效。

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

display acl all 命令可以查看所有已存在的 IPv4 高级 ACL 规则和 IPv4 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule rule-id** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule [rule-id] { deny | permit }** 命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }** 命令时，必须输入已存在规则的完整形式。

【举例】

为 IPv4 基本 ACL 2000 创建规则如下：仅允许来自 10.0.0.0/8、172.17.0.0/16 和 192.168.1.0/24 网段的报文通过，而拒绝来自所有其它网段的报文通过。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range** (ACL 和 QoS 命令参考/时间段)

1.1.17 rule (IPv6 advanced ACL view)

rule 命令用来为 IPv6 高级 ACL 创建一条规则。

undo rule 命令用来为 IPv6 高级 ACL 删除一条规则或删除规则中的部分内容。

【命令】

```
rule [ rule-id ] { deny | permit } protocol [ { { ack ack-value | fin fin-value |  
psh psh-value | rst rst-value | syn syn-value | urg urg-value } * | established }  
| counting | destination { object-group address-group-name | dest-address  
dest-prefix | dest-address/dest-prefix | any } | destination-port  
{ object-group port-group-name | operator port1 [ port2 ] } | dscp dscp |  
flow-label flow-label-value | fragment | icmp6-type { icmp6-type icmp6-code |  
icmp6-message } | logging | routing [ type routing-type ] | hop-by-hop [ type  
hop-type ] | source { object-group address-group-name | source-address  
source-prefix | source-address/source-prefix | any } | source-port  
{ object-group port-group-name | operator port1 [ port2 ] } | time-range  
time-range-name | vpn-instance vpn-instance-name ] *  
undo rule rule-id [ { { ack | fin | psh | rst | syn | urg } * | established }  
counting | destination | destination-port | dscp | flow-label | fragment |  
icmp6-type | logging | routing | hop-by-hop | source | source-port |  
time-range | vpn-instance ] *  
undo rule [ rule-id ] { deny | permit } protocol [ { { ack ack-value | fin  
fin-value | psh psh-value | rst rst-value | syn syn-value | urg urg-value } * |
```



```

established } | counting | destination { object-group address-group-name |
dest-address dest-prefix | dest-address/dest-prefix | any } |
destination-port { object-group port-group-name | operator port1 [ port2 ] } |
dscp dscp | flow-label flow-label-value | fragment | icmp6-type { icmp6-type
icmp6-code | icmp6-message } | logging | routing [ type routing-type ] |
hop-by-hop [ type hop-type ] | source { object-group address-group-name |
source-address source-prefix | source-address/source-prefix | any } |
source-port { object-group port-group-name | operator port1 [ port2 ] } |
time-range time-range-name | vpn-instance vpn-instance-name ] *

```

【缺省情况】

IPv6 高级 ACL 内不存在任何规则。

【视图】

IPv6 高级 ACL 视图

【缺省用户角色】

network-admin
context-admin

【参数】

rule-id: 指定 IPv6 高级 ACL 规则的编号，取值范围为 0~65534。若未指定本参数，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny: 表示拒绝符合条件的报文。

permit: 表示允许符合条件的报文。

protocol: 表示 IPv6 承载的协议类型，可输入的形式如下：

- 数字：取值范围为 0~255；
- 名称（括号内为对应的数字）：可选取 **gre**（47）、**icmpv6**（58）、**ipv6**、**ipv6-ah**（51）、**ipv6-esp**（50）、**ospf**（89）、**tcp**（6）或 **udp**（17）。**ipv6** 表示所有协议类型。

protocol之后可配置如 [表 1-10](#) 所示的规则信息参数。

表1-10 规则信息参数

参数	类别	作用	说明
source { object-group <i>address-group-name</i> <i>source-address source-prefix</i> <i>source-address/source-prefix</i> any }	源IPv6地址	指定ACL规则的源IPv6地址信息	<i>address-group-name</i> : 源地址对象组的名称 <i>source-address</i> : 源IPv6地址 <i>source-prefix</i> : 源IPv6地址的前缀长度，取值范围1~128 any : 任意源IPv6地址

参数	类别	作用	说明
destination { object-group <i>address-group-name</i> <i>dest-address dest-prefix</i> <i>dest-address/dest-prefix</i> any }	目的IPv6地址	指定ACL规则的目的地IPv6地址信息	<i>address-group-name</i> : 目的地址对象组的名称 <i>dest-address</i> : 目的IPv6地址 <i>dest-prefix</i> : 目的IPv6地址的前缀长度, 取值范围1~128 any : 任意目的IPv6地址
counting	统计	开启规则匹配软件统计功能, 缺省为关闭	本参数用于开启本规则的匹配统计功能
dscp <i>dscp</i>	报文优先级	指定DSCP优先级	<i>dscp</i> : 用数字表示时, 取值范围为0~63; 用名称表示时, 可选取 af11 (10)、 af12 (12)、 af13 (14)、 af21 (18)、 af22 (20)、 af23 (22)、 af31 (26)、 af32 (28)、 af33 (30)、 af41 (34)、 af42 (36)、 af43 (38)、 cs1 (8)、 cs2 (16)、 cs3 (24)、 cs4 (32)、 cs5 (40)、 cs6 (48)、 cs7 (56)、 default (0) 或 ef (46)
flow-label <i>flow-label-value</i>	流标签字段	指定IPv6基本报文头中流标签字段的值	<i>flow-label-value</i> : 流标签字段的值, 取值范围为0~1048575
fragment	报文分片	仅对分片报文的非首个分片有效, 而对非分片报文和分片报文的首个分片无效	若未指定本参数, 表示该规则对所有报文 (包括非分片报文和分片报文的每个分片) 均有效
logging	日志操作	表示记录规则匹配报文的日志信息, 包括匹配报文的规则和匹配报文的个数	该功能需要使用该ACL的模块支持日志记录功能, 例如报文过滤
routing [type <i>routing-type</i>]	路由头	指定路由头的类型	<i>routing-type</i> : 路由头类型的值, 取值范围为0~255 若指定了 type routing-type 参数, 表示仅对指定类型的路由头有效; 否则, 表示对IPv6所有类型的路由头都有效
hop-by-hop [type <i>hop-type</i>]	逐跳头	指定逐跳头的类型	<i>hop-type</i> : 逐跳头类型的值, 取值范围为0~255 若指定了 type hop-type 参数, 表示仅对指定类型的逐跳头有效; 否则, 表示对IPv6所有类型的逐跳头都有效

参数	类别	作用	说明
time-range <i>time-range-name</i>	时间段	指定本规则生效的时间段	<i>time-range-name</i> : 时间段的名称, 为1~32个字符的字符串, 不区分大小写。若该时间段尚未配置, 该规则仍会成功创建但系统将给出提示信息, 并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程, 请参见“ACL配置指导”中的“时间段”
vpn-instance <i>vpn-instance-name</i>	VPN实例	对指定VPN实例中的报文有效	<i>vpn-instance-name</i> : MPLS L3VPN的VPN实例名称, 为1~31个字符的字符串, 区分大小写 若未指定本参数, 表示该规则对非VPN报文和VPN报文均有效

当`protocol`为**tcp** (6) 或**udp** (17) 时, 用户还可配置如 [表 1-11](#) 所示的规则信息参数。

表1-11 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port { object-group <i>port-group-name</i> operator <i>port1</i> [<i>port2</i>] }	源端口	定义TCP/UDP报文的源端口信息	<i>port-group-name</i> : 端口对象组的名称 <i>operator</i> : 操作符, 取值可以为 lt (小于)、 gt (大于)、 eq (等于)、 neq (不等于) 或者 range (在范围内, 包括边界值)。只有 range 操作符需要两个端口号做操作数, 其它操作符只需要一个端口号做操作数
destination-port { object-group <i>port-group-name</i> operator <i>port1</i> [<i>port2</i>] }	目的端口	定义TCP/UDP报文的目的端口信息	<i>port1/port2</i> : TCP或UDP的端口号, 用数字表示时, 取值范围为0~65535; 用名称表示时, TCP端口号可选取 chargen (19)、 bgp (179)、 cmd (514)、 daytime (13)、 discard (9)、 dns (53)、 domain (53)、 echo (7)、 exec (512)、 finger (79)、 ftp (21)、 ftp-data (20)、 gopher (70)、 hostname (101)、 irc (194)、 klogin (543)、 kshell (544)、 login (513)、 lpd (515)、 nntp (119)、 pop2 (109)、 pop3 (110)、 smtp (25)、 sunrpc (111)、 tacacs (49)、 talk (517)、 telnet (23)、 time (37)、 uucp (540)、 whois (43) 或 www (80); UDP端口号可选取 biff (512)、 bootpc (68)、 bootps (67)、 discard (9)、 dns (53)、 dnsix (90)、 echo (7)、 mobilip-ag (434)、 mobilip-mn (435)、 nameserver (42)、 netbios-dgm (138)、 netbios-ns (137)、 netbios-ssn (139)、 ntp (123)、 rip (520)、 snmp (161)、 snmptrap (162)、 sunrpc (111)、 syslog (514)、 tacacs-ds (65)、 talk (517)、 tftp (69)、 time (37)、 who (513) 或 xdmcp (177)
{ ack <i>ack-value</i> fin <i>fin-value</i> psh <i>psh-value</i> rst <i>rst-value</i> syn <i>syn-value</i> urg <i>urg-value</i> } *	TCP报文标识	定义对携带不同标志位 (包括ACK、FIN、PSH、RST、SYN和URG六种) 的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文, 各 <i>value</i> 的取值可为0或1 (0表示不携带此标志位, 1表示携带此标志位) 对于一条规则中各标志位的配置组合, 处理方式为“或”。譬如: 当配置为 ack 0 psh 1 时, 则匹配不携带ACK或携带PSH标志位的TCP报文

参数	类别	作用	说明
established	TCP连接建立标识	定义对TCP连接报文的处理规则	TCP协议特有的参数，表示匹配携带ACK或RST标志位的TCP连接报文

当`protocol`为**icmpv6**（58）时，用户还可配置如 [表 1-12](#) 所示的规则信息参数。

表1-12 ICMPv6 特有的规则信息参数

参数	类别	作用	说明
icmp6-type { <i>icmp6-type</i> <i>icmp6-code</i> <i>icmp6-message</i> }	ICMPv6报文的 消息类型和 消息码	指定本规则中 ICMPv6报文的 消息类型和 消息码信息	<i>icmp6-type</i> : ICMPv6消息类型，取值范围为0~255 <i>icmp6-code</i> : ICMPv6消息码，取值范围为0~255 <i>icmp6-message</i> : ICMPv6消息名称。可以输入的 ICMPv6消息名称，及其与消息类型和消息码的对应关系如 表1-13 所示

表1-13 ICMPv6 消息名称与消息类型和消息码的对应关系

ICMPv6 消息名称	ICMPv6 消息类型	ICMPv6 消息码
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

创建的规则若与动态规则的内容完全相同，则会覆盖已有动态规则。新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。

display acl ipv6 all 命令可以查看所有已存在的 IPv6 高级 ACL 规则和 IPv6 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule rule-id** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule [rule-id] { deny | permit }** 命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }** 命令时，必须输入已存在规则的完整形式。

【举例】

为 IPv6 高级 ACL 3000 创建规则如下：允许 2030:5060::/64 网段内的主机与 FE80:5060::/96 网段内主机的 WWW 端口（端口号为 80）建立连接。

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3000
[Sysname-acl-ipv6-adv-3000] rule permit tcp source 2030:5060::/64 destination
fe80:5060::/96 destination-port eq 80
```

为 IPv6 高级 ACL 3001 创建规则如下：允许 IPv6 报文通过，但拒绝发往 FE80:5060:1001::/48 网段的 ICMPv6 报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3001
[Sysname-acl-ipv6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
[Sysname-acl-ipv6-adv-3001] rule permit ipv6
```

为 IPv6 高级 ACL 3002 创建规则如下：在出、入双方向上都允许建立 FTP 连接并传输 FTP 数据。

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3002
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp-data
```

为 IPv6 高级 ACL 3003 创建规则如下：在出、入双方向上都允许 SNMP 报文和 SNMP Trap 报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3003
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmptrap
```

为 IPv6 高级 ACL 3004 创建规则如下：在含有逐跳头的报文中，只允许转发含有 MLD 选项（Type =5）的报文，丢弃其他报文。

```
<Sysname> system-view
[Sysname] acl ipv6 advanced 3004
[Sysname-acl-ipv6-adv-3004] rule permit ipv6 hop-by-hop type 5
```

```
[Sysname-acl-ipv6-adv-3004] rule deny ipv6 hop-by-hop
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.18 rule (IPv6 basic ACL view)

rule 命令用来为 IPv6 基本 ACL 创建一条规则。

undo rule 命令用来为 IPv6 基本 ACL 删除一条规则或删除规则中的部分内容。

【命令】

```
rule [ rule-id ] { deny | permit } [ counting | fragment | logging | routing  
[ type routing-type ] | source { object-group address-group-name |  
source-address source-prefix | source-address/source-prefix | any } |  
time-range time-range-name | vpn-instance vpn-instance-name ] *  
undo rule rule-id [ counting | fragment | logging | routing | source |  
time-range | vpn-instance ] *  
undo rule [ rule-id ] { deny | permit } [ counting | fragment | logging | routing  
[ type routing-type ] | source { object-group address-group-name |  
source-address source-prefix | source-address/source-prefix | any } |  
time-range time-range-name | vpn-instance vpn-instance-name ] *
```

【缺省情况】

IPv6 基本 ACL 内不存在任何规则。

【视图】

IPv6 基本 ACL 视图

【缺省用户角色】

network-admin
context-admin

【参数】

rule-id: 指定 IPv6 基本 ACL 规则的编号，取值范围为 0~65534。若未指定本参数，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny: 表示拒绝符合条件的报文。

permit: 表示允许符合条件的报文。

counting: 表示开启规则匹配软件统计功能，缺省为关闭。

fragment: 表示仅对非首片分片报文有效，而对非分片报文和首片分片报文无效。若未指定本参数，表示该规则对非分片报文和分片报文均有效。

logging: 表示记录规则匹配报文的日志信息，包括匹配报文的规则和匹配报文的个数。该功能需要使用该 ACL 的模块支持日志记录功能，例如报文过滤。

routing [type routing-type]: 表示对所有或指定类型的路由头有效，*routing-type* 表示路由头类型的值，取值范围为 0~255。若指定了 **type routing-type** 参数，表示仅对指定类型的路由头有效；否则，表示对 IPv6 所有类型的路由头都有效。

source { object-group address-group-name | source-address source-prefix | source-address/source-prefix | any }: 指定规则的源 IPv6 地址信息。*address-group-name* 表示源 IP 地址对象组的名称，*source-address* 表示报文的源 IPv6 地址，*source-prefix* 表示源 IPv6 地址的前缀长度，取值范围为 1~128，**any** 表示任意源 IPv6 地址。

time-range time-range-name: 指定本规则生效的时间段。*time-range-name* 表示时间段的名称，为 1~32 个字符的字符串，不区分大小写。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL 配置指导”中的“时间段”。

vpn-instance vpn-instance-name: 表示对指定 VPN 实例中的报文有效。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。若未指定本参数，表示该规则对非 VPN 报文和 VPN 报文均有效。

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

display acl ipv6 all 命令可以查看所有已存在的 IPv6 高级 ACL 规则和 IPv6 基本 ACL 规则。删除规则时需要注意的是：

- 使用 **undo rule rule-id** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule [rule-id] { deny | permit }** 命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }** 命令时，必须输入已存在规则的完整形式。

【举例】

为 IPv6 基本 ACL 2000 创建规则如下：仅允许来自 1001::/16、3124:1123::/32 和 FE80:5060:1001::/48 网段的报文通过，而拒绝来自所有其它网段的报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source 1001:: 16
[Sysname-acl-ipv6-basic-2000] rule permit source 3124:1123:: 32
[Sysname-acl-ipv6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl-ipv6-basic-2000] rule deny source any
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range** (ACL 和 QoS 命令参考/时间段)

1.1.19 rule (Layer 2 ACL view)

rule 命令用来为二层 ACL 创建一条规则。

undo rule 命令用来为二层 ACL 删除一条规则或删除规则中的部分内容。

【命令】

```
rule [rule-id] { deny | permit } [ cos dot1p | counting | dest-mac dest-address dest-mask | { lsap lsap-type lsap-type-mask | type protocol-type protocol-type-mask } | source-mac source-address source-mask | time-range time-range-name ] *
```

```
undo rule rule-id [ counting | time-range ] *
```

```
undo rule [rule-id] { deny | permit } [ cos dot1p | counting | dest-mac dest-address dest-mask | { lsap lsap-type lsap-type-mask | type protocol-type protocol-type-mask } | source-mac source-address source-mask | time-range time-range-name ] *
```

【缺省情况】

二层 ACL 内不存在任何规则。

【视图】

二层 ACL 视图

【缺省用户角色】

network-admin

context-admin

【参数】

rule-id: 指定二层 ACL 规则的编号, 取值范围为 0~65534。若未指定本参数, 系统将从规则编号的起始值开始, 自动分配一个大于现有最大编号的步长最小倍数。譬如现有规则的最大编号为 28, 步长为 5, 那么自动分配的新编号将是 30。

deny: 表示拒绝符合条件的报文。

permit: 表示允许符合条件的报文。

cos dot1p: 指定 802.1p 优先级。**dot1p** 表示 802.1p 优先级, 可输入的形式如下:

- 数字: 取值范围为 0~7;
- 名称: **best-effort**、**background**、**spare**、**excellent-effort**、**controlled-load**、**video**、**voice** 和 **network-management**, 依次对应于数字 0~7。

counting: 表示开启规则匹配软件统计功能, 缺省为关闭。

dest-mac dest-address dest-mask: 指定目的 MAC 地址范围。*dest-address* 表示目的 MAC 地址，格式为 H-H-H。*dest-mask* 表示目的 MAC 地址的掩码，格式为 H-H-H。

lsap lsap-type lsap-type-mask: 指定 LLC 封装中的 DSAP 字段和 SSAP 字段。*lsap-type* 表示数据帧的封装格式，取值范围为十六进制数 0~ffff。*lsap-type-mask* 表示 LSAP 的类型掩码，用于指定屏蔽位，取值范围为十六进制数 0~ffff。

type protocol-type protocol-type-mask: 指定链路层协议类型。*protocol-type* 表示数据帧类型，对应 Ethernet_II 类型和 Ethernet_SNAP 类型帧中的 type 域，取值范围为十六进制数 0~ffff。*protocol-type-mask* 表示类型掩码，用于指定屏蔽位，取值范围为十六进制数 0~ffff。

source-mac source-address source-mask: 指定源 MAC 地址范围。*source-address* 表示源 MAC 地址，格式为 H-H-H。*source-mask* 表示源 MAC 地址的掩码，格式为 H-H-H。

time-range time-range-name: 指定本规则生效的时间段。*time-range-name* 表示时间段的名称，为 1~32 个字符的字符串，不区分大小写。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL 配置指导”中的“时间段”。

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

display acl mac all 命令可以查看所有已存在的二层 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule rule-id** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule [rule-id] { deny | permit }** 命令无法删除规则中的部分内容，使用 **undo rule { deny | permit }** 命令时，必须输入已存在规则的完整形式。

【举例】

为二层 ACL 4000 创建规则如下：允许 ARP 报文通过，但拒绝 RARP 报文通过。

```
<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000] rule permit type 0806 ffff
[Sysname-acl-mac-4000] rule deny type 8035 ffff
```

【相关命令】

- **acl**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.20 rule comment

rule comment 命令用来为规则配置描述信息。

undo rule comment 命令用来删除指定规则的描述信息。

【命令】

```
rule rule-id comment text
undo rule rule-id comment
```

【缺省情况】

规则没有描述信息。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图
IPv6 基本 ACL 视图/IPv6 高级 ACL 视图
二层 ACL 视图

【缺省用户角色】

network-admin
context-admin

【参数】

rule-id: 指定规则的编号，该规则必须存在。取值范围为 0~65534。
text: 表示规则的描述信息，为 1~127 个字符的字符串，区分大小写。

【使用指导】

使用 **rule comment** 命令时，如果指定的规则没有描述信息，则为其添加描述信息，否则修改其描述信息。

【举例】

为 IPv4 基本 ACL 2000 配置规则 0，并为该规则配置描述信息。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] rule 0 comment This rule is used on gigabitethernet 1/0/1.
```

【相关命令】

- **display acl**

1.1.21 step

step 命令用来配置规则编号的步长。

undo step 命令用来恢复缺省情况。

【命令】

```
step step-value
undo step
```

【缺省情况】

规则编号的步长为 5，起始值为 0。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图
IPv6 基本 ACL 视图/IPv6 高级 ACL 视图
二层 ACL 视图

【缺省用户角色】

network-admin
context-admin

【参数】

step-value: 表示规则编号的步长值，取值范围为 1~20。

【使用指导】

系统为规则自动分配编号的方式如下：系统从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如原有编号为 0、5、9、10 和 12 的五条规则，步长为 5，此时如果创建一条规则且不指定编号，那么系统将自动为其分配编号 15。

如果步长发生了改变，ACL 内原有全部规则的编号都将自动从规则编号的起始值开始按步长重新排列。譬如，某 ACL 内原有编号为 0、5、9、10 和 15 的五条规则，当修改步长为 2 之后，这些规则的编号将依次变为 0、2、4、6 和 8。

【举例】

将 IPv4 基本 ACL 2000 的规则编号的步长配置为 2。

```
<Sysname> system-view  
[Sysname] acl basic 2000  
[Sysname-acl-ipv4-basic-2000] step 2
```

【相关命令】

- **display acl**

目 录

1 时间段	1-1
1.1 时间段配置命令	1-1
1.1.1 display time-range	1-1
1.1.2 time-range	1-2

1 时间段

1.1 时间段配置命令

1.1.1 display time-range

display time-range 命令用来显示时间段的配置和状态信息。

【命令】

display time-range { *time-range-name* | **all** }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

time-range-name: 显示指定名称时间段的配置和状态信息。*time-range-name* 表示时间段的名称，为 1~32 个字符的字符串，不区分大小写。

all: 显示所有时间段的配置和状态信息。

【举例】

显示时间段 t4 的配置和状态信息。

```
<Sysname> display time-range t4  
Current time is 17:12:34 11/23/2010 Tuesday
```

```
Time-range : t4 (Inactive)  
10:00 to 12:00 Mon  
14:00 to 16:00 Wed  
from 00:00:00 1/1/2011 to 00:00:00 1/1/2012  
from 00:00:00 6/1/2011 to 00:00:00 7/1/2011
```

表1-1 display time-range 命令显示信息描述表

字段	描述
Current time	系统当前的时间
Time-range	时间段的配置信息，包括： - 时间段的名称 - 时间段的状态，包括 Active（生效）和 Inactive（未生效）两种状态 - 时间段的时间范围

1.1.2 time-range

time-range 命令用来创建一个时间段，来描述一个特定的时间范围。如果指定的时间段已经创建，则本命令可以修改时间段的时间范围。

undo time-range 命令用来删除一个时间段。

【命令】

```
time-range time-range-name { start-time to end-time days [ from time1 date1 ]  
[ to time2 date2 ] | from time1 date1 [ to time2 date2 ] | to time2 date2 }
```

```
undo time-range time-range-name [ start-time to end-time days [ from time1  
date1 ] [ to time2 date2 ] | from time1 date1 [ to time2 date2 ] | to time2 date2 ]
```

【缺省情况】

不存在时间段。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

time-range-name: 指定时间段的名称，为 1~32 个字符的字符串，不区分大小写。为避免混淆，时间段的名称不允许使用英文单词 **all**。

start-time to end-time: 指定周期时间段的时间范围。**start-time** 表示起始时间，格式为 hh:mm，取值范围为 00:00~23:59；**end-time** 表示结束时间，格式为 hh:mm，取值范围为 00:00~24:00，且结束时间必须大于起始时间。

days: 指定周期时间段在每周的周几生效。本参数可输入多次，但后输入的值不能与此前输入的值完全重叠（譬如输入 **6** 后不允许再输入 **Sat**，但允许再输入 **off-day**），系统将取各次输入值的并集作为最终值（譬如依次输入 **1**、**Wed** 和 **working-day** 之后，最终生效的时间将为每周的工作日）。

本参数可输入的形式如下：

- 数字：取值范围为 0~6，依次表示周日~周六；
- 周几的英文缩写（从周日到周六依次为 **Sun**、**Mon**、**Tue**、**Wed**、**Thu**、**Fri** 和 **Sat**）；
- 工作日（**working-day**）：表示从周一到周五；
- 休息日（**off-day**）：表示周六和周日；
- 每日（**daily**）：表示一周七天。

from time1 date1: 指定绝对时间段的起始时间。**time1** 的格式为 hh:mm 或 hh:mm:ss，取值范围为 00:00:00~23:59:59。**date1** 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月，取值范围为 1~12；DD 表示日，取值范围取决于所输入的月份；YYYY 表示年，取值范围为 1970~2100。若未指定本参数，绝对时间段的起始时间将为系统可表示的最早时间，即 1970 年 1 月 1 日 0 点 0 分 0 秒。

to time2 date2: 指定绝对时间段的结束时间。*time2* 的格式为 hh:mm 或 hh:mm:ss, 取值范围为 00:00:00~24:00:00。*date2* 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月, 取值范围为 1~12; DD 表示日, 取值范围取决于所输入的月份; YYYY 表示年, 取值范围为 1970~2100。结束时间必须大于起始时间。若未指定本参数, 绝对时间段的结束时间将为系统可表示的最晚时间, 即 2100 年 12 月 31 日 24 点 0 分 0 秒。

【使用指导】

如果指定名称的时间段不存在, 则创建一个新的时间段 (最多 1024 个); 如果指定名称的时间段已存在, 则对旧时间段进行修改, 即在其原有内容的基础上叠加新的内容。

在一个时间段中, 可以使用以下两种方式定义时间范围:

- 使用 *start-time to end-time days* 这组参数所创建的时间段为周期时间段, 它将以一周为周期循环生效。
- 使用 **from time1 date1** 和 **to time2 date2** 这组参数所创建的时间段为绝对时间段, 它将在指定时间范围内生效。

如果一个时间段中同时包含以上两种时间范围, 将取周期时间段和绝对时间段的交集作为生效的时间范围。例如在一个时间段中定义周期时间段为每周一的 8 点到 12 点, 定义绝对时间段为 2015 年全年, 那么该时间段的生效时间范围为 2015 年全年内每周一的 8 点到 12 点。

一个时间段内可包含一或多个周期时间段 (最多 32 个) 和绝对时间段 (最多 12 个), 当包含有多个周期时间段和绝对时间段时, 系统将先分别取各周期时间段的并集和各绝对时间段的并集, 再取这两个并集的交集作为该时间段最终生效的时间范围。

【举例】

创建名为 t1 的时间段, 其时间范围为每周工作日的 8 点到 18 点。

```
<Sysname> system-view
```

```
[Sysname] time-range t1 08:00 to 18:00 working-day
```

创建名为 t2 的时间段, 其时间范围为 2011 年全年。

```
<Sysname> system-view
```

```
[Sysname] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011
```

创建名为 t3 的时间段, 其时间范围为 2011 年全年内每周休息日的 8 点到 12 点。

```
<Sysname> system-view
```

```
[Sysname] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2011 to 24:00 12/31/2011
```

创建名为 t4 的时间段, 其时间范围为 2011 年 1 月和 6 月内每周一的 10 点到 12 点以及每周三的 14 到 16 点。

```
<Sysname> system-view
```

```
[Sysname] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
```

```
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

创建名为 t5 的时间段, 其时间范围为 2018 年 1 月 1 日的 8 点到 18 点。

```
<Sysname> system-view
```

```
[Sysname] time-range t5 from 08:00:00 1/1/2018 to 18:00:00 1/1/2018
```

【相关命令】

- **display time-range**



UNIS 入侵检测系统

可靠性命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《可靠性命令参考》主要介绍 Monitor Link、BFD、Track、冗余备份、进程分布优化和接口组联动相关的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。

格 式	意 义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 Monitor Link	1-1
1.1 Monitor Link配置命令	1-1
1.1.1 display monitor-link group	1-1
1.1.2 downlink up-delay	1-2
1.1.3 monitor-link disable	1-3
1.1.4 monitor-link group	1-3
1.1.5 port	1-4
1.1.6 port monitor-link group	1-5

1 Monitor Link

1.1 Monitor Link配置命令

1.1.1 display monitor-link group

display monitor-link group 命令用来显示 Monitor Link 组的信息。

【命令】

display monitor-link group { *group-id* | all }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

group-id: 显示指定 Monitor Link 组的信息。*group-id* 表示 Monitor Link 组的编号，取值范围 1~16。

all: 显示所有 Monitor Link 组的信息。

【使用指导】

使用本命令不会显示 Monitor Link 组中聚合成员端口的信息。

【举例】

显示所有 Monitor Link 组的信息。

```
<Sysname> display monitor-link group all
```

```
Monitor link protocol status: Disabled
```

```
Monitor link group 1 information:
```

```
Group status      : N/A
Downlink up-delay: 0(s)
Last-up-time      : -
Last-down-time    : -
```

Member	Role	Status
GE1/0/1	UPLINK	UP
GE1/0/2	DOWNLINK	UP

表1-1 display monitor-link group 命令显示信息描述表

字段	描述
Monitor link protocol status	Monitor Link协议的全局使能状态： - Enabled: 表示全局开启 - Disabled: 表示全局关闭
Monitor link group 1 information	Monitor Link组1的信息
Group status	Monitor Link组的状态： - DOWN: 故障 - UP: 正常 - N/A: Monitor Link 协议全局关闭，此时 Monitor Link 组失效
Downlink up-delay	Monitor Link组下行接口的回切延时，单位为秒
Last-up-time	Monitor Link组最近一次up的时间
Last-down-time	Monitor Link组最近一次down的时间
Member	Monitor Link组的成员接口
Role	成员接口的角色： - DOWNLINK: 下行接口 - UPLINK: 上行接口
Status	成员接口的状态： - DOWN: 故障 - DOWN (Monitor Link): Monitor Link 联动而导致接口被关闭 - UP: 正常

1.1.2 downlink up-delay

downlink up-delay 命令用来配置 Monitor Link 组下行接口的回切延时。

undo downlink up-delay 命令用来恢复缺省情况。

【命令】

downlink up-delay delay

undo downlink up-delay

【缺省情况】

Monitor Link 组下行接口的回切延时为 0 秒，即上行接口 up 后，下行接口立刻恢复为 up 状态。

【视图】

Monitor Link 组视图

【缺省用户角色】

network-admin

context-admin

【参数】

delay: 表示延时时间，取值范围为 1~300，单位为秒。

【使用指导】

通过延时回切机制可以避免由于 Monitor Link 组上行链路震荡而导致的下行链路频繁切换。其原理为：当 Monitor Link 组的上行接口恢复为 up 状态并维持了一段时间之后，下行接口才恢复为 up 状态，这段时间就称为 Monitor Link 组下行接口的回切延时。

【举例】

配置 Monitor Link 组 1 下行接口的回切延时为 50 秒。

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] downlink up-delay 50
```

1.1.3 monitor-link disable

monitor-link disable 命令用来全局关闭 Monitor Link 协议。

undo monitor-link disable 命令用来全局开启 Monitor Link 协议。

【命令】

```
monitor-link disable
undo monitor-link disable
```

【缺省情况】

Monitor Link 协议处于全局开启状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

全局开启 Monitor Link 协议时，Monitor Link 组才生效；全局关闭 Monitor Link 协议后，所有 Monitor Link 组失效，之前由 Monitor Link 协议联动触发更改状态为 down 的下行接口将恢复联动触发前的状态。

【举例】

```
# 全局关闭 Monitor Link 协议。
<Sysname> system-view
[Sysname] monitor-link disable
```

1.1.4 monitor-link group

monitor-link group 命令用来创建 Monitor Link 组，并进入 Monitor Link 组视图。如果指定的 Monitor Link 组已经存在，则直接进入 Monitor Link 组视图。

undo monitor-link group 命令用来删除 Monitor Link 组。

【命令】

```
monitor-link group group-id  
undo monitor-link group group-id
```

【缺省情况】

不存在 Monitor Link 组。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

group-id: 表示 Monitor Link 组的编号，取值范围 1~16。

【举例】

```
# 创建 Monitor Link 组 1，并进入 Monitor Link 组 1 的视图。  
<Sysname> system-view  
[Sysname] monitor-link group 1  
[Sysname-mtlk-group1]
```

1.1.5 port

port 命令用来配置 Monitor Link 组的成员接口。

undo port 命令用来取消 Monitor Link 组成员接口的配置。

【命令】

```
port interface-type { interface-number | interface-number.subnumber }  
{ downlink | uplink }  
undo port interface-type interface-number
```

【缺省情况】

Monitor Link 组中不存在成员接口。

【视图】

Monitor Link 组视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

interface-type: 表示接口类型。

interface-number: 表示接口编号。

interface-number.subnumber: 表示子接口的编号。其中, *interface-number* 为主接口编号; *subnumber* 为子接口编号, 取值范围为设备上已经创建的子接口编号。

downlink: 表示下行接口。

uplink: 表示上行接口。

【使用指导】

一个接口只能属于一个 Monitor Link 组。

配置 Monitor Link 组的成员接口也可在接口视图下使用 **port monitor-link group** 命令进行。如果已将一个接口的主接口配置为 Monitor Link 组的下行接口, 请勿再将该接口的子接口配置为任何 Monitor Link 组的上行接口。

由于同一接口的主接口和子接口的 **up/down** 状态本身是联动的, 因此请勿将它们加入同一个 Monitor Link 组中。

如果已将一个聚合组的选中端口配置为 Monitor Link 组的下行接口, 请勿再将该聚合组的非选中端口配置为该 Monitor Link 组的上行接口。

不允许将一个聚合接口及其所对应聚合组的成员端口加入同一个 Monitor Link 组中。

【举例】

配置 Monitor Link 组 1 的上行接口为 GigabitEthernet1/0/1, 下行接口为 GigabitEthernet1/0/2。

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] port gigabitethernet 1/0/1 uplink
[Sysname-mtlk-group1] port gigabitethernet 1/0/2 downlink
```

【相关命令】

- **port monitor-link group**

1.1.6 port monitor-link group

port monitor-link group 命令用来配置接口为 Monitor Link 组的成员接口。

undo port monitor-link group 命令用来取消接口为 Monitor Link 组成员接口的配置。

【命令】

```
port monitor-link group group-id { downlink | uplink }
undo port monitor-link group group-id
```

【缺省情况】

接口不是 Monitor Link 组的成员接口。

【视图】

二层以太网接口视图/三层以太网接口视图/三层以太网子接口视图

二层聚合接口视图/三层聚合接口视图/三层聚合子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

group-id: 表示 Monitor Link 组的编号，取值范围 1~16。

downlink: 表示下行接口。

uplink: 表示上行接口。

【使用指导】

一个接口只能属于一个 Monitor Link 组。

配置 Monitor Link 组的成员接口也可在 Monitor Link 组视图下使用 **port** 命令进行。

如果已将一个接口的主接口配置为 Monitor Link 组的下行接口，请勿再将该接口的子接口配置为任何 Monitor Link 组的上行接口。

由于同一接口的主接口和子接口的 up/down 状态本身是联动的，因此请勿将它们加入同一个 Monitor Link 组中。

如果已将一个聚合组的选中端口配置为 Monitor Link 组的下行接口，请勿再将该聚合组的非选中端口配置为该 Monitor Link 组的上行接口。

不允许将一个聚合接口及其所对应聚合组的成员端口加入同一个 Monitor Link 组中。

【举例】

将 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别配置为 Monitor Link 组 1 的上行接口和下行接口。

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port monitor-link group 1 uplink
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port monitor-link group 1 downlink
```

【相关命令】

- **Port**

目 录

1 BFD	1-1
1.1 BFD配置命令	1-1
1.1.1 bfd authentication-mode	1-1
1.1.2 bfd demand enable	1-2
1.1.3 bfd detect-interface first-fail-timer	1-3
1.1.4 bfd detect-interface source-ip	1-4
1.1.5 bfd detect-interface special-processing	1-5
1.1.6 bfd detect-multiplier	1-6
1.1.7 bfd echo enable	1-7
1.1.8 bfd echo-source-ip	1-8
1.1.9 bfd echo-source-ipv6	1-9
1.1.10 bfd init-fail timer	1-9
1.1.11 bfd min-echo-receive-interval	1-10
1.1.12 bfd min-receive-interval	1-11
1.1.13 bfd min-transmit-interval	1-12
1.1.14 bfd multi-hop authentication-mode	1-13
1.1.15 bfd multi-hop destination-port	1-14
1.1.16 bfd multi-hop detect-multiplier	1-14
1.1.17 bfd multi-hop min-receive-interval	1-15
1.1.18 bfd multi-hop min-transmit-interval	1-16
1.1.19 bfd session init-mode	1-16
1.1.20 bfd static	1-17
1.1.21 bfd template	1-19
1.1.22 display bfd session	1-20
1.1.23 first-fail-timer	1-26
1.1.24 process-interface-status	1-27
1.1.25 reset bfd session statistics	1-28
1.1.26 snmp-agent trap enable bfd	1-29
1.1.27 special-processing	1-29

1 BFD

1.1 BFD配置命令

1.1.1 bfd authentication-mode

bfd authentication-mode 命令用来配置单跳 BFD 控制报文进行认证的方式。

undo bfd authentication-mode 命令用来恢复缺省情况。

【命令】

```
bfd authentication-mode { hmac-md5 | hmac-mmd5 | hmac-msha1 | hmac-sha1 |  
m-md5 | m-sha1 | md5 | sha1 | simple } key-id { cipher | plain } string  
undo bfd authentication-mode
```

【缺省情况】

单跳 BFD 控制报文不进行认证。

【视图】

接口视图

BFD 模板视图

静态 BFD 会话视图

【缺省用户角色】

network-admin

context-admin

【参数】

hmac-md5: 采用基于 HMAC 的 MD5 算法进行认证。

hmac-mmd5: 采用基于 HMAC 的 Meticulous MD5 算法进行认证。

hmac-msha1: 采用基于 HMAC 的 Meticulous SHA1 算法进行认证。

hmac-sha1: 采用基于 HMAC 的 SHA1 算法进行认证。

m-md5: 采用 Meticulous MD5 算法进行认证。

m-sha1: 采用 Meticulous SHA1 算法进行认证。

md5: 采用 MD5 算法进行认证。

sha1: 采用 SHA1 算法进行认证。

simple: 采用简单认证。

key-id: 认证字标识符，取值范围为 1~255。

cipher: 以密文方式设置密钥。

plain: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~16 个字符的字符串，密文密钥为 33~53 个字符的字符串。

【使用指导】

本命令主要为了提高 BFD 会话的安全性。

在静态 BFD 会话视图下配置本命令，仅对单跳静态 BFD 会话生效。

BFD 版本 0 不支持本命令，配置不生效。

【举例】

配置接口 GigabitEthernet1/0/1 对单跳 BFD 控制报文进行简单明文认证，认证字标识符为 1，密钥为 123456。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] bfd authentication-mode simple 1 plain 123456
```

【相关命令】

- **bfd static**

1.1.2 bfd demand enable

bfd demand enable 命令用来配置 BFD 会话为查询模式。

undo bfd demand enable 命令用来恢复缺省情况。

【命令】

bfd demand enable

undo bfd demand enable

【缺省情况】

BFD 会话为异步模式。

【视图】

接口视图

静态 BFD 会话视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

在查询模式下，设备周期性发送 BFD 控制报文，但是对端（缺省为异步模式）会停止周期性发送 BFD 控制报文。如果通信双方都是查询模式，则双方都停止周期性发送 BFD 控制报文。此模式下，建议用户通过 **bfd echo enable** 命令使能回声功能，设备将周期性发送 echo 报文来检测链路的连通性，如果在检测时间内未收到对端返回的 echo 报文，则认为会话 down。

在异步模式下，设备周期性地发送 BFD 控制报文，如果在检测时间内对端没有收到 BFD 控制报文，则认为会话 down。

在静态 BFD 会话视图下配置本命令，仅对单跳静态 BFD 会话生效。

BFD 版本 0 不支持本命令，配置不生效。

【举例】

```
# 在接口 GigabitEthernet1/0/1 上配置 BFD 会话为查询模式。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd demand enable
```

1.1.3 bfd detect-interface first-fail-timer

bfd detect-interface first-fail-timer 命令用来配置首次建立检测接口状态的 BFD 会话失败时，通知数据链路层 BFD 会话 down 的超时时间。

undo bfd detect-interface first-fail-timer 命令用来恢复缺省情况。

【命令】

```
bfd detect-interface first-fail-timer seconds
undo bfd detect-interface first-fail-timer
```

【缺省情况】

首次建立检测接口状态的 BFD 会话失败时，不会通知数据链路层 BFD 会话 down。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

seconds：首次建立检测接口状态的 BFD 会话失败时，通知数据链路层 BFD 会话 down 的超时时间，即在 **seconds** 时间后如果检测接口状态的 BFD 会话仍未建立成功，BFD 会将此消息通知给数据链路层。取值范围为 1~10000，单位为秒。

【使用指导】

本端配置 **bfd detect-interface source-ip** 命令后，会尝试建立检测接口状态的 BFD 会话。如果对端未配置 **bfd detect-interface source-ip** 命令或两端 BFD 的认证配置不一致等原因，均会导致首次建立检测接口状态的 BFD 会话失败。如果需要关闭接口的数据链路层，快速定位首次建立检测接口状态的 BFD 会话失败的接口，可通过配置本命令来实现。

配置本命令后，如果接口首次建立检测接口状态的 BFD 会话失败，执行 **display bfd session** 命令显示该 BFD 会话的状态为 down，执行 **display interface** 命令会显示该接口的 Line protocol state 为 DOWN(BFD)。

【举例】

```
# 配置首次建立检测接口状态的 BFD 会话失败时，通知数据链路层 BFD 会话 down 的超时时间为 10 秒。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd detect-interface first-fail-timer 10
```

【相关命令】

- **bfd detect-interface source-ip**
- **display interface**（接口管理/以太网接口）

1.1.4 bfd detect-interface source-ip

bfd detect-interface source-ip 命令用来配置接口状态与 BFD 联动。

undo bfd detect-interface 命令用来取消接口状态与 BFD 联动的配置。

【命令】

bfd detect-interface source-ip ip-address [template template-name]
undo bfd detect-interface

【缺省情况】

接口状态不与 BFD 联动,即 BFD 检测到链路故障时,不会将接口链路层协议状态置为“DOWN(BFD)”。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: BFD 控制报文的源 IP 地址。

template template-name: 指定引用的 BFD 会话参数的模板名称,为 1~63 个字符的字符串,区分大小写。如果未指定本参数,则 BFD 会话使用接口视图下配置的单跳 BFD 会话参数。引用的 BFD 会话参数模板可以不存在,但要使引用 BFD 会话参数模板的配置生效,必须创建 BFD 模板。

【使用指导】

配置接口状态与 BFD 联动后,系统将通过发送 BFD 控制报文来协商建立单跳检测的 BFD 会话,实现对链路的快速检测。当检测到链路故障时,将接口链路层协议状态置为“DOWN(BFD)”,从而帮助依赖接口链路层协议状态的应用快速收敛。

系统发送的 BFD 控制报文中的源地址为用户手工指定的 IP 地址,目的地址固定为 224.0.0.184。对于有 IP 地址的接口,建议将源地址指定为该接口的 IP 地址;如果接口没有 IP 地址,建议将源地址指定为 0.0.0.0 以外的单播地址。

支持与 BFD 联动的接口类型为:

- 三层以太网接口及其子接口。请不要在三层以太网接口和该三层以太网接口创建的子接口上同时使用该功能,否则,将导致主接口或子接口的 BFD 检测功能失效。
- 三层聚合接口、三层聚合接口的子接口以及三层聚合口的成员端口,其中三层聚合口的成员端口全部为三层以太网接口。请不要在三层聚合接口、该三层聚合接口的子接口以及该三层聚合口的成员端口上同时使用此功能,否则可能导致 BFD 检测功能失效。
- VLAN 接口

不能通过重复执行本命令修改关联接口状态的 BFD 会话。如需修改关联接口状态的 BFD 会话，请先通过 **undo bfd detect-interface source-ip** 命令删除关联接口状态的 BFD 会话，再执行 **bfd detect-interface source-ip** 命令。

回声功能对接口状态与 BFD 联动的会话无效。

引用已经存在的 BFD 会话参数模板后，**bfd demand enable** 命令无法生效。

【举例】

```
# 配置检测 GigabitEthernet1/0/1 接口状态的 BFD 会话，其源地址为接口地址 20.1.1.1。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd detect-interface source-ip 20.1.1.1
```

【相关命令】

- **bfd demand enable**
- **bfd echo enable**
- **bfd template**

1.1.5 bfd detect-interface special-processing

bfd detect-interface special-processing 命令用来开启对检测接口状态的 BFD 会话进行特殊处理的功能。

undo bfd detect-interface special-processing 命令用来关闭对检测接口状态的 BFD 会话进行特殊处理的功能。

【命令】

```
bfd    detect-interface    special-processing    [    admin-down    |
authentication-change | session-up ] *
undo   bfd    detect-interface    special-processing    [    admin-down    |
authentication-change | session-up ] *
```

【缺省情况】

对检测接口状态的 BFD 会话进行特殊处理的功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

admin-down: 本端收到会话状态为 AdminDown 的 BFD 报文时，将 BFD 会话 down 的消息通知给数据链路层。使用本参数，有利于快速发现 BFD 会话被手工关闭的接口。如果未配置本参数，本端收到会话状态为 AdminDown 的 BFD 报文，将 BFD 会话状态置为 down，但是不会将 BFD 会话 down 的消息通知给数据链路层。

authentication-change: 本端认证信息发生变化时，立即将 BFD 会话状态置为 down。使用本参数，有利于快速发现认证信息不一致的接口。如果未配置本参数，本端认证信息发生变化时，会预留时间给用户修改本端或对端的认证参数，如果预留时间结束时，两端认证信息任未达成一致，本端会将 BFD 会话状态置为 down。

session-up: 本端 BFD 会话处于 up 状态时，不再检查收到的 BFD 报文中的认证信息。当设备上的 BFD 会话数量较多时，检查 BFD 报文中携带的认证信息会影响设备性能。配置本参数后，不再检查收到的报文中的认证信息，从而可以降低对设备性能的影响。如果未配置本参数，本端 BFD 会话处于状态 up 时，会检查收到的 BFD 报文中的认证信息，需要保证 BFD 会话两端认证信息的一致性，否则会导致 BFD 会话 down。

【使用指导】

如果未指定任何参数，将开启或关闭对检测接口状态的 BFD 会话进行所有特殊处理的功能。

【举例】

在 GigabitEthernet1/0/1 接口下开启对检测接口状态的 BFD 会话进行特殊处理的功能，包括收到会话状态为 AdminDown 的 BFD 报文、本端认证信息发生变化以及 BFD 会话处于 up 状态时对收到的 BFD 报文中认证信息检查的特殊处理。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd detect-interface special-processing admin-down
authentication-change session-up
```

1.1.1.6 bfd detect-multiplier

bfd detect-multiplier 命令用来配置控制报文方式单跳检测和 Echo 报文方式的 BFD 检测时间倍数。

undo bfd detect-multiplier 命令用来恢复缺省情况。

【命令】

```
bfd detect-multiplier value
undo bfd detect-multiplier
```

【缺省情况】

控制报文方式单跳检测和 Echo 报文方式的 BFD 检测时间倍数为 5。

【视图】

接口视图
BFD 模板视图
静态 BFD 会话视图

【缺省用户角色】

network-admin
context-admin

【参数】

value: BFD 检测时间倍数，取值范围为 3~50。

【使用指导】

检测时间倍数，即允许发送方发送 BFD 报文（包括 echo 报文和控制报文）的最大连续丢包数。
实际检测时间的计算方法遵循如下规则：

- 对于 echo 报文方式，实际检测时间为发送方的检测时间倍数和发送方的实际发送时间的乘积。
- 对于控制报文方式单跳检测的异步模式，实际检测时间为接收方的检测时间倍数和接收方的实际发送时间的乘积。
- 对于控制报文方式单跳检测的查询模式，实际检测时间为发送方的检测时间倍数和发送方的实际发送时间的乘积。

在静态 BFD 会话视图下配置本命令，仅对单跳静态 BFD 会话生效。

【举例】

配置接口 GigabitEthernet1/0/1 的控制报文方式单跳检测和 Echo 报文方式的 BFD 检测时间倍数为 6。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd detect-multiplier 6
```

1.1.7 bfd echo enable

bfd echo enable 命令用来使能回声功能。

undo bfd echo enable 命令用来关闭回声功能。

【命令】

```
bfd echo [ receive | send ] enable
undo bfd echo [ receive | send ] enable
```

【缺省情况】

回声功能处于关闭状态。

【视图】

接口视图

静态 BFD 会话视图

【缺省用户角色】

network-admin

context-admin

【参数】

receive: 表示设备接收 echo 报文的能力。

send: 表示设备发送 echo 报文的能力。

【使用指导】

本功能在发送控制报文的 BFD 会话时使用。使能回声功能并且会话 up 后，设备周期性发送 echo 报文检测链路连通性，同时降低控制报文的接收速率。

使用 **bfd echo receive enable** 命令，表示使能回声功能后，只开启设备接收 echo 报文的能力；使用 **bfd echo send enable** 命令，表示使能回声功能后，只开启设备发送 echo 报文的能力。当不指定 **receive** 和 **send** 参数时，表示使能回声功能后，同时开启设备收、发 echo 报文的能力。

回声功能对接口状态与 BFD 联动的会话无效。

在静态 BFD 会话视图下配置本命令，仅对单跳静态 BFD 会话生效。

BFD 版本 0 不支持本命令，配置不生效。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 使能回声功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd echo enable
```

【相关命令】

- **bfd static**

1.1.8 bfd echo-source-ip

bfd echo-source-ip 命令用来配置 echo 报文的源 IP 地址。

undo bfd echo-source-ip 命令用来删除 echo 报文的源 IP 地址。

【命令】

```
bfd echo-source-ip ip-address
undo bfd echo-source-ip
```

【缺省情况】

未配置 echo 报文的源 IP 地址。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ip-address：echo 报文的源 IP 地址。

【使用指导】

echo 报文的源 IP 地址用户可以任意指定。为了避免对端发送大量的 ICMP 重定向报文造成网络拥塞，建议配置 echo 报文的源 IP 地址不属于该设备任何一个接口所在网段。

【举例】

```
# 配置 echo 报文的源 IP 地址为 8.8.8.8。
<Sysname> system-view
[Sysname] bfd echo-source-ip 8.8.8.8
```

1.1.9 bfd echo-source-ipv6

bfd echo-source-ipv6 命令用来配置 echo 报文的源 IPv6 地址。

undo bfd echo-source-ipv6 命令用来删除 echo 报文的源 IPv6 地址。

【命令】

bfd echo-source-ipv6 *ipv6-address*

undo bfd echo-source-ipv6

【缺省情况】

未配置 echo 报文的源 IPv6 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address: echo 报文的源 IPv6 地址。

【使用指导】

echo 报文源 IPv6 地址仅支持全球单播地址。

为了避免对端发送大量的 ICMPv6 重定向报文造成网络拥塞，建议不要将 echo 报文的源 IPv6 地址配置为属于该设备任何一个接口所在网段。

【举例】

配置 echo 报文的源 IPv6 地址为 80::2。

```
<Sysname> system-view
```

```
[Sysname] bfd echo-source-ipv6 80::2
```

1.1.10 bfd init-fail timer

bfd init-fail-timer 命令用来配置 BFD 会话无法建立时，通知上层协议 BFD 会话 down 的超时时间。

undo bfd init-fail-timer 命令用来恢复缺省情况。

【命令】

bfd init-fail-timer *seconds*

undo bfd init-fail-timer

【缺省情况】

BFD 会话无法建立时，不会通知上层协议 BFD 会话 down。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

seconds: BFD 会话无法建立时，通知上层协议 BFD 会话 down 的超时时间，即在 **seconds** 时间后将 BFD 会话 down 的消息通知给上层协议。取值范围为 5～600，单位为秒。

【使用指导】

缺省情况下，控制报文工作方式的 BFD 会话无法建立时，不会通知上层协议 BFD 会话 down。某些情况下，需要将 BFD 会话无法建立的消息通知给上层协议，以使上层协议作出正确的处理。比如在聚合链路中，由于链路故障等原因，BFD 会话无法进入 up 状态，从而导致聚合模块无法及时将成员端口的选中状态修改为非选中状态，配置本命令可避免上述情况的发生。

配置本命令后，对于由于配置原因（比如对端设备没有使能 BFD，或者两端的 BFD 认证配置不一致等）造成 BFD 会话无法进入 up 状态的情况，如果配置了本定时器，会导致上层协议作出错误的处理，所以，请谨慎使用本命令。

对于 Echo 报文方式的 BFD 会话，本命令不生效。

【举例】

```
# 配置 BFD 会话无法建立时，通知上层协议 BFD 会话 down 的超时时间为 10 秒。  
<Sysname> system-view  
[Sysname] bfd init-fail-timer 10
```

1.1.11 bfd min-echo-receive-interval

bfd min-echo-receive-interval 命令用来配置接收 echo 报文的最小时间间隔。

undo bfd min-echo-receive-interval 命令用来恢复缺省情况。

【命令】

```
bfd min-echo-receive-interval interval  
undo bfd min-echo-receive-interval
```

【缺省情况】

接收 echo 报文的最小时间间隔为 400 毫秒。

【视图】

接口视图
BFD 模板视图
静态 BFD 会话视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval: 接收 echo 报文的最小时间间隔，单位为毫秒。取值范围为 0，100～1000。

【使用指导】

使用本命令，设备能够控制接收两个 **echo** 报文之间的时间间隔，即 **echo** 报文实际发送时间间隔。对于控制报文方式的 BFD 会话，本端使能回声功能后，如果对端通过本命令将 *interval* 设置为 0 毫秒，那么本端设备与对端设备自动协商后，本端设备不再周期性发送 **echo** 报文。

在静态 BFD 会话视图下配置本命令，仅对单跳静态 BFD 会话生效。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 接收 echo 报文的最小时间间隔为 500 毫秒。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd min-echo-receive-interval 500
```

【相关命令】

- **bfd static**

1.1.12 bfd min-receive-interval

bfd min-receive-interval 命令用来配置接收单跳 BFD 控制报文的最小时间间隔。

undo bfd min-receive-interval 命令用来恢复缺省情况。

【命令】

```
bfd min-receive-interval interval
undo bfd min-receive-interval
```

【缺省情况】

接收单跳 BFD 控制报文的最小时间间隔为 400 毫秒。

【视图】

接口视图
BFD 模板视图
静态 BFD 会话视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval：接收单跳 BFD 控制报文的最小时间间隔，单位为毫秒。取值范围为 100~1000。

【使用指导】

本命令主要为了防止对端发送控制报文的速度超过本地接收控制报文的速度。

对端的控制报文实际发送时间为对端发送控制报文的最小时间间隔和本地接收控制报文的最小时间间隔之间的较大值。

在静态 BFD 会话视图下配置本命令，仅对单跳静态 BFD 会话生效。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 接收单跳 BFD 控制报文的最小时间间隔为 500 毫秒。
```

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd min-receive-interval 500
```

【相关命令】

- **bfd static**

1.1.13 bfd min-transmit-interval

bfd min-transmit-interval 命令用来配置发送单跳 BFD 控制报文的最小时间间隔。

undo bfd min-transmit-interval 命令用来恢复缺省情况。

【命令】

```
bfd min-transmit-interval interval
undo bfd min-transmit-interval
```

【缺省情况】

发送单跳 BFD 控制报文的最小时间间隔为 400 毫秒。

【视图】

接口视图
BFD 模板视图
静态 BFD 会话视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval：发送单跳 BFD 控制报文的最小时间间隔，单位为毫秒。取值范围为 100～1000。

【使用指导】

本命令主要是为了保证发送 BFD 控制报文的速度不能超过设备发送报文的能力。

本地实际发送 BFD 控制报文的时间间隔，为本地配置的发送 BFD 控制报文的最小时间间隔和对端接收 BFD 控制报文的最小时间间隔的最大值。

在静态 BFD 会话视图下配置本命令，仅对单跳静态 BFD 会话生效。

【举例】

配置接口 GigabitEthernet1/0/1 发送单跳 BFD 控制报文的最小时间间隔为 500 毫秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bfd min-transmit-interval 500
```

【相关命令】

- **bfd static**

1.1.14 bfd multi-hop authentication-mode

bfd multi-hop authentication-mode 命令用来配置多跳 BFD 控制报文进行认证的方式。

undo bfd multi-hop authentication-mode 命令用来恢复缺省情况。

【命令】

```
bfd multi-hop authentication-mode { hmac-md5 | hmac-mmd5 | hmac-msha1 |  
hmac-sha1 | m-md5 | m-sha1 | md5 | sha1 | simple } key-id { cipher | plain }  
string  
undo bfd multi-hop authentication-mode
```

【缺省情况】

多跳 BFD 控制报文不进行认证。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

hmac-md5: 采用基于 HMAC 的 MD5 算法进行认证。

hmac-mmd5: 采用基于 HMAC 的 Meticulous MD5 算法进行认证。

hmac-msha1: 采用基于 HMAC 的 Meticulous SHA1 算法进行认证。

hmac-sha1: 采用基于 HMAC 的 SHA1 算法进行认证。

m-md5: 采用 Meticulous MD5 算法进行认证。

m-sha1: 采用 Meticulous SHA1 算法进行认证。

md5: 采用 MD5 算法进行认证。

sha1: 采用 SHA1 算法进行认证。

simple: 采用简单认证。

key-id: 认证字标识符，取值范围为 1~255。

cipher: 以密文方式设置密钥。

plain: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~16 个字符的字符串，密文密钥为 33~53 个字符的字符串。

【使用指导】

本命令主要为了提高 BFD 会话的安全性。

BFD 版本 0 不支持本命令，配置不生效。

【举例】

配置多跳 BFD 控制报文进行简单明文认证，认证字标识符为 1，密钥为 123456。

```
<Sysname> system-view
```

```
[Sysname] bfd multi-hop authentication-mode simple 1 plain 123456
```


1.1.15 bfd multi-hop destination-port

bfd multi-hop destination-port 命令用来配置多跳 BFD 控制报文的目的端口号。

undo bfd multi-hop destination-port 命令用来恢复缺省情况。

【命令】

bfd multi-hop destination-port *port-number*

undo bfd multi-hop destination-port

【缺省情况】

多跳 BFD 控制报文的目的端口号为 4784。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

port-number: 多跳 BFD 控制报文的目的端口号，取值可以为 3784 或者 4784。

【举例】

配置多跳 BFD 控制报文的目的端口号为 3784。

<Sysname> system-view

[Sysname] bfd multi-hop destination-port 3784

1.1.16 bfd multi-hop detect-multiplier

bfd multi-hop detect-multiplier 命令用来配置控制报文方式多跳检测的 BFD 检测时间倍数。

undo bfd multi-hop detect-multiplier 命令用来恢复缺省情况。

【命令】

bfd multi-hop detect-multiplier *value*

undo bfd multi-hop detect-multiplier

【缺省情况】

控制报文方式多跳检测的 BFD 检测时间倍数为 5。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

value: BFD 检测时间倍数，取值范围为 3~50。

【使用指导】

检测时间倍数，即接收方允许发送方发送 BFD 控制报文的最大连续丢包数。

实际检测时间的计算方法遵循如下规则：

- 对于控制报文方式的多跳检测异步模式，实际检测时间为接收方的检测时间倍数和接收方的实际发送时间的乘积。

对于控制报文方式的多跳检测查询模式，实际检测时间为发送方的检测时间倍数和发送方的实际发送时间的乘积。

【举例】

配置多跳 BFD 检测时间倍数为 6。

```
<Sysname> system-view
```

```
[Sysname] bfd multi-hop detect-multiplier 6
```

1.1.17 bfd multi-hop min-receive-interval

bfd multi-hop min-receive-interval 命令用来配置接收多跳 BFD 控制报文的最小时间间隔。

undo bfd multi-hop min-receive-interval 命令用来恢复缺省情况。

【命令】

bfd multi-hop min-receive-interval interval

undo bfd multi-hop min-receive-interval

【缺省情况】

接收多跳 BFD 控制报文的最小时间间隔为 400 毫秒。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval：接收 BFD 控制报文的最小时间间隔，单位为毫秒。取值范围为 100～1000。

【使用指导】

本命令主要为了防止对端设备发送报文的速度超出本地接收报文的能力（接收 BFD 控制报文的最小时间间隔），若超出，则对端设备将发送 BFD 控制报文的时间间隔动态调整为本地接收 BFD 控制报文的最小时间间隔。

【举例】

配置接收多跳 BFD 控制报文的最小时间间隔为 500 毫秒。

```
<Sysname> system-view
```

```
[Sysname] bfd multi-hop min-receive-interval 500
```

1.1.18 bfd multi-hop min-transmit-interval

bfd multi-hop min-transmit-interval 命令用来配置发送多跳 BFD 控制报文的最小时间间隔。

undo bfd multi-hop min-transmit-interval 命令用来恢复缺省情况。

【命令】

bfd multi-hop min-transmit-interval interval

undo bfd multi-hop min-transmit-interval

【缺省情况】

发送多跳 BFD 控制报文的最小时间间隔为 400 毫秒。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval: 发送 BFD 控制报文的最小时间间隔，单位为毫秒。取值范围为 100~1000。

【使用指导】

本命令主要是为了保证发送 BFD 控制报文的速度不能超过设备发送报文的能力。

本地实际发送 BFD 控制报文的时间间隔，为本地配置的发送 BFD 控制报文的最小时间间隔和对端接收 BFD 控制报文的最小时间间隔的最大值。

【举例】

配置发送多跳 BFD 控制报文的最小时间间隔为 500 毫秒。

```
<Sysname> system-view
```

```
[Sysname] bfd multi-hop min-transmit-interval 500
```

1.1.19 bfd session init-mode

bfd session init-mode 命令用来配置 BFD 会话建立前的运行模式。

undo bfd session init-mode 命令用来恢复缺省情况。

【命令】

bfd session init-mode { active | passive }

undo bfd session init-mode

【缺省情况】

BFD 会话建立前的运行模式为主动模式。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

active: 主动模式。在建立会话前不管是否收到对端发来的 BFD 控制报文，都会主动向会话的对端发送 BFD 控制报文。

passive: 被动模式。在建立会话前不会主动向会话的对端发送 BFD 控制报文，只有等收到 BFD 控制报文后才会向对端发送 BFD 控制报文。

【使用指导】

通信双方至少要有一方运行在主动模式才能成功建立起 BFD 会话。

BFD 版本 0 不支持本命令，配置不生效。

【举例】

配置 BFD 会话建立前的运行模式为被动模式。

```
<Sysname> system-view  
[Sysname] bfd session init-mode passive
```

1.1.20 bfd static

bfd static 命令用来创建静态 BFD 会话，并进入静态 BFD 会话视图。如果指定的 BFD 会话已经存在，则直接进入静态 BFD 会话视图。

undo bfd static 命令用来删除静态 BFD 会话及静态 BFD 会话视图下的所有配置。

【命令】

```
bfd static session-name [ peer-ip ipv4-address [ vpn-instance  
vpn-instance-name | interface interface-type interface-number ] source-ip  
ipv4-address discriminator local local-value remote remote-value ]  
bfd static session-name [ peer-ipv6 ipv6-address [ vpn-instance  
vpn-instance-name | interface interface-type interface-number ] source-ipv6  
ipv6-address discriminator local local-value remote remote-value ]  
bfd static session-name [ peer-ip default-ip interface interface-type  
interface-number source-ip ip-address discriminator local discr-value  
remote discr-value ]  
undo bfd static session-name
```

【缺省情况】

不存在静态 BFD 会话。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

session-name: 静态 BFD 会话的名称，为 1~15 个字符的字符串，区分大小写。

peer-ip ipv4-address: 静态 BFD 会话的对端 IPv4 地址，点分十进制形式，取值范围为合法的单播 IPv4 地址。

peer-ipv6 ipv6-address: 静态 BFD 会话的对端 IPv6 地址。

default-ip: 静态 BFD 会话的对端地址固定为组播地址 224.0.0.184。

vpn-instance vpn-instance-name: 指定静态 BFD 会话所属的 VPN 实例，**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，表示静态 BFD 会话属于公网实例。

interface interface-type interface-number: 指定 BFD 会话所在的本地接口。**interface-type interface-number** 表示接口类型和接口编号。指定本参数后，将对以该接口为出接口、以 **peer-ip/peer-ipv6** 为下一跳的链路进行单跳检测。

source-ip ipv4-address: BFD 控制报文的源 IPv4 地址，点分十进制形式，取值范围为合法的单播 IPv4 地址。

source-ipv6 ipv6-address: BFD 控制报文的源 IPv6 地址。

discriminator: 指定 BFD 会话的标识符。

local local-value: 指定 BFD 会话的本地标识符。**local-value** 表示 BFD 会话的本地标识符，取值范围为 1~32768。

remote remote-value: 指定 BFD 会话的远端标识符。**remote-value** 表示 BFD 会话的远端标识符，取值范围为 1~4294967295。

【使用指导】

创建的静态 BFD 会话可以用来进行控制报文方式的 BFD 单跳检测和多跳检测，通过与 Track 配合可为对链路故障响应速度要求较高的业务提供故障检测服务。关于 Track 与 BFD 联动的详细信息，请参见“可靠性配置指导”中的“Track”。

如果对端静态创建 BFD 会话，那么本端必须通过本命令创建静态 BFD 会话，且两端的静态 BFD 会话的配置项必须匹配，例如，本端配置 **bfd static abc peer-ip 20.1.1.1 vpn-instance vpn1 source-ip 20.1.1.2 discriminator local 513 remote 514**，对端要配置 **bfd static bcd peer-ip 20.1.1.2 vpn-instance vpn1 source-ip 20.1.1.1 discriminator local 514 remote 513**。

首次创建静态 BFD 会话时，必须指定静态 BFD 会话的对端 IPv4 或 IPv6 地址。通过 **bfd static session-name** 命令只能进入已经存在的静态 BFD 会话视图。

系统仅检查 IP 地址的形式，不检查其正确性。指定错误的对端 IP 地址或源 IP 地址均会导致静态 BFD 会话无法建立。

不能通过重复执行本命令修改静态 BFD 会话。如需修改静态 BFD 会话，请先通过 **undo bfd static** 命令删除静态 BFD 会话，再执行 **bfd static** 命令。

如果未指定 **vpn-instance** 和 **interface** 参数，将在公网实例下进行多跳检测。

检测设备间网络层的连通性时，请配置如下命令。这种情况下，需要保证 **peer-ip** 为对端静态 BFD 会话所在的接口的 IP 地址，**source-ip** 为本端静态 BFD 会话所在的接口的 IP 地址，否则无法建立静态 BFD 会话。

- **bfd static session-name peer-ip** *ipv4-address* **interface** *interface-type interface-number* **source-ip** *ipv4-address* **discriminator local** *local-value* **remote** *remote-value*
- **bfd static session-name peer-ipv6** *ipv6-address* **interface** *interface-type interface-number* **source-ipv6** *ipv6-address* **discriminator local** *local-value* **remote** *remote-value*

检测设备间数据链路层的连通性时，请配置 **bfd static session-name peer-ip default-ip interface interface-type interface-number source-ip ip-address discriminator local discr-value remote discr-value** 命令。如果同时配置了 **process-interface-status** 命令，当 BFD 检测到链路故障时，将 **interface** 参数对应的接口的数据链路层协议置为“DOWN(BFD)”。对于配置了 IP 地址的接口，建议将 **source-ip** 指定为该接口的 IP 地址；如果接口未配置或无法配置 IP 地址，建议将 **source-ip** 指定为 0.0.0.0 以外的单播地址。一个接口上只能采用一个静态 BFD 会话进行链路层故障检测。

支持对如下同种类型的接口之间建立的数据链路进行故障快速检测：

- 三层以太网接口、三层以太网子接口。请不要在三层以太网接口和该三层以太网接口创建的子接口上同时使用该功能，否则，将导致主接口或子接口的 BFD 检测功能失效。
- 加入聚合组的三层以太网接口
- 三层聚合接口、三层聚合接口的子接口以及三层聚合口的成员端口。请不要在三层聚合接口、该三层聚合接口的子接口以及该三层聚合口的成员端口上同时使用 BFD 故障检测功能，否则可能导致 BFD 检测功能失效。
- VLAN 接口

不同的静态 BFD 会话的本地标识符不能相同。

【举例】

创建名称为 abc 的静态 BFD 会话，并进入静态 BFD 会话视图。对出接口为 GigabitEthernet1/0/1、下一跳为 1.1.1.2 的链路进行检测。其中，BFD 会话的源 IP 地址为 1.1.1.1，本地标识符为 1537，远端标识符为 2048。

```
<Sysname> system-view
[Sysname] bfd static abc peer-ip 1.1.1.2 interface gigabitethernet 1/0/1 source-ip 1.1.1.1
discriminator local 1537 remote 2048
[Sysname-bfd-static-session-abc]
```

【相关命令】

- **process-interface-status**

1.1.21 bfd template

bfd template 命令用来创建 BFD 模板，并进入 BFD 模板视图。如果指定的 BFD 模板已经存在，则直接进入 BFD 模板视图。

undo bfd template 命令用来删除 BFD 模板。

【命令】

```
bfd template template-name
undo bfd template template-name
```

【缺省情况】

不存在 BFD 模板。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

template-name: BFD 模板名称，为 1~63 个字符的字符串，区分大小写。

【举例】

创建 BFD 模板 bfd1，并进入 BFD 模板视图。

```
<Sysname> system-view
[Sysname] bfd template bfd1
[Sysname-bfd-template-bfd1]
```

1.1.22 display bfd session

display bfd session 命令用来显示 BFD 会话信息。

【命令】

```
display bfd session [ discriminator local local-value | static session-name
| verbose ]
display bfd session [ [ dynamic ] [ control | echo ] [ ip ] [ state { down |
admin-down | init | up } ] [ discriminator remote remote-value ] [ peer-ip
ipv4-address [ vpn-instance vpn-instance-name ] ] [ verbose ] ]
display bfd session [ [ dynamic ] [ control | echo ] [ ipv6 ] [ state { down
| admin-down | init | up } ] [ discriminator remote remote-value ] [ peer-ipv6
ipv6-address [ vpn-instance vpn-instance-name ] ] [ verbose ] ]
display bfd session [ [ dynamic ] [ control | echo ] [ state { down | admin-down
| init | up } ] [ discriminator remote remote-value ] [ [ peer-ip ipv4-address
[ vpn-instance vpn-instance-name ] ] | [ peer-ipv6 ipv6-address
[ vpn-instance vpn-instance-name ] ] ] [ verbose ] ]
display bfd session [ [ static ] [ ip ] [ state { down | admin-down | init |
up } ] [ discriminator remote remote-value ] [ peer-ip ipv4-address
[ vpn-instance vpn-instance-name ] ] [ verbose ] ]
display bfd session [ [ static ] [ ipv6 ] [ state { down | admin-down | init |
up } ] [ discriminator remote remote-value ] [ peer-ipv6 ipv6-address
[ vpn-instance vpn-instance-name ] ] [ verbose ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

discriminator local local-value: 显示指定本地标识符的 BFD 会话信息。*value* 为本地标识符的值，取值范围为 1~4294967295。

dynamic: 显示动态 BFD 会话的信息。

static: 显示静态 BFD 会话的信息。

session-name: 显示指定名称的静态 BFD 会话的详细信息，*session-name* 表示静态 BFD 会话的名称，为 1~15 个字符的字符串，区分大小写。

control: 显示控制报文方式的 BFD 会话信息。

echo: 显示 echo 报文方式的 BFD 会话信息。

ip: 显示检测 IPv4 链路的 BFD 会话信息。

ipv6: 显示检测 IPv6 链路的 BFD 会话信息。

state: 显示不同状态下的 BFD 会话信息。

down: 显示会话状态为 Down 的 BFD 会话信息。

admin-down: 显示会话状态为 AdminDown 的 BFD 会话信息。

init: 显示会话状态为 Init 的 BFD 会话信息。

up: 显示会话状态为 Up 的 BFD 会话信息。

discriminator remote remote-value: 显示指定远端标识符的 BFD 会话信息。*remote-value* 表示 BFD 会话的远端标识符的值，取值范围为 1~4294967295。

peer-ip ipv4-address: 显示指定对端 IPv4 地址的静态 BFD 会话信息，*ipv4-address* 表示对端 IPv4 地址。

peer-ipv6 ipv6-address: 显示指定对端 IPv6 地址的静态 BFD 会话信息，*ipv6-address* 表示对端 IPv6 地址。

vpn-instance vpn-instance-name: 显示指定 VPN 实例的 BFD 会话信息。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果不指定该参数，则显示公网实例的 BFD 会话信息。

verbose: 显示 BFD 会话的详细信息。

【使用指导】

如果未指定 **dynamic** 或 **static** 参数，将显示所有动态 BFD 会话和静态 BFD 会话的信息。

【举例】

显示所有 BFD 会话的概要信息。

```
<Sysname> display bfd session
Total sessions: 7          Up sessions: 7          Init mode: Active

IPv4 session working in control packet mode:
```


LD/RD	SourceIP	DestinationIP	State	Holdtime	Interface
513/513	1.1.1.1	1.1.1.2	Up	2297ms	GE1/0/1

IPv6 session working in control packet mode:

```

Local discr: 513                      Remote discr: 513
Source IP: FE80::20C:29FF:FED4:7171
Destination IP: FE80::20C:29FF:FE72:AC4D
Session state: Up                      Interface: GE1/0/1
Hold time: 2142ms

```

IPv4 static session working in control packet mode:

LD/RD	SourceIP	DestinationIP	State	Holdtime	Interface
1017/7101	2.1.1.1	2.1.1.2	Up	4988ms	GE1/0/1

IPv6 static session working in control packet mode:

```

Local discr: 1226                      Remote discr: 6221
Source IP: 12::1
Destination IP: 12::2
Session state: Up                      Interface: GE1/0/1
Hold time: 4812ms

```

表1-1 display bfd session 命令显示信息描述表

字段	描述
Total sessions	所有BFD会话的数目
Up sessions	up的BFD会话的数目
Init mode	BFD运行模式： - Active: 主动模式 - Passive: 被动模式
IPv4 session working in control packet mode	BFD会话类型及工作方式，有以下几种情况： - IPv4 session working in control packet mode: IPv4 BFD 会话，工作方式为控制报文方式 - IPv4 session working in echo mode: IPv4 BFD 会话，工作方式为echo 报文方式 - IPv6 session working in control packet mode: IPv6 BFD 会话，工作方式为控制报文方式 - IPv6 session working in echo mode: IPv6 BFD 会话，工作方式为echo 报文方式 - IPv4 static session working in control packet mode: IPv4 静态 BFD 会话，工作方式为控制报文方式 - IPv6 static session working in control packet mode: IPv6 静态 BFD 会话，工作方式为控制报文方式
LD/RD	LD表示会话的本地标识符，RD表示会话的远端标识符

字段	描述
Source IP	会话的源IP地址
Destination IP	会话的目的IP地址
State	会话状态，包括Down、ADown、Init和Up
Holdtime	离会话检测时间超时的剩余时间。BFD会话处于down状态时，显示为0ms
Interface	会话所在的接口名
Local discr	会话的本地标识符
Remote discr	会话的远端标识符
Session state	会话状态，包括Down、ADown、Init和Up
Interface	会话所在的接口名
Hold time	离会话检测时间超时的剩余时间。BFD会话处于down状态时，显示为0ms

显示 BFD 会话的详细信息。

```
<Sysname> display bfd session verbose
```

```
Total sessions: 7          Up sessions: 7          Init mode: Active
```

```
IPv4 session working in control packet mode:
```

```

    Local discr: 33793                Remote discr: 33793
    Source IP: 23.1.1.2              Destination IP: 23.1.1.3
    Session state: Up
    Interface: GigabitEthernet1/0/1
    Min Tx interval: 1000ms          Actual Tx interval: 1000ms
    Min Rx interval: 1000ms          Detection time: 5000ms
    Rx count: 133                    Tx count: 142
    Connection type: Direct           Up duration: 00:02:01
    Hold time: 4571ms                Auth mode: None
    Detection mode: Async             Slot: 0
    Protocol: OSPF
    Version: 1
    Diag info: No Diagnostic
```

```
IPv6 session working in control packet mode:
```

```

    Local discr: 33794                Remote discr: 33794
    Source IP: FE80::5457:A5FF:FE0F:306
    Destination IP: FE80::5457:A1FF:FEB5:206
    Session state: Up
    Interface: GigabitEthernet1/0/1
    Min Tx interval: 1000ms          Actual Tx interval: 1000ms
    Min Rx interval: 1000ms          Detection time: 5000ms
    Rx count: 3262                    Tx count: 3048
    Connection type: Direct           Up duration: 00:44:26
```

```

        Hold time: 4409ms                      Auth mode: None
Detection mode: Async                          Slot: 0
        Protocol: OSPFv3
        Version: 1
        Diag info: No Diagnostic

```

IPv4 static session working in control packet mode:

```

        Session name: abc
        Local discr: 1017                      Remote discr: 7101
        Source IP: 2.1.1.1                    Destination IP: 2.1.1.2
        Session state: Up
        Interface: GigabitEthernet1/0/1
Min Tx interval: 1000ms                      Actual Tx interval: 1000ms
Min Rx interval: 1000ms                      Detection time: 5000ms
        Rx count: 1012                        Tx count: 1064
Connection type: Direct                      Up duration: 00:14:41
        Hold time: 4438ms                     Auth mode: None
Detection mode: Async                        Slot: 0
        Protocol: STATIC_IPv4
        Version: 1
        Diag info: No Diagnostic

```

IPv6 static session working in control packet mode:

```

        Session name: blue
        Local discr: 1226                      Remote discr: 6221
        Source IP: 12::1
Destination IP: 12::2
        Session state: Up
        Interface: GigabitEthernet1/0/1
Min Tx interval: 1000ms                      Actual Tx interval: 1000ms
Min Rx interval: 1000ms                      Detection time: 5000ms
        Rx count: 225                          Tx count: 266
Connection type: Direct                      Up duration: 00:03:13
        Hold time: 4371ms                     Auth mode: None
Detection mode: Async                        Slot: 0
        Protocol: STATIC_IPv6
        Version: 1
        Diag info: No Diagnostic

```

表1-2 display bfd session verbose 命令显示信息描述表

字段	描述
Total sessions	所有BFD会话的数目
Up sessions	up的BFD会话的数目

字段	描述
Init mode	BFD运行模式： • Active: 主动模式 • Passive: 被动模式
IPv4 session working in control packet mode	BFD会话类型及工作方式，有以下几种情况： • IPv4 session working in control packet mode: IPv4 BFD 会话，工作方式为控制报文方式 • IPv4 session working in echo mode: IPv4 BFD 会话，工作方式为echo 报文方式 • IPv6 session working in control packet mode: IPv6 BFD 会话，工作方式为控制报文方式 • IPv6 session working in echo mode: IPv6 BFD 会话，工作方式为echo 报文方式 • IPv4 static session working in control packet mode: IPv4 静态 BFD 会话，工作方式为控制报文方式 • IPv6 static session working in control packet mode: IPv6 静态 BFD 会话，工作方式为控制报文方式
Local discr	会话的本地标识符
Remote discr	会话的远端标识符
Source IP	会话的源IP地址
Destination IP	会话的目的IP地址
Session State	会话状态，包括Down、ADown、Init和Up
Interface	会话所在的接口名
Min Tx interval	最小发送时间间隔
Actual Tx interval	实际发送间隔
Min Rx interval	最小接收时间间隔
Detection time	实际检测时间
Rx count	接收的报文数
Tx count	发送的报文数
Connection type	接口的连接类型： • Direct: 直连 • Indirect: 非直连
Up duration	会话持续up的时间
Hold time	离会话检测时间超时的剩余时间。BFD会话处于down状态时，显示为0ms
Auth mode	会话的认证模式

字段	描述
Detection mode	检测模式： • Async: 异步模式 • Demand: 查询模式 • Async/Echo: 开启了回声功能的异步模式 • Demand/Echo: 开启了回声功能的查询模式
Slot	BFD会话所在单板： 格式为“ <i>slot-number</i> ”， <i>slot-number</i> 表示BFD会话所在单板的槽位号
Protocol	协议名： • OSPF: OSPF 与 BFD 联动的 BFD 会话 • STATIC4: 静态路由与 BFD 联动的 BFD 会话 • TRACK: Track 与 BFD 联动的 BFD 会话 • RIP: RIP 与 BFD 联动的 BFD 会话 • IPFRR: FIB IP FRR 与 BFD 联动的 BFD 会话 • MAD: MAD 与 BFD 联动的 BFD 会话 • OSPFv3: OSPFv3 与 BFD 联动的 BFD 会话 • STATIC6: IPv6 静态路由与 BFD 联动的 BFD 会话 • RIPNG: RIPng 与 BFD 联动的 BFD 会话 • Interface: 检测接口状态类型的 BFD 会话 • STATIC_IPv4: IPv4 静态 BFD 会话 • STATIC_IPv6: IPv6 静态 BFD 会话
Version	版本号
Diag Info	会话的诊断信息： • No Diagnostic: 表示无诊断信息 • Control Detection Time Expired: 表示 Ctrl 会话本端检测时间超时，会话 down • Echo Function Failed: 表示 Echo 会话本端检测时间超时或 echo 报文的源 IP 地址被删除，会话 down • Neighbor Signaled Session Down: 表示对端通知本端 BFD 会话 down • Administratively Down: 表示本端系统阻止 BFD 会话的建立

1.1.23 first-fail-timer

first-fail-timer 命令用来配置首次建立检测设备间数据链路层连通性的静态 BFD 会话失败时，通知数据链路层 BFD 会话 down 的超时时间。

undo first-fail-timer 命令用来恢复缺省情况。

【命令】

first-fail-timer seconds

undo first-fail-timer

【缺省情况】

首次建立检测设备间数据链路层连通性的静态 BFD 会话失败时，不会通知数据链路层 BFD 会话 down。

【视图】

静态 BFD 会话视图

【缺省用户角色】

network-admin
context-admin

【参数】

seconds：首次建立检测设备间数据链路层连通性的静态 BFD 会话失败时，通知数据链路层 BFD 会话 down 的超时时间，取值范围为 1~10000，单位为秒。

【使用指导】

配置本命令后，在 **seconds** 时间内，检测设备间数据链路层连通性的静态 BFD 会话未能成功建立时，BFD 会将此消息通知给数据链路层，并将接口的数据链路层协议状态置为“DOWN(BFD)”。

此时，执行 **display bfd session** 命令显示该静态 BFD 会话的状态为 Down，执行 **display interface** 命令会显示与该静态 BFD 会话联动的接口的 Line protocol state 为 DOWN(BFD)。

本命令仅用于接口状态与静态 BFD 会话（通过 **bfd static** 命令创建）联动的场景中，即只有将接口状态与该静态 BFD 会话关联后（配置 **process-interface-status** 命令），本命令才会生效。

本端配置设备间数据链路层连通性的静态 BFD 会话后，如果对端未配置检测设备间数据链路层连通性的静态 BFD 会话或两端 BFD 的认证配置不一致等原因，均会导致首次建立检测数据链路层连通性的 BFD 会话失败。

【举例】

配置首次建立检测设备间数据链路层连通性的静态 BFD 会话 abc 失败时，通知数据链路层 BFD 会话 down 的超时时间为 100 秒。

```
<Sysname> system-view
[Sysname] bfd static abc peer-ip default-ip interface gigabitethernet 1/0/1 source-ip 10.1.1.1 discriminator local 1 remote 1
[Sysname-bfd-static-session-1] first-fail-timer 100
```

【相关命令】

- **bfd static**
- **display interface**（接口管理/以太网接口）
- **processing-interface-status**

1.1.24 process-interface-status

process-interface-status 命令用来配置接口状态与静态 BFD 会话联动。

undo process-interface-status 命令用来恢复缺省情况。

【命令】

```
process-interface-status
undo process-interface-status
```

【缺省情况】

接口状态不与静态会话联动，即静态 BFD 会话状态的改变不会影响接口数据链路层协议状态。

【视图】

静态 BFD 会话视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

通过对端地址固定为组播地址 224.0.0.184 的静态 BFD 会话检测到数据链路发生故障时，若开启了本功能，则 BFD 检测到故障且会话进入 Down 状态时，将建立数据链路的接口链路层协议状态置为 DOWN(BFD)。可通过 **display interface** 命令查看接口的 Line protocol state 状态信息。

【举例】

```
# 配置接口 GigabitEthernet1/0/1 的状态与静态 BFD 会话 abc 联动。
<Sysname> system-view
[Sysname] bfd static abc peer-ip default-ip interface gigabitethernet 1/0/1 source-ip 10.1.1.
1 discriminator local 1 remote 1
[Sysname-bfd-static-session-abc] process-interface-status
```

【相关命令】

- **bfd static**
- **display interface**

1.1.25 reset bfd session statistics

reset bfd session statistics 命令用来清除所有 BFD 会话的统计信息。

【命令】

```
reset bfd session statistics
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 清除所有 BFD 会话的统计信息。
<Sysname> reset bfd session statistics
```

1.1.26 snmp-agent trap enable bfd

snmp-agent trap enable bfd 命令用来开启 BFD 的告警功能。

undo snmp-agent trap enable bfd 命令用来关闭 BFD 的告警功能。

【命令】

```
snmp-agent trap enable bfd
undo snmp-agent trap enable bfd
```

【缺省情况】

BFD 的告警功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启 BFD 模块的告警功能后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。（有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。）

【举例】

```
# 关闭 BFD 的告警功能。
<Sysname> system-view
[Sysname] undo snmp-agent trap enable bfd
```

1.1.27 special-processing

special-processing 命令用来开启对检测数据链路层连通性的静态 BFD 会话进行特殊处理的功能。

undo special-processing 命令用来关闭对检测数据链路层连通性的静态 BFD 会话进行特殊处理的功能。

【命令】

```
special-processing [ admin-down | authentication-change | session-up ] *
undo special-processing [ admin-down | authentication-change | session-up ]
*
```

【缺省情况】

对检测数据链路层连通性的静态 BFD 会话进行特殊处理的功能处于关闭状态。

【视图】

静态 BFD 会话视图

【缺省用户角色】

network-admin
context-admin

【参数】

admin-down: 本端收到会话状态为 AdminDown 的 BFD 报文时，将静态 BFD 会话 down 的消息通知给数据链路层。使用本参数，有利于快速发现 BFD 会话被手工关闭的建立数据链路的接口。如果未配置本参数，本端收到会话状态为 AdminDown 的 BFD 报文，将静态 BFD 会话状态置为 down，但是不会将 BFD 会话 down 的消息通知给数据链路层。

authentication-change: 本端认证信息发生变化时，立即将静态 BFD 会话状态置为 down。使用本参数，有利于快速发现认证信息不一致的建立数据链路的接口。如果未配置本参数，本端认证信息发生变化时，会预留时间给用户修改本端或对端的认证参数，如果预留时间结束时，两端认证信息仍未达成一致，本端会将静态 BFD 会话状态置为 down。

session-up: 本端静态 BFD 会话处于 up 状态时，不再检查收到的 BFD 报文中的认证信息。当设备上的 BFD 会话数量较多时，检查 BFD 报文中携带的认证信息会影响设备性能。配置本参数后，不再检查收到的报文中的认证信息，从而可以降低对设备性能的影响。如果未配置本参数，本端静态 BFD 会话处于状态 up 时，会检查收到的 BFD 报文中的认证信息，需要保证静态 BFD 会话两端认证信息的一致性，否则会导致静态 BFD 会话 down。

【使用指导】

如果未指定任何参数，将开启或关闭对检测数据链路层连通性的静态 BFD 会话进行所有特殊处理的功能。

【举例】

开启对检测数据链路层连通性的静态 BFD 会话 abc 进行特殊处理的功能，其中建立数据链路的本端接口为 GigabitEthernet1/0/1。对静态 BFD 会话 abc 进行的特殊处理包括收到会话状态为 AdminDown 的 BFD 报文、本端认证信息发生变化以及 BFD 会话处于 up 状态时对收到的 BFD 报文中认证信息检查的特殊处理。

```
<Sysname> system-view
[Sysname] bfd static abc peer-ip default-ip interface gigabitethernet 1/0/1 source-ip 10.1.1.1 discriminator local 1 remote 1
[Sysname-bfd-static-session-1] special-processing
```

【相关命令】

- **bfd static**
- **process-interface-status**

目 录

1 Track	1-1
1.1 Track配置命令	1-1
1.1.1 delay	1-1
1.1.2 display track	1-2
1.1.3 object	1-6
1.1.4 threshold percentage	1-7
1.1.5 threshold weight	1-8
1.1.6 track bfd	1-9
1.1.7 track interface	1-10
1.1.8 track interface physical	1-11
1.1.9 track interface protocol	1-12
1.1.10 track ip route reachability	1-13
1.1.11 track list boolean	1-14
1.1.12 track list threshold percentage	1-15
1.1.13 track list threshold weight	1-16
1.1.14 track nqa	1-17

1 Track

1.1 Track配置命令

1.1.1 delay

delay 命令用来配置 Track 项状态变化时，延迟通知应用模块的时间。

undo delay 命令用来删除配置的时间。

【命令】

```
delay { negative negative-time | positive positive-time } *  
undo delay
```

【缺省情况】

Track 项状态变化时，立即通知模块处理。

【视图】

Track 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

negative *negative-time*: 指定 Track 项状态变为 Negative 时，延迟通知应用模块的时间。
negative-time 为延迟通知应用模块时间，取值范围为 1~300，单位为秒。

positive *positive-time*: 指定 Track 项状态变为 Positive 时，延迟通知应用模块的时间。
positive-time 为延迟通知应用模块时间，取值范围为 1~300，单位为秒。

【使用指导】

Track 项状态发生变化后，如果立即通知应用模块，则可能会由于路由无法及时恢复等原因，导致通信中断。在这种情况下，用户可以配置 Track 项状态发生变化时，延迟一定的时间通知应用模块。
当 Track 项没有与应用模块联动时，配置 **delay** 命令不生效。

可以通过重复执行 **delay** 命令修改延迟通知应用模块的时间。多次执行 **delay** 命令，最后一次执行的命令生效。

【举例】

创建与布尔类型列表关联的 Track 项 101，并进入 Track 视图。指定 Track 项状态变为 Negative 时，延迟通知应用模块时间为 50 秒；Track 项状态变为 Positive 时，延迟通知应用模块时间为 30 秒。

```
<Sysname> system-view  
[Sysname] track 101 list boolean or  
[Sysname-track-101] delay negative 50 positive 30
```

【相关命令】

- **track bfd**
- **track interface**
- **track interface physical**
- **track interface protocol**
- **track ip route reachability**
- **track list boolean**
- **track list threshold percentage**
- **track list threshold weight**
- **track nqa**

1.1.2 display track

display track 命令用来显示 Track 项信息。

【命令】

display track { *track-entry-number* | **all** [**negative** | **positive**] } [**brief**]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

track-entry-number: 显示指定 Track 项的信息。*track-entry-number* 为 Track 项的序号，取值范围为 1~1024。

all: 显示所有 Track 项的信息。

negative: 显示 Negative 状态的 Track 项的信息。如果未指定本参数，则显示所有 Track 项信息。

positive: 显示 Positive 状态的 Track 项的信息。如果未指定本参数，则显示所有 Track 项信息。

brief: 显示 Track 项的简要信息。如果未指定本参数，则显示 Track 项的详细信息。

【举例】

显示所有 Track 项的信息。

```
<Sysname> display track all
```

```
Track ID: 1
```

```
State: Positive
```

```
Duration: 0 days 0 hours 0 minutes 7 seconds
```

```
Tracked object type: NQA
```

```
Notification delay: Positive 20, Negative 30 (in seconds)
```

```
Tracked object:
```

NQA entry: admin test
Reaction: 10
Remote IP/URL: 2.2.2.2
Local IP: 1.1.1.1
Interface: GigabitEthernet1/0/1
Tracked by:
 Track-list 6
 Track-list 7
Track ID: 2
State: NotReady
Duration: 0 days 0 hours 0 minutes 32 seconds
Tracked object type: BFD
Notification delay: Positive 20, Negative 30 (in seconds)
Tracked object:
 BFD session mode: Echo
 Outgoing interface: GigabitEthernet1/0/1
 VPN instance name: --
 Remote IP: 192.168.40.1
 Local IP: 192.168.40.2
Track ID: 3
State: Negative
Duration: 0 days 0 hours 0 minutes 32 seconds
Tracked object type: Interface
Notification delay: Positive 20, Negative 30 (in seconds)
Tracked object:
 Interface: GigabitEthernet1/0/2
 Protocol: IPv4
Tracked by:
 Track-list 6
 Track-list 7
Track ID: 5
State: Positive
Duration: 0 days 0 hours 0 minutes 32 seconds
Tracked object type: Route
Notification delay: Positive 20, Negative 30 (in seconds)
Tracked object:
 IP route: 0.0.0.0/0 reachability
 VPN instance name: --
 Protocol: Static
 Nexthop interface : GigabitEthernet1/0/3
Track ID: 6
State: Positive
Duration: 0 days 0 hours 0 minutes 32 seconds
Tracked object type: Percentage threshold list
Notification delay: Positive 20, Negative 30 (in seconds)
Threshold: Positive 40, Negative 30
Percentage of positive objects: 50%
Tracked objects:

```

    Object 1: Positive
    Object 3: Negative
Track ID: 7
    State: Positive
    Duration: 0 days 0 hours 0 minutes 32 seconds
    Tracked object type: Weight threshold list
    Notification delay: Positive 20, Negative 30 (in seconds)
    Threshold: Positive 50, Negative 30
    Positive weight/total weight: 50/80
    Tracked objects:
        Object 1: Positive, Weight: 50
Object 3: Negative, Weight: 30
Track ID: 8
    State: Positive
    Duration: 0 days 0 hours 0 minutes 32 seconds
    Tracked object type: Boolean and list
    Notification delay: Positive 20, Negative 30 (in seconds)
    Tracked objects:
        Object 1: Positive
        Object 3: Negative(not)
        Object 10: NotReady(not)

```

显示所有 **Negative** 状态的 **Track** 项的简要信息。

```
<Sysname> display track all negative brief
```

ID	Status	Type	Remote IP/URL	Local IP	Interface
1	Negative	Interface	--	--	GE1/0/1
10	Negative	Interface	--	--	GE1/0/2
12	Negative	List	--	--	--

表1-1 display track 命令输出信息描述

字段	描述
Track ID	Track项序号
State	Track项的状态，取值包括： - Positive: 表示状态正常 - NotReady: 表示无效值 - Negative: 表示状态异常
Duration	Track项处于当前状态的持续时间
Type	Track项的关联类型，本信息只在配置命令 display track brief 时显示，取值包括： - BFD: 表示 BFD 类型 - Interface: 表示接口类型 - Route: 表示路由类型 - NQA: 表示 NQA 类型 - List: 表示列表类型

字段	描述
Tracked object type	Track关联探测项类型，取值包括： • BFD：表示 BFD 类型 • Interface：表示接口类型 • Route：表示路由类型 • NQA：表示 NQA 类型 • Boolean and list：表示布尔与列表类型 • Boolean or list：表示布尔或列表类型 • Percentage threshold list：表示比例列表类型 • Weight threshold list：表示权重列表类型
Notification delay: Positive 20, Negative 30 (in seconds)	通知延迟： • Track 项状态变为 Positive 后，延迟 20 秒通知应用模块 • Track 项状态变为 Negative 后，延迟 30 秒通知应用模块
Threshold: Positive 40, Negative 30	门限值，包括Positive状态门限值和Negative状态门限值 只有比例列表和权重列表类型的Track项才显示该字段
Percentage of positive objects	关联列表中所有Positive对象所占比例，只有比例列表类型的Track项才显示该字段
Positive weight/total weight: 50/80	关联列表中所有Positive状态对象的权重之和/所有对象的权重值，只有权重列表类型的Track项才显示该字段
Tracked object	Track项关联的对象
NQA entry	Track项关联的NQA测试组
Reaction	Track项关联的联动项
BFD session mode	BFD会话的模式，当前只支持Echo模式
Outgoing interface	出接口
VPN instance name	VPN实例的名称。如果属于公网，则显示为“--”
Remote IP/URL	远端IP地址或URL路径，不存在时则显示“--”
Local IP	本地IP地址，不存在时则显示“--”
Interface	Track项关联的接口，不存在时则显示“--”
Protocol	监视接口的链路状态或网络层协议状态，取值包括： • None：监视接口的链路状态 • IPv4：监视三层接口的 IPv4 协议状态 • IPv6：监视三层接口的 IPv6 协议状态
IP route	Track项关联的路由
Protocol	关联路由的协议类型，如果路由不存在，则显示为“N/A”
Next hop interface	关联路由的下一跳，如果路由不存在，则显示为“N/A”

字段	描述
Object 10 : Positive	表示关联Track项，包括其状态值和权重值。在配置Track关联功能中，只在关联类型为列表的Track项中出现。如果关联类型不是权重列表，则不显示权重。（not）表示其是反状态。状态的取值包括： - Positive: 表示状态正常 - NotReady: 表示无效值 - Negative: 表示状态异常
Tracked by	该 Track 项作为其他 Track 项的对象
Track-list 6	类型为列表的 Track 项

【相关命令】

- **track bfd**
- **track interface**
- **track interface physical**
- **track interface protocol**
- **track ip route reachability**
- **track nqa**

1.1.3 object

object 命令用来向列表中添加与单个监测项联动的 Track 项。

undo object 命令用来删除与单个监测项联动的 Track 项。

【命令】

object track-entry-number [not] [weight weight]

undo object track-entry-number

【缺省情况】

列表中不存在与单个监测项联动的 Track 项。

【视图】

Track 视图

【缺省用户角色】

network-admin

context-admin

【参数】

track-entry-number: Track 项序号，取值范围为 1~1024。

not: Track 项的反状态，例如：如果 Track 项的状态为 Positive，则其反状态为 Negative。该参数只在与布尔类型列表的 Track 视图下可配。

weight weight: Track 项的权重，取值范围为 1~255。该参数只在权重类型列表 Track 视图下可配，缺省权重值为 10。

【使用指导】

- Track 视图中不能添加与 Track 视图序号相同的 Track 对象。
- 一个列表类型的 track 项中最多只能添加 16 个 Track 对象。
- Track 项不能互相关联形成环路。例如：如果 Track 项 1 中添加 Track 对象 2，Track 项 2 中添加 Track 对象 3，那么 Track 项 3 中不能再添加 Track 对象 1。

【举例】

创建与类型的布尔列表关联的 Track 项 100，并进入 Track 视图。添加与单个监测对象联动的 Track 对象 1，添加与单个监测对象联动的 Track 对象 2 的反状态。

```
<Sysname> system-view
[Sysname] track 100 list boolean and
[Sysname-track-100] object 1
[Sysname-track-100] object 2 not
```

【相关命令】

- **track list boolean**
- **track list threshold percentage**
- **track list threshold weight**

1.1.4 threshold percentage

threshold percentage 命令用来在比例型列表 Track 项中配置状态门限值。

undo threshold percentage 命令用来恢复缺省情况。

【命令】

```
threshold percentage { negative negative-threshold | positive positive-threshold } *
undo threshold percentage
```

【缺省情况】

Negative 状态门限值为 0%，Positive 状态门限值为 1%。

【视图】

Track 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

negative *negative-threshold*: 指定 Track 项状态变为 Negative 所要达到的门限，以百分数形式表示。*negative-threshold* 的取值范围为 0~100。当关联列表中 Positive 对象所占比例小于或等于 Negative 参数指定值时，Track 项状态变为 Negative。

positive *positive-threshold*: 指定 Track 项状态变为 Positive 所要达到的门限，以百分数形式表示。*positive-threshold* 的取值范围为 0~100。当关联列表中 Positive 对象所占比例

大于或等于 **Positive** 参数指定值时，Track 项状态变为 **Positive**。配置的 **Positive** 门限值需大于 **Negative** 门限值。

【使用指导】

当关联列表中的 **Positive** 对象比例小于 **Positive** 参数指定值且大于 **Negative** 参数指定值时，Track 项状态保持不变。

该命令只适用于比例类型列表 Track 项。

【举例】

创建和比例类型列表关联的 Track 项 1，并进入 Track 视图。配置 Track 项 1 的 **Negative** 门限值为 30%，**Positive** 门限值为 50%。

```
<Sysname> system-view
[Sysname] track 1 list threshold percentage
[Sysname-track-1] threshold percentage negative 30 positive 50
```

【相关命令】

- **track list threshold percentage**

1.1.5 threshold weight

threshold weight 命令用来在权重型列表 Track 项中配置状态门限值权重。

undo threshold weight 命令用来恢复缺省情况。

【命令】

```
threshold weight { negative negative-threshold | positive positive-threshold } *
undo threshold weight
```

【缺省情况】

Negative 门限值权重为 0，**Positive** 门限值权重为 1。

【视图】

Track 视图

【缺省用户角色】

network-admin
context-admin

【参数】

negative *negative-threshold*: 指定 Track 项状态变为 **Negative** 所要达到的门限值，以权重形式表示。*negative-threshold* 的取值范围为 0~254。当关联列表中当处于 **Positive** 的监测项的权重之和小于或等于 **Negative** 参数指定值时，Track 项状态变为 **Negative**。

positive *positive-threshold*: 指定 Track 项状态变为 **Positive** 所要达到的门限值，以权重形式表示。*positive-threshold* 的取值范围为 1~255。当关联列表中处于 **Positive** 的监测项的权重之和大于或等于 **Positive** 参数指定值时，Track 项状态变为 **Positive**。配置的 **Positive** 权重门限需大于 **Negative** 权重门限。

【使用指导】

当关联列表中的 **Positive** 对象权重小于 **Positive** 参数指定值且大于 **Negative** 参数指定值时，Track 项状态保持不变。

该命令只适用于权重类型列表 Track 项。

【举例】

创建和权重类型列表关联的 Track 项 1，并进入 Track 视图。设置 Track 项 1 的 **Negative** 门限值权重为 30，**Positive** 门限值权重为 50。

```
<Sysname> system-view
[Sysname] track 1 list threshold weight
[Sysname-track-1] threshold weight negative 30 positive 50
```

【相关命令】

- **track list threshold weight**

1.1.6 track bfd

track bfd 命令用来创建和 BFD 会话关联的 Track 项，并进入 Track 视图。如果指定的 Track 项已经存在，则直接进入 Track 视图。

undo track 命令用来删除指定的 Track 项及 Track 视图下所有配置。

【命令】

```
track track-entry-number bfd echo interface interface-type
interface-number remote ip remote-ip-address local ip local-ip-address
undo track track-entry-number
```

【缺省情况】

不存在 Track 项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

track-entry-number: Track 项的序号，取值范围为 1~1024。

interface *interface-type* *interface-number*: BFD 会话报文的出接口。
interface-type *interface-number* 为接口类型和接口编号。

remote ip *remote-ip-address*: BFD 会话探测的远端 IP 地址。

local ip *local-ip-address*: BFD 会话探测的本地 IP 地址。

【使用指导】

创建 Track 项时，必须指定 Track 项的关联类型。可以通过 **track track-entry-number** 进入已创建的 Track 项的视图，而无需指定关联类型。

不能通过重复执行本命令修改 Track 项关联的内容。如需修改 Track 项关联的内容，请先通过 **undo track** 命令删除 Track 项，再执行 **track bfd** 命令。

【举例】

创建与 BFD 会话关联的 Track 项 1，并进入 Track 视图。BFD 会话使用 Echo 报文进行探测，出接口为 GigabitEthernet1/0/1，远端 IP 地址为 192.168.40.1，本地 IP 地址为 192.168.40.2。

```
<Sysname> system-view
[Sysname] track 1 bfd echo interface gigabitethernet 1/0/1 remote ip 192.168.40.1 local ip 192.168.40.2
[Sysname-track-1]
```

【相关命令】

- **delay**
- **display track**

1.1.7 track interface

track interface 命令用来创建与指定接口链路状态关联的 Track 项，并进入 Track 视图。如果指定的 Track 项已经存在，则直接进入 Track 视图。

undo track 命令用来删除指定的 Track 项及 Track 视图下所有配置。

【命令】

```
track track-entry-number interface interface-type interface-number
undo track track-entry-number
```

【缺省情况】

不存在 Track 项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

track-entry-number: Track 项的序号，取值范围为 1~1024。

interface-type interface-number: 监视的接口类型和接口编号。

【使用指导】

创建 Track 项时，必须指定 Track 项的关联类型。可以通过 **track track-entry-number** 进入已创建的 Track 项的视图，而无需指定关联类型。

创建与接口链路状态关联的 Track 项后，接口的链路状态为 up 时，Track 项的状态为 Positive；接口的链路状态为 down 时，Track 项的状态为 Negative。通过 **display ip interface brief** 命令可以查看接口的链路状态。

不能通过重复执行本命令修改 Track 项关联的内容。如需修改 Track 项关联的内容，请先通过 **undo track** 命令删除 Track 项，再执行 **track interface** 命令。

【举例】

```
# 创建与接口 GigabitEthernet1/0/1 的链路状态关联的 Track 项 1，并进入 Track 视图。  
<Sysname> system-view  
[Sysname] track 1 interface gigabitethernet 1/0/1  
[Sysname-track-1]
```

【相关命令】

- **delay**
- **display ip interface brief**（三层技术-IP 业务命令参考/IP 地址）
- **display track**

1.1.8 track interface physical

track interface physical 命令用来创建与指定接口物理状态关联的 Track 项，并进入 Track 视图。如果指定的 Track 项已经存在，则直接进入 Track 视图。

undo track 命令用来删除指定的 Track 项及 Track 视图下所有配置。

【命令】

```
track track-entry-number interface interface-type interface-number  
physical  
undo track track-entry-number
```

【缺省情况】

不存在 Track 项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

track-entry-number: Track 项的序号，取值范围为 1~1024。

interface-type interface-number: 监视的接口类型和接口编号。

【使用指导】

创建 Track 项时，必须指定 Track 项的关联类型。可以通过 **track track-entry-number** 进入已创建的 Track 项的视图，而无需指定关联类型。

不能通过重复执行本命令修改 Track 项关联的内容。如需修改 Track 项关联的内容，请先通过 **undo track** 命令删除 Track 项，再执行 **track interface physical** 命令。

【举例】

```
# 创建与接口 GigabitEthernet1/0/1 的物理状态关联的 Track 项 1，并进入 Track 视图。  
<Sysname> system-view  
[Sysname] track 1 interface gigabitethernet 1/0/1 physical  
[Sysname-track-1]
```

【相关命令】

- **delay**
- **display ip interface brief**（三层技术-IP 业务命令参考/IP 地址）
- **display track**

1.1.9 track interface protocol

track interface protocol 命令用来创建与指定接口网络层协议状态关联的 Track 项，并进入 Track 视图。如果指定的 Track 项已经存在，则直接进入 Track 视图。

undo track 命令用来删除指定的 Track 项及 Track 视图下所有配置。

【命令】

```
track track-entry-number interface interface-type interface-number
protocol { ipv4 | ipv6 }
undo track track-entry-number
```

【缺省情况】

不存在 Track 项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

track-entry-number: Track 项的序号，取值范围为 1~1024。

interface-type interface-number: 监视的接口类型和接口编号。

ipv4: 监视接口的 IPv4 协议状态。接口的 IPv4 协议状态为 up 时，Track 项的状态为 Positive；接口的 IPv4 协议状态为 down 时，Track 项的状态为 Negative。通过 **display ip interface brief** 命令可以查看接口的 IPv4 协议状态。

ipv6: 监视接口的 IPv6 协议状态。接口的 IPv6 协议状态为 up 时，Track 项的状态为 Positive；接口的 IPv6 协议状态为 down 时，Track 项的状态为 Negative。通过 **display ipv6 interface brief** 命令可以查看接口的 IPv6 协议状态。

【使用指导】

创建 Track 项时，必须指定 Track 项的关联类型。可以通过 **track track-entry-number** 进入已创建的 Track 项的视图，而无需指定关联类型。

不能通过重复执行本命令修改 Track 项关联的内容。如需修改 Track 项关联的内容，请先通过 **undo track** 命令删除 Track 项，再执行 **track interface protocol** 命令。

【举例】

创建与接口 GigabitEthernet1/0/1 的 IPv4 协议状态关联的 Track 项 1，并进入 Track 视图。

```
<Sysname> system-view
```

```
[Sysname] track 1 interface gigabitethernet 1/0/1 protocol ipv4
```

[Sysname-track-1]

【相关命令】

- **delay**
- **display ip interface brief**（三层技术-IP 业务命令参考/IP 地址）
- **display ipv6 interface brief**（三层技术-IP 业务命令参考/IPv6 基础）
- **display track**

1.1.10 track ip route reachability

track ip route reachability 命令用来创建与路由管理关联的 Track 项并进入 Track 视图，指定 Track 项状态变化时通知应用模块的延迟时间。如果指定的 Track 项已经存在，则直接进入 Track 视图。

undo track 命令用来删除指定的 Track 项及 Track 视图下所有配置。

【命令】

```
track track-entry-number ip route [ vpn-instance vpn-instance-name ]  
ip-address { mask-length | mask } reachability  
undo track track-entry-number
```

【缺省情况】

不存在 Track 项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

track-entry-number: Track 项的序号，取值范围为 1~1024。

vpn-instance vpn-instance-name: 在指定 VPN 实例中创建和路由条目关联的 Track 项。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示在公网中创建和路由关联的 Track 项。

ip-address: 路由条目中的 IP 地址，点分十进制格式。

mask-length/mask: IP 地址掩码长度/掩码，以整数形式表示掩码长度或以点分十进制格式表示掩码。当用整数形式时，取值范围为 0~32。

【使用指导】

创建 Track 项时，必须指定 Track 项的关联类型。可以通过 **track track-entry-number** 进入已创建的 Track 项的视图，而无需指定关联类型。

不能通过重复执行本命令修改 Track 项关联的内容。如需修改 Track 项关联的内容，请先通过 **undo track** 命令删除 Track 项，再执行 **track ip route reachability** 命令。

当发生主备设备倒换或者 RIB 进程倒换后，如果路由协议进程平滑重启一直未结束，并且此时路由条目发生变化，路由管理不会立刻向 Track 模块通知路由变化信息，通过配置路由管理的不间断路由功能，可以解决上述问题。

【举例】

创建与路由管理关联的 Track 项 1，并进入 Track 视图。路由条目目的地址 10.1.1.0，掩码长度为 24。

```
<Sysname> system-view
[Sysname] track 1 ip route 10.1.1.0 24 reachability
[Sysname-track-1]
```

【相关命令】

- **delay**
- **display ip route**（三层技术-IP 路由命令参考/IP 路由基础）
- **display track**

1.1.11 track list boolean

track list boolean 命令用来创建布尔类型列表 Track 项，并进入 Track 视图。如果指定的 Track 项已经存在，则直接进入 Track 视图。

undo track 命令用来删除指定的 Track 项及 Track 视图下所有配置。

【命令】

```
track track-entry-number list boolean { and | or }
undo track track-entry-number
```

【缺省情况】

不存在 Track 项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

track-entry-number：Track 项的序号，取值范围为 1~1024。

and：使用布尔与运算决定 Track 项的状态。

or：使用布尔或运算决定 Track 项的状态。

【使用指导】

本命令创建布尔类型列表 Track 项，Track 项的状态由 Track 列表中对象状态的布尔运算结果决定，共有两种类型的布尔列表：

- **布尔与列表类型**：基于列表中对象状态的布尔与运算结果决定 Track 项的状态。如果关联列表中的所有对象的状态都是 Positive，那么此 Track 项的状态为 Positive；如果有一个或多个对象的状态为 Negative，那么此 Track 项的状态为 Negative。

- 布尔或列表类型：基于列表中对象状态的布尔或运算结果决定 Track 项的状态。如果关联列表中至少有一个对象的状态是 Positive，那么此 Track 项的状态为 Positive；如果所有的对象的状态都是 Negative，那么此 Track 项的状态为 Negative。

创建 Track 项时，必须指定 Track 项的关联类型。可以通过 **track track-entry-number** 进入已创建的 Track 视图，而无需指定关联类型。

不能通过重复执行本命令修改 Track 项的关联类型。如需修改 Track 项的关联类型，请先通过 **undo track** 命令删除 Track 项，再执行 **track list boolean** 命令。

【举例】

创建布尔类型列表 Track 项 101，并进入 Track 视图。Track 项 101 使用布尔或运算。

```
<Sysname> system-view
[Sysname] track 101 list boolean or
[Sysname-track-101]
```

【相关命令】

- **delay**
- **object**

1.1.12 track list threshold percentage

track list threshold percentage 命令用来创建比例类型列表 Track 项，并进入 Track 视图。如果指定的 Track 项已经存在，则直接进入 Track 视图。

undo track 命令用来删除指定的 Track 项及 Track 视图下所有配置。

【命令】

```
track track-entry-number list threshold percentage
undo track track-entry-number
```

【缺省情况】

不存在 Track 项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

track-entry-number：Track 项的序号，取值范围为 1~1024。

【使用指导】

本命令创建比例类型列表 Track 项，Track 项的状态由 Track 列表中 Positive 对象/所有对象的总比例和 **threshold percentage** 命令配置的阈值的大小决定。

创建 Track 项时，必须指定 Track 项的关联类型。可以通过 **track track-entry-number** 进入已创建的 Track 视图，而无需指定关联类型。

不能通过重复执行本命令修改 Track 项的关联类型。如需修改 Track 项的关联类型，请先通过 **undo track** 命令删除 Track 项，再执行 **track list threshold percentage** 命令。

【举例】

创建比例类型列表 Track 项 101，并进入 Track 视图。

```
<Sysname> system-view
[Sysname] track 101 list threshold percentage
[Sysname-track-101]
```

【相关命令】

- **delay**
- **object**
- **threshold percentage**

1.1.13 track list threshold weight

track list threshold weight 命令用来创建权重类型列表 Track 项，并进入 Track 视图。如果指定的 Track 项已经存在，则直接进入 Track 视图。

undo track 命令用来删除指定的 Track 项及 Track 视图下所有配置。

【命令】

```
track track-entry-number list threshold weight
undo track track-entry-number
```

【缺省情况】

不存在 Track 项。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

track-entry-number：Track 项的序号，取值范围为 1~1024。

【使用指导】

本命令创建权重类型列表 Track 项，Track 项的状态由 Track 列表中 Positive 对象的总权重和 **threshold weight** 命令配置的权重值的大小决定。

创建 Track 项时，必须指定 Track 项的关联类型。可以通过 **track track-entry-number** 进入已创建的 Track 视图，而无需指定关联类型。

不能通过重复执行本命令修改 Track 项的关联类型。如需修改 Track 项的关联类型，请先通过 **undo track** 命令删除 Track 项，再执行 **track list threshold weight** 命令。

【举例】

创建权重类型列表 Track 项 101，并进入 Track 视图。

```
<Sysname> system-view
[Sysname] track 101 list threshold weight
[Sysname-track-101]
```

【相关命令】

- **delay**
- **object**
- **threshold weight**

1.1.14 track nqa

track nqa 命令用来创建与 NQA 测试组中指定联动项关联的 Track 项，并进入 Track 视图。如果指定的 Track 项已经存在，则直接进入 Track 视图。

undo track 命令用来删除指定的 Track 项及 Track 视图下所有配置。

【命令】

```
track track-entry-number nqa entry admin-name operation-tag reaction  
item-number  
undo track track-entry-number
```

【缺省情况】

不存在 Track 项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

track-entry-number: Track 项的序号，取值范围为 1~1024。

entry admin-name operation-tag: 指定与 Track 项关联的 NQA 测试组。其中，*admin-name* 为创建 NQA 测试组的管理员的名字，为 1~32 个字符的字符串，不区分大小写；*operation-tag* 为 NQA 测试操作的标签，为 1~32 个字符的字符串，不区分大小写。

reaction item-number: 指定与 Track 项关联的联动项。其中，*item-number* 为联动项的序号，取值范围为 1~10。

【使用指导】

创建 Track 项时，必须指定 Track 项的关联类型。可以通过 **track track-entry-number** 进入已创建的 Track 视图，而无需指定关联类型。

不能通过重复执行本命令修改 Track 项关联的内容。如需修改 Track 项关联的内容，请先通过 **undo track** 命令删除 Track 项，再执行 **track nqa** 命令。

【举例】

创建与 NQA 测试组（admin-test）中联动项 3 关联的 Track 项 1，并进入 Track 视图。

```
<Sysname> system-view
```

```
[Sysname] track 1 nqa entry admin test reaction 3  
[Sysname-track-1]
```

【相关命令】

- **delay**
- **display track**

目 录

1 以太网冗余接口	1-1
1.1 以太网冗余接口配置命令	1-1
1.1.1 bandwidth	1-1
1.1.2 default	1-1
1.1.3 description	1-2
1.1.4 display counters interface reth	1-3
1.1.5 display counters rate interface reth	1-4
1.1.6 display interface reth	1-5
1.1.7 display reth interface	1-9
1.1.8 interface reth	1-10
1.1.9 member interface	1-11
1.1.10 mtu	1-12
1.1.11 reset counters interface reth	1-13
1.1.12 reth advertise retransmit	1-14
1.1.13 shutdown	1-15
1.1.14 sub-interface rate-statistic	1-15
2 冗余组	2-1
2.1 冗余组配置命令	2-1
2.1.1 bind slot	2-1
2.1.2 display redundancy group	2-1
2.1.3 hold-down-interval	2-4
2.1.4 member interface	2-4
2.1.5 node	2-5
2.1.6 node-member interface	2-6
2.1.7 preempt-delay	2-7
2.1.8 priority	2-7
2.1.9 redundancy group	2-8
2.1.10 snmp-agent trap enable rddc	2-9
2.1.11 switchover request	2-9
2.1.12 switchover reset	2-10
2.1.13 track	2-10

1 以太网冗余接口

1.1 以太网冗余接口配置命令

1.1.1 bandwidth

bandwidth 命令用来配置以太网冗余接口/以太网冗余子接口的期望带宽。

undo bandwidth 命令用来恢复缺省情况。

【命令】

bandwidth *bandwidth-value*

undo bandwidth

【缺省情况】

接口的期望带宽为 10000kbps。

【视图】

以太网冗余接口视图

以太网冗余子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

bandwidth-value: 表示接口的期望带宽，取值范围为 1~400000000，单位为 kbps。

【使用指导】

期望带宽供业务模块使用，不会对接口实际带宽造成影响。

【举例】

配置以太网冗余接口 Reth1 的期望带宽为 50kbps。

```
<Sysname> system-view
```

```
[Sysname] interface reth 1
```

```
[Sysname-Reth1] bandwidth 50
```

1.1.2 default

default 命令用来恢复以太网冗余接口/以太网冗余子接口的缺省配置。

【命令】

default

【视图】

以太网冗余接口视图

以太网冗余子接口视图

【缺省用户角色】

network-admin
context-admin

【使用指导】



注意

接口下的某些配置恢复到缺省情况后，会对设备上当前运行的业务产生影响。建议您在执行该命令前，完全了解其对网络产生的影响。

您可以在执行 **default** 命令后通过 **display this** 命令确认执行效果。对于未能成功恢复缺省的配置，建议您查阅相关功能的命令手册，手工执行恢复该配置缺省情况的命令。如果操作仍然不能成功，您可以通过设备的提示信息定位原因。

【举例】

将以太网冗余接口 Reth1 恢复为缺省配置。

```
<Sysname> system-view  
[Sysname] interface reth 1  
[Sysname-Reth1] default
```

1.1.3 description

description 命令用来配置以太网冗余接口/以太网冗余子接口的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*
undo description

【缺省情况】

接口的描述信息为“接口名 Interface”，比如：Reth1 Interface。

【视图】

以太网冗余接口视图

以太网冗余子接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

text: 以太网冗余接口/以太网冗余子接口的描述信息，为 1~255 个字符的字符串，区分大小写。

【举例】

配置以太网冗余接口 Reth1 的描述信息为 master-interface。

```
<Sysname> system-view
```

```
[Sysname] interface reth 1
[Sysname-Reth1] description master-interface
```

1.1.4 display counters interface reth

display counters interface reth 命令用来显示以太网冗余接口的流量统计信息。

【命令】

```
display counters { inbound | outbound } interface [ reth
[ interface-number ] ]
```

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【参数】

- inbound**: 显示输入报文的流量统计信息。
- outbound**: 显示输出报文的流量统计信息。
- reth**: 显示以太网冗余接口的流量统计信息。不指定该参数时，显示所有可统计的接口的流量统计信息。
- interface-number**: 指定以太网冗余接口编号。不指定该参数时，显示所有以太网冗余接口的流量统计信息。

【使用指导】

本命令显示的是统计周期内报文的数量，统计周期可以通过 **flow-interval** 命令来配置。
执行 **reset counters interface reth** 命令会清除本命令的统计信息。

【举例】

```
# 显示接口 Reth1 的报文输入流量统计信息。
<Sysname> display counters inbound interface reth 1
Interface          Total (pkts)    Broadcast (pkts)  Multicast (pkts)  Err (pkts)
Reth1              100            100              0                 0

Overflow: More than 14 digits (7 digits for column "Err").
--: Not supported.
```

表1-1 display counters interface reth 命令显示信息描述表

字段	描述
Interface	接口名称缩写
Total (pkts)	接口接收或发送报文的总数（单位为包）
Broadcast (pkts)	接口接收或发送广播报文的总数（单位为包）

字段	描述
Multicast (pkts)	接口接收或发送组播报文的总数（单位为包）
Err (pkts)	接口接收或发送错误报文的总数（单位为包）
Overflow: More than 14 digits (7 digits for column "Err").	当某个统计信息的值为Overflow时，表示该项数据的长度超过了显示范围： - 对于 Err 项，Overflow 表示数据的长度超过了 7 位十进制数 - 对于其它项，Overflow 表示数据的长度超过了 14 位十进制数
--: Not supported.	当某个统计信息的值为 "--" 时，表示设备不支持该项数据的统计

【相关命令】

- **flow-interval**（接口管理命令参考/以太网接口）
- **reset counters interface reth**

1.1.5 display counters rate interface reth

display counters rate interface reth 命令用来显示最近一个统计周期内处于 up 状态的接口的报文速率统计信息。

【命令】

```
display counters rate { inbound | outbound } interface [ reth  
[ interface-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

inbound: 显示报文接收速率统计信息。

outbound: 显示报文发送速率统计信息。

reth: 显示以太网冗余接口的相应信息。不指定该参数时，显示所有可统计的接口的相应信息。

interface-number: 指定以太网冗余接口编号。不指定该参数时，显示所有以太网冗余接口的相应信息。

【使用指导】

关于统计周期的值，统计周期可以通过 **flow-interval** 命令来配置。

执行 **reset counters interface reth** 命令会清除本命令的统计信息。

【举例】

显示接口 Reth1 的报文接收速率统计信息。

```
<Sysname> display counters rate inbound interface reth 1
Usage: Bandwidth utilization in percentage
Interface          Usage (%)    Total (pps)    Broadcast (pps)    Multicast (pps)
Reth1              3          200           100              100

Overflow: More than 14 digits.
--: Not supported.
```

表1-2 display counters rate interface reth 命令显示信息描述表

字段	描述
Interface	接口名称缩写
Usage (%)	在最近一个统计周期内，接口的带宽利用率（单位为百分比）
Total (pps)	在最近一个统计周期内，接口接收或发送所有类型报文的平均速率（单位为包/秒）
Broadcast (pps)	在最近一个统计周期内，接口接收或发送广播报文的平均速率（单位为包/秒）
Multicast (pps)	在最近一个统计周期内，接口接收或发送组播报文的平均速率（单位为包/秒）
Overflow: More than 14 digits.	当某个统计信息的值为Overflow时，表示该项数据的长度超过了14位十进制数
--: Not supported.	当某个统计信息的值为“--”时，则表示设备不支持该项数据的统计

【相关命令】

- **flow-interval**（接口管理命令参考/以太网接口）
- **reset counters interface reth**

1.1.6 display interface reth

display interface reth 命令用来显示以太网冗余接口/以太网冗余子接口的相关信息。

【命令】

```
display interface [ reth [ interface-number | interface-number.subnumber ] ]
[ brief [ description | down ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

reth: 显示以太网冗余接口/以太网冗余子接口的相关信息。

interface-number: 表示以太网冗余接口的编号，取值为已创建的以太网冗余接口的编号。

interface-number.subnumber: 表示以太网冗余子接口的编号。其中, *interface-number* 为主接口编号, *subnumber* 为子接口编号。

brief: 显示接口的概要信息。不指定该参数时, 将显示接口的详细信息。

down: 显示当前物理状态为 **down** 的接口的信息以及 **down** 的原因。不指定该参数时, 将不会根据接口物理状态来过滤显示信息。

description: 显示用户配置的接口的全部描述信息。不指定该参数时, 显示接口的概要信息时接口的描述信息最多可显示 27 个字符, 超出部分不显示。

【使用指导】

如果不指定 **reth** 参数, 则显示所有接口的信息。

如果指定 **reth** 参数, 不指定 *interface-number* 和 *interface-number.subnumber* 参数, 将显示所有以太网冗余接口和以太网冗余子接口的相关信息。

如果指定 **reth** 参数, 同时指定了 *interface-number* 或 *interface-number.subnumbe* 参数, 将显示指定以太网冗余接口或以太网冗余子接口的相关信息。

【举例】

```
# 显示以太网冗余接口 Reth1 的详细信息。
<Sysname> display interface reth 1
Reth1
Current state: UP
Line protocol state: UP
Description: Reth1 Interface
Bandwidth: 10000kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 0cda-41b5-cf30
IPv6 packet frame type: Ethernet II, hardware address: 0cda-41b5-cf30
Physical: Reth, baudrate: 10000000 bps
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

表1-3 display interface reth 命令显示信息描述表

字段	描述
Current state	接口的物理状态, 取值为: - Administratively DOWN: 表示该接口已经通过 shutdown 命令被关闭, 即管理状态为关闭 - DOWN: 表示该接口的管理状态为开启, 但物理状态为关闭 (可能因为没有物理连线或者线路故障) - UP: 表示该接口的管理状态和物理状态均为开启。只要有一个成员接口状态为 UP, 以太网冗余接口的状态就为 UP

字段	描述
Line protocol state	接口的链路层协议状态。其值由链路层经过参数协商决定，取值为： - UP：表示数据链路层协议状态为开启 - DOWN：表示数据链路层协议状态为关闭
Description	接口的描述信息
Bandwidth	接口的期望带宽
Maximum transmission unit	接口的MTU
Internet protocol processing: Disabled	接口未配置IP地址，不能处理IP报文
Internet address: <i>ip-address/mask-length</i> (<i>Type</i>)	接口IP地址。<i>Type</i>表示地址获取方式，取值如下： - Primary：手动配置的主地址 - Sub：手动配置的从地址。当配置了主地址时，仅显示主地址；仅配置从地址时，才显示本信息 - Unnumbered：借用其他接口的IP地址 - MAD：成员设备上配置的MAD IP地址，详细介绍请参见“虚拟化技术配置指导”中的“IRF”  说明 <i>Type</i>的取值情况与接口类型有关，请以实际情况为准
IP packet frame type	IPv4报文发送帧格式
hardware address	接口的MAC地址
IPv6 packet frame type	IPv6报文发送帧格式
Physical	接口的类型为Reth
baudrate	接口的波特率为10000000bps
Last clearing of counters	最近一次使用 reset counters interface 命令清除接口下的统计信息的时间（如果从设备启动一直没有执行 reset counters interface 命令清除过该接口下的统计信息，则显示Never）
Last 300 second input: 0 bytes/sec, 0 bits/sec, 0 packets/sec Last 300 second output: 0 bytes/sec, 0 bits/sec, 0 packets/sec	端口在最近300秒接收和发送报文的平均速率，单位分别为字节/秒、比特/秒和数据包/秒。对于以太网冗余子接口，只有配置 sub-interface rate-statistic 命令后，才会显示该信息
Input: 0 packets, 0 bytes, 0 drops	该接口接收的数据报文个数、字节数，以及由于没有接收缓冲而被丢弃的报文个数
Output: 0 packets, 0 bytes, 0 drops	该接口发送的数据报文个数、字节数，以及由于没有发送缓冲而被丢弃的报文个数
Brief information on interfaces in route mode	三层接口的概要信息

字段	描述
Link: ADM - administratively down; Stby - standby	- 如果某接口的 Link 属性值为“ADM”，则表示该接口被管理员手工关闭了，需要在该接口下执行 undo shutdown 命令才能恢复端口本身的物理状态 - 如果某接口的 Link 属性值为“Stby”，则表示该接口是一个备份接口，使用 display interface-backup state 命令可以查看该备份接口对应的主接口
Protocol: (s) - spoofing	如果某接口的 Protocol 属性值中带有“(s)”字符串，则表示该接口的数据链路层协议状态显示是UP的，但实际可能没有对应的链路，或者所对应的链路不是永久存在而是按需建立
Interface	接口名称缩写
Link	接口物理连接状态，取值可能为： - UP：表示本链路物理上是连通的 - DOWN：表示本链路物理上是不通的
Protocol	接口数据链路层协议状态，取值为： - UP：表示接口的数据链路层协议状态为开启 - DOWN：表示接口的数据链路层协议状态为关闭
Primary IP	接口主IP地址。取值为“--”时，表示接口尚未配置IP地址
Description	接口的描述信息。使用 display interface brief 命令，不指定 description 参数时，该字段最多显示27个字符；指定 description 参数时，可显示配置的全部描述信息

显示 Reth1 接口的概要信息。

```
<Sysname> display interface reth 1 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP      Description
Reth1              DOWN DOWN      --
```

显示 Reth1 接口 down 的原因。

```
<Sysname> display interface reth 1 brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
Reth1              DOWN Not connected
```

表1-4 display interface brief 命令显示信息描述表

字段	描述
Brief information on interfaces in route mode:	三层接口的概要信息

字段	描述
Link: ADM - administratively down; Stby - standby	- 如果某接口的 Link 属性值为“ADM”，则表示该接口被管理员通过 shutdown 命令关闭，需要在该接口下执行 undo shutdown 命令才能恢复接口本身的物理状态 - 如果某接口的 Link 属性值为“Stby”，则表示该接口是一个处于 Standby 状态的备份接口，使用 display interface-backup state 命令可以查看该备份接口对应的主接口
Protocol: (s) - spoofing	如果某接口的 Protocol 属性值中带有“(s)”，则表示该接口的数据链路层协议状态显示为 UP，但实际可能没有对应的链路，或者对应的链路不是永久存在而是按需建立的。通常 NULL、LoopBack 等接口会具有该属性
Interface	接口名称缩写
Link	接口物理连接状态，取值为： - UP：表示接口物理上是连通的 - DOWN：表示接口物理上不通 - ADM：表示接口被管理员通过 shutdown 命令关闭，需要执行 undo shutdown 命令才能恢复接口本身的物理状态 - Stby：表示该接口是一个处于 Standby 状态的备份接口
Protocol	接口数据链路层协议状态，取值为： - UP：表示接口的数据链路层是连通的 - DOWN：表示接口的数据链路层不通
Primary IP	接口主 IP 地址。当显示“--”时，表示接口下还未配置 IP 地址
Description	接口的描述信息
Cause	接口物理连接状态为 down 的原因，取值为： - Administratively：表示本链路被手工关闭了（配置了 shutdown 命令），需要执行 undo shutdown 命令才能恢复真实的物理状态 - Not connected：表示没有物理连接（可能没有插网线或者网线故障）

1.1.7 display reth interface

display reth interface 命令用来显示以太网冗余接口的成员接口的信息。

【命令】

display reth interface reth interface-number

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

reth interface-number: 表示接口编号，取值范围为已创建的以太网冗余接口的编号。

【举例】

```
# 显示以太网冗余接口 Reth1 的信息。
<Sysname> display reth interface reth 1
Reth1 :
  Redundancy group   : aaa
  Member             Physical status      Forwarding status    Presence status
  GE1/0/1             UP                  Active               Normal
  GE1/0/2             UP                  Inactive             Normal
```

表1-5 display reth 命令显示信息描述表

字段	描述
Reth1	以太网冗余接口Reth1的信息
Redundancy group	以太网冗余接口所在的冗余组，未加入冗余组时显示为N/A
Member	成员接口的名称
Physical status	成员接口的物理状态： - Down(redundancy down): 表示该接口被 Reth 模块关闭，即接口状态为冗余关闭 - Down: 表示该接口的管理状态为开启，但物理状态为关闭（可能因为没有物理连线或者线路关闭） - Up: 该接口的管理状态和物理状态均为开启
Forwarding status	成员接口的转发状态： - Active: 成员接口可以正常收发报文 - Inactive: 成员接口不能收发报文
Presence status	成员接口的状态： - Normal 表示存在该接口 - Absent 表示该接口不存在

1.1.8 interface reth

interface reth 命令用来创建以太网冗余接口/以太网冗余子接口，并进入该接口视图。如果指定的以太网冗余接口/以太网冗余子接口已经存在，则直接进入该接口视图。

undo interface reth 命令用来删除以太网冗余接口/以太网冗余子接口。

【命令】

```
interface reth { interface-number | interface-number.subnumber }
undo interface reth { interface-number | interface-number.subnumber }
```

【缺省情况】

不存在以太网冗余接口/以太网冗余子接口。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-number: 接口编号，取值范围为 1~255。

interface-number.subnumber: 以太网冗余子接口的编号。其中 *interface-number* 为主接口编号，*subnumber* 为子接口编号，子接口的编号取值范围为 1~4094。

【使用指导】

以太网冗余接口是一种三层虚拟接口。一个以太网冗余接口中包含两个成员接口，使用以太网冗余接口可以实现这两个接口之间的冗余备份。

请先创建以太网冗余接口，才能创建以太网冗余子接口。

如果以太网冗余接口的成员接口为三层以太网子接口、三层聚合接口子接口，或者成员接口下创建了子接口，则不允许以太网冗余接口下再创建子接口。

删除以太网冗余接口时，如果该接口下存在成员接口，则不允许删除。

【举例】

```
# 创建以太网冗余接口 Reth1。
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1]
# 创建以太网冗余子接口 Reth1.1，并进入该接口视图。
<Sysname> system-view
[Sysname] interface reth 1.1
[Sysname-Reth1.1]
```

1.1.9 member interface

member interface 命令用来给以太网冗余接口添加成员接口。

undo member interface 命令用来将成员接口从以太网冗余接口中删除。

【命令】

member interface *interface-type interface-number priority priority*

undo member interface *interface-type interface-number*

【缺省情况】

以太网冗余接口下不存在成员接口。

【视图】

以太网冗余接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type interface-number: 接口类型和接口编号。接口类型可以为三层以太网接口、三层聚合口及上述接口的子接口。

priority: 成员接口的优先级，取值范围为 1~255。数值越大，优先级越高。

【使用指导】

每个以太网冗余接口下最多可添加两个成员接口。当两成员接口的链路状态均为 UP 时，系统会让优先级高的成员接口处于激活状态，优先级低的处于非激活状态。激活接口可以收发报文，非激活接口不能收发报文。

同一以太网冗余接口的成员接口的类型和速率最好相同。

一个物理接口加入一个以太网冗余接口后，不能加入其它以太网冗余接口。

两个成员接口如果都是子接口，则不能是同一主接口的两个子接口。

如果以太网冗余接口下创建了子接口，则该以太网冗余接口下的成员接口不能为子接口或者带有子接口的主接口。

当以太网冗余接口的成员接口包含子接口时，不能指定该以太网冗余接口为 IPv6 静态邻居表项的出接口。关于 IPv6 静态邻居表项的详细描述请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。

【举例】

给以太网冗余接口 Reth1 中添加成员接口 GigabitEthernet1/0/1，并指定优先级为 100；添加成员接口 GigabitEthernet1/0/2，并指定优先级为 50。

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1] member interface gigabitethernet 1/0/1 priority 100
[Sysname-Reth1] member interface gigabitethernet 1/0/2 priority 50
```

1.1.10 mtu

mtu 命令用来配置以太网冗余接口/以太网冗余子接口的 MTU（Maximum Transmission Unit，最大传输单元）值。

undo mtu 命令用来恢复缺省情况。

【命令】

mtu size
undo mtu

【缺省情况】

以太网冗余接口/以太网冗余子接口的 MTU 值为 1500 字节。

【视图】

以太网冗余接口视图

以太网冗余子接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

size: 以太网冗余接口/以太网冗余子接口的 MTU 值，单位为字节，取值范围为 46～8192。

【使用指导】

以太网冗余接口/以太网冗余子接口的 MTU 值影响 IP 协议报文在该接口上传输时的分片与重组。

需要注意的是，配置了 **mtu** 命令后需要执行命令 **shutdown** 和 **undo shutdown**，这样该配置才能在接口上生效。

【举例】

配置以太网冗余接口 Reth1 的 MTU 值为 200 字节。

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1] mtu 200
```

1.1.11 reset counters interface reth

reset counters interface reth 命令用来清除以太网冗余接口/以太网冗余子接口的统计信息。

【命令】

```
reset counters interface [ reth [ interface-number | interface-number.subnumber ] ]
```

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【参数】

interface-number: 以太网冗余接口的编号。

interface-number.subnumber: 表示以太网冗余子接口的编号。其中，**interface-number** 为主接口编号，**subnumber** 为子接口编号。

【使用指导】

在某些情况下，需要统计一定时间内某接口的流量，这就需要在统计开始前清除该接口原有的统计信息，重新进行统计。

如果不指定 **reth** 参数，则清除所有接口的统计信息。

如果指定了 **reth** 参数而不指定 **interface-number** 和 **interface-number.subnumber**，则清除所有以太网冗余接口和以太网冗余子接口的统计信息。

如果指定了 **reth** 参数，同时指定了 **interface-number** 或 **interface-number.subnumber** 参数，将清除指定以太网冗余接口或以太网冗余子接口的统计信息。

【举例】

```
# 清除以太网冗余接口 Reth1 的统计信息。  
<Sysname> reset counters interface reth 1
```

【相关命令】

- **display counters interface reth**
- **display counters rate interface reth**
- **display interface reth**

1.1.12 reth advertise retransmit

reth advertise retransmit 命令用来配置当以太网冗余接口的成员接口的激活状态切换时，向邻居设备重新发送通告报文的次数和时间间隔。

undo reth advertise retransmit 命令用来恢复缺省情况。

【命令】

```
reth advertise retransmit times interval seconds  
undo reth advertise retransmit
```

【缺省情况】

当以太网冗余接口的成员接口的激活状态切换时，向邻居设备重新发送通告报文的次数为 5，时间间隔为 1 秒。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

times: 向邻居设备重新发送通告报文的次数，取值范围为 5～30。

seconds: 向邻居设备重新发送通告报文的时间间隔，取值范围为 1～10，单位为秒。

【使用指导】

配置本命令后，当以太网冗余接口的成员接口的激活状态切换时，以太网冗余接口会立即发送一次通告报文（包括免费 ARP、NA 报文），并在接下来的时间，会按照指定时间间隔重复发送指定次数的通告报文，来通告邻居设备成员接口的激活状态发生了变化。

如果以太网冗余接口下创建了子接口，以太网冗余接口发送通告报文时，子接口也会发送通告报文，为避免子接口太多，导致通告报文太多，长时间占用 CPU 资源，本命令仅对以太网冗余接口发送的通告报文生效，对子接口发送的通告报文不生效。

【举例】

```
# 配置当冗余成员接口的激活状态切换时，向邻居设备重新发送通告报文的次数为 10、时间间隔为 5 秒。  
<Sysname> system-view
```

```
[Sysname] reth advertise retransmit 10 interval 5
```

1.1.13 shutdown

shutdown 命令用来关闭以太网冗余接口/以太网冗余子接口。

undo shutdown 命令用来打开以太网冗余接口/以太网冗余子接口。

【命令】

shutdown

undo shutdown

【缺省情况】

以太网冗余接口/以太网冗余子接口处于开启状态。

【视图】

以太网冗余接口视图

以太网冗余子接口视图

【缺省用户角色】

network-admin

context-admin

【举例】

关闭以太网冗余接口 Reth1。

```
<Sysname> system-view
```

```
[Sysname] interface reth 1
```

```
[Sysname-Reth1] shutdown
```

1.1.14 sub-interface rate-statistic

sub-interface rate-statistic 命令用来开启以太网冗余子接口的速率统计功能。

undo sub-interface rate-statistic 命令用来关闭以太网冗余子接口的速率统计功能。

【命令】

sub-interface rate-statistic

undo sub-interface rate-statistic

【缺省情况】

以太网冗余子接口的速率统计功能处于关闭状态。

【视图】

以太网冗余接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启本功能后可能需要耗费大量系统资源，请谨慎使用。

配置该命令后，设备会定时统计以太网冗余接口下所有子接口的速率，用户可以通过 **display interface reth** 命令的 Last 300 seconds input rate 和 Last 300 seconds output rate 字段查看统计结果。

【举例】

开启以太网冗余接口 Reth1 的子接口速率统计功能。

```
<Sysname> system-view
[Sysname] interface reth 1
[Sysname-Reth1] sub-interface rate-statistic
```

【相关命令】

- **display interface reth**

2 冗余组

2.1 冗余组配置命令

2.1.1 bind slot

bind slot 命令用来将冗余组节点和 IRF 成员设备绑定。

undo bind slot 命令用来取消冗余组节点和 IRF 成员设备的绑定。

【命令】

```
bind slot slot-number
undo bind slot
```

【缺省情况】

冗余组节点未绑定成员设备。

【视图】

冗余组节点视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

slot-number: 设备在 IRF 中的成员编号。

【使用指导】

一个冗余组节点只能绑定一个成员设备。冗余组节点和成员设备绑定后，可以将这个成员设备上的部分接口添加到冗余组节点中作为冗余组节点的成员接口。这样，使用两个冗余组节点，就能实现一台成员设备上的部分接口和另一台成员设备上的部分接口互为备份。

一个成员设备只能和一个节点绑定。

冗余组节点下有成员接口时不能使用该命令修改绑定关系。

【举例】

将冗余组 **aaa** 节点 **1** 与成员设备 **1** 绑定。

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] node 1
[Sysname-redundancy-group-aaa-node1] bind slot 1
```

2.1.2 display redundancy group

display redundancy group 命令用来显示冗余组的相关信息。

【命令】

display redundancy group [*group-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

group-name: 冗余组的名称，为 1~15 个字符的字符串，区分大小写。不指定该参数时，显示所有冗余组的相关信息。

【举例】

显示冗余组 aaa 的相关信息。

<Sysname> display redundancy group aaa

Redundancy group aaa (ID 1):

Node ID	Slot	Priority	Status	Track weight
1	Slot1	100	Secondary	-255
2	Slot2	99	Primary	255

Preempt delay time remained : 0 min
Preempt delay timer setting : 1 min
Remaining hold-down time : 0 sec
Hold-down timer setting : 300 sec
Manual switchover request : No

Member interfaces:

Reth1 Reth2

Node 1:

Node member	Physical status
GE1/0/2	DOWN
GE1/0/4	DOWN(redundancy down)

Track info:

Track	Status	Reduced weight	Interface
1	Negative(Faulty)	255	GE1/0/2
2	Negative	255	GE1/0/4

Node 2:

Node member	Physical status
GE2/0/2	UP
GE2/0/4	UP

Track info:

Track	Status	Reduced weight	Interface

3	Positive	55	GE2/0/2
4	Positive	55	GE2/0/4

表2-1 display redundancy group 命令显示信息描述表

字段	描述
Redundancy group aaa (ID 1)	冗余组aaa（该冗余组的编号为1）
Node ID	冗余组节点的编号
Priority	节点的优先级
Status	对应节点当前所处的状态： • Primary：当前节点为主节点，能够正常收发报文 • Secondary：当前节点为备节点；当优先级高的节点为备节点时，节点上的所有成员接口会被冗余组强制设置为 Down 状态，不能收发报文；当优先级低的节点为备节点时，节点的所有成员接口能够正常收发报文，为主节点分担流量
Track weight	节点的当前权重值
Preempt delay time remained	剩余的倒回延时，单位为分钟
Preempt delay timer setting	配置的倒回延时，单位为分钟
Remaining hold-down time	剩余的状态保持时间，单位为秒
Hold-down timer setting	配置的状态保持时间，单位为秒
Manual switchover request	手工倒换请求，取值为： • Yes：表示存在手动倒换请求 • No：表示无倒换请求
Member interfaces	冗余组中添加的以太网冗余接口
Node 1	冗余组节点的详细信息
Node member	冗余组节点的成员接口
Physical status	成员接口的物理状态： • Down(redundancy down)：表示该接口被 Reth 模块关闭，即接口状态为冗余关闭 • Down：表示该接口的管理状态为开启，但物理状态为关闭（可能因为没有物理连线或者线路关闭） • Up：该接口的管理状态和物理状态均为开启
Track info	冗余组节点关联的Track项的信息
Track	Track项的编号
Status	Track项的状态。在优先级高的节点中，首个状态变为NotReady或Negative的Track项会被标识为Faulty
Reduced weight	Track项的权重增量
Interface	Track项的关联接口。如果显示为Absent，则表示该接口当前不在位

2.1.3 hold-down-interval

hold-down-interval 命令用来配置冗余组节点状态的保持时间，这段时间内不能发生主备倒换。

undo hold-down-interval 命令用来恢复缺省情况。

【命令】

hold-down-interval *second*

undo hold-down-interval

【缺省情况】

冗余组节点状态的保持时间为 1 秒。

【视图】

冗余组视图

【缺省用户角色】

network-admin

context-admin

【参数】

second：保持时间，取值范围为 0~1800，单位为秒。

【使用指导】

当网络不稳定，监测接口/链路状态频繁改变，会导致 Track 项状态在短时间内频繁改变，连带导致冗余组需要不断的响应主备倒换事件，使用保持定时器可以避免这种情况的发生。当节点完成主备倒换后，系统启动保持定时器。在保持时间内，不允许再次发生主备倒换。

【举例】

将冗余节点的状态保持时间配置为 300 秒。

```
<Sysname> system-view
```

```
[Sysname] redundancy group aaa
```

```
[Sysname-redundancy-group-aaa] hold-down-interval 300
```

2.1.4 member interface

member interface 命令用来将以太网冗余接口加入冗余组。

undo member interface 命令用来将以太网冗余接口从冗余组下删除。

【命令】

member interface *reth interface-number* [**quick-fallback**]

undo member interface *reth interface-number*

【缺省情况】

冗余组下不存在以太网冗余接口。

【视图】

冗余组视图

【缺省用户角色】

network-admin
context-admin

【参数】

reth interface-number: 已经创建的以太网冗余接口的编号，取值范围为设备上已创建的以太网冗余接口的编号。

quick-fallback: 表示以太网冗余接口跟随冗余组进行倒换，优先级高的接口从 **active** 状态变为 **inactive** 状态时，接口的物理状态不会被设置为 **Down**，仅将该接口的协议状态设置为 **Down**。不指定该参数时，如果以太网冗余接口跟随冗余组进行倒换，以太网冗余接口的当前激活接口的物理状态和协议状态均会被设置为 **Down**。当配置冗余组节点的倒回延时为秒级时，建议配置该参数。

【使用指导】

一个以太网冗余接口只能加入一个冗余组。

一个冗余组下最多可以加入 32 个以太网冗余接口。

【举例】

```
# 将以太网冗余接口 Reth1 加到冗余组 aaa 中。  
<Sysname> system-view  
[Sysname] redundancy group aaa  
[Sysname-redundancy-group-aaa] member interface reth 1
```

2.1.5 node

node 命令用来创建冗余组节点，并进入冗余组节点视图。如果指定的冗余组节点已经存在，则直接进入冗余组节点视图。

undo node 命令用来删除冗余组节点。

【命令】

```
node node-id  
undo node node-id
```

【缺省情况】

不存在冗余组节点。

【视图】

冗余组视图

【缺省用户角色】

network-admin
context-admin

【参数】

node-id: 表示冗余组节点编号，取值范围为 1~2。

【使用指导】

每个冗余组下最多可创建两个冗余组节点，这两个冗余组节点为主备关系。

当冗余组节点绑定了 IRF 成员设备时，不能删除该冗余组节点。

【举例】

```
# 在冗余组 aaa 下，创建冗余组节点 1。  
<Sysname> system-view  
[Sysname] redundancy group aaa  
[Sysname-redundancy-group-aaa] node 1
```

【相关命令】

- **bind slot**

2.1.6 node-member interface

node-member interface 命令用来将物理以太网接口和冗余组节点绑定。

undo node-member interface 命令用来消物理以太网接口和冗余组节点的绑定。

【命令】

```
node-member interface interface-type interface-number  
undo node-member interface interface-type interface-number
```

【缺省情况】

冗余组节点下不存在成员接口。

【视图】

冗余组节点视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

interface-type interface-number: 接口类型和编号。该接口必须是冗余组节点绑定的 IRF 成员设备上的物理接口。

【使用指导】

执行本命令前，请先执行 **bind slot** 命令。否则，本命令执行失败。

本命令中指定的接口不能是以太网冗余接口的成员接口。

一个接口加入一个冗余组节点后，就不能再加入其它的冗余组节点。

【举例】

```
# 将接口 GigabitEthernet1/0/1 和冗余组 aaa 的节点 1 绑定。  
<Sysname> system-view  
[Sysname] redundancy group aaa  
[Sysname-redundancy-group-aaa] node 1  
[Sysname-redundancy-group-aaa-node1] node-member interface gigabitethernet 1/0/1
```

【相关命令】

- **bind slot**

2.1.7 preempt-delay

preempt-delay 命令用来配置冗余组节点的倒回延时。

undo preempt-delay 命令用来恢复情况。

【命令】

preempt-delay seconds sec

undo preempt-delay

【缺省情况】

冗余组节点的倒回延时为 1 分钟（60 秒）。

【视图】

冗余组视图

【缺省用户角色】

network-admin

context-admin

【参数】

seconds sec: 冗余组将业务倒回到高优先级节点的等待时间，取值范围为 0~720，单位为秒。

【使用指导】

当冗余组内优先级高的节点倒回条件就绪时（譬如故障恢复），会触发倒回事件，但启动倒回定时器。由于需要整体倒回，在冗余组倒回的过程中会同时触发很多事件（比如接口状态变化等），这些事件的处理需要时间。倒回定时器能够为冗余组提供一段时间，让节点准备完毕后，再将业务从优先级低的节点倒换到优先级高的节点。

将冗余组节点的倒回延时配置为 0 时，表示不允许自动倒回，但可以手工倒回。

【举例】

配置冗余组 aaa 的倒回等待时间为 2 分钟。

```
<Sysname> system-view
```

```
[Sysname] redundancy group aaa
```

```
[Sysname-redundancy-group-aaa] preempt-delay 2
```

配置冗余组 aaa 的倒回等待时间为 120 秒。

```
<Sysname> system-view
```

```
[Sysname] redundancy group aaa
```

```
[Sysname-redundancy-group-aaa] preempt-delay seconds 120
```

2.1.8 priority

priority 命令用来配置冗余组节点的优先级。

undo priority 命令用来恢复缺省情况。

【命令】

priority priority

undo priority

【缺省情况】

冗余组节点的优先级为 1。

【视图】

冗余组节点视图

【缺省用户角色】

network-admin

context-admin

【参数】

priority: 冗余组节点的优先级，取值范围为 1~255。数值越大，节点的优先级越高。

【使用指导】

缺省情况下，优先级高的冗余组节点为主节点，优先级低的为备节点。当冗余组下两个节点优先级相同时，编号小的为主节点，编号大的为备节点。

【举例】

将冗余组 **aaa** 节点 1 的优先级设置为 3。

```
<Sysname> system-view
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] node 1
[Sysname-redundancy-group-aaa-node1] priority 3
```

2.1.9 redundancy group

redundancy group 命令用来创建冗余组，并进入该冗余组视图。如果指定的冗余组已经存在，则直接进入该冗余组视图。

undo redundancy group 命令用来删除冗余组。

【命令】

redundancy group *group-name*

undo redundancy group *group-name*

【缺省情况】

不存在冗余组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-name: 冗余组的名称，为 1~15 个字符的字符串，区分大小写。

【使用指导】

当冗余组中还有冗余接口或冗余组节点时，不能删除该冗余组。

【举例】

```
# 创建名称为 aaa 的冗余组。  
<Sysname> system-view  
[Sysname] redundancy group aaa
```

2.1.10 snmp-agent trap enable rddc

snmp-agent trap enable rddc 命令用来开启冗余组告警功能。

undo snmp-agent trap enable rddc 命令用来关闭冗余组告警功能。

【命令】

```
snmp-agent trap enable rddc  
undo snmp-agent trap enable rddc
```

【缺省情况】

冗余组告警功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

开启冗余组告警功能后，在冗余组人工倒换、故障接口恢复、故障接口生成时，会生成告警信息，并将该信息发送到设备的 SNMP 模块。通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关特性。

有关告警信息的详细描述，请参见“网络管理和监控配置指导”中的“SNMP”。

【举例】

```
# 开启冗余组告警功能。  
<Sysname> system-view  
[Sysname] snmp-agent trap enable rddc
```

2.1.11 switchover request

switchover request 命令用来手工触发指定冗余组进行主备倒换，让冗余组工作在优先级低的节点。

【命令】

```
switchover request
```

【视图】

冗余组视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

当冗余组主备结点无故障，业务运行在优先级高的节点时，用户可通过此命令触发冗余组主备倒换，让业务运行到备结点，以使用户可更换主节点上的部件。

【举例】

```
# 手工触发指定冗余组的主备倒换。  
<Sysname> system-view  
[Sysname] redundancy group aaa  
[Sysname-redundancy-group-aaa] switchover request
```

【相关命令】

- **switchover reset**

2.1.12 switchover reset

switchover reset 命令用来手工触发一次冗余组倒回，让冗余组工作在优先级高的节点。

【命令】

switchover reset

【视图】

冗余组视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

当冗余组主备结点无故障，业务运行在优先级低的节点时，用户可通过此命令手工触发冗余组进行倒回。

【举例】

```
# 在冗余组 aaa 内手动触发一次倒回。  
<Sysname> system-view  
[Sysname] redundancy group aaa  
[Sysname-redundancy-group-aaa] switchover reset
```

【相关命令】

- **preempt-delay**
- **switchover request**

2.1.13 track

track 命令用来关联 Track 项。

undo track 命令用来取消关联。

【命令】

```
track track-entry-number [ reduced weight-reduced ] [ interface  
interface-type interface-number ]  
undo track track-entry-number
```

【缺省情况】

冗余组节点下未关联 Track 项。

【视图】

冗余组节点视图

【缺省用户角色】

network-admin
context-admin

【参数】

track-entry-number: Track 项的序号，取值范围为 1~1024。

reduced weight-reduced: 权重的变化值，取值范围为 1~255，缺省值为 255。

interface interface-type interface-number: Track 项关联接口的类型和编号。当影响 Track 项状态改变的接口是以太网冗余接口的成员接口或是冗余组节点的成员接口时，建议配置该参数，并将该参数配置成与 Track 项接口一致。不指定本参数，则表示 Track 项未关联接口。

【使用指导】

一个节点最多能够配置 64 个 Track 项。

建议先创建 Track 项，再将该 Track 项和冗余组关联。否则，可能会导致冗余组没有有效的 Track 项来触发倒换。

当已将某物理接口配置为某冗余组内高优先级冗余组节点的成员接口，或者为某冗余组内以太网冗余接口的高优先级成员接口时，请不要将该物理接口的子接口配置为该冗余组内高优先级冗余组节点的 Track 项关联接口。因为物理接口被协议关闭时，会导致其子接口状态为 Down，该子接口将无法触发自动倒回，此时，需要手工倒回。

【举例】

将冗余组 aaa 和 track 1 关联并指定关联接口为 gigabitethernet 1/0/1；将冗余组 aaa 和 track 2 关联并指定关联接口为 GigabitEthernet 1/0/2。

```
<Sysname> system-view  
[Sysname] track 1 interface gigabitethernet 1/0/1  
[Sysname] track 2 interface gigabitethernet 1/0/2  
[Sysname] redundancy group aaa  
[Sysname-redundancy-group-aaa] node 1  
[Sysname-redundancy-group-aaa-node1] track 1 reduced 50 interface gigabitethernet 1/0/1  
[Sysname-redundancy-group-aaa-node1] track 2 reduced 50 interface gigabitethernet 1/0/2
```


目 录

1 进程分布优化.....	1-1
1.1 进程分布优化配置命令.....	1-1
1.1.1 affinity location-set	1-1
1.1.2 affinity location-type	1-1
1.1.3 affinity program	1-2
1.1.4 affinity self.....	1-3
1.1.5 display ha service-group	1-4
1.1.6 display placement location.....	1-6
1.1.7 display placement policy	1-6
1.1.8 display placement program	1-7
1.1.9 display placement reoptimize	1-8
1.1.10 placement program	1-9
1.1.11 placement reoptimize	1-10

1 进程分布优化

1.1 进程分布优化配置命令

1.1.1 affinity location-set

affinity location-set 命令用来配置进程对于节点位置的偏好。

undo affinity location-set 命令用来取消进程对于指定节点位置的偏好。

【命令】

```
affinity location-set { slot slot-number }&<1-5> { attract strength | default  
| none | repulse strength }  
undo affinity location-set { slot slot-number }&<1-5>
```

【缺省情况】

系统未配置进程对节点位置的偏好。

【视图】

分布策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。

&<1-5>: 表示前面的参数最多可以输入 5 次。

attract strength: 正向偏好程度，表示希望运行在该位置。**strength** 表示偏好程度，取值范围为 1~100000。值越大表示进程运行在该位置的可能性越大。

default: 缺省偏好，取值为正向偏好 200。

none: 配置偏好为 0，即主控进程对具体节点没有偏好，主控进程的运行位置由系统来决定。

repulse strength: 反向偏好程度，表示不希望运行在该位置。**strength** 表示偏好程度，取值范围为 1~100000。值越大表示进程运行在该位置的可能性越小。

【举例】

配置 staticroute 对于指定 slot 的正向偏好为 500。

```
<Sysname> system-view  
[Sysname] placement program staticroute  
[Sysname-program-staticroute] affinity location-set slot 1 attract 500
```

1.1.2 affinity location-type

affinity location-type 命令用来配置进程对于位置类型的偏好。

undo affinity location-type 命令用来取消进程对于指定位置类型的偏好。

【命令】

```
affinity location-type { current | paired | primary } { attract strength |  
default | none | repulse strength }  
undo affinity location-type { current | paired | primary }
```

【缺省情况】

系统未配置进程对位置类型的偏好。

【视图】

分布策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

current: 用来配置对主控进程当前运行位置的偏好。主控进程当前运行位置可以通过 **display placement program** 命令查看。

paired: 用来配置对所有备份进程当前运行位置的偏好。

primary: 用来配置对主设备的偏好。

attract strength: 正向偏好程度，表示希望运行在该位置。*strength* 表示偏好程度，取值范围为 1~100000。值越大表示进程运行在该位置类型的可能性越大。

default: 缺省偏好，取值为正向偏好 200。

none: 配置偏好为 0，即主控进程对位置类型没有偏好，主控进程的运行位置由系统来决定。

repulse strength: 反向偏好程度，表示不希望运行在该位置。*strength* 表示偏好程度，取值范围为 1~100000。值越大表示进程运行在该位置类型的可能性越小。

【举例】

```
# 配置 staticroute 对于当前位置的正向偏好为 500。  
<Sysname> system-view  
[Sysname] placement program staticroute  
[Sysname-program-staticroute] affinity location-type current attract 500
```

【相关命令】

- **affinity location-set**
- **affinity program**

1.1.3 affinity program

affinity program 命令用来配置进程和其它进程运行在同一位置的偏好。

undo affinity program 命令用来取消本进程和指定进程运行在同一位置的偏好。

【命令】

```
affinity program program-name { attract strength | default | none | repulse  
strength }  
undo affinity program program-name
```

【缺省情况】

未配置进程和其它进程运行在同一位置的偏好。

【视图】

分布策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

program-name: 为当前设备上正在运行的进程的名称, 为 1~15 个字符的字符串, 不区分大小写。

用户可以通过 **display placement program all** 命令查看设备上正在运行的进程。

attract strength: 正向偏好程度, 表示希望运行在该位置。**strength** 表示偏好程度, 取值范围为 1~100000。值越大表示进程运行于同一位置的可能性越大。

default: 缺省偏好, 取值为正向偏好 200。

none: 配置偏好为 0, 即主控进程对于是否和其它进程运行在同一位置没有偏好, 主控进程的运行位置由系统来决定。

repulse strength: 反向偏好程度, 表示不希望运行在该位置。**strength** 表示偏好程度, 取值范围为 1~100000。值越大表示进程运行于同一位置的可能性越小。

【举例】

配置 staticroute 和 syslog 运行于同一位置的偏好为反向 200。

```
<Sysname> system-view
```

```
[Sysname] placement program staticroute
```

```
[Sysname-program-staticroute] affinity program syslog repulse 200
```

【相关命令】

- **affinity location-set**
- **affinity location-type**

1.1.4 affinity self

affinity self 命令用来配置本进程所有实例运行于同一位置的偏好。

undo affinity self 命令用来恢复缺省情况。

【命令】

```
affinity self { attract strength | default | none | repulse strength }
```

```
undo affinity self
```

【缺省情况】

进程未配置所有实例运行于同一位置的偏好。

【视图】

分布策略视图

【缺省用户角色】

network-admin
context-admin

【参数】

attract strength: 正向偏好程度，表示希望运行在该位置。*strength* 表示偏好程度，取值范围为 1~100000。值越大表示进程运行于同一位置的可能性越大。

default: 缺省偏好，取值为正向偏好 200。

none: 配置偏好为 0，即进程对所有实例是否运行于同一位置没有偏好，运行位置由系统来决定。

repulse strength: 反向偏好程度，表示不希望运行在该位置。*strength* 表示偏好程度，取值范围为 1~100000。值越大表示进程运行于同一位置的可能性越小。

【使用指导】

该配置用以决定一个进程的多个实例是否运行于同一个位置上，如果进程只有一个实例，则该配置不会产生作用。

本命令在进程的分布策略视图和进程任意实例的分布策略视图下配置效果相同，均对所有实例生效。多次配置该命令，最新配置生效。

进程是否包含多个实例可以通过 **display placement program all** 命令查看。

【举例】

配置 staticroute 进程所有实例运行于同一位置的偏好为反向 200。

```
<Sysname> system-view  
[Sysname] placement program staticroute  
[Sysname-program-staticroute] affinity self repulse 200
```

【相关命令】

- **affinity location-set**
- **affinity location-type**

1.1.5 display ha service-group

display ha service-group 命令用来显示服务组的信息。

【命令】

```
display ha service-group { service-group-name [ instance instance-name ] | all }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

service-group-name: 为当前设备上正在运行的服务组的名称，为 1~15 个字符的字符串，不区分大小写。

instance instance-name: 表示服务组的实例的名称，为 1~31 个字符的字符串，不区分大小写。

all: 表示当前设备上运行的所有服务组。

【使用指导】

服务组是进程的集合。目前，大部分服务组只包含一个进程。如果进程支持实例，则服务组也有相应的实例。

【举例】

```
# 显示所有服务组的信息。
<Sysname> display ha service-group all
Service Group          Current Location      State
-----
syslog                 1/0                  Realtime Backup
其它显示信息略……

# 显示指定服务组 staticroute 的信息。
<Sysname> display ha service-group staticroute
Service Group          Current Location      State
-----
staticroute            1/0 (Active)         Realtime Backup

Detailed information about services of the program:
Service                PID    Type    Location  State
-----
ifm                    200    Active  1/0       Realtime Backup
staticroute            200    Active  1/0       Realtime Backup
```

表1-1 display ha service-group 命令显示信息描述表

字段	描述
Service Group	服务组的名称
Current Location	服务组主控进程当前运行的位置
State	服务组主控进程和备份进程的备份状态
Detailed information about services of the program	服务组包含的所有进程（包括主进程和备进程）的详细信息
Service	服务组内的服务的名称
PID	进程的编号
Type	进程的主备身份，取值为： - Active: 表示服务组主控进程 - Standby: 表示服务组备用进程
Location	当前服务主控进程的运行位置

字段	描述
State	进程的状态： • Realtime Backup: 实时备份状态 • Batch Backup: 批量备份状态 • Stopping: 停止状态 • Degrading: 降级状态 • Upgrading: 升级状态

1.1.6 display placement location

display placement location 命令用来显示具体位置上正在运行的进程信息。

【命令】

```
display placement location { all | slot slot-number }
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

all: 表示当前设备上运行的所有进程。

slot slot-number: 表示设备在 IRF 中的成员编号。

【举例】

```
# 显示所有正在运行的进程信息。
<Sysname> display placement location all
Program(s) placed at location: 1/0
    syslog
其它显示信息略……
```

1.1.7 display placement policy

display placement policy 命令用来显示进程的分布策略。

【命令】

```
display placement policy program { program-name | all | default }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

program-name: 显示指定进程的分布策略，为 1~15 个字符的字符串，不区分大小写。
all: 显示所有配置的进程分布策略。
default: 显示用户配置的缺省分布策略的信息。如果没有通过 **placement program default** 配置，则没有显示信息。

【使用指导】

只有为进程成功配置分布策略后，才会输出相应的显示信息。

【举例】

显示缺省分布策略的信息。
<Sysname> display placement policy program default
Program: [default] : source

affinity location-set slot 1 attract 500 : system [default]

表1-2 display placement policy 命令显示信息描述表

字段	描述
Program	进程的名称以及进程的分布策略。当执行 display placement policy program default 命令时，进程名会显示为[default]
source	进程分布策略的来源，如果显示 system [default] ，则表示采用系统缺省分布策略，该策略是通过 placement program default 命令进入缺省分布策略视图后再配置的；如果显示形如 system staticroute ，则表示采用staticroute进程分布策略，该策略是通过 placement program program-name 命令进入staticroute的分布策略视图后再配置的

1.1.8 display placement program

display placement program 命令用来显示主控进程的当前运行位置。

【命令】

display placement program { program-name | all }

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin

context-operator

【参数】

program-name: 为当前设备上正在运行的进程的名称, 为 1~15 个字符的字符串, 不区分大小写。
all: 表示当前设备上运行的所有进程。

【举例】

```
# 显示 staticroute 主控进程的当前运行位置。  
<Sysname> display placement program staticroute  
Program                      Placed at location  
-----  
staticroute                   1/0
```

表1-3 display placement program 命令显示信息描述表

字段	描述
Program	进程的名称
Placed at location	主控进程运行的位置 当显示为NA时表示该业务的主控进程异常或者正在启动

1.1.9 display placement reoptimize

display placement reoptimize 命令用来显示进程分布优化后的预测位置。

【命令】

```
display placement reoptimize program { program-name [ instance  
instance-name ] | all }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

program-name: 为当前设备上正在运行的、支持进程优化配置的进程的名称, 为 1~15 个字符的字符串, 不区分大小写。
instance instance-name: 表示实例名, 为 1~31 个字符的字符串, 不区分大小写。一个进程是否存在多个实例, 由系统软件决定。
all: 表示当前设备上运行的、支持进程优化配置的所有进程。

【举例】

显示分布优化后所有进程的预测位置。

```
<Sysname> display placement reoptimize program all
Predicted changes to the placement
Program                Current location      New location
-----
staticroute            1/0                  1/0
其它显示信息略……
```

以上显示信息中，**Program** 表示进程的名称，**Current location** 表示主控进程当前运行的位置，**New location** 表示分布优化后，主控进程将运行的位置。

1.1.10 placement program

placement program 命令用来进入进程的分布策略视图。

undo placement program 命令用来删除进程的分布策略。

【命令】

```
placement program { program-name [ instance instance-name ] | default }
undo placement program { program-name [ instance instance-name ] | default }
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

program-name: 用来进入指定进程的分布策略视图。**program-name** 表示当前设备上正在运行的进程的名称，为 1~15 个字符的字符串，不区分大小写。

instance instance-name: 用来进入指定进程指定实例的分布策略视图。**instance-name** 表示实例名，为 1~31 个字符的字符串，不区分大小写。未指定该参数时，进入进程的分布策略视图，进程分布策略视图下的配置对所有的实例生效。一个进程是否存在多个实例，由系统软件决定。

default: 用来进入缺省分布策略视图。进入该视图后，配置的是所有进程（所有实例）的缺省分布策略。

【使用指导】

进入进程的分布策略视图后，用户可以为进程配置分布策略，让多个业务的主控进程分散运行在不同节点上，从而提高设备 CPU、内存等资源的利用率。

对于进程的实例，优先使用实例的分布策略视图下的配置，再使用进程的分布策略视图下的配置，最后使用缺省分布策略视图下的配置；对于进程，优先使用进程的分布策略视图下的配置，再使用缺省分布策略视图下的配置。

分布策略的内容包括 **affinity location-type**、**affinity location-set**、**affinity program** 和 **affinity self**，这些命令从不同角度表达了用户对进程在某个位置运行的期望。

一个进程对应一个分布策略，所有的 **affinity** 命令可以同时配置。系统将根据用户的配置按照一定的算法，最后决定主控进程的预测位置（可以通过 **display placement reoptimize** 命令查看）。当发生主备倒换时，该位置的进程就能当选为主控进程，其它位置的进程则均为备份进程。

执行 **undo placement program** 后，系统会删除该进程视图下配置的所有分布策略。

【举例】

```
# 进入 staticroute 分布策略视图。
<Sysname> system-view
[Sysname] placement program staticroute
[Sysname-program-staticroute]
# 进入缺省分布策略视图。
<Sysname> system-view
[Sysname] placement program default
[Sysname-program-default]
```

1.1.11 placement reoptimize

placement reoptimize 命令用来优化进程运行位置，使进程分布策略生效。

【命令】

placement reoptimize

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

执行该命令后，系统会根据当前硬件的在位情况、主控进程的运行位置和状态、分布策略的配置来综合计算主控进程的新位置，并将该位置上的进程当选为主控进程，其它位置上的进程均为备份进程。如果新当选的主控进程和原主控进程不同，则会触发进程的主备倒换。可使用 **display placement program** 命令查看倒换后新主控进程的运行位置。

执行此命令时请保持系统的稳定性，不建议在执行此命令的过程中进行任务涉及进程的重启操作。

【举例】

```
# 手工进行进程分布优化。
<Sysname> system-view
[Sysname] placement reoptimize
Predicted changes to the placement
Program                Current location      New location
-----
staticroute            1/0                   1/0
Continue? [y/n]:y
Re-optimization of the placement start. You will be notified on completion
Re-optimization of the placement complete. Use 'display placement' to view the new placement
本举例仅选择 staticroute 进程作为示例，其它进程不在提示信息中罗列。
```

目 录

1 接口组联动	1-1
1.1 接口组联动配置命令	1-1
1.1.1 collaboration-group	1-1
1.1.2 collaboration-group clean	1-1
1.1.3 display collaboration-group	1-2
1.1.4 port	1-3
1.1.5 port collaboration-group	1-4
1.1.6 up-delay	1-5

1 接口组联动

1.1 接口组联动配置命令

1.1.1 collaboration-group

collaboration-group 命令用来创建联动组，并进入联动组视图。如果指定的联动组已经存在，则直接进入联动组视图。

undo collaboration-group 命令用来删除联动组。

【命令】

collaboration-group *group-id*

undo collaboration-group *group-id*

【缺省情况】

不存在联动组。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-id: 表示联动组的编号，取值范围 1~16。

【使用指导】

接口组联动功能通过将同一台设备上不同的接口加入到同一个联动组中，实现同一个联动组内接口状态之间相互关联，使得这些成员接口都具备或不具备报文传输能力。

只有全局开启了 Monitor Link 协议，创建的联动组才能生效。

删除联动组前，所有成员接口必须先退出该联动组。

【举例】

创建联动组 1，并进入联动组 1 的视图。

```
<Sysname> system-view
```

```
[Sysname] collaboration-group 1
```

```
[Sysname-collaboration-group1]
```

1.1.2 collaboration-group clean

collaboration-group clean 命令用来清除所有联动组中失效的成员接口。

【命令】

collaboration-group clean

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

当联动组内某个成员接口所在的单板被拔出或者更换了槽位时，此成员接口变为失效的成员接口。执行本命令可以清除所有联动组中失效的成员接口，避免因联动组内一个接口失效而造成该联动组的状态变为 **DOWN**。

执行本配置后，成员接口所在单板被重新插入或换回原槽位，此成员接口将不能自动加入原联动组。如果需要加入原联动组，请手工加入。

【举例】

```
# 清除所有联动组中失效的成员接口。
<Sysname> system-view
[Sysname] collaboration-group clean
```

1.1.3 display collaboration-group

display collaboration-group 命令用来显示联动组的信息。

【命令】

display collaboration-group { *group-id* | **all** } [**verbose**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

group-id: 显示指定联动组的信息。**group-id** 表示联动组的编号，取值范围 1~16。

all: 显示所有联动组的信息。

verbose: 显示详细信息。未指定本参数时，显示简要信息。

【举例】

```
# 显示所有联动组的简要信息。
<Sysname> display collaboration-group all
  Group ID           Group status
  1                  DOWN
  2                  DOWN

# 显示所有联动组的详细信息。
```

```

<Sysname> display collaboration-group all verbose
Collaboration group protocol status: Enabled
Collaboration group 1 information:
  Group status      : DOWN
  Member up delay   : 0 seconds
  Last up time      : 16:55:34 2017/04/05
  Last down time    : 16:57:22 2017/04/05
  Member            Status
  GE1/0/1           DOWN
  GE1/0/2           Collaboration-down

```

表1-1 display collaboration-group 命令显示信息描述表

字段	描述
Group ID	联动组编号
Group status	联动组的状态： - DOWN: 联动组内接口均处于关闭状态 - UP: 联动组内接口均处于 UP 状态 - N/A: 接口组联动功能协议全局关闭，此时接口组联动功能失效 - UP-Pending: 表示联动组处于由 DOWN 到 UP 的过渡状态，需要等待 10 秒联动组状态才能最终确定是 DOWN 或者 UP
Collaboration group protocol status	接口组联动功能协议的全局使能状态： - Enabled: 表示全局开启 - Disabled: 表示全局关闭
Collaboration group 1 information	联动组1的信息
Member up delay	联动组接口的回切延时，单位为秒
Last up time	联动组最近一次UP的时间
Last down time	联动组最近一次DOWN的时间
Member	联动组的成员接口
Status	成员接口的状态： - UP: 接口状态为 UP - DOWN: 接口被关闭。关于接口被关闭的原因，可以通过 display interface 命令查看 - Collaboration-down: 接口被接口组联动协议强制关闭 - Not available: 单板不在位时，接口处于失效状态

1.1.4 port

port 命令用来给联动组添加成员接口。

undo port 命令用来从联动组中将成员接口删除。

【命令】

```
port interface-type interface-number  
undo port interface-type interface-number
```

【缺省情况】

联动组中不存在成员接口。

【视图】

联动组视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

interface-type interface-number: 表示接口类型和接口编号。

【使用指导】

一个接口只能属于一个联动组。

请勿将联动组的成员接口加入冗余组。

请勿将一个动态聚合组的选中端口和非选中端口同时配置为同一个联动组的成员接口。

如果已将联动组中一个接口配置为 Monitor Link 组的上行接口/下行接口，请勿再将该联动组中其它接口配置为任何 Monitor Link 组的下行接口/上行接口。

使用接口视图下的 **port collaboration-group** 命令也可以将接口加入联动组。

【举例】

#将 GigabitEthernet1/0/1 加入联动组 1。

```
<Sysname> system-view  
[Sysname] collaboration-group 1  
[Sysname-collaboration-group1] port gigabitethernet 1/0/1
```

【相关命令】

- **port collaboration-group**

1.1.5 port collaboration-group

port collaboration-group 命令用来将接口加入联动组。

undo port collaboration-group 命令用来将成员接口从联动组中删除。

【命令】

```
port collaboration-group group-id  
undo collaboration-group group-id
```

【缺省情况】

接口不是联动组的成员接口。

【视图】

二层以太网接口视图
三层以太网接口视图
二层聚合接口视图
三层聚合接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

group-id: 表示联动组的编号，取值范围 1~16。

【使用指导】

一个接口只能属于一个联动组。

通过 **port collaboration-group** 命令将接口加入指定联动组前，必须确保指定联动组已创建，否则无法加入。

请勿将联动组的成员接口加入冗余组。

请勿将一个动态聚合组的选中端口和非选中端口同时配置为同一个联动组的成员接口。

如果已将联动组中一个接口配置为 Monitor Link 组的上行接口/下行接口，请勿再将该联动组中其它接口配置为任何 Monitor Link 组的下行接口/上行接口。

使用联动组视图下的 **port** 命令也可以将接口加入联动组。

【举例】

将 GigabitEthernet1/0/1 加入联动组 1。

```
<Sysname> system-view
[Sysname] collaboration-group 1
[Sysname-collaboration-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port collaboration-group 1
```

【相关命令】

- **port**

1.1.6 up-delay

up-delay 命令用来配置成员接口 UP 延时。

undo up-delay 命令用来恢复缺省情况。

【命令】

up-delay *delay*
undo up-delay

【缺省情况】

成员接口 UP 延时为 0 秒，即设备完成重启后，联动组的所有成员接口立即恢复为 UP 状态。

【视图】

联动组视图

【缺省用户角色】

network-admin

context-admin

【参数】

delay: 表示成员接口 UP 延时时间，取值范围为 1~3600，单位为秒。

【使用指导】

up-delay 命令的作用是在设备重启后，即便所有成员接口准备就绪，也会使联动组的成员接口在延迟指定时间后才变为 UP 状态。

【举例】

配置联动组 1 成员接口 UP 延时为 10 秒。

```
<Sysname> system-view
```

```
[Sysname] collaboration-group 1
```

```
[Sysname-collaboration-group1] up-delay 10
```



UNIS 入侵检测系统

网络管理和监控命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《网络管理和监控命令参考》主要介绍系统维护与调试、NQA、NTP、进程监控和维护、NETCONF、信息中心、SNMP、RMON、快速日志输出、报文捕获和 Event MIB 的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用 “[]” 括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由 “#” 号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号 “< >” 表示按钮名，如 “单击<确定>按钮”。
[]	带方括号 “[]” 表示窗口名、菜单名和数据表，如 “弹出[新建用户]窗口”。

格 式	意 义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 系统维护与调试	1-1
1.1 系统维护与调试命令	1-1
1.1.1 debugging	1-1
1.1.2 display debugging	1-2
1.1.3 ping	1-2
1.1.4 ping ipv6	1-5
1.1.5 tracert	1-7
1.1.6 tracert ipv6	1-10

1 系统维护与调试

1.1 系统维护与调试命令

1.1.1 debugging

debugging 命令用来打开指定模块的调试开关。

undo debugging 命令用来关闭指定模块的调试开关。

【命令】

debugging *module-name* [*option*]

undo debugging { **all** | *module-name* [*option*] }

【缺省情况】

所有模块的调试开关均处于关闭状态。

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

module-name: 模块名称，比如 arp、device 等。可以使用 **debugging ?** 命令查询设备当前支持的模块名。

option: 模块的调试选项。对于不同的模块，调试选项的数量和内容都不相同。可以使用 **debugging module-name ?** 命令查询设备当前支持的指定模块的调试选项。

all: 所有模块的调试开关。仅当需要关闭所有调试开关时可使用本参数。

【使用指导】

调试信息的输出会影响系统的运行效率，所以建议在进行网络故障诊断时根据需要打开某个功能模块的调试开关，不要同时打开多个功能模块的调试开关。

执行本命令后设备会将生成的调试信息发送到设备的信息中心模块，通过设置信息中心的参数，最终决定调试信息的输出规则（即是否允许输出以及输出方向）。有关调试信息输出规则的详细介绍请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

打开设备管理模块的调试开关。

```
<Sysname> debugging dev
```

```
This command is CPU intensive and might affect ongoing services. Are you sure you want to continue? [Y/N]:Y
```

【相关命令】

- **display debugging**

1.1.2 display debugging

display debugging 命令用来显示系统中已经打开的调试开关。

【命令】

display debugging [*module-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

module-name: 显示指定模块调试开关的设置情况。**module-name** 表示模块名，具体取值可通过执行 **display debugging ?** 命令来获取。如果不指定本参数，则显示所有打开的调试开关。

【举例】

```
# 显示所有打开的调试开关。  
<Sysname> display debugging  
DEV debugging switch is on
```

【相关命令】

- **debugging**

1.1.3 ping

ping 命令用来检查指定 IP 地址是否可达，并输出相应的统计信息。

【命令】

ping [**ip**] [-a *source-ip* | -c *count* | -f | -h *ttl* | -i *interface-type* *interface-number* | -m *interval* | -n | -p *pad* | -q | -r | -s *packet-size* | -t *timeout* | -tos *tos* | -v | -vpn-instance *vpn-instance-name*] * *host*

【视图】

任意视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip: 支持 IPv4 协议以及区分有特定字母的目的主机名。不指定该参数时，也表示支持 IPv4 协议。如果 **ping** 的目的主机名为 **i**、**ip**、**ipv**、**ipv6**、**l**、**ls**、**lsp** 时，需要先指定该关键字再指定主机名，如：**ping ip ip**。

-a source-ip: 指定 ICMP 回显请求 (ECHO-REQUEST) 报文的源 IP 地址。该地址必须是设备上已配置的 IP 地址。不指定该参数时, ICMP 回显请求报文的源 IP 地址是该报文出接口的主 IP 地址。

-c count: 指定 ICMP 回显请求报文的发送次数, 取值范围为 1~4294967295, 缺省值为 5。

-f: 将长度大于出接口 MTU 的报文直接丢弃, 即不允许对发送的 ICMP 回显请求报文进行分片。

-h ttl: 指定 ICMP 回显请求报文中的 TTL 值, 取值范围为 1~255, 缺省值为 255。

-i interface-type interface-number: 指定发送 ICMP 回显请求报文的接口的类型和编号。不指定该参数时, 将根据目的 IP 查找路由表或者转发表来确定发送 ICMP 回显请求报文的接口。

-m interval: 指定发送 ICMP 回显请求报文的时间间隔, 取值范围为 1~65535, 单位为毫秒, 缺省值为 200。

-n: 对 *host* 参数不进行域名解析。不指定该参数时, 如果 *host* 参数表示的是目的端的主机名, 则设备会对 *host* 进行域名解析。

-p pad: 指定 ICMP 回显请求报文的“PAD”字段的填充值, 为 1~8 位的 16 进制数, 取值范围为 0~FFFFFFFF。如果指定的参数不够 8 位, 则会在首部补 0, 使填充值达到 8 位。比如将 *pad* 设置为 0x2f, 则会重复使用 0x0000002f 去填充报文, 以使发送报文的总长度达到设备要求值。填充值从 0x01 开始, 逐渐递增, 直到 0xff, 然后又从 0x01 开始循环, 形如 0x010203……feff01……, 直至发送报文的总长度达到设备要求值。

-q: 只显示统计信息。不指定该参数时, 系统将显示包括统计信息在内的全部信息。

-r: 记录路由信息。不指定该参数时, 系统不记录路由。

-s packet-size: 指定发送的 ICMP 回显请求报文的长度 (不包括 IP 和 ICMP 报文头), 取值范围为 20~9600, 单位为字节, 缺省值为 56。

-t timeout: 指定 ICMP 回显应答 (ECHO-REPLY) 报文的超时时间, 发送 ICMP 回显请求报文 *timeout* 时长后还没有收到 ICMP 回显应答报文, 源端则认为 ICMP 回显应答报文超时。取值范围为 0~65535, 单位为毫秒, 缺省值为 2000。

-tos tos: 指定 ICMP 回显请求报文中的 ToS 域的值, 取值范围为 0~255, 缺省值为 0。

-v: 显示接收到的非回显应答的 ICMP 报文。不指定该参数时, 系统不显示非回显应答的 ICMP 报文。

-vpn-instance vpn-instance-name: 指定目的端所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示目的端位于公网中。

host: 目的端的 IP 地址或主机名。其中, 主机名为 1~253 个字符的字符串, 不区分大小写, 字符串仅可包含字母、数字、“-”、“_”或“.”。

【使用指导】

如果要使用目的端的主机名执行 ping 操作, 事先必须在设备上配置 DNS (Domain Name System, 域名系统) 功能, 否则会 ping 失败。

在执行命令过程中, 键入 <Ctrl+C> 可终止 ping 操作。

【举例】

检查 IP 地址为 1.1.2.2 的设备是否可达。

```
<Sysname> ping 1.1.2.2
```

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms
```

--- Ping statistics for 1.1.2.2 ---

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

检查私网 vpn1 中 IP 地址为 1.1.2.2 的设备是否可达。

```
<Sysname> ping -vpn-instance vpn1 1.1.2.2
```

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms
```

--- Ping statistics for 1.1.2.2 in VPN instance vpn1 ---

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

检查 IP 地址为 1.1.2.2 的设备是否可达，只显示检查结果。

```
<Sysname> ping -q 1.1.2.2
```

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
```

--- Ping statistics for 1.1.2.2 ---

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.962/2.196/2.665/0.244 ms
```

检查 IP 地址为 1.1.2.2 的设备是否可达，并显示路由信息。

```
<Sysname> ping -r 1.1.2.2
```

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
```

```
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms
```

```
RR:      1.1.2.1
         1.1.2.2
         1.1.1.2
         1.1.1.1
```

```
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=4.834 ms (same route)
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=4.770 ms (same route)
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=4.812 ms (same route)
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=4.704 ms (same route)
```

--- Ping statistics for 1.1.2.2 ---

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms
```

以上显示信息表明本设备与 1.1.2.2 之间路由可达，具体路由为 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2。

表1-1 ping 命令显示信息描述表

字段	描述
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break	检查IP地址为1.1.2.2的设备是否可达。每个ICMP回显请求报文中的数据为56字节，按组合键Ctrl+C可以终止ping操作
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms	收到IP地址为1.1.2.2的设备回复的ICMP响应报文，若超时仍没有收到ICMP响应报文，则不输出信息 - bytes 表示 ICMP 响应报文中的数据字节数 - icmp_seq 表示报文序号，用来判断报文是否有分组丢失、失序或重复 - ttl 表示 ICMP 响应报文中的 TTL 值 - time 表示响应时间
RR:	ICMP回显请求报文经过的路由器，采用倒序显示，距离目的端越近的路由器越先显示
--- Ping statistics for 1.1.2.2 ---	Ping操作中收发数据的统计结果
--- Ping statistics for 1.1.2.2 in VPN instance vpn1 ---	在VPN实例中执行Ping操作，Ping过程中收发数据的统计结果
5 packet(s) transmitted	发送的ICMP回显请求报文数
5 packet(s) received	收到的ICMP响应报文数
0.0% packet loss	未响应请求报文占发送的总请求报文的百分比
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms	响应时间的最小值、平均值、最大值和标准方差，单位为毫秒

1.1.4 ping ipv6

ping ipv6 命令用来检查指定 IPv6 地址是否可达，并输出相应的统计信息。

【命令】

```
ping ipv6 [ -a source-ipv6 | -c count | -i interface-type interface-number |
-m interval | -q | -s packet-size | -t timeout | -tc traffic-class | -v |
-vpn-instance vpn-instance-name ] * host
```

【视图】

任意视图

【缺省用户角色】

network-admin
context-admin

【参数】

-a source-ipv6: 指定 ICMPv6 回显请求报文中的源 IPv6 地址。该地址必须是设备上已配置的合法 IPv6 地址。不指定该参数时，ICMPv6 回显请求报文的源 IPv6 地址是该报文出接口的地址（地址选择原则遵循 RFC 3484）。

-c count: 指定发送的 ICMPv6 回显请求报文的数目，取值范围为 1~4294967295，缺省值为 5。

-i interface-type interface-number: 指定出接口的接口类型与接口编号。对端是组播地址或者是链路本地地址则必须指定此参数。不指定该参数时，将根据目的 IP 查找路由表或者转发表来确定发送 ICMPv6 回显请求报文的接口。

-m interval: 指定发送 ICMPv6 回显请求报文的时间间隔，取值范围为 1~65535，单位为毫秒，缺省值为 1000。

-q: 只显示统计信息。不指定该参数时，系统将显示包括统计信息在内的全部信息。

-s packet-size: 指定发送的 ICMPv6 回显请求报文的长度（不包括 IPv6 和 ICMPv6 报文头），取值范围为 20~9600，单位为字节，缺省值为 56。

-t timeout: 指定 ICMPv6 回显应答报文的超时时间，取值范围为 0~65535，单位为毫秒，缺省值为 2000。

-tc traffic-class: IPv6 ICMP 报文中的 Traffic Class 域的值。取值范围为 0~255，缺省值为 0。

-v: 显示 ICMPv6 回显应答报文的详细信息。不指定该参数时，显示 ICMPv6 回显应答报文的简要信息。详细信息比简要信息多 dst 和 idx 字段，dst 表示回显应答报文的地址，idx 表示回显应答报文的入接口索引。

-vpn-instance vpn-instance-name: 指定目的端所属的 VPN 实例。vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的端位于公网中。

host: 目的端的 IPv6 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

【使用指导】

如果要使用目的端的主机名执行 ping ipv6 操作，事先必须在设备上配置 DNS 功能，否则 IPv6 ping 操作将会失败。

在执行命令过程中，键入<Ctrl+C>可终止 ping ipv6 操作。

【举例】

检查 IPv6 地址为 2001::2 的设备是否可达。

```
<Sysname> ping ipv6 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 time=16.000 ms
```

```
--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

检查 IPv6 地址为 2001::2 的设备是否可达，只显示统计信息。

```
<Sysname> ping ipv6 -q 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break
```

```
--- Ping6 statistics for 2001::2 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
# 检查 IPv6 地址为 2001::2 的设备是否可达，显示详细 ping 信息。
<Sysname> ping ipv6 -v 2001::2
Ping6(56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break
56 bytes from 2001::2, icmp_seq=0 hlim=64 dst=2001::1 idx=3 time=62.000 ms
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=23.000 ms
56 bytes from 2001::2, icmp_seq=2 hlim=64 dst=2001::1 idx=3 time=20.000 ms
56 bytes from 2001::2, icmp_seq=3 hlim=64 dst=2001::1 idx=3 time=4.000 ms
56 bytes from 2001::2, icmp_seq=4 hlim=64 dst=2001::1 idx=3 time=16.000 ms

--- Ping6 statistics for 2001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.000/25.000/62.000/20.000 ms
```

以上信息表明，目的端可达，源端发出的 ICMPv6 回显请求报文均能得到回应，报文往返时间的最小值、平均值、最大值和标准方差分别为 4ms、25ms、62ms 和 20ms。

表1-2 ping ipv6 命令显示信息描述表

字段	描述
Ping6 (56 data bytes) 2001::1 --> 2001::2, press CTRL_C to break	从源地址2001::1给目的地址2001::2发送一个ICMPv6回显请求报文，每个ICMPv6回显请求报文中的数据为56字节，按组合键Ctrl+C可以终止IPv6 ping操作
56 bytes from 2001::2, icmp_seq=1 hlim=64 dst=2001::1 idx=3 time=62.000 ms	收到IPv6地址为2001::2的设备回复的ICMPv6响应报文，其中： • 数据字节数为 56 • 报文序号为 1 • hop limit 值为 64 • 目的地址为 2001::1（使用-v 参数时才显示该字段） • 报文入接口的索引为 3（使用-v 参数时才显示该字段） • 响应时间是 62ms
--- Ping6 statistics for 2001::2 ---	IPv6 ping操作中收发数据的统计结果
5 packet(s) transmitted	发送的ICMPv6回显请求报文数
5 packet(s) received	收到的ICMPv6响应报文数
0.0% packet loss	未响应请求报文占发送的总请求报文的百分比
round-trip min/avg/max/ std-dev =4.000/25.000/62.000/20.000 ms	响应时间的最小值、平均值、最大值和标准方差，单位为毫秒

1.1.5 tracert

tracert 命令用来查看 IPv4 报文从源端传到目的端所经过的路径。

【命令】

```
tracert [ -a source-ip | -f first-ttl | -m max-ttl | -p port | -q packet-number  
| -t tos | -vpn-instance vpn-instance-name [ -resolve-as { global | none |  
vpn } ] | -w timeout ] * host
```

【视图】

任意视图

【缺省用户角色】

network-admin

context-admin

【参数】

-a source-ip: 指定 tracert 报文的源 IP 地址。该地址必须是设备上已配置的合法 IP 地址。不指定该参数时，tracert 报文的源 IP 地址是该报文出接口的主 IP 地址。

-f first-ttl: 指定一个初始 TTL，即第一个报文所允许的最大跳数。取值范围为 1~255，且小于或等于最大 TTL，缺省值为 1。

-m max-ttl: 指定一个最大 TTL，即一个报文所允许的最大跳数。取值范围为 1~255，且大于或等于初始 TTL，缺省值为 30。

-p port: 指定目的端的 UDP 端口号，取值范围为 1~65535，缺省值为 33434。用户一般不需要更改此选项。当 tracert 的目的地址为远端 LISP 站点的 EID 地址时，目的端的 UDP 端口号必须大于或等于 33434。

-q packet-number: 指定每次发送的探测报文个数，取值范围为 1~65535，缺省值为 3。

-t tos: Tracert 报文中 ToS 域的值。取值范围为 0~255，缺省值为 0。

-vpn-instance vpn-instance-name: 指定目的端所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的端位于公网中。

-resolve-as: 指定从哪个路由表中解析 AS 号。使用该参数，能够帮助用户了解 Tracert 路径中三层设备所属 AS 的编号。不指定该参数时，表示从公网路由表解析 AS 号。

global: 表示从公网路由表解析 AS 号。指定该参数后，Tracert 在显示公网三层设备的地址信息时，会同时显示该地址对应的 AS 号。如果公网路由表中没有记录该地址的 AS 号，则不显示。

none: 表示不解析 AS 号。Tracert 显示信息中不会携带 AS 号。

vpn: 表示从当前 VPN 的路由表解析 AS 号。指定该参数后，Tracert 在显示当前 VPN 中三层设备的地址信息时，会同时显示该地址对应的 AS 号。如果当前 VPN 路由表中没有记录该地址的 AS 号，则不显示。

-w timeout: 指定探测报文的响应报文的超时时间，取值范围是 1~65535，单位为毫秒，缺省值为 5000。

host: 目的端的 IP 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

【使用指导】

tracert 命令用来查看 IPv4 报文从源端传到目的端所经过的路径。

当用户使用 **ping** 命令测试发现网络出现故障后，可以用 **tracert** 命令分析出现故障的网络节点。

当目的地址为公网地址时，设备会自动从公网路由表解析 AS 号，如果存在则显示。当目的地址为私网地址时，路径上的三层设备的地址可能存在于公网路由表或私网路由表，这时需要用户执行两次 **tracert** 命令，分别指定 **global** 参数和 **vpn** 参数，然后根据网络拓扑确定源端到目的端实际途经的 AS。

tracert 命令的输出信息包括到达目的端所经过的所有三层设备的 IP 地址，如果某设备不能回应 ICMP 错误消息（可能因为路由不可达或者没有开启 ICMP 错误报文处理功能），则输出 “* * *”。在 Tracert 过程中，并且中间设备开启了 ICMP 不可达报文处理功能（参考 **ip unreachable enable** 命令），如果命令执行结果中显示以下字符，则表示目的设备已不可达，设备会停止发包，Tracert 过程停止。

- !N: 表示网络不可达。
- !H: 表示目的主机不可达。
- !P: 表示协议不可达（未知的协议号）。
- !F: 表示需要进行分片但中间设备设置了不分片导致的不可达。
- !W: 表示未知的目的主机不可达，即目的主机不存在。
- !Q: 表示目的网络不可达的服务类型不可达，即不可用的服务类型（网络）。
- !T: 表示目的主机不可达的服务类型不可达，即不可用的服务类型（主机）。
- !X: 表示管理禁止通信不可达，即通信被过滤策略禁止。
- !V: 表示违反主机优先级不可达，即报文优先级为 **src/dst/port** 不赞许的优先级，则报文不被允许转发。
- !C: 表示优先级终止生效不可达，即报文优先级被终止生效而不允许转发。

在执行命令过程中，键入<Ctrl+C>可终止此次 **tracert** 操作。

【举例】

查看报文从源端到目的端（IP 地址为 1.1.2.2）所经过的路径。

```
<Sysname> tracert 1.1.2.2
tracert to 1.1.2.2 (1.1.2.2), 30 hops at most, 40 bytes each packet, press CTRL_C to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms
```

查看报文从源端到目的端（IP 地址为 1.1.3.2，属于 vpn1）所经过的路径，并显示报文经过的私网中的三层设备的 AS 信息。

```
<Sysname> tracert -vpn-instance vpn1 -resolve-as vpn 1.1.3.2
tracert to 1.1.3.2 (1.1.3.2), 30 hops at most, 40 bytes each packet, press CTRL_C to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) 580 ms 470 ms 80 ms
 3  1.1.3.2 (1.1.3.2) [AS 65535] 530 ms 472 ms 380 ms
```

表1-3 tracert 命令显示信息描述表

字段	描述
tracert to 1.1.2.2 (1.1.2.2)	查看IP报文从当前设备传到地址为1.1.2.2的设备所经过的路径
hops at most	探测报文的最大跳数，可使用 -m 参数配置
bytes each packet	探测报文字节数

字段	描述
press CTRL_C to break	在执行命令过程中，键入<Ctrl+C>可终止此次tracert操作
2 1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms	TTL值为2的探测报文的探测结果，内容包括：第二跳的域名（如果没有配置域名则显示IP地址）、IP地址、所属AS号（如果不存在则不显示）、三份探测报文的往返时间 每次发送探测报文的份数可以使用 -q 参数配置
1 1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms	TTL值为1的探测报文的探测结果，内容包括：第一跳的域名（如果没有配置域名则显示IP地址）、IP地址、三份探测报文的往返时间 每次发送探测报文的份数可以使用 -q 参数配置

1.1.6 tracert ipv6

tracert ipv6 命令用来查看 IPv6 报文从源端传到目的端所经过的路径。

【命令】

```
tracert ipv6 [ -f first-hop | -m max-hops | -p port | -q packet-number | -t traffic-class | -vpn-instance vpn-instance-name [ -resolve-as { global | none | vpn } ] | -w timeout ] * host
```

【视图】

任意视图

【缺省用户角色】

network-admin
context-admin

【参数】

-f first-hop: 指定一个初始 hoplimit，即第一个报文所允许的跳数。取值范围为 1~255，且小于或等于 **max-hops**，缺省值为 1。

-m max-hops: 指定一个最大 hoplimit，即一个报文所允许的最大跳数。取值范围为 1~255，且大于或等于 **first-hop**，缺省值为 30。

-p port: 指定目的端的 UDP 端口号，取值范围为 1~65535，缺省值为 33434。用户一般不需要更改此选项。

-q packet-number: 指定每次发送的探测报文个数，取值范围为 1~65535，缺省值为 3。

-t traffic-class: IPv6 tracert 报文中的 Traffic Class 域的值。取值范围为 0~255，缺省值为 0。

-vpn-instance vpn-instance-name: 指定目的端所属的 VPN 实例。**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的端位于公网中。

-resolve-as: 指定从哪个路由表中解析 AS 号。使用该参数，能够帮助用户了解 Tracert 路径中三层设备所属 AS 的编号。不指定该参数时，表示从公网路由表解析 AS 号。

global: 表示从公网路由表解析 AS 号。指定该参数后，Tracert 在显示公网三层设备的地址信息时，会同时显示该地址对应的 AS 号。如果公网路由表中没有记录该地址的 AS 号，则不显示。

none: 表示不解析 AS 号。Tracert 显示信息中不会携带 AS 号。

vpn: 表示从当前 VPN 的路由表解析 AS 号。指定该参数后，Tracert 在显示当前 VPN 中三层设备的地址信息时，会同时显示该地址对应的 AS 号。如果当前 VPN 路由表中没有记录该地址的 AS 号，则不显示。

-w timeout: 指定探测报文的响应报文的超时时间，取值范围为 1~65535，单位为毫秒，缺省值为 5000。

host: 目的端的 IPv6 地址或主机名。其中，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。

【使用指导】

当用户使用 **ping ipv6** 命令测试发现网络出现故障后，可以用 **tracert ipv6** 命令来帮助查找出现故障的网络节点。

当目的地址为公网地址时，设备会自动从公网路由表解析 AS 号，如果存在则显示。当目的地址为私网地址时，路径上的三层设备的地址可能存在于公网路由表或私网路由表，这时需要用户执行两次 **tracert** 命令，分别指定 **global** 参数和 **vpn** 参数，然后根据网络拓扑确定源端到目的端实际途经的 AS。

本命令的输出信息包括到达目的端所经过的所有三层设备的 IPv6 地址，如果某设备不能回应 ICMP 错误消息（可能因为路由不可达或者没有开启 ICMP 错误报文处理功能），则输出 “* * *”。

在 Tracert 过程中，并且中间设备开启了 ICMP 不可达报文处理功能（参考 **ipv6 unreachable enable** 命令），如果命令执行结果中显示以下字符，则表示目的设备已不可达，设备会停止发包，Tracert 过程停止。

- !N: 表示目的不可达，即路由表中没有匹配的目的地地址。
- !P: 表示因安全类业务流量管理禁止导致通信不可达，即通信被过滤策略禁止。
- !A: 表示地址不可达，即未知的不可达消息。
- !S: 表示超出源地址范围不可达，即当源地址为链路本地地址目的地地址不是链路本地地址时返回此字符。

在执行命令过程中，键入<Ctrl+C>可终止此次 Tracert IPv6 操作。

【举例】

查看报文从源端到目的端（IPv6 地址为 2001:3::2）所经过的路径。

```
<Sysname> tracert ipv6 2001:3::2
```

```
traceroute to 2001:3::2(2001:3::2), 30 hops at most, 60 byte packets , press CTRL_C to break
```

```
1  2001:1::2  0.661 ms  0.618 ms  0.579 ms
2  2001:2::2 [AS 100]  0.861 ms  0.718 ms  0.679 ms
3  2001:3::2 [AS 200]  0.822 ms  0.731 ms  0.708 ms
```

查看报文从源端到目的端（IPv6 地址为 2001:3::2，属于 vpn1）所经过的路径，并显示报文经过的私网中的三层设备的 AS 信息。

```
<Sysname> tracert ipv6 -vpn-instance vpn1 -resolve-as vpn 2001:3::2
```

```
traceroute to 2001:3::2(2001:3::2), 30 hops at most, 60 byte packets , press CTRL_C to break
```

```
1  2001:1::2  0.661 ms  0.618 ms  0.579 ms
2  2001:2::2  0.861 ms  0.718 ms  0.679 ms
3  2001:3::2 [AS 65535]  0.822 ms  0.731 ms  0.708 ms
```

表1-4 tracert ipv6 命令显示信息描述表

字段	描述
tracert to 2001:3::2	查看IPv6报文从当前设备发送到地址为2001:3::2的设备所经过的路径
hops at most	探测报文的最大跳数，可使用 -m 参数配置
byte packets	探测报文字节数
2 2001:2::2 [AS 100] 0.861 ms 0.718 ms 0.679 ms	hoplimit值为2的探测报文的探测结果，内容包括：第二跳的IPv6地址、所属AS号（如果不存在则不显示）、三份探测报文的往返时间（每次发送探测报文的份数可以使用 -q 参数配置）

目 录

1 NQA	1-1
1.1 NQA客户端配置命令	1-1
1.1.1 advantage-factor	1-1
1.1.2 agent-type	1-1
1.1.3 codec-type	1-2
1.1.4 community read	1-3
1.1.5 cpu	1-4
1.1.6 data-fill	1-5
1.1.7 data-size	1-6
1.1.8 description	1-7
1.1.9 destination ip	1-8
1.1.10 destination ipv6	1-9
1.1.11 destination port	1-10
1.1.12 disconnect-mode	1-11
1.1.13 disk	1-12
1.1.14 display nqa history	1-12
1.1.15 display nqa reaction counters	1-14
1.1.16 display nqa result	1-16
1.1.17 display nqa statistics	1-24
1.1.18 expect { data hex-data }	1-33
1.1.19 expect { failed-data hex-failed-data }	1-34
1.1.20 expect ip	1-36
1.1.21 expect ipv6	1-36
1.1.22 expect status	1-37
1.1.23 filename	1-38
1.1.24 frequency	1-39
1.1.25 hex-data-fill	1-40
1.1.26 high-performance-mode	1-40
1.1.27 history-record enable	1-41
1.1.28 history-record keep-time	1-42
1.1.29 history-record number	1-43
1.1.30 init-ttl	1-44
1.1.31 key	1-44

1.1.32	lsr-path	1-45
1.1.33	mailbox	1-46
1.1.34	max-failure	1-46
1.1.35	memory	1-47
1.1.36	mode	1-48
1.1.37	next-hop ip	1-49
1.1.38	next-hop ipv6	1-49
1.1.39	no-fragment enable	1-50
1.1.40	nqa	1-51
1.1.41	nqa agent enable	1-51
1.1.42	nqa agent udp-jitter high-performance enable	1-52
1.1.43	nqa schedule	1-53
1.1.44	nqa template	1-54
1.1.45	oid	1-55
1.1.46	operation (FTP test type view)	1-56
1.1.47	operation (HTTP test type view)	1-57
1.1.48	operation (HTTPS template view)	1-58
1.1.49	out interface	1-59
1.1.50	password	1-60
1.1.51	port-detect enable	1-61
1.1.52	probe count	1-62
1.1.53	probe packet-interval	1-63
1.1.54	probe packet-number	1-64
1.1.55	probe packet-timeout	1-64
1.1.56	probe timeout	1-65
1.1.57	proxy-url	1-66
1.1.58	raw-request	1-67
1.1.59	reaction checked-element { jitter-ds jitter-sd }	1-68
1.1.60	reaction checked-element { owd-ds owd-sd }	1-69
1.1.61	reaction checked-element icpif	1-70
1.1.62	reaction checked-element mos	1-71
1.1.63	reaction checked-element packet-loss	1-72
1.1.64	reaction checked-element probe-duration	1-73
1.1.65	reaction checked-element probe-fail (for trap)	1-75
1.1.66	reaction checked-element probe-fail (for trigger)	1-76
1.1.67	reaction checked-element rtt	1-77

1.1.68 reaction trap	1-78
1.1.69 reaction trigger per-probe	1-79
1.1.70 reaction trigger probe-fail	1-80
1.1.71 reaction trigger probe-pass	1-81
1.1.72 request-method	1-82
1.1.73 resolve-target	1-83
1.1.74 resolve-type	1-83
1.1.75 resource-release { data-fill hex-data-fill }	1-84
1.1.76 route-option bypass-route	1-85
1.1.77 source interface	1-86
1.1.78 source ip	1-86
1.1.79 source ipv6	1-87
1.1.80 source port	1-88
1.1.81 ssl-client-policy	1-89
1.1.82 statistics hold-time	1-90
1.1.83 statistics interval	1-91
1.1.84 statistics max-group	1-91
1.1.85 target-only	1-92
1.1.86 tos	1-93
1.1.87 ttl	1-93
1.1.88 transport-protocol	1-94
1.1.89 type	1-95
1.1.90 url	1-96
1.1.91 username	1-97
1.1.92 version (HTTP/HTTPS test type view and HTTPS template view)	1-98
1.1.93 version (SNMP-DCA template view)	1-99
1.1.94 vpn-instance	1-99
1.2 NQA服务器端命令	1-100
1.2.1 display nqa server	1-100
1.2.2 nqa server enable	1-102
1.2.3 nqa server tcp-connect	1-102
1.2.4 nqa server udp-echo	1-103
1.2.5 nqa server udp-echo high-performance enable	1-105

1 NQA

1.1 NQA客户端配置命令

1.1.1 advantage-factor

advantage-factor 命令用来配置用于计算 MOS 值和 ICPIF 值的补偿因子。

undo advantage-factor 命令用来恢复缺省情况。

【命令】

advantage-factor *factor*

undo advantage-factor

【缺省情况】

补偿因子取值为 0。

【视图】

Voice 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

factor: 用于计算 MOS 值和 ICPIF 值的补偿因子，取值范围为 0~20。

【使用指导】

用户对语音质量的评价具有一定的主观性，不同用户对语音质量的容忍程度不同，因此，衡量语音质量时，需要考虑用户的主观因素。对语音质量容忍程度较强的用户，可以通过 **advantage-factor** 命令配置补偿因子，在计算 ICPIF 值时将减去该补偿因子，修正 ICPIF 和 MOS 值，以便在比较语音质量时综合考虑客观和主观因素。

【举例】

在 Voice 测试类型下配置计算 MOS 值和 ICPIF 值的补偿因子为 10。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type voice
```

```
[Sysname-nqa-admin-test-voice] advantage-factor 10
```

1.1.2 agent-type

agent-type 命令用来配置 SNMP-DCA 测试的 SNMP Agent 类型。

undo agent-type 命令用来恢复缺省情况。

【命令】

agent-type { net-snmp | user-defined | windows }

undo agent-type

【缺省情况】

SNMP-DCA 测试的 SNMP Agent 类型为 Net-SNMP。

【视图】

SNMP-DCA 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

net-snmp: 表示 SNMP Agent 的类型为 Net-SNMP。

user-defined: 表示 SNMP Agent 的类型为 User-defined。

windows: 表示 SNMP Agent 的类型为 Windows。

【使用指导】

SNMP-DCA 测试用于监测 SNMP Agent 的状态。设备通常以 SNMP Agent 的 CPU/内存/硬盘的使用率作为参数，和用户配置的阈值、权重计算后得到的结果来判断 SNMP Agent 的状态。

不同类型的 SNMP Agent，其 CPU/内存/硬盘使用率 MIB 节点的 OID 不同。建议设备上配置的类型和需要监测的 SNMP Agent 的类型一致。

对于 Net-SNMP 和 Windows 类型，开启 SNMP-DCA 测试后，设备会自动获取 SNMP Agent 的 CPU/内存/硬盘使用率来判断 SNMP Agent 的状态。用户可通过 **cpu**、**memory** 和 **disk** 命令修改相应的阈值和权重，也可以使用 **oid** 命令增加关注的节点。

对于 User-defined 类型，因为设备不能自动获取到 SNMP Agent 上 MIB 节点的 OID，所以，需要用户使用 **oid** 命令配置每个需要关注的 MIB 节点，包括 CPU/内存/硬盘使用率对应的 MIB 节点。

【举例】

在 SNMP-DCA 类型的 NQA 模板视图下配置 SNMP-DCA 测试的 SNMP Agent 类型为 Windows。

```
<Sysname> system-view
```

```
[Sysname] nqa template snmpdca test
```

```
[Sysname-nqatplt-snmpdca-test] agent-type windows
```

【相关命令】

- **cpu**
- **disk**
- **memory**
- **oid**

1.1.3 codec-type

codec-type 命令用来配置语音测试的编码格式。

undo codec-type 命令用来恢复缺省情况。

【命令】

```
codec-type { g711a | g711u | g729a }  
undo codec-type
```

【缺省情况】

语音编码格式为 G.711 A 律。

【视图】

Voice 测试类型视图

【缺省用户角色】

network-admin
context-admin

【参数】

g711a: G.711 A 律语音编码格式。

g711u: G.711 μ 律语音编码格式。

g729a: G.729 A 律语音编码格式。

【举例】

在 Voice 测试类型下配置语音测试的编码格式为 G.729 A 律。

```
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type voice  
[Sysname-nqa-admin-test-voice] codec-type g729a
```

1.1.4 community read

community read 命令用来配置用于 SNMP 测试使用的团体名。

undo community read 命令用来恢复缺省情况。

【命令】

```
community read { cipher | simple } community-name  
undo community read
```

【缺省情况】

SNMP 测试使用的团体名为 public。

【视图】

SNMP 测试类型视图

SNMP/SNMP-DCA 类型的模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

cipher: 以密文方式配置团体名。

simple: 以明文方式配置团体名，该密码将以密文形式存储。

community-name: 测试使用的团体名，区分大小写。当以明文形式配置时，团体名为 1~32 个字符的字符串；当以密文形式配置时，团体名为 33~73 个字符的字符串。

【使用指导】

当被测试的 SNMP Agent 的版本为 SNMPv1 或者 SNMPv2c 时，若 SNMP Agent 配置了团体名，则 SNMP 测试组必须配置本命令，且配置的团体名必须与 SNMP Agent 上已配置的只读或读写权限团体名保持一致，才能通过 SNMP Agent 的认证，并进行探测。当 SNMP Agent 的版本为 SNMPv3 时，由于 SNMPv3 没有团体名概念，不需要配置团体名，直接进行探测。有关团体名及 SNMP 认证的具体介绍请参见“网络管理和监控”中的“SNMP”。

【举例】

配置 SNMP 探测报文使用的团体名称为 readaccess。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type snmp
[Sysname-nqa-admin-test-snmp] community read simple readaccess
```

1.1.5 cpu

cpu 命令用来配置 SNMP-DCA 测试的 SNMP Agent 的 CPU 的阈值和权重。

undo cpu 命令用来恢复缺省情况。

【命令】

```
cpu { threshold threshold-value | weight weight-value } *
undo cpu
```

【缺省情况】

SNMP-DCA 测试的 SNMP Agent 的 CPU 阈值为 80，权重为 3。

【视图】

SNMP-DCA 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

threshold *threshold-value*: 阈值，表示 CPU 使用率可达到的上限。取值范围为 0~100，取值为 0 时表示 CPU 不作为判断 SNMP Agent 是否繁忙的参考。不指定该参数时，表示使用缺省值。

weight *weight-value*: 权重，表示 CPU 在用于计算 SNMP Agent 状态时应占有的比重。取值范围为 0~100，取值为 0 时表示 CPU 不参与 SNMP Agent 状态的计算。不指定该参数时，表示使用缺省值。

【使用指导】

本命令仅对 Net-SNMP 或 Windows 类型的 SNMP Agent 生效。

NQA 客户端对 Net-SNMP 或 Windows 类型的 SNMP Agent 进行 SNMP-DCA 测试时，会自动获取 SNMP Agent 当前的 CPU 利用率。

【举例】

在 SNMP-DCA 类型的 NQA 模板视图下配置测试的 SNMP Agent 的 CPU 阈值为 90、权重为 90。

```
<Sysname> system-view
[Sysname] nqa template snmpdca test
[Sysname-nqatplt-snmpdca-test] cpu threshold 90 weight 90
```

【相关命令】

- **agent-type**

1.1.1.6 data-fill

data-fill 命令用来配置探测报文的填充字符串。

undo data-fill 命令用来恢复缺省情况。

【命令】

```
data-fill string [ raw ]
undo data-fill
```

【缺省情况】

探测报文的填充内容为十六进制 00010203040506070809。

【视图】

ICMP-echo/UDP-echo 测试类型视图

Path-jitter/UDP-jitter/Voice 测试类型视图

ICMP/TCP/UDP 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

string: 探测报文的填充内容，为 1~200 个字符的字符串，区分大小写。

raw: 表示仅使用 **string** 来填充探测报文，该参数仅在 UDP 类型的 NQA 模板视图下支持。

【使用指导】

对于不同的测试类型，填充字符串的情况有所不同：

- 在 ICMP-echo 测试中，配置的字符串用来填充 ICMP Echo 消息的数据字段。
- 在 UDP-echo 测试中，由于 UDP 报文数据字段的前 5 个字节具有特定用途，所以只用所配置的字符串填充报文中剩余的字节。
- 在 UDP-jitter 测试中，UDP 报文数据字段的前 68 个字节具有特定用途，所以只用所配置的字符串填充报文中剩余的字节。

- 在 Voice 测试中，UDP 报文数据字段的前 16 个字节具有特定用途，所以只用所配置的字符串填充报文中剩余的字节。
- 在 Path-jitter 测试中，由于 ICMP 探测阶段 ICMP 报文数据字段的前 4 个字节具有特定用途，所以只用所配置的字符串填充 ICMP 报文中剩余的字节。

若指定 **raw** 参数，表示 *string* 参数位置的填充字符串在探测时将被直接发送。

未指定 **raw** 参数时，实际填充的字符与填充数据长度有关：

- 如果探测报文的数据段长度比配置的填充数据长度小，系统在报文封装时以报文的数据段长度为界截取该字符串的前一部分；
- 如果探测报文的数据段长度比配置的填充数据长度大，系统在报文封装时用该字符串进行循环填充，直到填满。

例如，配置填充数据为“abcd”，当探测报文数据段长度为 3 字节时，则取“abc”作为填充数据；当探测报文数据段长度为 6 字节时，则使用“adcdab”作为填充数据。

【举例】

在 ICMP-echo 测试类型下配置探测报文的填充字符串为 abcd。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-fill abcd
```

在 TCP 类型的 NQA 模板视图下配置探测报文的填充字符串为 abcd。

```
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] data-fill abcd
```

1.1.7 data-size

data-size 命令用来配置探测报文中的填充内容的大小。

undo data-size 命令用来恢复缺省情况。

【命令】

data-size size

undo data-size

【缺省情况】

缺省情况如 [表 1-1](#) 所示。

表1-1 探测报文中的填充内容大小的缺省值

测试类型	编码类型	缺省值（字节）
ICMP-echo	-	100
UDP-echo	-	100
UDP-jitter	-	100
UDP-tracert	-	100
Path-jitter	-	100

测试类型	编码类型	缺省值（字节）
Voice	G.711 A律	172
Voice	G.711 μ 律	172
Voice	G.729 A律	32

【视图】

ICMP-echo/UDP-echo 测试类型视图

UDP-tracert 测试类型视图

Path-jitter/UDP-jitter/Voice 测试类型视图

ICMP/UDP 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

size: 探测报文中的填充内容的大小，单位为字节，ICMP-echo、UDP-echo 和 UDP-tracert 测试类型取值范围为 20～65507，UDP-jitter 和 Path-jitter 测试类型取值范围为 68～65507，Voice 测试类型取值范围为 16～65507。

【使用指导】

对于 ICMP-echo 和 Path-jitter 测试，探测报文中填充内容的大小为 ICMP Echo 消息中数据字段的长度。

对于 UDP-echo、UDP-jitter、UDP-tracert 和 Voice 测试，探测报文中填充内容的大小为 UDP 报文中数据字段的长度。

【举例】

在 ICMP-echo 测试类型下配置探测报文中的填充内容的大小为 80 字节。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-size 80
```

在 ICMP 类型的 NQA 模板视图下配置 ICMP-echo 探测报文中的填充内容的大小为 80 字节。

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] data-size 80
```

1.1.8 description

description 命令用来配置测试组的描述信息，通常用于描述一个测试组的测试类型或测试目的。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

未配置描述信息。

【视图】

ICMP-echo/UDP-echo/TCP 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

UDP-tracert 测试类型视图

ICMP-jitter/UDP-jitter/Path-jitter/Voice 测试类型视图

任意类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: 测试组的描述，为 1~200 个字符的字符串，区分大小写。

【举例】

在 ICMP-echo 测试类型下配置测试组的描述信息为 icmp-probe。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] description icmp-probe
```

在 ICMP 类型的 NQA 模板视图下配置描述信息为 icmp-probe。

```
<Sysname> system-view
```

```
[Sysname] nqa template icmp icmptplt
```

```
[Sysname-nqatplt-icmp-icmptplt] description icmp-probe
```

1.1.9 destination ip

destination ip 命令用来配置探测报文的目的 IPv4 地址。

undo destination ip 命令用来恢复缺省情况。

【命令】

destination ip *ip-address*

undo destination ip

【缺省情况】

未配置探测报文的目的 IPv4 地址。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/SNMP 测试类型视图

UDP-tracert 测试类型视图

ICMP-jitter/Path-jitter/UDP-jitter/Voice 测试类型视图

ARP/DNS/ICMP/IMAP/POP3/RADIUS 认证探测 /RADIUS-ACCOUNT 计费探测 /SMTP/SNMP/SNMP-DCA/SSL/TCP/TCPHalf Open/UDP/WAP 类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: 探测报文的目的 IPv4 地址。

【举例】

```
# 在 ICMP-echo 测试类型下配置探测报文的目的 IPv4 地址为 10.1.1.1。
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
# 在 ICMP 类型的 NQA 模板视图下配置探测报文的目的 IPv4 地址为 10.1.1.1。
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] destination ip 10.1.1.1
```

1.1.10 destination ipv6

destination ipv6 命令用来配置探测报文的目的 IPv6 地址。

undo destination ipv6 命令用来恢复缺省情况。

【命令】

destination ipv6 *ipv6-address*
undo destination ipv6

【缺省情况】

未配置探测报文的目的 IPv6 地址。

【视图】

ICMP-echo/TCP/UDP-echo/UDP-jitter 测试类型视图

DNS/ICMP/IMAP/POP3/RADIUS 认证探测 /RADIUS-ACCOUNT 计费探测 /SMTP/SIP/SNMP/SNMP-DCA/SSL/TCP/TCP Half Open/UDP/WAP 类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address: 探测报文的目的 IPv6 地址，不支持 IPv6 链路本地地址。

【举例】

```
# 在 ICMP-echo 测试类型下配置探测报文的目的 IPv6 地址为 1::1。
<Sysname> system-view
```



```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ipv6 1::1
# 在 ICMP 类型的 NQA 模板视图下配置探测报文的目的 IPv6 地址为 1::1。
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] destination ipv6 1::1
```

1.1.11 destination port

destination port 命令用来配置测试操作的目的端口号。

undo destination port 命令用来恢复缺省情况。

【命令】

```
destination port port-number
undo destination port
```

【缺省情况】

对于 UDP-tracert 测试，目的端口号缺省为 33434；对于 SNMP 测试，目的端口号缺省为 161；对于其他类型测试，未配置测试操作的目的端口号。

对于 NQA 模板，缺省目的端口号分别为：DNS（53）、IMAP（143）、POP3（110）、RADIUS 认证探测（1812）、RADIUS-ACCOUNT 计费探测（1813）、SIP（5060）、SMTP（25）、SNMP（161）、SNMP-DCA（161）、WAP（9201）、其他类型模板未配置测试操作的目的端口号。

【视图】

TCP/UDP-echo 测试类型视图

SNMP 测试类型视图

UDP-tracert 测试类型视图

UDP-jitter/Voice 测试类型视图

DNS/IMAP/POP3/RADIUS 认证探测 /RADIUS-ACCOUNT 计费探测
/SIP/SMTP/SNMP/SNMP-DCA/SSL/TCP/TCP Half Open /UDP/WAP 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

port-number：测试操作的目的端口号，取值范围为 1～65535。

【使用指导】

对于 TCP Half Open 类型的 NQA 模板，只有在通过 **port-detect enable** 命令开启 TCP Half Open 的端口检测功能的情况下，才需要配置本命令。

【举例】

```
# 在 UDP-echo 测试类型视图下配置测试操作的目的端口号为 9000。
<Sysname> system-view
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] destination port 9000
# 在 TCP 类型的 NQA 模板视图下配置测试操作的目的端口号为 9000。
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] destination port 9000
```

【相关命令】

- **port-detect enable**

1.1.12 disconnect-mode

disconnect-mode 命令用来设置 TCP 测试的 TCP 连接断开方式。

undo disconnect-mode 命令用来恢复缺省情况。

【命令】

```
disconnect-mode { fin | rst }
undo disconnect-mode
```

【缺省情况】

TCP 测试的 TCP 连接断开方式为 RST。

【视图】

TCP 类型的模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

fin: TCP 测试的 TCP 连接断开方式为 FIN。
rst: TCP 测试的 TCP 连接断开方式为 RST。

【使用指导】

一次 TCP 测试包括三次握手建立 TCP 连接和断开 TCP 连接，完成该过程表示 NQA 的 TCP 测试成功，本命令可以设置断开 TCP 连接的方式：

- **RST:** 通过发送 RST 报文，快速释放 TCP 连接。收到 RST 报文后，另一端就终止连接，不需要发送任何响应。
- **FIN:** 四次握手断开 TCP 连接，不支持 RST 方式情况下可以设置为该方式。被断开的一方收到 FIN 报文后需要发送 ACK。

【举例】

```
# 在 TCP 类型的 NQA 模板视图下设置 TCP 测试的 TCP 连接断开方式为 FIN。
<Sysname> system-view
[Sysname] nqa template tcp test
[Sysname-nqatplt-tcp-test] disconnect-mode fin
```

1.1.13 disk

disk 命令用来配置 SNMP-DCA 测试的 SNMP Agent 硬盘的阈值和权重。

undo disk 命令用来恢复缺省情况。

【命令】

```
disk { threshold threshold-value | weight weight-value } *  
undo disk
```

【缺省情况】

SNMP-DCA 测试的 SNMP Agent 硬盘的阈值为 90，权重为 4。

【视图】

SNMP-DCA 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

threshold *threshold-value*: 阈值，表示硬盘使用率可达到的上限。取值范围为 0~100，取值为 0 时表示硬盘不作为判断 SNMP Agent 是否繁忙的参考。不指定该参数时，表示使用缺省值。

weight *weight-value*: 权重，表示硬盘在用于计算 SNMP Agent 状态时应占有的比重，取值范围为 0~100，取值为 0 时表示硬盘不参与 SNMP Agent 状态的计算。不指定该参数时，表示使用缺省值。

【使用指导】

本命令仅对 Net-SNMP 或 Windows 类型的 SNMP Agent 生效。

NQA 客户端对 Net-SNMP 或 Windows 类型的 SNMP Agent 进行 SNMP-DCA 测试时，会自动获取 SNMP Agent 当前的硬盘使用率

【举例】

在 SNMP-DCA 类型的 NQA 模板视图下配置测试的 SNMP Agent 硬盘阈值为 90、权重为 90。

```
<Sysname> system-view  
[Sysname] nqa template snmpdca test  
[Sysname-nqatplt-snmpdca-test] disk threshold 90 weight 90
```

【相关命令】

- **agent-type**

1.1.14 display nqa history

display nqa history 命令用来显示 NQA 测试组的历史记录。

【命令】

```
display nqa history [ admin-name operation-tag ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

admin-name: 创建 NQA 测试组的管理员名称, 为 1~32 个字符的字符串, 字符串中不能包括“-”, 不区分大小写。

operation-tag: 测试操作的标签, 为 1~32 个字符的字符串, 字符串中不能包括“-”, 不区分大小写。

【使用指导】

display nqa history 命令的显示信息无法反映 ICMP-jitter、Path-jitter、UDP-jitter 和 Voice 测试的结果。如果了解 ICMP-jitter、Path-jitter、UDP-jitter 和 Voice 测试的结果, 建议通过 **display nqa result** 命令查看最近一次 NQA 测试的结果, 或通过 **display nqa statistics** 命令查看 NQA 测试的统计信息。

不指定任何参数, 则表示显示所有测试组的历史记录。

【举例】

显示管理员名称为 administrator、测试类型标签为 tracert 的 UDP-tracert 测试项的历史记录。

```
<Sysname> display nqa history administrator tracert
```

NQA entry (admin administrator, tag tracert) history records:

Index	TTL	Response	Hop IP	Status	Time
1	2	328	4.1.1.1	Succeeded	2013-09-09 14:46:06.2
1	2	328	4.1.1.1	Succeeded	2013-09-09 14:46:05.2
1	2	328	4.1.1.1	Succeeded	2013-09-09 14:46:04.2
1	1	328	3.1.1.2	Succeeded	2013-09-09 14:46:03.2
1	1	328	3.1.1.1	Succeeded	2013-09-09 14:46:02.2
1	1	328	3.1.1.1	Succeeded	2013-09-09 14:46:01.2

查看管理员名称为 administrator、测试操作标签为 test 的 NQA 测试组的历史记录。

```
<Sysname> display nqa history administrator test
```

NQA entry (admin administrator, tag test) history records:

Index	Response	Status	Time
10	329	Succeeded	2011-04-29 20:54:26.5
9	344	Succeeded	2011-04-29 20:54:26.2
8	328	Succeeded	2011-04-29 20:54:25.8
7	328	Succeeded	2011-04-29 20:54:25.5
6	328	Succeeded	2011-04-29 20:54:25.1
5	328	Succeeded	2011-04-29 20:54:24.8
4	328	Succeeded	2011-04-29 20:54:24.5
3	328	Succeeded	2011-04-29 20:54:24.1
2	328	Succeeded	2011-04-29 20:54:23.8

表1-2 display nqa history 命令显示信息描述表

字段	描述
Index	历史记录编号，一次UDP-tracert测试中的所有记录此编号一致
TTL	本次探测发送的探测报文的TTL值。如果设备配置了路由旁路功能，则TTL显示值与 init-ttl 命令配置相关，实际发送的TTL值固定为1
Response	测试成功时，为探测报文的往返时延；如果测试超时，则为超时时间；不能完成测试时，则为0。单位为毫秒
Hop IP	回复应答的节点IP地址
Status	测试结果的状态值，具体如下： • Succeeded: 测试成功，接收到响应报文 • Unknown error: 未知错误 • Internal error: 内部错误 • Timeout: 请求超时
Time	测试完成时间

1.1.15 display nqa reaction counters

display nqa reaction counters 命令用来显示阈值告警组的当前监测结果。

【命令】

display nqa reaction counters [*admin-name operation-tag* [*item-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

admin-name: 创建 NQA 测试组的管理员名称，为 1~32 个字符的字符串，字符串中不能包括“-”，不区分大小写。

operation-tag: 测试操作的标签，为 1~32 个字符的字符串，字符串中不能包括“-”，不区分大小写。

item-number: 显示指定阈值告警组的当前监测结果。如果不指定该参数，将显示所有阈值告警组的当前监测结果。**item-number** 为阈值告警组的编号，取值范围为 1~10。

【使用指导】

如果 NQA 阈值告警组的阈值类型为平均值，或监测对象为 Voice 测试的 ICPIF 或 MOS 值，则显示的监测结果为无效值。

测试结束后，不会清除监测结果，即测试组启动后，监测结果会不断累加。

不指定任何参数，则表示显示所有测试组中所有阈值告警组的当前监测结果。

【举例】

显示 NQA 测试组管理员名称为 admin、测试操作标签为 test 的 ICMP-echo 测试组的所有阈值告警组的当前监测结果。

```
<Sysname> display nqa reaction counters admin test
NQA entry (admin admin, tag test) reaction counters:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      probe-duration  accumulate      12           4
  2      probe-duration  average         -           -
  3      probe-duration  consecutive     160         56
  4      probe-fail      accumulate      12           0
  5      probe-fail      consecutive     162          2
```

表1-3 display nqa reaction counters 命令显示信息描述

字段	描述
Index	阈值告警组的编号
Checked Element	监测的对象（不同的NQA测试类型支持的监测对象不同，具体请参见 表1-4 、 表1-5 ）
Threshold Type	阈值类型
Checked Num	已监测的样本个数
Over-threshold Num	超出阈值的样本个数

表1-4 display nqa reaction counters 命令显示字段取值描述

（DHCP/DLSw/DNS/FTP/HTTP/ICMP-echo/SNMP/TCP/UDP-echo 测试类型）

监测对象	阈值类型	监测的样本范围	Checked Num 取值	Over-threshold Num 取值
probe-duration	accumulate	启动NQA测试组后进行的探测	启动NQA测试组后已完成的探测次数	启动NQA测试组后累计的探测持续时间不在阈值范围内的探测次数
	average	-	-	-
	consecutive	启动NQA测试组后进行的探测	启动NQA测试组后已完成的探测次数	启动NQA测试组后连续的探测持续时间不在阈值范围内的探测次数
probe-fail	accumulate	启动NQA测试组后进行的探测	启动NQA测试组后已完成的探测次数	启动NQA测试组后累计的探测失败次数
	consecutive	启动NQA测试组后进行的探测	启动NQA测试组后已完成的探测次数	启动NQA测试组后连续的探测失败次数

表1-5 display nqa reaction counters 命令显示字段取值描述（ICMP-jitter/UDP-jitter/Voice 测试类型）

监测对象	阈值类型	监测的样本范围	Checked Num 取值	Over-threshold Num 取值
RTT	accumulate	启动NQA测试组后发送的报文	启动NQA测试组后已发送的报文个数	启动NQA测试组后累计的往返时间不在阈值范围内的报文个数
	average	-	-	-
jitter-DS/jitter-SD	accumulate	启动NQA测试组后发送的报文	启动NQA测试组后已发送的报文个数	启动NQA测试组后累计的单向抖动时间不在阈值范围内的报文个数
	average	-	-	-
OWD-DS/OWD-SD	-	启动NQA测试组后发送的报文	启动NQA测试组后已发送的报文个数	启动NQA测试组后单向时延不在阈值范围内的报文个数
packet-loss	accumulate	启动NQA测试组后发送的报文	启动NQA测试组后已发送的报文个数	启动NQA测试组后累计的丢包数
ICPIF/MOS（仅Voice测试支持）	-	-	-	-

1.1.16 display nqa result

display nqa result 命令用来显示最近一次 NQA 测试的结果。

【命令】

display nqa result [*admin-name operation-tag*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

admin-name: 创建 NQA 测试组的管理员名称, 为 1~32 个字符的字符串, 字符串中不能包括“-”, 不区分大小写。

operation-tag: 为测试操作的标签, 为 1~32 个字符的字符串, 字符串中不能包括“-”, 不区分大小写。

【使用指导】

不指定任何参数, 则表示显示所有测试组的最近一次测试的结果。

【举例】

显示 NQA 测试组管理员名称为 **admin**、测试操作标签为 **test** 的 TCP 测试的最近一次测试结果。

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Send operation times: 1          Receive response times: 1
  Min/Max/Average round trip time: 35/35/35
  Square-Sum of round trip time: 1225
  Last succeeded probe time: 2011-05-29 10:50:33.2
Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
```

显示 NQA 测试组管理员名称为 **admin**、测试操作标签为 **test** 的 ICMP-jitter 测试的最近一次测试结果。

```
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
  Send operation times: 10         Receive response times: 10
  Min/Max/Average round trip time: 1/2/1
  Square-Sum of round trip time: 13
  Last packet received time: 2015-03-09 17:40:29.8
Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
ICMP-jitter results:
  RTT number: 10
  Min positive SD: 0              Min positive DS: 0
  Max positive SD: 0              Max positive DS: 0
  Positive SD number: 0           Positive DS number: 0
  Positive SD sum: 0              Positive DS sum: 0
  Positive SD average: 0          Positive DS average: 0
  Positive SD square-sum: 0       Positive DS square-sum: 0
  Min negative SD: 1              Min negative DS: 2
  Max negative SD: 1              Max negative DS: 2
  Negative SD number: 1           Negative DS number: 1
  Negative SD sum: 1              Negative DS sum: 2
  Negative SD average: 1          Negative DS average: 2
  Negative SD square-sum: 1       Negative DS square-sum: 4
  SD average: 1                  DS average: 2
One way results:
  Max SD delay: 1                Max DS delay: 2
```


Min SD delay: 1	Min DS delay: 2
Number of SD delay: 1	Number of DS delay: 1
Sum of SD delay: 1	Sum of DS delay: 2
Square-Sum of SD delay: 1	Square-Sum of DS delay: 4
Lost packets for unknown reason: 0	

显示 NQA 测试组管理员名称为 **admin**、测试操作标签为 **test** 的 UDP-jitter 测试的最近一次测试结果。

<Sysname> display nqa result admin test

NQA entry (admin admin, tag test) test results:

Send operation times: 10	Receive response times: 10
Min/Max/Average round trip time: 15/46/26	
Square-Sum of round trip time: 8103	
Last packet received time: 2011-05-29 10:56:38.7	

Extended results:

Packet loss ratio: 0%

Failures due to timeout: 0

Failures due to internal error: 0

Failures due to other errors: 0

Packets out of sequence: 0

Packets arrived late: 0

UDP-jitter results:

RTT number: 10

Min positive SD: 8	Min positive DS: 8
Max positive SD: 18	Max positive DS: 8
Positive SD number: 5	Positive DS number: 2
Positive SD sum: 75	Positive DS sum: 32
Positive SD average: 15	Positive DS average: 16
Positive SD square-sum: 1189	Positive DS square-sum: 640
Min negative SD: 8	Min negative DS: 1
Max negative SD: 24	Max negative DS: 30
Negative SD number: 4	Negative DS number: 7
Negative SD sum: 56	Negative DS sum: 99
Negative SD average: 14	Negative DS average: 14
Negative SD square-sum: 946	Negative DS square-sum: 1495
SD average: 14	DS average: 14

One way results:

Max SD delay: 22	Max DS delay: 23
Min SD delay: 7	Min DS delay: 7
Number of SD delay: 10	Number of DS delay: 10
Sum of SD delay: 125	Sum of DS delay: 132
Square-Sum of SD delay: 1805	Square-Sum of DS delay: 1988
SD lost packets: 0	DS lost packets: 0
Lost packets for unknown reason: 0	

显示 NQA 测试组管理员名称为 **admin**、测试操作标签为 **test** 的 Voice 测试的最近一次测试结果。

<Sysname> display nqa result admin test

NQA entry (admin admin, tag test) test results:

Send operation times: 1000	Receive response times: 0
Min/Max/Average round trip time: 0/0/0	

```

    Square-Sum of round trip time: 0
    Last packet received time: 0-00-00 00:00:00.0
Extended results:
    Packet loss ratio: 100%
    Failures due to timeout: 1000
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
Voice results:
RTT number: 0
    Min positive SD: 0
    Max positive SD: 0
    Positive SD number: 0
    Positive SD sum: 0
    Positive SD average: 0
    Positive SD square-sum: 0
    Min negative SD: 0
    Max negative SD: 0
    Negative SD number: 0
    Negative SD sum: 0
    Negative SD average: 0
    Negative SD square-sum: 0
    SD average: 0
    Min positive DS: 0
    Max positive DS: 0
    Positive DS number: 0
    Positive DS sum: 0
    Positive DS average: 0
    Positive DS square-sum: 0
    Min negative DS: 0
    Max negative DS: 0
    Negative DS number: 0
    Negative DS sum: 0
    Negative DS average: 0
    Negative DS square-sum: 0
    DS average: 0
One way results:
    Max SD delay: 0
    Min SD delay: 0
    Number of SD delay: 0
    Sum of SD delay: 0
    Square-Sum of SD delay: 0
    SD lost packets: 0
    Lost packets for unknown reason: 1000
    Max DS delay: 0
    Min DS delay: 0
    Number of DS delay: 0
    Sum of DS delay: 0
    Square-Sum of DS delay: 0
    DS lost packets: 0
Voice scores:
    MOS value: 0.99
    ICPIF value: 87
# 显示 NQA 测试组管理员名称为 admin、测试操作标签为 test 的 Path-jitter 测试的最近一次测试结果。
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
Hop IP 192.168.40.210
    Basic Results:
        Send operation times: 10
        Receive response times: 10
        Min/Max/Average round trip time: 1/1/1
        Square-Sum of round trip time: 10
    Extended Results:
        Packet loss ratio: 0%
        Failures due to timeout: 0
        Failures due to internal error: 0

```

```

    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
Path-Jitter Results:
    Jitter number: 9
        Min/Max/Average jitter: 0/0/0
    Positive jitter number: 0
        Min/Max/Average positive jitter: 0/0/0
        Sum/Square-Sum positive jitter: 0/0
    Negative jitter number: 0
        Min/Max/Average negative jitter: 0/0/0
        Sum/Square-Sum negative jitter: 0/0
Hop IP 192.168.50.209
Basic Results:
    Send operation times: 10
    Receive response times: 10
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 10
Extended Results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
Path-Jitter Results:
    Jitter number: 9
        Min/Max/Average jitter: 0/0/0
    Positive jitter number: 0
        Min/Max/Average positive jitter: 0/0/0
        Sum/Square-Sum positive jitter: 0/0
    Negative jitter number: 0
        Min/Max/Average negative jitter: 0/0/0
        Sum/Square-Sum negative jitter: 0/0
# 显示 NQA 测试组管理员名称为 admin、测试操作标签为 test 的 UDP-tracert 测试的最近一次测试结果。
<Sysname> display nqa result admin test
NQA entry (admin admin, tag test) test results:
    Send operation times: 6                Receive response times: 6
    Min/Max/Average round trip time: 35/35/35
    Square-Sum of round trip time: 1225
    Last succeeded probe time: 2013-09-09 14:23:24.5
Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
UDP-tracert results:

```

TTL	Hop	IP	Time
1	3	1.1.1	2013-09-09 14:23:24.5
2	4	1.1.1	2013-09-09 14:23:24.5

表1-6 display nqa result 命令显示信息描述

字段	描述
Data collecting in progress	测试正在进行中
Path jitter result is not available	测试没有生成结果
Send operation times	发送的探测报文数
Receive response times	收到的响应报文数
Min/Max/Average round trip time	最小/最大/平均往返时间，单位为毫秒
Square-Sum of round trip time	往返时间平方和
Last succeeded probe time	一次测试中最后一次成功探测的完成时间，如果一次测试中的探测均失败，则该时间显示为全0，UDP-jitter、Path-jitter和Voice测试中无此信息
Last packet received time	一次探测中最后一次成功收到正确响应报文的时间，如果一次探测中没有收到过正确的响应报文，则该时间显示为全0，只在UDP-jitter和Voice测试中存在此信息
Packet loss ratio	平均丢包率
Failures due to timeout	测试过程中超时的次数
Failures due to disconnect	对方强制断开连接的次数
Failures due to no connection	和对方建立连接失败的次数
Failures due to internal error	因内部错误失败的次数
Failures due to other errors	因其它错误失败的次数
Packets out of sequence	报文失序的次数
ICMP-jitter results	ICMP-jitter测试的结果，只在ICMP-jitter测试中存在此信息
Packets arrived late	探测超时后，收到的响应报文个数
UDP-jitter results	UDP-jitter测试的结果，只在UDP-jitter测试中存在此信息
Voice results	Voice测试的结果，只在Voice测试中存在此信息
RTT number	收到的响应报文数
Min positive SD	源到目的方向正抖动时延的最小值
Min positive DS	目的到源方向正抖动时延的最小值
Max positive SD	源到目的方向正抖动时延的最大值
Max positive DS	目的到源方向正抖动时延的最大值
Positive SD number	源到目的方向正抖动时延的数目
Positive DS number	目的到源方向正抖动时延的数目
Positive SD sum	源到目的方向正抖动时延之和

字段	描述
Positive DS sum	目的到源方向正抖动时延之和
Positive SD average	源到目的方向正抖动时延的平均值
Positive DS average	目的到源方向正抖动时延的平均值
Positive SD square-sum	源到目的方向正抖动时延的平方和
Positive DS square-sum	目的到源方向正抖动时延的平方和
Min negative SD	源到目的方向负抖动时延的绝对值的最小值
Min negative DS	目的到源方向负抖动时延的绝对值的最小值
Max negative SD	源到目的方向负抖动时延的绝对值的最大值
Max negative DS	目的到源方向负抖动时延的绝对值的最大值
Negative SD number	源到目的方向负抖动时延的数目
Negative DS number	目的到源方向负抖动时延的数目
Negative SD sum	源到目的方向负抖动时延的绝对值之和
Negative DS sum	目的到源方向负抖动时延的绝对值之和
Negative SD average	源到目的方向负抖动时延的绝对值的平均值
Negative DS average	目的到源方向负抖动时延的绝对值的平均值
Negative SD square-sum	源到目的方向负抖动时延的平方和
Negative DS square-sum	目的到源方向负抖动时延的平方和
SD average	源到目的方向抖动时延的平均值
DS average	目的到源方向抖动时延的平均值
One way results	单向延迟测试结果，只有ICMP-jitter、UDP-Jitter和Voice类型测试有单向延迟测试结果
Max SD delay	源到目的的最大时延
Max DS delay	目的到源的最大时延
Min SD delay	源到目的的最小时延
Min DS delay	目的到源的最小时延
Number of SD delay	源到目的计算的时延数
Number of DS delay	目的到源计算的时延数
Sum of SD delay	源到目的的时延和
Sum of DS delay	目的到源的时延和
Square-Sum of SD delay	源到目的的时延的平方和
Square-Sum of DS delay	目的到源的时延的平方和
SD lost packets	源到目的方向丢失的报文个数
DS lost packets	目的到源方向丢失的报文个数

字段	描述
Lost packets for unknown reason	不能确定原因丢失的报文个数
Voice scores	语音参数，只在Voice类型测试有此信息
MOS value	为语音计算的MOS值
ICPIF value	为语音计算的ICPIF值
Hop IP	本跳IP地址，只在Path-jitter测试中存在此信息
Path-jitter results	Path-jitter测试的结果，只在Path-jitter测试中存在此信息
Jitter number	计算抖动次数，只在Path-jitter测试中存在此信息
Min/Max/Average jitter	最小/最大/平均抖动时延，单位为毫秒，只在Path-jitter测试中存在此信息
Positive jitter number	正抖动时延的数目，只在Path-jitter测试中存在此信息
Min/Max/Average positive jitter	最小/最大/平均正抖动时延，单位为毫秒，只在Path-jitter测试中存在此信息
Sum/Square-Sum positive jitter	正抖动时延之和/平方和，只在Path-jitter测试中存在此信息
Negative jitter number	负抖动时延的数目，只在Path-jitter测试中存在此信息
Min/Max/Average negative jitter	最小/最大/平均负抖动时延，单位为毫秒，只在Path-jitter测试中存在此信息
Sum/Square-Sum negative jitter	负抖动时延之和/平方和，只在Path-jitter测试中存在此信息
TTL	本次探测发送的探测报文的TTL值。如果设备配置了路由旁路功能，则TTL显示值与 init-ttl 命令配置相关，实际发送的TTL值固定为1
Hop IP	回复应答的节点IP地址
Time	收到应答报文的时间
Status	测试状态： • Succeeded: 测试成功 • Failed: 测试失败。 • In progress: 测试正在进行 • Aborted: 测试终止，表示用户手动停止测试 • Timeout: 测试超时 • Unknown error: 未知错误 • --测试状态无意义。颜色标记模式下，Yellow 和 Summary 显示结果无意义
Last completed test	当前完成的最后一步测试： • CIR test: CIR 测试 • PIR test: PIR 测试 • Traffic policing test: 流量监管测试 • Service performance test: 服务性能测试
Estimated total time	测试估算全部时间，单位秒

Actual test time used	测试实际使用时间，单位秒 说明： 测试开始结束时间以秒为单位，定时器精度为1秒，因此结果表中显示的实际测试时长（结束时间 - 开始时间）与用户配置时长存在1秒误差
CIR test (with the step of 1)	CIR测试，step取值范围为1~1000
Start time	测试开始时间
End time	测试结束时间
Min/Max/Average IR(Kbps)	最小/最大/平均速率，单位为kbit/s
Min/Max/Average FTD(us)	最小/最大/平均传输时延，单位为微秒
Min/Max/Average FDV(us)	最小/最大/平均时延抖动，单位为微秒
FL count/FLR	丢包个数/丢包率
Packets out of order	乱序报文个数
Severely Err Secs/AVAIL	SES（Severely Errored Second，严重错误秒）：测试开始后，每一秒统计一次丢包率，若该秒内丢包率大于50%，记为严重错误秒。 - 不可用周期：连续 10 个 SES 发生时，进入不可用周期，直到连续 10 个非 SES 发生时结束。 - 可用周期：连续 10 个非 SES 发生时，进入可用周期，直到连续 10 个 SES 发生时结束。 Severely Err Secs：严重错误秒总数。 AVAIL = 可用周期/总时间。测试开始时，默认为可用周期。
PIR test (color green)	PIR测试，颜色标记为绿色
PIR test (color yellow)	PIR测试，颜色标记为黄色
PIR test (summary)	PIR测试，汇总
PIR test (color-blind)	PIR测试，非颜色标记模式
Traffic policing test (color green)	流量监管测试，颜色标记为绿色
Traffic policing test (color yellow)	流量监管测试，颜色标记为黄色
Traffic policing test (summary)	流量监管测试，汇总
Traffic policing test (color-blind)	流量监管测试，非颜色标记模式
Service performance test	服务性能测试

1.1.17 display nqa statistics

display nqa statistics 命令用来显示 NQA 测试的统计信息。

【命令】

display nqa statistics [*admin-name operation-tag*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

admin-name : 创建 NQA 测试组的管理员名称, 为 1~32 个字符的字符串, 字符串中不能包括“-”, 不区分大小写。

operation-tag: 测试操作的标签, 为 1~32 个字符的字符串, 字符串中不能包括“-”, 不区分大小写。

【使用指导】

测试开始后, 如果第一次测试中的所有探测尚未完成, 则无法生成统计信息。若此时通过该命令查看统计信息, 则显示信息为全 0。

如果配置了阈值告警组, 将显示在 **statistics interval** 命令指定的统计周期内的监测结果。若阈值告警组的阈值类型为平均值, 或监测对象为 Voice 测试的 ICPIF 或 MOS 值, 则显示的监测结果为无效值。

UDP-tracert 测试类型不支持用该命令显示统计信息。

不指定任何参数, 则表示显示所有测试组的统计信息。

【举例】

显示 NQA 测试组管理员名称为 admin、测试操作标签为 test 的 TCP 测试的统计信息。

```
<Sysname> display nqa statistics admin test  
NQA entry (admin admin, tag test) test statistics:
```

```
NO. : 1  
Start time: 2007-01-01 09:30:20.0  
Life time: 2 seconds  
Send operation times: 1          Receive response times: 1  
Min/Max/Average round trip time: 13/13/13  
Square-Sum of round trip time: 169  
Extended results:  
Packet loss ratio: 0%  
Failures due to timeout: 0  
Failures due to disconnect: 0  
Failures due to no connection: 0  
Failures due to internal error: 0  
Failures due to other errors: 0
```

显示 NQA 测试组管理员名称为 admin、测试操作标签为 test 的 ICMP-jitter 测试的统计信息。

```
<Sysname> display nqa statistics admin test  
NQA entry (admin admin, tag test) test statistics:
```

```
NO. : 1  
Start time: 2015-03-09 17:42:10.7
```



```

Life time: 156 seconds
Send operation times: 1560          Receive response times: 1560
Min/Max/Average round trip time: 1/2/1
Square-Sum of round trip time: 1563
Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
ICMP-jitter results:
  RTT number: 1560
  Min positive SD: 1                Min positive DS: 1
  Max positive SD: 1                Max positive DS: 2
  Positive SD number: 18            Positive DS number: 46
  Positive SD sum: 18                Positive DS sum: 49
  Positive SD average: 1            Positive DS average: 1
  Positive SD square-sum: 18        Positive DS square-sum: 55
  Min negative SD: 1                Min negative DS: 1
  Max negative SD: 1                Max negative DS: 2
  Negative SD number: 24            Negative DS number: 57
  Negative SD sum: 24                Negative DS sum: 58
  Negative SD average: 1            Negative DS average: 1
  Negative SD square-sum: 24        Negative DS square-sum: 60
  SD average: 1                    DS average: 1
One way results:
  Max SD delay: 1                   Max DS delay: 2
  Min SD delay: 1                   Min DS delay: 1
  Number of SD delay: 4             Number of DS delay: 4
  Sum of SD delay: 4                Sum of DS delay: 5
  Square-Sum of SD delay: 4         Square-Sum of DS delay: 7
  Lost packets for unknown reason: 0
Reaction statistics:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      jitter-DS       accumulate     1500         10
  2      jitter-SD       average        -            -
  3      OWD-DS         -             1560         2
  4      OWD-SD         -             1560         0
  5      packet-loss    accumulate     0            0
  6      RTT            accumulate     1560         0
# 显示 NQA 测试组管理员名称为 admin、测试操作标签为 test 的 UDP-jitter 测试的统计信息。
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
NO. : 1
  Start time: 2007-01-01 09:33:22.3
  Life time: 23 seconds
  Send operation times: 100          Receive response times: 100

```

```

Min/Max/Average round trip time: 1/11/5
Square-Sum of round trip time: 24360
Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
UDP-jitter results:
  RTT number: 550
  Min positive SD: 1
  Max positive SD: 7
  Positive SD number: 220
  Positive SD sum: 283
  Positive SD average: 1
  Positive SD square-sum: 709
  Min negative SD: 2
  Max negative SD: 10
  Negative SD number: 81
  Negative SD sum: 556
  Negative SD average: 6
  Negative SD square-sum: 4292
  SD average: 2
  Min positive DS: 1
  Max positive DS: 1
  Positive DS number: 97
  Positive DS sum: 287
  Positive DS average: 2
  Positive DS square-sum: 1937
  Min negative DS: 1
  Max negative DS: 1
  Negative DS number: 94
  Negative DS sum: 191
  Negative DS average: 2
  Negative DS square-sum: 967
  DS average: 2
One way results:
  Max SD delay: 5
  Min SD delay: 1
  Number of SD delay: 550
  Sum of SD delay: 1475
  Square-Sum of SD delay: 5407
  SD lost packets: 0
  Lost packets for unknown reason: 0
  Max DS delay: 5
  Min DS delay: 1
  Number of DS delay: 550
  Sum of DS delay: 1201
  Square-Sum of DS delay: 3959
  DS lost packets: 0
Reaction statistics:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      jitter-DS      accumulate      90           25
  2      jitter-SD      average         -            -
  3      OWD-DS         -              100          24
  4      OWD-SD         -              100          13
  5      packet-loss    accumulate      0            0
  6      RTT            accumulate      100          52
# 显示 NQA 测试组管理员名称为 admin、测试操作标签为 test 的 Voice 测试的统计信息。
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
NO. : 1
  Start time: 2007-01-01 09:33:45.3
  Life time: 120 seconds
  Send operation times: 10
  Receive response times: 10
  Min/Max/Average round trip time: 1/12/7

```

```

    Square-Sum of round trip time: 620
Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
Voice results:
    RTT number: 10
    Min positive SD: 3
    Max positive SD: 10
    Positive SD number: 3
    Positive SD sum: 18
    Positive SD average: 6
    Positive SD square-sum: 134
    Min negative SD: 3
    Max negative SD: 9
    Negative SD number: 4
    Negative SD sum: 25
    Negative SD average: 6
    Negative SD square-sum: 187
    SD average: 6
    Min positive DS: 1
    Max positive DS: 1
    Positive DS number: 2
    Positive DS sum: 2
    Positive DS average: 1
    Positive DS square-sum: 2
    Min negative DS: 1
    Max negative DS: 1
    Negative DS number: 2
    Negative DS sum: 2
    Negative DS average: 1
    Negative DS square-sum: 2
    DS average: 1
One way results:
    Max SD delay: 0
    Min SD delay: 0
    Number of SD delay: 0
    Sum of SD delay: 0
    Square-Sum of SD delay: 0
    SD lost packets: 0
    Lost packets for unknown reason: 0
    Max DS delay: 0
    Min DS delay: 0
    Number of DS delay: 0
    Sum of DS delay: 0
    Square-Sum of DS delay: 0
    DS lost packets: 0
Voice scores:
    Max MOS value: 4.40
    Min MOS value: 4.40
    Max ICPIF value: 0
    Min ICPIF value: 0
Reaction statistics:
    Index   Checked Element   Threshold Type   Checked Num   Over-threshold Num
    1       ICPIF             -                -              -
    2       MOS               -                -              -
# 显示 NQA 测试组管理员名称为 admin、测试操作标签为 test 的 Path-jitter 测试的统计信息。
<Sysname> display nqa statistics admin test
NQA entry (admin admin, tag test) test statistics:
NO. : 1
Path 1:
Hop IP 192.168.40.210
Basic Results:
    Send operation times: 10
    Receive response times: 10
    Min/Max/Average round trip time: 1/1/1

```

```

    Square-Sum of round trip time: 10
Extended Results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
Path-Jitter Results:
    Jitter number: 9
        Min/Max/Average jitter: 0/0/0
    Positive jitter number: 0
        Min/Max/Average positive jitter: 0/0/0
        Sum/Square-Sum positive jitter: 0/0
    Negative jitter number: 0
        Min/Max/Average negative jitter: 0/0/0
        Sum/Square-Sum negative jitter: 0/0
Hop IP 192.168.50.209
Basic Results:
    Send operation times: 10
    Receive response times: 10
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 10
Extended Results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
Path-Jitter Results:
    Jitter number: 9
        Min/Max/Average jitter: 0/0/0
    Positive jitter number: 0
        Min/Max/Average positive jitter: 0/0/0
        Sum/Square-Sum positive jitter: 0/0
    Negative jitter number: 0
        Min/Max/Average negative jitter: 0/0/0
        Sum/Square-Sum negative jitter: 0/0

```

表1-7 display nqa statistics 命令显示信息描述

字段	描述
No.	统计组的组号
Start time	测试组启动时间
Life time	测试的持续时间，单位为秒
Send operation times	发送的探测报文数

字段	描述
Receive response times	收到的响应报文数
Min/Max/Average round trip time	最小/最大/平均往返时间，单位为毫秒
Square-Sum of round trip time	往返时间平方和
Packet loss ratio	平均丢包率
Failures due to timeout	测试过程中超时的次数
Failures due to disconnect	对方强制断开连接的次数
Failures due to no connection	和对方建立连接失败的次数
Failures due to internal error	因内部错误失败的次数
Failures due to other errors	因其它错误失败的次数
Packets out of sequence	报文失序的次数
Packets arrived late	迟到报文个数
ICMP-jitter results	ICMP-jitter测试的结果，只在ICMP-jitter测试中存在此信息
UDP-jitter results	UDP-jitter测试的结果，只在UDP-jitter测试中存在此信息
Voice results	Voice测试的结果，只在Voice测试中存在此信息
RTT number	收到的响应报文数
Min positive SD	源到目的方向抖动时延为正值的的最小值
Min positive DS	目的到源方向抖动时延为正值的的最小值
Max positive SD	源到目的方向抖动时延为正值的最大值
Max positive DS	目的到源方向抖动时延为正值的最大值
Positive SD number	源到目的方向抖动时延为正值的数目
Positive DS number	目的到源方向抖动时延为正值的数目
Positive SD sum	源到目的方向抖动时延为正值的和
Positive DS sum	目的到源方向抖动时延为正值的和
Positive SD average	源到目的方向抖动时延为正值的平均值
Positive DS average	目的到源方向抖动时延为正值的平均值
Positive SD square-sum	源到目的方向抖动时延为正值的平方和
Positive DS square-sum	目的到源方向抖动时延为正值的平方和
Min negative SD	源到目的方向抖动时延为负值的最小绝对值
Min negative DS	目的到源方向抖动时延为负值的最小绝对值
Max negative SD	源到目的方向抖动时延为负值的最大绝对值
Max negative DS	目的到源方向抖动时延为负值的最大绝对值
Negative SD number	源到目的方向抖动时延为负值的数目

字段	描述
Negative DS number	目的到源方向抖动时延为负值的数目
Negative SD sum	源到目的方向抖动时延为负值的绝对值和
Negative DS sum	目的到源方向抖动时延为负值的绝对值和
Negative SD average	源到目的方向抖动时延为负值的绝对值的平均值
Negative DS average	目的到源方向抖动时延为负值的绝对值的平均值
Negative SD square-sum	源到目的方向抖动时延为负值的平方和
Negative DS square-sum	目的到源方向抖动时延为负值的平方和
SD average	源到目的方向抖动时延的平均值
DS average	目的到源方向抖动时延的平均值
One way results	单向延迟测试结果，只有ICMP-jitter、UDP-Jitter和Voice类型测试有单向延迟测试结果
Max SD delay	源到目的的最大时延
Max DS delay	目的到源的最大时延
Min SD delay	源到目的的最小时延
Min DS delay	目的到源的最小时延
Number of SD delay	源到目的计算的时延数
Number of DS delay	目的到源计算的时延数
Sum of SD delay	源到目的的时延和
Sum of DS delay	目的到源的时延和
Square-Sum of SD delay	源到目的的时延的平方和
Square-Sum of DS delay	目的到源的时延的平方和
SD lost packets	源到目的方向丢失的报文个数
DS lost packets	目的到源方向丢失的报文个数
Lost packets for unknown reason	不能确定原因丢失的报文个数
Voice scores	语音参数，只在voice类型测试有此信息
Max MOS value	最大MOS值
Min MOS value	最小MOS值
Max ICPIF value	最大ICPIF值
Min ICPIF value	最小ICPIF值
Reaction statistics	阈值告警组在统计周期内的监测结果
Index	阈值告警组的编号
Checked Element	监测对象
Threshold Type	阈值类型

字段	描述
Checked Num	已监测的样本个数
Over-threshold Num	超出阈值的样本个数
Path	Path-jitter测试结果的路径序号，只在Path-jitter测试中存在此信息
Hop IP	本跳IP地址，只在Path-jitter测试中存在此信息
Path-jitter results	Path-jitter测试的结果，只在Path-jitter测试中存在此信息
Jitter number	计算抖动次数，只在Path-jitter测试中存在此信息
Min/Max/Average jitter	最小/最大/平均抖动时延，单位为毫秒，只在Path-jitter测试中存在此信息
Positive jitter number	正抖动时延的数目，只在Path-jitter测试中存在此信息
Min/Max/Average positive jitter	最小/最大/平均正抖动时延，单位为毫秒，只在Path-jitter测试中存在此信息
Sum/Square-Sum positive jitter	正抖动时延之和/平方和，只在Path-jitter测试中存在此信息
Negative jitter number	负抖动时延的数目，只在Path-jitter测试中存在此信息
Min/Max/Average negative jitter	最小/最大/平均负抖动时延，单位为毫秒，只在Path-jitter测试中存在此信息
Sum/Square-Sum negative jitter	负抖动时延之和/平方和，只在Path-jitter测试中存在此信息

表1-8 display nqa statistics 命令显示阈值告警功能相关字段取值描述
(DHCP/DLSw/DNS/FTP/HTTP/ICMP-echo/SNMP/TCP/UDP-echo 测试类型)

监测对象	阈值类型	监测的样本范围	Checked Num 取值	Over-threshold Num 取值
probe-duration	accumulate	统计周期内，进行的探测	统计周期内，已完成的探测次数	统计周期内，累计的探测持续时间不在阈值范围内的探测次数
	average	-	-	-
	consecutive	统计周期内，进行的探测	统计周期内，已完成的探测次数	统计周期内，连续的探测持续时间不在阈值范围内的探测次数
probe-fail	accumulate	统计周期内，进行的探测	统计周期内，已完成的探测次数	统计周期内，累计的失败的探测次数
	consecutive	统计周期内，进行的探测	统计周期内，已完成的探测次数	统计周期内，连续的失败的探测次数

表1-9 display nqa statistics 命令显示阈值告警功能相关字段取值描述 (ICMP-jitter/UDP-jitter/Voice 测试类型)

监测对象	阈值类型	监测的样本范围	Checked Num 取值	Over-threshold Num 取值
RTT	accumulate	统计周期内, 发送的报文	统计周期内, 已发送的报文个数	统计周期内, 累计的往返时间不在阈值范围内的报文个数
	average	-	-	-
jitter-DS/jitter-SD	accumulate	统计周期内, 发送的报文	统计周期内, 已发送的报文个数	统计周期内, 累计的单向抖动时间不在阈值范围内的报文个数
	average	-	-	-
OWD-DS/OWD-SD	-	统计周期内, 发送的报文	统计周期内, 已发送的报文个数	统计周期内, 单向时延不在阈值范围内的报文个数
packet-loss	accumulate	统计周期内, 发送的报文	统计周期内, 已发送的报文个数	统计周期内累计的丢包数
ICPIF/MOS (仅 Voice 测试支持)	-	-	-	-

【相关命令】

- **statistics interval**

1.1.18 expect { data | hex-data }

expect { data | hex-data } 命令用来配置期望测试成功的应答内容。

undo expect { data | hex-data } 命令用来恢复缺省情况。

【命令】

expect { data | hex-data } string [{ offset | strict-offset } number]
undo expect { data | hex-data }

【缺省情况】

未配置期望测试成功的应答内容。

【视图】

HTTP/HTTPS/TCP/UDP/WAP 类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

data: 表示使用文本格式的字符串来填充探测报文。

hex-data: 表示使用十六进制字符串来填充探测报文。该参数仅在 TCP/UDP/WAP 类型的 NQA 模板视图下支持。

string: 期望测试成功的应答内容。和 **data** 关键字配合使用时，为 1~200 个字符的字符串，区分大小写；和 **hex-data** 关键字配合使用时，为 2~200 个字符的字符串，字符串长度必须是偶数且不区分大小写。

offset number: 所期望的内容在返回报文中的偏移量，取值范围为 0~1000，缺省值为 0。

strict-offset number: 所期望的内容在返回报文中的严格偏移量，取值范围为 0~1000，缺省值为 0。

【使用指导】

NQA 客户端对于返回报文中期望成功的应答内容匹配方式如下：

- 如果未配置 **offset** 参数和 **strict-offset** 参数，则设备直接从返回报文对应字段的第一个字节开始匹配，若不匹配，继续从第二个字节开始匹配，以此类推，直到匹配成功，则认为测试成功，否则认为测试失败。
- 如果配置了 **offset** 参数，则设备从返回报文对应字段偏移量之后的第一个字节开始匹配，若匹配失败，则忽略该偏移量，从返回报文的第一个字节开始匹配，若不匹配，继续从第二个字节开始匹配，以此类推，直到匹配成功，则认为测试成功，否则认为测试失败。
- 如果配置了 **strict-offset** 参数，则设备从返回报文对应字段偏移量之后的第一个字节开始匹配，若匹配失败，继续从第二个字节开始匹配，以此类推，直到匹配成功，则认为测试成功，否则认为测试失败。

对于 HTTP/HTTPS 类型的 NQA 模板，仅当回应报文中存在 Content-Length 头域时，从 Content-Length 字段进行期望应答内容的检查，否则不做检查。

对于 TCP 类型的 NQA 模板，仅当 **data-fill** 和 **expect { data | hex-data }** 命令都配置时，进行期望应答内容的检查，否则不做检查。

对于 UDP 类型的 NQA 模板：

- 仅当 **data-fill** 和 **expect { data | hex-data }** 命令都配置时，进行期望应答内容的检查，否则不做检查。
- 偏移检查和 **data-fill** 是否指定 **raw** 关键字命令有关，当指定 **raw** 关键字时，从收到报文的第一个字节开始检查；当未指定 **raw** 关键字时，UDP 报文数据字段的前五个字节具有特定用途，从第六个字节开始进行偏移检查。

对于 WAP 类型的 NQA 模板，从 WSP reply 报文的 headers 字段开始进行期望应答内容的检查。当配置 **url** 命令时，WAP 测试需要通过配置本命令进行期望应答内容的检查来判断测试是否成功。当同时配置了本命令和 **expect { failed-data | hex-failed-data }** 时，如果两条命令同时匹配上，则以 **expect { failed-data | hex-failed-data }** 的匹配结果为准，认为测试失败。

【举例】

在 HTTP 类型的 NQA 模板视图下配置期望的应答内容为 welcome!。

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] expect data welcome!
```

1.1.19 expect { failed-data | hex-failed-data }

expect { failed-data | hex-failed-data } 命令用来配置期望测试失败的应答内容。

undo expect { failed-data | hex-failed-data } 命令用来恢复缺省情况。

【命令】

```
expect { failed-data | hex-failed-data } string [ { offset | strict-offset }  
number ]  
undo expect { failed-data | hex-failed-data }
```

【缺省情况】

未配置期望测试失败的应答内容。

【视图】

TCP/UDP 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

failed-data: 表示使用文本格式的字符串来填充探测报文。

hex-failed-data: 表示使用十六进制字符串来填充探测报文。

string: 期望测试失败的应答内容。和 **failed-data** 关键字配合使用时，为 1~200 个字符的字符串，区分大小写；和 **hex-failed-data** 关键字配合使用时，为 2~200 个字符的字符串，字符串长度必须是偶数且不区分大小写。

offset number: 所期望的内容在返回报文中的偏移量，取值范围为 0~1000，缺省值为 0。

strict-offset number: 所期望的内容在返回报文中的严格偏移量，取值范围为 0~1000，缺省值为 0。

【使用指导】

NQA 客户端对于返回报文中期望失败的应答内容匹配方式如下：

- 如果未配置 **offset** 参数和 **strict-offset** 参数，则设备直接从返回报文对应字段的第一个字节开始匹配，若不匹配，继续从第二个字节开始匹配，以此类推，直到匹配成功，则认为测试失败，否则认为测试成功。
- 如果配置了 **offset** 参数，则设备从返回报文对应字段偏移量之后的第一个字节开始匹配，若匹配失败，则忽略该偏移量，从返回报文的第一个字节开始匹配，若不匹配，继续从第二个字节开始匹配，以此类推，直到匹配成功，则认为测试失败，否则认为测试成功。
- 如果配置了 **strict-offset** 参数，则设备从返回报文对应字段偏移量之后的第一个字节开始匹配，若匹配失败，继续从第二个字节开始匹配，以此类推，直到匹配成功，则认为测试失败，否则认为测试成功。

对于 TCP 类型的 NQA 模板，仅当 **data-fill** 和 **expect { failed-data | hex-failed-data }** 命令都配置时，进行期望失败应答内容的检查，否则不做检查。

对于 UDP 类型的 NQA 模板：

- 仅当 **data-fill** 和 **expect { failed-data | hex-failed-data }** 命令都配置时，进行期望失败应答内容的检查，否则不做检查。

- 偏移检查和 **data-fill** 是否指定 **raw** 关键字命令有关，当指定 **raw** 关键字时，从收到报文的第一个字节开始检查；当未指定 **raw** 关键字时，UDP 报文数据字段的前五个字节具有特定用途，从第六个字节开始进行偏移检查。

当同时配置了本命令和 **expect { data | hex-data }** 时，如果两条命令同时匹配上，则以本命令的匹配结果为准，认为测试失败。

【举例】

在 TCP 类型的 NQA 模板视图下配置期望失败的应答内容为 error。

```
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] expect failed-data error
```

1.1.20 expect ip

expect ip 命令用来配置期望返回的 IP 地址。

undo expect ip 命令用来恢复缺省情况。

【命令】

```
expect ip ip-address
undo expect ip
```

【缺省情况】

未配置期望返回的 IP 地址。

【视图】

DNS 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

ip-address：DNS 探测期望返回的 IP 地址。

【使用指导】

在 DNS 测试中，NQA 客户端通过该命令配置的 IP 地址与 DNS 服务器通过域名解析出的 IP 地址进行比较，若相同，则证明目前测试的 DNS 服务器合法，否则为非法 DNS 服务器。

【举例】

在 DNS 类型的 NQA 模板视图下配置期望返回的 IP 地址为 1.1.1.1。

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] expect ip 1.1.1.1
```

1.1.21 expect ipv6

expect ipv6 命令用来配置期望返回的 IPv6 地址。

undo expect ipv6 命令用来恢复缺省情况。

【命令】

```
expect ipv6 ipv6-address  
undo expect ipv6
```

【缺省情况】

未配置期望返回的 IPv6 地址。

【视图】

DNS 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

ipv6-address: DNS 探测期望返回的 IPv6 地址。

【使用指导】

在 DNS 测试中，NQA 客户端通过该命令配置的 IPv6 地址与 DNS 服务器通过域名解析出的 IPv6 地址进行比较，若相同，则证明目前测试的 DNS 服务器合法，否则为非法 DNS 服务器。

【举例】

在 DNS 类型的 NQA 模板视图下配置期望返回的 IPv6 地址为 1::1。

```
<Sysname> system-view  
[Sysname] nqa template dns dnstplt  
[Sysname-nqatplt-dns-dnstplt] expect ipv6 1::1
```

1.1.22 expect status

expect status 命令用来配置期望的应答状态码。

undo expect status 命令用来恢复缺省情况。

【命令】

```
expect status status-list  
undo expect status [status-list]
```

【缺省情况】

未配置期望的应答状态码。

【视图】

HTTP/HTTPS/RTSP/SIP 类型的模板视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

status-list: 状态码列表, 即 HTTP/HTTPS/RTSP/SIP 模板类型期望收到的状态码范围。表示方式为 **status-list = { status-num1 [to status-num2] }&<1-10>**, **status-num** 取值范围为 0~999, **status-num2** 的值要大于或等于 **status-num1** 的值, &<1-10>表示前面的参数最多可以重复输入 10 次。

【使用指导】

HTTP/HTTPS/RTSP/SIP 类型的 NQA 模板支持配置状态码。报文的状态码是由 3 位十进制数组成的字段, 它包含服务器的状态信息, 用户可以根据该状态码了解服务器的状态。状态码的第一位规定状态码的类型。

【举例】

在 HTTP 类型的 NQA 模板视图下配置期望的应答状态码, 允许状态码为 200、300、400~500。

```
<Sysname> system-view
[Sysname] nqa template http httpplt
[Sysname-nqatplt-http-httpplt] expect status 200 300 400 to 500
```

1.1.23 filename

filename 命令用来配置 FTP 服务器和客户端之间传送文件的文件名。

undo filename 命令用来恢复缺省情况。

【命令】

```
filename filename
undo filename
```

【缺省情况】

未配置 FTP 服务器和客户端之间传送文件的文件名。

【视图】

FTP 测试类型视图

FTP 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

filename: FTP 服务器和客户端之间传送文件的文件名, 为 1~200 个字符的字符串, 字符串中不能包括 “/”, 区分大小写。

【举例】

在 FTP 测试类型下配置 FTP 服务器和客户端之间要传送文件的文件名为 config.txt。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] filename config.txt
```

```
# 在 FTP 类型的 NQA 模板视图下配置 FTP 服务器和客户端之间要传送文件的文件名为 config.txt。
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] filename config.txt
```

1.1.24 frequency

frequency 命令用来配置测试组连续两次测试开始时间的时间间隔。

undo frequency 命令用来恢复缺省情况。

【命令】

frequency *interval*

undo frequency

【缺省情况】

在 NQA 测试类型视图下，Voice、Path-jitter 测试中连续两次测试开始时间的时间间隔为 60000 毫秒；其他类型的测试中连续两次测试开始时间的时间间隔为 0 毫秒，即只进行一次测试。

在 NQA 模板视图下，测试中连续两次测试开始时间的时间间隔为 5000 毫秒。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

UDP-tracert 测试类型视图

ICMP-jitter/Path-jitter/UDP-jitter/Voice 测试类型视图

任意类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

interval：连续两次测试开始时间的时间间隔，取值范围为 0~604800000，单位为毫秒。时间间隔为 0，表示两次测试的时间间隔为无穷，即只进行一次测试，此时不会生成统计结果。

【使用指导】

通过 **nqa schedule** 命令启动 NQA 测试组后，每隔 *interval* 时间启动一次测试。

需要注意的是，如果到达 **frequency** 指定的时间间隔时，上次测试尚未完成，则不启动新一轮测试。

【举例】

在 ICMP-echo 测试类型下配置连续两次测试开始时间的时间间隔为 1000 毫秒。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] frequency 1000
```

在 DNS 类型的 NQA 模板视图下配置连续两次测试开始时间的时间间隔为 1000 毫秒。

```
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] frequency 1000
```

1.1.25 hex-data-fill

hex-data-fill 命令用来配置探测报文十六进制的填充字符串。

undo hex-data-fill 命令用来恢复缺省情况。

【命令】

```
hex-data-fill hex [ raw ]
undo hex-data-fill
```

【缺省情况】

探测报文的填充内容为十六进制数值 00010203040506070809。

【视图】

TCP/UDP 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

hex: 探测报文的填充内容，为 2~200 个字符的十六进制字符串，字符串长度必须是偶数位，不区分大小写。

raw: 表示仅使用 **hex** 来填充探测报文，该参数仅在 UDP 类型的 NQA 模板视图下支持。

【使用指导】

若指定 **raw** 参数，表示 **hex** 参数位置的填充字符串在探测时将被直接发送。

未指定 **raw** 参数，填充时，实际填充的字符与填充数据长度有关：

- 如果探测报文的数据段长度比配置的填充数据长度小，系统在报文封装时以报文的数据段长度为界截取该字符串的前一部分；
- 如果探测报文的数据段长度比配置的填充数据长度大，系统在报文封装时用该字符串进行循环填充，直到填满。

例如，配置填充数据为“abcd”，当探测报文数据段长度为 3 字节时，则取“abc”作为填充数据；当探测报文大小为 6 字节时，则使用“adcdab”作为填充数据。

【举例】

在 TCP 类型的 NQA 模板视图下配置探测报文的填充字符串为 abcd。

```
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] hex-data-fill abcd
```

1.1.26 high-performance-mode

high-performance-mode enable 命令用来开启 UDP-jitter 测试的高性能模式。

undo high-performance-mode enable 命令用来关闭 UDP-jitter 测试的高性能模式。

【命令】

```
high-performance-mode enable
undo high-performance-mode enable
```

【缺省情况】

UDP-jitter 测试的高性能模式处于关闭状态。

【视图】

UDP-jitter 测试类型视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

配置本命令后，UDP-jitter 测试将开启高性能模式，该模式下 UDP-jitter 测试的测试效率和测试结果的精确度将大大提升。

开启高性能模式后，命令 **route-option bypass-route**、**data-size**、**reaction checked-element { jitter-ds | jitter-sd } threshold-type accumulate**、**reaction checked-element rtt threshold-type accumulate** 将不再生效。

当有多个 UDP-jitter 测试需要开启高性能模式时，可以通过 **nqa agent udp-jitter high-performance enable** 命令开启 NQA 客户端所有 UDP-jitter 测试类型的高性能模式。

【举例】

```
# 开启 UDP-jitter 测试的高性能模式。
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] high-performance-mode enable
```

【相关命令】

- **nqa agent udp-jitter high-performance enable**

1.1.27 history-record enable

history-record enable 命令用来开启 NQA 测试组的历史记录保存功能。

undo history-record enable 命令用来关闭 NQA 测试组的历史记录保存功能。

【命令】

```
history-record enable
undo history-record enable
```

【缺省情况】

UDP-tracert 测试类型的历史记录保存功能处于开启状态，其他类型的 NQA 测试组的历史记录保存功能处于关闭状态。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

UDP-tracert 测试类型视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果开启 NQA 测试组的历史记录保存功能，则系统会记录该 NQA 测试组的历史信息，通过 **display nqa history** 命令可以查看该测试组的历史记录信息。

如果关闭 NQA 测试组的历史记录保存功能，则系统不会记录该测试组的历史信息，原有的历史记录信息也会被删除。

【举例】

在 ICMP-echo 测试类型下开启 NQA 测试组的历史记录保存功能。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] history-record enable
```

【相关命令】

- **display nqa history**

1.1.28 history-record keep-time

history-record keep-time 命令用来配置 NQA 测试组中历史记录的保存时间。

undo history-record keep-time 命令用来恢复缺省情况。

【命令】

history-record keep-time *keep-time*

undo history-record keep-time

【缺省情况】

NQA 测试组中历史记录的保存时间为 120 分钟。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

UDP-tracert 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

keep-time: 历史记录的保存时间, 取值范围为 1~1440, 单位为分钟。

【使用指导】

NQA 测试结束后, 开始计算该测试组中所有历史记录的保存时间。保存时间达到配置的值后, 将删除这些记录。

【举例】

在 ICMP-echo 测试类型下配置 NQA 测试组中历史记录的保存时间为 100 分钟。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record keep-time 100
```

1.1.29 history-record number

history-record number 命令用来配置在一个测试组中能够保存的最大历史记录个数。

undo history-record number 命令用来恢复缺省情况。

【命令】

history-record number *number*

undo history-record number

【缺省情况】

一个测试组中能够保存的最大历史记录个数为 50。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

UDP-tracert 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

number: 在一个测试组中能够保存的最大历史记录个数, 取值范围为 0~50。

【使用指导】

如果一个测试组中历史记录个数超过设定的最大数目, 则最早的历史记录将会被删除。

【举例】

在 ICMP-echo 测试类型下配置一个测试组中能够保存的最大历史记录数为 10 个。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-record number 10
```

1.1.30 init-ttl

init-ttl 命令用来配置 UDP-tracert 探测报文的初始跳数。

undo init-ttl 命令用来恢复缺省情况。

【命令】

```
init-ttl value  
undo init-ttl
```

【缺省情况】

UDP-tracert 探测报文的初始跳数为 1。

【视图】

UDP-tracert 测试类型视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

value: UDP-tracert 探测报文的初始跳数，取值范围 1～255。

【举例】

```
# 在 UDP-tracert 测试类型下配置 UDP-tracert 探测报文的初始跳数为 5 跳。  
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type udp-tracert  
[Sysname-nqa-admin-test-udp-tracert] init-ttl 5
```

1.1.31 key

key 命令用来设置 RADIUS 认证和计费使用的共享密钥。

undo key 命令用来恢复缺省情况。

【命令】

```
key { cipher | simple } string  
undo key
```

【缺省情况】

未设置 RADIUS 认证和计费使用的共享密钥。

【视图】

RADIUS 认证探测/RADIUS-ACCOUNT 计费探测类型的 NQA 模板视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~64 个字符的字符串，密文密钥为 1~117 个字符的字符串。

【使用指导】

必须保证设备上设置的共享密钥与 RADIUS 认证和计费服务器上的完全一致。

【举例】

在 RADIUS 类型的 NQA 模板视图下设置 RADIUS 认证使用的共享密钥为明文 abc。

```
<Sysname> system-view  
[Sysname] nqa template radius radiustplt  
[Sysname-nqatplt-radius-radiustplt] key simple abc
```

1.1.32 lsr-path

lsr-path 命令用来配置松散路由。

undo lsr-path 命令用来恢复缺省情况。

【命令】

```
lsr-path ip-address&<1-8>  
undo lsr-path
```

【缺省情况】

未配置松散路由。

【视图】

Path-jitter 测试类型视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

ip-address&<1-8>: 松散路由 IP 地址，&<1-8>表示最多可以输入 8 个 IP 地址，每个 IP 地址之间用空格分隔。

【使用指导】

通过本命令配置松散路由，用户只需给出 NQA 探测报文必须经过的一些“节点”，并不需要给出一条完备的路径，无直接连接的“节点”之间的路由需要路由器寻址功能补充。

Path-jitter 测试中，NQA 客户端通过 **tracert** 过程使用该命令配置的松散路由进行探路，并根据收到 ICMP 报文计算主要“节点”时延和抖动时间。

【举例】

在 Path-jitter 测试类型下配置松散路由为 10.1.1.20 和 10.1.2.10 两跳。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type path-jitter
[Sysname-nqa-admin-test- path-jitter] lsr-path 10.1.1.20 10.1.2.10
```

1.1.33 mailbox

mailbox 命令用来配置 IMAP 测试操作的邮箱名称。

undo mailbox 命令用来恢复缺省情况。

【命令】

```
mailbox mailbox-name
undo mailbox
```

【缺省情况】

IMAP 测试操作的邮箱名称为 INBOX。

【视图】

IMAP 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

mailbox-name: IMAP 探测使用的邮箱名称，为 1~64 个字符的字符串，区分大小写。

【举例】

在 IMAP 类型的 NQA 模板视图下配置邮箱名称为 fortest1。

```
<Sysname> system-view
[Sysname] nqa template imapimaptplt
[Sysname-nqatplt-imap-imaptplt] mailbox fortest1
```

1.1.34 max-failure

max-failure 命令用来配置一次 UDP-tracert 测试中连续探测失败的最大次数。

undo max-failure 命令用来恢复缺省情况。

【命令】

```
max-failure times
undo max-failure
```

【缺省情况】

一次 UDP-tracert 测试中连续探测失败的最大次数为 5。

【视图】

UDP-tracert 测试类型视图

【缺省用户角色】

```
network-admin
```

context-admin

【参数】

times: 表示一次 UDP-tracert 测试中连续探测失败的最大次数，取值范围 0~255。0 和 255 意味着 UDP-tracert 探测不会因为连续探测失败而停止测试。

【使用指导】

当 UDP-tracert 测试中连续探测失败的次数达到指定的最大值时，设备认为测试失败并停止探测。

【举例】

在 UDP-tracert 测试类型下配置一次 UDP-tracert 测试中连续探测失败的最大次数为 20 次。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-tracert
[Sysname-nqa-admin-test-udp-tracert] max-failure 20
```

1.1.35 memory

memory 命令用来配置 SNMP-DCA 测试的 SNMP Agent 内存的阈值和权重。

undo memory 命令用来恢复缺省情况。

【命令】

```
memory { threshold threshold-value | weight weight-value } *
undo memory
```

【缺省情况】

SNMP-DCA 测试的 SNMP Agent 内存的阈值为 70，权重为 2。

【视图】

SNMP-DCA 类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

threshold threshold-value: 阈值，表示内存使用率可达到的上限。取值范围为 0~100，取值为 0 时表示内存不作为判断 SNMP Agent 是否繁忙的参考。不指定该参数时，表示使用缺省值。

weight weight-value: 权重，表示内存存在用于计算 SNMP Agent 状态时应占有的比重。取值范围为 0~100，取值为 0 时表示内存权重不参与计算 SNMP Agent 的状态。不指定该参数时，表示使用缺省值。

【使用指导】

本命令仅对 Net-SNMP 或 Windows 类型的 SNMP Agent 生效。

NQA 客户端对 Net-SNMP 或 Windows 类型的 SNMP Agent 进行 SNMP-DCA 测试时，会自动获取 SNMP Agent 当前的内存使用率。

【举例】

在 SNMP-DCA 类型的 NQA 模板视图下配置测试的 SNMP Agent 内存的阈值为 90、权重为 90。

```
<Sysname> system-view
[Sysname] nqa template snmpdca test
[Sysname-nqatplt-snmpdca-test] memory threshold 90 weight 90
```

【相关命令】

- **agent-type**

1.1.36 mode

mode 命令用来配置 FTP 测试的数据传输方式。

undo mode 命令用来恢复缺省情况。

【命令】

```
mode { active | passive }
undo mode
```

【缺省情况】

FTP 测试的数据传输方式为主动方式。

【视图】

FTP 测试类型视图

FTP 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

active: 设置 FTP 的数据传输方式为主动方式。表示在建立数据连接时由服务器主动发起连接请求。

passive: 设置 FTP 的数据传输方式为被动方式。表示在建立数据连接时由客户端主动发起连接请求。

【举例】

在 FTP 测试类型下配置 FTP 测试的数据传输方式为被动方式。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] mode passive
# 在 FTP 类型的 NQA 模板视图下配置数据传输方式为被动方式。
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] mode passive
```

1.1.37 next-hop ip

next-hop ip 命令用来配置探测报文的下一跳 IP 地址。

undo next-hop ip 命令用来恢复缺省情况。

【命令】

next-hop ip *ip-address*

undo next-hop ip

【缺省情况】

未配置探测报文的下一跳 IP 地址。

【视图】

ICMP-echo 测试类型视图

DNS/ICMP/TCP Half Open 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: 探测报文的下一跳 IP 地址。

【使用指导】

配置本命令之后，设备按照指定的下一跳地址发送探测报文；若未配置本命令，则按照路由表缺省的转发规则发送探测报文。

【举例】

在 ICMP-echo 测试类型下配置探测报文的下一跳 IP 地址为 10.1.1.1。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.1
```

1.1.38 next-hop ipv6

next-hop ipv6 命令用来配置探测报文的下一跳 IPv6 地址。

undo next-hop ipv6 命令用来恢复缺省情况。

【命令】

next-hop ipv6 *ipv6-address*

undo next-hop ipv6

【缺省情况】

未配置探测报文的下一跳 IPv6 地址。

【视图】

ICMP-echo 测试类型视图

DNS/ICMP/TCP Half Open 类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

ipv6-address: 探测报文的下一跳 IPv6 地址，不支持 IPv6 链路本地地址。

【使用指导】

配置本命令之后，设备按照指定的下一跳地址发送探测报文；若未配置本命令，则按照路由表缺省的转发规则发送探测报文。

【举例】

```
# 在 ICMP-echo 测试类型下配置探测报文的下一跳 IPv6 地址为 10::1。  
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type icmp-echo  
[Sysname-nqa-admin-test-icmp-echo] next-hop ipv6 10::1
```

1.1.39 no-fragment enable

no-fragment enable 命令用来开启 UDP-tracert 探测类型的禁止报文分片功能。

undo no-fragment enable 命令用来关闭 UDP-tracert 探测类型的禁止报文分片功能。

【命令】

no-fragment enable
undo no-fragment enable

【缺省情况】

UDP-tracert 测试类型的禁止报文分片功能处于关闭状态。

【视图】

UDP-tracert 测试类型视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

开启此功能后，设备发送的 IP 报文头部的 DF（don't fragment）字段会被置一，这样报文在转发过程中将无法被分片。通过配置这条命令可以对一条链路的路径 MTU 值进行测试。

【举例】

```
# 在 UDP-tracert 测试类型下开启 UDP-tracert 探测类型的禁止报文分片功能。  
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type udp-tracert  
[Sysname-nqa-admin-test-udp-tracert] no-fragment enable
```

1.1.40 nqa

nqa 命令用来创建 NQA 测试组，并进入 NQA 测试组视图。如果指定的 NQA 测试组视图已经存在，则直接进入 NQA 测试组视图。

undo nqa 命令用来删除指定的 NQA 测试组。

【命令】

```
nqa entry admin-name operation-tag  
undo nqa { all | entry admin-name operation-tag }
```

【缺省情况】

不存在 NQA 测试组。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

admin-name: 创建 NQA 测试组的管理员名称，为 1~32 个字符的字符串，字符串中不能包括“-”，不区分大小写。

operation-tag: 测试操作的标签，为 1~32 个字符的字符串，字符串中不能包括“-”，不区分大小写。

all: 所有 NQA 测试组、模板和操作组。

【举例】

```
# 创建一个管理员名为 admin，测试操作标签为 test 的 NQA 测试组，并进入 NQA 测试组视图。  
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test]
```

1.1.41 nqa agent enable

nqa agent enable 命令用来开启 NQA 客户端功能。

undo nqa agent enable 命令用来关闭 NQA 客户端功能，并停止所有正在进行的测试。

【命令】

```
nqa agent enable  
undo nqa agent enable
```

【缺省情况】

NQA 客户端功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 开启 NQA 客户端功能。  
<Sysname> system-view  
[Sysname] nqa agent enable
```

【相关命令】

- **nqa server enable**

1.1.42 nqa agent udp-jitter high-performance enable

nqa agent udp-jitter high-performance enable 命令用来全局开启 UDP-jitter 测试的高性能模式。

undo nqa agent udp-jitter high-performance enable 命令用来全局关闭 UDP-jitter 测试的高性能模式。

【命令】

```
nqa agent udp-jitter high-performance enable  
undo nqa agent udp-jitter high-performance enable
```

【缺省情况】

UDP-jitter 测试的高性能探测模式处于全局关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

用户可在系统视图和 UDP-jitter 测试类型视图下开启 UDP-jitter 测试的高性能模式。

- 系统视图下可以开启所有 UDP-jitter 测试的高性能模式，UDP-jitter 测试类型视图下只能开启该视图下 UDP-jitter 测试的高性能模式。
- 从系统视图和 UDP-jitter 测试类型视图任意一个都能开启 UDP-jitter 测试的高性能模式，但若关闭 UDP-jitter 测试的高性能模式，则必须将两个视图下的 UDP-jitter 测试的高性能模式都关闭。

开启全局高性能模式后，命令 **route-option bypass-route、data-size、reaction checked-element { jitter-ds | jitter-sd } threshold-type accumulate、reaction checked-element rtt threshold-type accumulate** 将不再生效。

【举例】

```
# 全局开启 UDP-jitter 的高性能模式。
```

<Sysname> system-view

[Sysname] nqa agent udp-jitter high-performance enable

【相关命令】

- **high-performance enable**

1.1.43 nqa schedule

nqa schedule 命令用来配置测试组的启动时间和持续时间。

undo nqa schedule 命令用来停止指定测试组的测试。

【命令】

nqa schedule *admin-name operation-tag start-time* { *hh:mm:ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

undo nqa schedule *admin-name operation-tag*

【缺省情况】

未配置 NQA 调度功能。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

admin-name: 创建 NQA 测试组的管理员名称, 为 1~32 个字符的字符串, 字符串中不能包括“-”, 不区分大小写。

operation-tag: 测试操作的标签, 为 1~32 个字符的字符串, 字符串中不能包括“-”, 不区分大小写。

start-time: 指定测试组的启动时间和日期。

hh:mm:ss: 测试组的启动时间, 小时:分钟:秒。

yyyy/mm/dd: 测试组的启动日期, 年:月:日, 缺省值为系统的当前日期, 年的取值范围为 2000~2035。

mm/dd/yyyy: 测试组的启动日期, 月:日:年, 缺省值为系统的当前日期, 年的取值范围为 2000~2035。

now: 测试组立即开始测试。

lifetime: 指定测试的持续时间。

lifetime: 测试的持续时间, 取值范围为 1~2147483647, 单位为秒。

forever: 测试组将一直进行测试。

recurring: 指定测试组每天都被调度运行。每天启动测试的时间由 **start-time** 参数指定。若不指定该参数, 则测试组只在当天的指定时间内调度运行一次。

【使用指导】

测试组被调度后不允许进入测试类型视图。若需要重新进入测试类型视图，请使用 **undo nqa schedule** 命令停止指定测试组的测试。

系统时间在启动时间～启动时间+持续时间范围内时，测试组进行测试。执行 **nqa schedule** 命令时，如果系统时间尚未到达启动时间，则到达启动时间后，启动测试；如果系统时间在启动时间～启动时间+持续时间之间，则立即启动测试；如果系统时间已经超过启动时间+持续时间，则不会启动测试。通过 **display clock** 命令可以显示系统的当前时间。

测试组被调度后不允许进入测试类型视图。若需要重新进入测试类型视图，请使用 **undo nqa schedule** 命令停止指定测试组的测试。

配置 lifetime 时间请保证一次测试能够完成，否则无法完成正常的联动操作。

【举例】

启动管理员名称为 admin，标签为 test 的测试组进行测试，测试组的启动时间为 2008 年 8 月 8 日以后（包含当天）的每天的 08:08:08，测试持续时间为 1000 秒。

```
<Sysname> system-view
```

```
[Sysname] nqa schedule admin test start-time 08:08:08 2008/08/08 lifetime 1000 recurring
```

【相关命令】

- **destination ip**
- **display clock**（基础配置命令参考/设备管理）
- **nqa entry**
- **type**

1.1.44 nqa template

nqa template 命令用来创建指定类型 NQA 模板，并进入 NQA 模板视图。如果指定的 NQA 模板视图已经存在，则直接进入 NQA 模板视图。

undo nqa template 命令用来删除指定类型的 NQA 模板。

【命令】

```
nqa template { arp | dns | ftp | http | https | icmp | imap | pop3 | radius |  
radius-account | rtsp | sip | smtp | snmp | snmpdca | ssl | tcp | tcphalfopen  
| udp | wap } name
```

```
undo nqa template { arp | dns | ftp | http | https | icmp | imap | pop3 | radius  
| radius-account | rtsp | sip | smtp | snmp | snmpdca | ssl | tcp | tcphalfopen  
| udp | wap } name
```

【缺省情况】

不存在 NQA 模板。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

arp: 配置 ARP 模板类型。
dns: 配置 DNS 模板类型。
ftp: 配置 FTP 模板类型。
http: 配置 HTTP 模板类型。
https: 配置 HTTPS 模板类型。
icmp: 配置 ICMP 模板类型。
imap: 配置 IMAP 模板类型。
pop3: 配置 POP3 模板类型。
radius: 配置 RADIUS 认证探测模板类型。
radius-account: 配置 RADIUS-ACCOUNT 计费探测模板类型。
rtsp: 配置 RTSP 模板类型。
sip: 配置 SIP 模板类型。
smtp: 配置 SMTP 模板类型。
snmp: 配置 SNMP 模板类型。
snmpdca: 配置 SNMP DCA 模板类型。
ssl: 配置 SSL 模板类型。
tcp: 配置 TCP 模板类型。
tcphalfopen: 配置 TCP Half Open 模板类型。
udp: 配置 UDP 模板类型。
wap: 配置 WAP 模板类型。
name: NQA 模板名称，为 1~32 个字符的字符串，不区分大小写。

【举例】

```
# 创建一个类型为 ICMP、名称为 icmptplt 的模板，并进入 NQA 模板视图。  
<Sysname> system-view  
[Sysname] nqa template icmp icmptplt  
[Sysname-nqatplt-icmp-icmptplt]
```

1.1.45 oid

oid 命令用来配置 SNMP-DCA 测试的 SNMP Agent 上 MIB 节点的阈值和权重。
undo oid 命令用来恢复缺省情况。

【命令】

```
oid oid threshold threshold-value weight weight-value  
undo oid oid
```

【缺省情况】

未配置 SNMP-DCA 测试的 SNMP Agent 上 MIB 节点的阈值和权重。

【视图】

SNMP-DCA 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

oid: SNMP-DCA 测试的 SNMP Agent 上 MIB 节点的 OID，为 1~255 个字符的字符串，其中 OID 指代的 MIB 节点的返回值必须为 MIB 节点的资源使用率。

threshold threshold-value: 阈值，表示 MIB 节点的资源使用率可达到的上限，取值范围为 0~100。取值为 0 时表示该 MIB 节点不作为判断 SNMP Agent 是否繁忙的参考。

weight weight-value: 权重，表示 MIB 节点在用于计算 SNMP Agent 状态时应占有的比重。取值范围为 0~100，取值为 0 时表示该 MIB 节点的权重不参与 SNMP Agent 状态的计算。

【使用指导】

当 **agent-type** 配置为 User-defined 时，必须进行本配置，用户最多可以配置 8 条自定义的 OID 命令。

NQA 客户端对 Net-SNMP 或 Windows 类型的 SNMP Agent 进行 SNMP-DCA 测试时，会自动获取 SNMP Agent 当前 MIB 节点的资源使用率。

【举例】

在 SNMP-DCA 类型的 NQA 模板视图下配置测试的 SNMP Agent 上 MIB 节点的阈值和权重。

```
<Sysname> system-view
```

```
[Sysname] nqa template snmpdca test
```

```
[Sysname-nqatplt-snmpdca-test] oid 1.3.6.1.4.1.2021.11.11.0 threshold 90 weight 90
```

【相关命令】

- **agent-type**

1.1.46 operation (FTP test type view)

operation 命令用来配置 FTP 测试的操作方式。

undo operation 命令用来恢复缺省情况。

【命令】

operation { get | put }

undo operation

【缺省情况】

FTP 测试的操作方式为 **get** 操作。

【视图】

FTP 测试类型视图

FTP 类型的模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

get: 从 FTP 服务器获取文件。

put: 向 FTP 服务器传送文件。

【使用指导】

进行 **put** 操作时，若配置了 **filename**，发送数据前判断 **filename** 指定的文件是否存在，如果存在则上传该文件，如果不存在则探测失败。

进行 **get** 操作时，如果 FTP 服务器上没有以 **url** 中所配置的文件名为名称的文件，则测试不会成功。进行 **get** 操作时，设备上不会保存从服务器获取的文件。

进行 **get**、**put** 操作时，请选用较小的文件进行测试，如果文件较大，可能会因为超时而导致测试失败，或由于占用较多的网络带宽而影响其他业务。

【举例】

在 FTP 测试类型下配置 FTP 测试的操作方式为 **put** 操作。

```
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type ftp  
[Sysname-nqa-admin-test-ftp] operation put
```

在 FTP 类型的 NQA 模板视图下配置测试的操作方式为 **put** 操作。

```
<Sysname> system-view  
[Sysname] nqa template ftp ftptplt  
[Sysname-nqatplt-ftp-ftptplt] operation put
```

【相关命令】

- **password**
- **username**

1.1.47 operation (HTTP test type view)

operation 命令用来配置 HTTP 测试的操作方式。

undo operation 命令用来恢复缺省情况。

【命令】

```
operation { get | post | raw }  
undo operation
```

【缺省情况】

HTTP 测试的操作方式为 **get** 操作。

【视图】

HTTP 测试类型视图

HTTP 类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

get: 从 HTTP 服务器获取数据。
post: 向 HTTP 服务器提交数据。
raw: 向 HTTP 服务器发送 RAW 请求报文。

【使用指导】

HTTP 测试中以 HTTP 请求报文作为探测报文。

测试的操作方式为 **get** 或 **post** 时，请求报文内容从 url 中获取。

测试的操作方式为 **raw** 时，请求报文为 **raw-request** 子视图中配置的内容。在配置 HTTP 操作方式中的 **raw** 操作可以通过在 **raw-request** 子视图中配置 **get**、**post** 或其他服务器支持的请求类型的 HTTP 报文，以此直接作为探测报文。请确保 **raw-request** 子视图中所配置报文内容的正确性。

【举例】

```
# 在 HTTP 测试类型下配置 HTTP 测试的操作方式为 raw 操作。
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] operation raw
# 在 HTTP 类型的 NQA 模板视图下配置测试的操作方式为 raw 操作。
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] operation raw
```

【相关命令】

- **password**
- **raw-request**
- **username**

1.1.48 operation (HTTPS template view)

operation 命令用来配置 HTTPS 测试的操作方式。

undo operation 命令用来恢复缺省情况。

【命令】

```
operation { get | post | raw }
undo operation
```

【缺省情况】

HTTPS 测试的操作方式为 **get** 操作。

【视图】

HTTPS 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

get: 从 HTTPS 服务器获取数据。

post: 向 HTTPS 服务器提交数据。

raw: 向 HTTPS 服务器发送 RAW 请求报文。

【使用指导】

HTTPS 测试中以 HTTPS 请求报文作为探测报文。

测试的操作方式为 **get** 或 **post** 时，请求报文内容从 url 中获取。

测试的操作方式为 **raw** 时，请求报文为 **raw-request** 子视图中配置的内容。在配置 HTTPS 操作方式中的 **raw** 操作可以通过在 **raw-request** 子视图中配置 **get**、**post** 或其他服务器支持的请求类型的 HTTPS 报文，以此直接作为探测报文。请确保 **raw-request** 子视图中所配置报文内容的正确性。

【举例】

在 HTTPS 类型的 NQA 模板视图下配置测试的操作方式为 **raw** 操作。

```
<Sysname> system-view  
[Sysname] nqa template https httptplt  
[Sysname-nqatplt-https-httptplt] operation raw
```

【相关命令】

- **password**
- **raw-request**
- **username**

1.1.49 out interface

out interface 命令用来指定探测报文的出接口。

undo out interface 命令用来恢复缺省情况。

【命令】

```
out interface interface-type interface-number  
undo out interface
```

【缺省情况】

未指定探测报文的出接口。

【视图】

ICMP-echo 测试类型视图

DHCP 测试类型视图

UDP-tracert 测试类型视图

UDP-jitter 测试类型视图

DNS/ICMP/TCP Half Open 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type interface-number: 探测报文出接口的接口类型和接口编号。

【使用指导】

该命令指定的接口必须处于 UP 状态，否则 NQA 探测过程将会失败。

对于 ICMP-echo 测试类型和 DNS/ICMP/TCP Half Open 类型的 NQA 模板，如果配置 **next-hop** 命令，此配置不生效。

【举例】

1.1.50 password

password 命令用来配置测试服务器的用户登录密码。

undo password 命令用来恢复缺省情况。

【命令】

password { cipher | simple } string

undo password

【缺省情况】

未配置测试服务器的用户登录密码。

【视图】

FTP/HTTP 测试类型视图

FTP/HTTP/HTTPS/IMAP/POP3/RADIUS 认证探测类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

cipher: 以密文方式设置密码。

simple: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。对于 FTP/HTTP/HTTPS，明文密码为 1~32 个字符的字符串，密文密码为 1~73 个字符的字符串；对于 RADIUS，明文密码为 1~64 个字符的字符串，密文密码为 1~117 个字符的字符串；对于 IMAP/POP3，明文密码为 1~40 个字符的字符串，密文密码为 1~85 个字符的字符串。

【举例】

在 FTP 测试类型下配置 FTP 服务器的用户登录密码为 ftpuser。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] password simple ftpuser
```

在 FTP 类型的 NQA 模板视图下配置 FTP 服务器的用户登录密码为 ftpuser。

```
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] password simple ftpuser
```

【相关命令】

- operation
- username

1.1.51 port-detect enable

port-detect enable 命令用来开启端口检测功能。

undo port-detect enable 命令用来关闭端口检测功能。

【命令】

```
port-detect enable
undo port-detect enable
```

【缺省情况】

端口检测功能处于关闭状态。

【视图】

TCP Half Open/UDP 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启 TCP Half Open 模板的端口检测功能是为了测试对端 TCP 服务的端口是否可用。NQA 客户端将主动向对端发出 TCP SYN 报文，如果在探测超时时间（**probe timeout** 命令配置）内，收到目的端回应的 SYN+ACK 报文，则认为测试成功，反之则认为测试失败。

开启 UDP 模板的端口检测功能用于测试对端 UDP 服务的端口是否可用。如果在探测超时时间（**probe timeout** 命令配置）内，没有收到任何标识目的端不可达的 ICMP 差错报文，则认为测试成功，反之则认为测试失败。需要在目的端开启 ICMP 目的不可达报文发送功能，如果目的端是 UNIS 设备，需要在设备上执行 **ip unreachable enable** 命令。另外，需要配置 **data-fill string raw** 或 **hex-data-fill hex raw** 命令，填充字符串可以在参数允许范围内的任意值。

要使本功能生效，必须通过 **destination port** 命令配置目的端口号。

【举例】

在 TCP Half Open 类型的 NQA 模板视图下开启 TCP Half Open 的端口检测功能。

```
<Sysname> system-view
[Sysname] nqa template tcphalfopen tplt
[Sysname-nqatplt-tcphalfopen-tplt] port-detect enable
```

【相关命令】

- **data-fill**
- **destination port**
- **hex-data-fill**
- **ip unreachable enable**（三层技术-IP 业务命令参考/IP 性能优化）

1.1.52 probe count

probe count 命令用来配置一次 NQA 测试中探测的次数。

undo probe count 命令用来恢复缺省情况。

【命令】

```
probe count times
undo probe count
```

【缺省情况】

对于 UDP-tracert 测试类型，对于一个 TTL 值的节点发送的探测报文次数为 3 次；其他类型的 NQA 测试一次 NQA 测试中的探测次数为 1 次。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

UDP-tracert 测试类型视图

ICMP-jitter/UDP-jitter 测试类型视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

times：对于 UDP-tracert 测试类型，表示对于一个 TTL 值的节点发送的探测报文次数，取值范围为 1~10；对于其他测试类型，表示一次 NQA 测试中进行探测的次数，取值范围为 1~15。

【使用指导】

不同测试类型中，探测的含义不同：

- 对于 TCP 和 DLSw 测试，一次探测操作是指建立一次连接。
- 对于 ICMP-jitter 和 UDP-jitter 测试，一次探测操作是指连续发送多个探测报文，发送探测报文的个数由 **probe packet-number** 命令指定。

- 对于 FTP、HTTP、DHCP 和 DNS 测试，一次探测操作是指完成一次相应的功能，例如上传或下载一个文件，获取一个 Web 页面，为接口申请一个 IP 地址，将一个域名解析为 IP 地址。
- 对于 ICMP-echo 和 UDP-echo 测试，一次探测操作是指发送一个探测报文。
- 对于 SNMP 测试，一次探测操作是指发送三个 SNMP 协议报文，分别对应 SNMP v1、SNMP v2c 和 SNMP v3 三个版本。
- 对于 Path-jitter 测试，一次探测操作分为两个步骤：首先通过 **tracert** 探路获取到达目的地址的路径（最大为 64 跳）；再根据 **tracert** 结果，分别向路径上的每一跳发送多个 ICMP-echo 探测报文，发送探测报文的个数由用户来设定。
- 对于 UDP-tracert 测试，一次探测操作是指一个特定 TTL 值的节点发送一个探测报文的操作。

对于 UDP-tracert 测试，同一个 TTL 的节点，设备会发送数量为 **probe count** 命令配置的探测报文，系统在进行第一次探测之后，等待回应；对于其他类型的测试，如果配置的次数大于 1，那么系统在进行第一次探测之后，等待回应。如果到达 **probe timeout** 命令指定的探测超时时间时，仍然没有收到回应，则发起第二次探测。如此反复，直到完成指定次数的探测。

Voice 和 Path-jitter 测试不支持该命令，一次测试中只能进行一次探测。

【举例】

```
# 在 ICMP-echo 测试类型下配置一次 ICMP-echo 测试中探测的次数为 10 次。
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] probe count 10
```

1.1.53 probe packet-interval

probe packet-interval 命令用来配置发送探测报文的时间间隔。

undo probe packet-interval 命令用来恢复缺省情况。

【命令】

```
probe packet-interval interval
undo probe packet-interval
```

【缺省情况】

发送探测报文的时间间隔为 20 毫秒。

【视图】

ICMP-jitter/Path-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interval：测试中发送探测报文的时间间隔，取值范围为 10~60000，单位为毫秒。

【举例】

```
# 在 UDP-jitter 测试类型下配置测试中发送探测报文的时间间隔为 100 毫秒。
```

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-interval 100
```

1.1.54 probe packet-number

probe packet-number 命令用来配置一次探测中发送探测报文的个数。

undo probe packet-number 命令用来恢复缺省情况。

【命令】

probe packet-number *packet-number*

undo probe packet-number

【缺省情况】

一次 ICMP-jitter、UDP-jitter 或 Path-jitter 探测中发送 10 个探测报文；一次 Voice 探测中发送 1000 个探测报文。

【视图】

ICMP-jitter/Path-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

packet-number：一次探测中发送探测报文的个数，对于 ICMP-jitter、UDP-jitter 和 Path-jitter 测试，取值范围为 10～1000；对于 Voice 测试，取值范围为 10～60000。

【举例】

在 UDP-jitter 测试类型下配置一次探测中发送 100 个探测报文。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-number 100
```

1.1.55 probe packet-timeout

probe packet-timeout 命令用来配置一次探测中等待响应报文的超时时间。

undo probe packet-timeout 命令用来恢复缺省情况。

【命令】

probe packet-timeout *timeout*

undo probe packet-timeout

【缺省情况】

ICMP-jitter、UDP-jitter 和 Path-jitter 测试中等待响应报文的超时时间为 3000 毫秒；Voice 测试中等待响应报文的超时时间为 5000 毫秒。

【视图】

ICMP-jitter/Path-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

timeout: 一次探测中等待响应报文的超时时间，取值范围为 10~3600000，单位为毫秒。

【举例】

在 UDP-jitter 测试类型下配置一次探测中等待响应报文的超时时间为 100 毫秒。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] probe packet-timeout 100
```

1.1.56 probe timeout

probe timeout 命令用来配置探测的超时时间。

undo probe timeout 命令用来恢复缺省情况。

【命令】

probe timeout *timeout*

undo probe timeout

【缺省情况】

探测的超时时间为 3000 毫秒。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

UDP-tracert 测试类型视图

任意类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

timeout: 一次探测的超时时间，单位为毫秒。在 FTP、HTTP 探测中，取值范围为 10~86400000；在 DHCP、DLSw、DNS、ICMP-echo、SNMP、TCP、UDP-echo 和 UDP-tracert 探测中，取值范围为 10~3600000。对于 NQA 模板类型来说，FTP、HTTP 和 HTTPS 模板的范围为 10~86400000，其他模板范围为 10~3600000。

【使用指导】

如果 NQA 探测没有在 **probe timeout** 命令指定的时间内完成，则认为本次探测超时。

【举例】

在 ICMP-echo 测试类型下配置探测的超时时间为 10000 毫秒。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] probe timeout 10000
```

在 HTTP 类型的 NQA 模板视图下配置探测的超时时间为 10000 毫秒。

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] probe timeout 10000
```

1.1.57 proxy-url

proxy-url 命令用来配置 HTTP/HTTPS 代理服务器的网址。

undo proxy-url 命令用来恢复缺省情况。

【命令】

```
proxy-url url
undo proxy-url
```

【缺省情况】

未配置 HTTP/HTTPS 代理服务器的网址。

【视图】

HTTP/HTTPS 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

url: HTTP/HTTPS 代理服务器的网址，为 1~255 个字符的字符串，区分大小写。url 的主机名部分，由“.”分隔的字符串组成（如 aabbcc.com），每个字符串的长度不超过 63 个字符，区分大小写；字符串中可以包含字母、数字、“-”及“_”，不能出现连续“.”。

- HTTP 测试类型时，url 格式为 http://host 或 http://host:port。
- HTTPS 测试类型时，url 格式为 https://host 或 https://host:port。

【使用指导】

在必须通过代理服务器才能访问 HTTP/HTTPS 服务器的组网环境下，必须配置本命令。配置本命令后，设备发送的探测报文以及 HTTP/HTTPS 服务器返回的响应报文，都会经过代理服务器中转。

【举例】

在 HTTP 类型的 NQA 模板视图下配置 HTTP 代理服务器的网址为 http://www.company.com。

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] proxy-url http://www.company.com
```

1.1.58 raw-request

raw-request 命令用来进入 raw-request 子视图，并在该子视图下配置 HTTP/HTTPS 测试请求报文内容。

undo raw-request 命令用来恢复缺省情况。

【命令】

```
raw-request
undo raw-request
```

【缺省情况】

未配置 HTTP/HTTPS 测试请求报文的内容。

【视图】

HTTP 测试类型视图
HTTP/HTTPS 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

每次使用 **raw-request** 命令进入 raw-request 子视图时，之前在该子视图下配置的 HTTP 测试请求报文内容会被清除。

HTTP/HTTPS 测试的操作方式为 **raw** 时，必须配置该命令。raw-request 子视图中所配置报文内容为 HTTP/HTTPS 的请求报文，要求报文内容中不能包含 **alias** 命令配置的别名，请用户自行确保报文的正确性，否则探测将失败。有关 **alias** 命令的详细介绍请参见“基础配置命令参考”中的“CLI”。

【举例】

进入 raw-request 子视图，并在该子视图下配置 HTTP 测试 GET 操作的请求报文的内容。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] raw-request
[Sysname-nqa-admin-test-http-raw-request] GET /sdn/ui/app/index HTTP/1.0\r\nHost:
172.0.0.2\r\n\r\n
```

在 HTTP 类型的 NQA 模板视图下，进入 raw-request 子视图，并在该子视图下配置 HTTP 测试 POST 操作的请求报文的内容。

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] raw-request
[Sysname-nqatplt-http-httptplt-raw-request] POST /sdn/ui/app/index HTTP/1.0\r\nHost:
172.0.0.2\r\nAuthorization: Basic cm9vdDoxMjM0NTY=\r\n\r\n
```

1.1.59 reaction checked-element { jitter-ds | jitter-sd }

reaction checked-element { jitter-ds | jitter-sd }命令用来创建监测单向抖动时间的阈值告警组。

undo reaction 命令用来删除指定的阈值告警组。

【命令】

```
reaction item-number checked-element { jitter-ds | jitter-sd }  
threshold-type { accumulate accumulate-occurrences | average }  
threshold-value upper-threshold lower-threshold [ action-type { none |  
trap-only } ]  
undo reaction item-number
```

【缺省情况】

不存在监测单向抖动时间的阈值告警组。

【视图】

ICMP-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

network-admin
context-admin

【参数】

item-number: 阈值告警组编号，取值范围为 1~10。

jitter-ds: 监测从目的到源的单向抖动时间。

jitter-sd: 监测从源到目的的单向抖动时间。

threshold-type: 指定阈值类型。

accumulate accumulate-occurrences: 每次测试中，累计的单向抖动时间超出阈值的报文个数。对于 ICMP-jitter 与 UDP-jitter 测试，取值为 1~14999；对于 Voice 测试，取值范围为 1~59999。

average: 每次测试中，单向抖动时间的平均值。

threshold-value: 指定阈值范围。

upper-threshold: 阈值上限，取值范围为 0~3600000，单位为毫秒。

lower-threshold: 阈值下限，取值范围为 0~3600000，且必须小于等于阈值上限，单位为毫秒。

action-type: 触发的动作类型，缺省动作类型为 none。

none: 只在显示信息中记录监测结果，不向网管发送 Trap 消息。

trap-only: 条件满足时，在显示信息中记录监测结果的同时，向网管发送 Trap 消息。

【使用指导】

阈值告警组创建后，不能再通过 **reaction** 命令修改该阈值告警组的内容。若要修改阈值告警组的内容，则需要先通过 **undo reaction** 命令用来删除阈值告警组，再利用新的参数创建阈值告警组。

监测的对象是探测成功的报文，探测失败的报文不参与计数。

【举例】

在 UDP-jitter 测试类型下创建编号为 1 的阈值告警组，监测 UDP-jitter 探测报文的从目的到源的单向抖动时间，阈值上限为 50 毫秒，下限为 5 毫秒。NQA 测试组启动前，初始的阈值状态为 invalid。每次测试结束后，检查本次测试的平均单向抖动时间，若超出阈值，阈值状态置为 over-threshold；反之，置为 below-threshold。当阈值状态改变时，向网管发送 Trap 消息。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type udp-jitter
```

```
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element jitter-ds threshold-type  
average threshold-value 50 5 action-type trap-only
```

在 UDP-jitter 测试类型下创建编号为 2 的阈值告警组，监测 UDP-jitter 探测报文的从目的到源的单向抖动时间，阈值上限为 50 毫秒，下限为 5 毫秒。NQA 测试组启动前，初始的阈值状态为 invalid。每次测试结束后，检查本次测试中累计的单向抖动时间超出阈值的报文个数，若达到或超过 100 个，阈值状态置为 over-threshold；反之，置为 below-threshold。当阈值状态改变时，向网管发送 Trap 消息。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type udp-jitter
```

```
[Sysname-nqa-admin-test-udp-jitter] reaction 2 checked-element jitter-ds threshold-type  
accumulate 100 threshold-value 50 5 action-type trap-only
```

1.1.60 reaction checked-element { owd-ds | owd-sd }

reaction checked-element { owd-ds | owd-sd } 命令用来创建监测单向时延的阈值告警组。

undo reaction 命令用来删除指定的阈值告警组。

【命令】

**reaction item-number checked-element { owd-ds | owd-sd } threshold-value
upper-threshold lower-threshold**

undo reaction item-number

【缺省情况】

不存在监测单向时延的阈值告警组。

【视图】

ICMP-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

item-number：阈值告警组编号，取值范围为 1~10。

owd-ds：监测每个探测报文的从目的到源的单向时延。

owd-sd：监测每个探测报文的从源到目的的单向时延。

threshold-value: 指定阈值范围。

upper-threshold: 阈值上限，取值范围为 0~3600000，单位为毫秒。

lower-threshold: 阈值下限，取值范围为 0~3600000，单位为毫秒，且必须小于等于阈值上限。

【使用指导】

阈值告警组创建后，不能再通过 **reaction** 命令修改该阈值告警组的内容。若要修改阈值告警组的内容，则需要先通过 **undo reaction** 命令用来删除阈值告警组，再利用新的参数创建阈值告警组。

监测的对象是探测成功的报文，探测失败的报文不参与计数。

监测单向时延的阈值告警组不支持触发动作，但可以通过相关显示命令 **display nqa reaction counters** 和 **display nqa statistics** 显示当前的监测结果。

【举例】

在 UDP-jitter 测试类型下创建编号为 1 的阈值告警组，监测每个 UDP-jitter 探测报文的从目的到源的单向时延，阈值上限为 50 毫秒，下限为 5 毫秒。NQA 测试组启动前，初始的阈值状态为 **invalid**。收到探测报文的应答报文后，计算该探测报文从目的到源的单向时延，若超出阈值范围，阈值状态置为 **over-threshold**；反之，置为 **below-threshold**。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element owd-ds threshold-value 50 5
```

1.1.61 reaction checked-element icpif

reaction checked-element icpif 命令用来创建监测 Voice 测试 ICPIF 值的阈值告警组。

undo reaction 命令用来删除指定的阈值告警组。

【命令】

```
reaction item-number checked-element icpif threshold-value upper-threshold  
lower-threshold [ action-type { none | trap-only } ]  
undo reaction item-number
```

【缺省情况】

不存在监测 Voice 测试 ICPIF 值的阈值告警组。

【视图】

Voice 测试类型视图

【缺省用户角色】

network-admin
context-admin

【参数】

item-number: 阈值告警组编号，取值范围为 1~10。

threshold-value: 指定阈值范围。

upper-threshold: 阈值上限，取值范围为 1~100。

lower-threshold: 阈值下限，取值范围为 1~100，且必须小于等于阈值上限。

action-type: 触发的动作类型，缺省动作类型为 **none**。

none: 只在显示信息中记录监测结果，不向网管发送 Trap 消息。

trap-only: 条件满足时，在显示信息中记录监测结果的同时，向网管发送 Trap 消息。

【使用指导】

阈值告警组创建后，不能再通过 **reaction** 命令修改该阈值告警组的内容。若要修改阈值告警组的内容，则需要先通过 **undo reaction** 命令用来删除阈值告警组，再利用新的参数创建阈值告警组。

【举例】

在 Voice 测试类型下创建编号为 1 的阈值告警组，监测每次 Voice 测试的 ICPIF 值，阈值上限为 50，下限为 5。NQA 测试组启动前，初始的阈值状态为 **invalid**。每次测试结束后，检查本次测试的 ICPIF 值，若超出阈值范围，阈值状态置为 **over-threshold**；反之，置为 **below-threshold**。当阈值状态改变时，向网管发送 Trap 消息。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] reaction 1 checked-element icpif threshold-value 50 5
action-type trap-only
```

1.1.62 reaction checked-element mos

reaction checked-element mos 命令用来创建监测 Voice 测试 MOS 值的阈值告警组。

undo reaction 命令用来删除指定的阈值告警组。

【命令】

```
reaction item-number checked-element mos threshold-value upper-threshold
lower-threshold [action-type { none | trap-only } ]
undo reaction item-number
```

【缺省情况】

不存在监测 Voice 测试 MOS 值的阈值告警组。

【视图】

Voice 测试类型视图

【缺省用户角色】

network-admin
context-admin

【参数】

item-number: 阈值告警组的编号，取值范围为 1~10。

threshold-value: 指定阈值范围。

upper-threshold: 阈值上限，取值范围为 1~500。

lower-threshold: 阈值下限，取值范围为 1~500，且必须小于等于阈值上限。

action-type: 触发的动作类型，缺省动作类型为 **none**。

none: 只在显示信息中记录监测结果，不向网管发送 Trap 消息。

trap-only: 条件满足时，在显示信息中记录监测结果的同时，向网管发送 Trap 消息。

【使用指导】

实际的阈值下限（或阈值上限）为输入的阈值下限/100（或阈值上限/100），即如果输入的阈值下限和阈值上限分别为 100、200，则 MOS 值在 1~2 之间时，未超出阈值。

阈值告警组创建后，不能再通过 **reaction** 命令修改该阈值告警组的内容。若要修改阈值告警组的内容，则需要先通过 **undo reaction** 命令用来删除阈值告警组，再利用新的参数创建阈值告警组。

【举例】

在 Voice 测试类型下创建编号为 1 的阈值告警组，监测每次 Voice 测试的 MOS 值，阈值上限为 200，下限为 100。NQA 测试组启动前，初始的阈值状态为 invalid。每次测试结束后，检查本次测试的 MOS 值，若超出阈值范围，阈值状态置为 over-threshold；反之，置为 below-threshold。当阈值状态改变时，向网管发送 Trap 消息。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] reaction 1 checked-element mos threshold-value 200 100
action-type trap-only
```

1.1.63 reaction checked-element packet-loss

reaction checked-element packet-loss 命令用来创建监测每次测试中丢包数的阈值告警组。

undo reaction 命令用来删除指定的阈值告警组。

【命令】

```
reaction item-number checked-element packet-loss threshold-type accumulate
accumulate-occurrences [action-type { none | trap-only } ]
undo reaction item-number
```

【缺省情况】

不存在监测每次测试中丢包数的阈值告警组。

【视图】

ICMP-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

network-admin
context-admin

【参数】

item-number: 阈值告警组的编号，取值范围为 1~10。

threshold-type: 指定阈值类型。

accumulate accumulate-occurrences: 每次测试中，累计的丢包数。对于 ICMP-jitter 与 UDP-jitter 测试，取值范围为 1~15000；对于 Voice 测试，取值范围为 1~60000。

action-type: 触发的动作类型，缺省动作类型为 **none**。

none: 只在显示信息中记录监测结果，不向网管发送 Trap 消息。

trap-only: 条件满足时，在显示信息中记录监测结果的同时，向网管发送 Trap 消息。

【使用指导】

阈值告警组创建后，不能再通过 **reaction** 命令修改该阈值告警组的内容。若要修改阈值告警组的内容，则需要先通过 **undo reaction** 命令用来删除阈值告警组，再利用新的参数创建阈值告警组。

【举例】

在 UDP-jitter 测试类型下创建编号为 1 的阈值告警组，监测每次 UDP-jitter 测试的丢包数。NQA 测试组启动前，初始的阈值状态为 **invalid**。每次测试结束后，检查本次测试中累计的丢包数，若达到或超过 100 个，阈值状态置为 **over-threshold**；反之，置为 **below-threshold**。当阈值状态改变时，向网管发送 Trap 消息。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element packet-loss threshold-type
accumulate 100 action-type trap-only
```

1.1.64 reaction checked-element probe-duration

reaction checked-element probe-duration 命令用来创建监测探测持续时间的阈值告警组。

undo reaction 命令用来删除指定的阈值告警组。

【命令】

```
reaction item-number checked-element probe-duration threshold-type
{ accumulate accumulate-occurrences | average | consecutive
consecutive-occurrences } threshold-value upper-threshold lower-threshold
[ action-type { none | trap-only } ]
undo reaction item-number
```

【缺省情况】

不存在监测探测持续时间的阈值告警组。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

item-number: 阈值告警组的编号，取值范围为 1~10。

threshold-type: 指定阈值类型。

accumulate *accumulate-occurrences*: 每次测试中, 累计的探测持续时间超出阈值的探测次数。*accumulate-occurrences* 取值范围为 1~15。

average: 每次测试中, 探测持续时间的平均值。

consecutive *consecutive-occurrences*: 测试组启动后, 连续的探测持续时间超出阈值的探测次数。*consecutive-occurrences* 取值范围为 1~16。

threshold-value: 指定阈值范围。

upper-threshold: 阈值上限, 取值范围为 0~3600000, 单位为毫秒。

lower-threshold: 阈值下限, 取值范围为 0~3600000, 单位为毫秒, 且必须小于等于阈值上限。

action-type: 触发的动作类型, 缺省动作类型为 **none**。

none: 只在显示信息中记录监测结果, 不向网管发送 Trap 消息。

trap-only: 条件满足时, 在显示信息中记录监测结果的同时, 向网管发送 Trap 消息。DNS 测试不支持发送 Trap, DNS 测试类型视图下无此参数。

【使用指导】

阈值告警组创建后, 不能再通过 **reaction** 命令修改该阈值告警组的内容。若要修改阈值告警组的内容, 则需要先通过 **undo reaction** 命令用来删除阈值告警组, 再利用新的参数创建阈值告警组。监测的对象是成功的探测, 失败的探测不参与计数。

【举例】

在 ICMP-echo 测试类型下创建编号为 1 的阈值告警组, 监测 ICMP-echo 探测的持续时间, 阈值上限为 50 毫秒, 下限为 5 毫秒。NQA 测试组启动前, 初始的阈值状态为 **invalid**。每次测试结束后, 检查本次测试的平均探测持续时间, 若超出阈值, 阈值状态置为 **over-threshold**; 反之, 置为 **below-threshold**。当阈值状态改变时, 向网管发送 Trap 消息。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-duration  
threshold-type average threshold-value 50 5 action-type trap-only
```

在 ICMP-echo 测试类型下创建编号为 2 的阈值告警组, 监测 ICMP-echo 探测的持续时间, 阈值上限为 50 毫秒, 下限为 5 毫秒。NQA 测试组启动前, 初始的阈值状态为 **invalid**。每次测试结束后, 检查本次测试中累计的持续时间超出阈值的探测次数, 若达到或超过 10 次, 阈值状态置为 **over-threshold**; 反之, 置为 **below-threshold**。当阈值状态改变时, 向网管发送 Trap 消息。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-duration  
threshold-type accumulate 10 threshold-value 50 5 action-type trap-only
```

在 ICMP-echo 测试类型下创建编号为 3 的阈值告警组, 监测 ICMP-echo 探测的持续时间, 阈值上限为 50 毫秒, 下限为 5 毫秒。NQA 测试组启动前, 初始的阈值状态为 **invalid**。每次探测结束后, 检查测试组启动以来连续的持续时间超出阈值的探测次数, 若达到或超过 10 次, 阈值状态置为 **over-threshold**; 反之, 置为 **below-threshold**。当阈值状态改变时, 向网管发送 Trap 消息。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction 3 checked-element probe-duration
threshold-type consecutive 10 threshold-value 50 5 action-type trap-only
```

1.1.65 reaction checked-element probe-fail (for trap)

reaction checked-element probe-fail 命令用来创建监测探测失败次数的阈值告警组。

undo reaction 命令用来删除指定的阈值告警组。

【命令】

```
reaction item-number checked-element probe-fail threshold-type { accumulate
accumulate-occurrences | consecutive consecutive-occurrences }
[ action-type { none | trap-only } ]
undo reaction item-number
```

【缺省情况】

不存在监测探测失败次数的阈值告警组。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

item-number: 阈值告警组编号，取值范围为 1~10。

threshold-type: 指定阈值类型。

accumulate accumulate-occurrences: 一次测试中，累计的探测失败次数。
accumulate-occurrences 取值范围为 1~15。

consecutive consecutive-occurrences: NQA 测试组启动以来，连续的探测失败次数。
consecutive-occurrences 取值范围为 1~16。

action-type: 触发的动作类型，缺省动作类型为 **none**。

none: 只在显示信息中记录监测结果，不向网管发送 Trap 消息。

trap-only: 条件满足时，在显示信息中记录监测结果的同时，向网管发送 Trap 消息。DNS 测试不支持发送 trap，DNS 测试类型视图下无此参数。

【使用指导】

阈值告警组创建后，不能再通过 **reaction** 命令修改该阈值告警组的内容。若要修改阈值告警组的内容，则需要先通过 **undo reaction** 命令用来删除阈值告警组，再利用新的参数创建阈值告警组。

【举例】

在 ICMP-echo 测试类型下创建编号为 1 的阈值告警组，监测 ICMP-echo 探测的失败次数。NQA 测试组启动前，初始的阈值状态为 **invalid**。每次测试结束后，检查本次测试中累计的探测失败次数，

若达到或超过 10 次，阈值状态置为 **over-threshold**；反之，置为 **below-threshold**。当阈值状态改变时，向网管发送 **Trap** 消息。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type  
accumulate 10 action-type trap-only
```

在 **ICMP-echo** 测试类型下创建编号为 2 的阈值告警组，监测 **ICMP-echo** 探测的失败次数。NQA 测试组启动前，初始的阈值状态为 **invalid**。每次探测结束后，检查测试组启动以来连续的探测失败次数，若达到或超过 10 次，阈值状态置为 **over-threshold**；反之，置为 **below-threshold**。当阈值状态改变时，向网管发送 **Trap** 消息。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-fail threshold-type  
consecutive 10 action-type trap-only
```

1.1.66 reaction checked-element probe-fail (for trigger)

reaction checked-element probe-fail 命令用来建立联动项，对当前所在测试组中的探测进行监测，当连续探测失败次数达到阈值时，就触发其他模块联动。

undo reaction 命令用来删除指定的联动项。

【命令】

**reaction *item-number* checked-element probe-fail threshold-type consecutive
consecutive-occurrences action-type trigger-only**

undo reaction *item-number*

【缺省情况】

不存在联动项。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

item-number: 联动项序号，取值范围为 1~10。

threshold-type: 指定门限类型。

consecutive consecutive-occurrences: NQA 测试组启动以来连续的探测失败次数，取值范围为 1~16。

action-type: 触发的动作类型。

trigger-only: 条件满足时，触发其它模块联动。

【使用指导】

联动项创建后,不能再通过 **reaction** 命令修改该联动项的内容。若要修改联动项的内容,则需要先通过 **undo reaction** 命令用来删除联动项,再利用新的参数创建联动项。

【举例】

在 TCP 测试类型下建立序号为 1 的联动项,连续探测失败 3 次,触发其他模块联动。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type tcp
[Sysname-nqa-admin-test-tcp] reaction 1 checked-element probe-fail threshold-type
consecutive 3 action-type trigger-only
```

【相关命令】

- **track** (可靠性命令参考/Track)

1.1.67 reaction checked-element rtt

reaction checked-element rtt 命令用来创建监测报文往返时延的阈值告警组。

undo reaction 命令用来删除指定的阈值告警组。

【命令】

```
reaction item-number checked-element rtt threshold-type { accumulate
accumulate-occurrences | average } threshold-value upper-threshold
lower-threshold [ action-type { none | trap-only } ]
undo reaction item-number
```

【缺省情况】

不存在监测报文往返时延的阈值告警组。

【视图】

ICMP-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

network-admin
context-admin

【参数】

item-number: 阈值告警组编号,取值范围为 1~10。

threshold-type: 指定阈值类型。

accumulate accumulate-occurrences: 每次测试中,累计的 RTT 超出阈值的报文个数。对于 ICMP-jitter 与 UDP-jitter 测试,取值范围为 1~15000;对于 Voice 测试,取值范围为 1~60000。

average: 每次测试中,报文往返时间的平均值。

threshold-value: 指定阈值范围。

upper-threshold: 阈值上限,取值范围为 0~3600000,单位为毫秒。

lower-threshold: 阈值下限,取值范围为 0~3600000,单位为毫秒,且必须小于等于阈值上限。

action-type: 触发的动作类型，缺省动作类型为 **none**。

none: 只在显示信息中记录监测结果，不向网管发送 Trap 消息。

trap-only: 条件满足时，在显示信息中记录监测结果的同时，向网管发送 Trap 消息。

【使用指导】

阈值告警组创建后，不能再通过 **reaction** 命令修改该阈值告警组的内容。若要修改阈值告警组的内容，则需要先通过 **undo reaction** 命令用来删除阈值告警组，再利用新的参数创建阈值告警组。

监测的对象是探测成功的报文，探测失败的报文不参与计数。

【举例】

在 UDP-jitter 测试类型下创建编号为 1 的阈值告警组，监测 UDP-jitter 探测报文的往返时间，阈值上限为 50 毫秒，下限为 5 毫秒。NQA 测试组启动前，初始的阈值状态为 **invalid**。每次测试结束后，检查本次测试的平均报文往返时间，若超出阈值，阈值状态置为 **over-threshold**；反之，置为 **below-threshold**。当阈值状态改变时，向网管发送 Trap 消息。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element rtt threshold-type average
threshold-value 50 5 action-type trap-only
```

在 UDP-jitter 测试类型下创建编号为 2 的阈值告警组，监测每个 UDP-jitter 探测报文的往返时间，阈值上限为 50 毫秒，下限为 5 毫秒。NQA 测试组启动前，初始的阈值状态为 **invalid**。每次测试结束后，检查本次测试中累计的 RTT 超出阈值的报文个数，若达到或超过 100 个，阈值状态置为 **over-threshold**；反之，置为 **below-threshold**。当阈值状态改变时，向网管发送 Trap 消息。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Sysname-nqa-admin-test-udp-jitter] reaction 1 checked-element rtt threshold-type
accumulate 100 threshold-value 50 5 action-type trap-only
```

1.1.68 reaction trap

reaction trap 命令用来配置在指定条件下向网管服务器发送 Trap 消息。

undo reaction trap 命令用来恢复缺省情况。

【命令】

```
reaction trap { path-change | probe-failure consecutive-probe-failures |
test-complete | test-failure [ accumulate-probe-failures ] }
undo reaction trap { path-change | probe-failure | test-complete |
test-failure }
```

【缺省情况】

不向网管服务器发送 Trap 消息。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

UDP-tracert 测试类型视图

ICMP-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

path-change: 当进行 UDP-tracert 类型测试时，在配置了 **frequency** 命令后进行连续测试后，如果检测到当前路径相对于上一次测试路径发生变化，则设备发送一次 Trap 消息。

probe-failure consecutive-probe-failures: 每次探测结束后，计算本次 NQA 测试中探测连续失败的次数，如果连续失败次数大于或等于 **consecutive-probe-failures**，则向网管服务器发送探测失败的 Trap 消息。一次测试中，可能发送多次 Trap 消息。**consecutive-probe-failures** 为一次测试中连续探测失败的次数，取值范围为 1~15。

test-complete: 对于非 UDP-tracert 类型测试，当测试完成时发送测试完成的 Trap 消息。对于 UDP-tracert 类型测试，测试出到达目的设备的路径后，发送测试完成的 Trap 消息。

test-failure accumulate-probe-failures: 对于非 UDP-tracert 类型测试，一次 NQA 测试结束后，计算本次 NQA 测试中探测失败的累计次数，如果累计失败次数大于或等于 **accumulate-probe-failures**，则向网管服务器发送测试失败的 Trap 消息。**accumulate-probe-failures** 为一次测试中累计探测失败的次数，为必须输入的参数，取值范围为 1~15。对于 UDP-tracert 类型测试，只要未能测试出到达目的地的路径，就发送一次 Trap 消息。用户不能输入参数 **accumulate-probe-failures**。

【使用指导】

ICMP-jitter、UDP-jitter 和 Voice 测试只支持 **reaction trap test-complete**。

UDP-tracert 测试支持 **reaction trap path-change**、**reaction trap test-complete** 和 **reaction trap test-failure**（其中 UDP-tracert 测试不支持 **reaction trap test-failure** 的 **accumulate-probe-failures** 参数）。

【举例】

在 ICMP-echo 测试类型下配置测试中连续探测失败次数大于或等于 5 次时，发送探测失败的 Trap 消息。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction trap probe-failure 5
```

1.1.69 reaction trigger per-probe

reaction trigger per-probe 命令用来配置每次探测结果发送机制，即每次探测结束时都会将探测结果发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

undo reaction trigger per-probe 命令用来恢复缺省情况。

【命令】

reaction trigger per-probe

undo reaction trigger per-probe

【缺省情况】

连续探测成功或失败 3 次时，NQA 客户端会把探测成功或失败的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

【视图】

DNS/ICMP/TCP Half Open 类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

本命令与 **reaction trigger probe-fail** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

本命令与 **reaction trigger probe-pass** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

【举例】

在 ICMP 类型的 NQA 模板视图下配置每次探测结果发送机制，即每次探测结束时都会将探测结果发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

```
<Sysname> system-view  
[Sysname] nqa template icmp icmptplt  
[Sysname-nqatplt-icmp-icmptplt] reaction trigger per-probe
```

【相关命令】

- **reaction trigger probe-fail**
- **reaction trigger probe-pass**

1.1.70 reaction trigger probe-fail

reaction trigger probe-fail 命令用来配置连续探测失败的次数。

undo reaction trigger probe-fail 命令用来恢复缺省情况。

【命令】

reaction trigger probe-fail *count*
undo reaction trigger probe-fail

【缺省情况】

连续探测失败 3 次时，NQA 客户端会把探测失败的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

【视图】

任意类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

count: 连续探测失败的次数，取值范围为 1~15。

【使用指导】

当连续探测失败次数达到命令配置的数值时，NQA 客户端会把探测失败的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

外部特性调用 NQA 模板后进行相应的 NQA 测试，使用此命令可以设定节点失效的连续测试失败次数。

本命令与 **reaction trigger per-probe** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

【举例】

在 HTTP 类型的 NQA 模板视图下配置确定节点失效需要连续探测失败 5 次。当连续探测失败的次数达到 5 次时，NQA 客户端把探测失败的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] reaction trigger probe-fail 5
```

【相关命令】

- **reaction trigger per-probe**
- **reaction trigger probe-pass**

1.1.71 reaction trigger probe-pass

reaction trigger probe-pass 命令用来配置连续探测成功次数。

undo reaction trigger probe-pass 命令用来恢复缺省情况。

【命令】

```
reaction trigger probe-pass count
undo reaction trigger probe-pass
```

【缺省情况】

连续探测成功 3 次时，NQA 客户端会把探测成功的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

【视图】

任意类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

count: 连续探测成功的次数，取值范围为 1~15。

【使用指导】

当连续探测成功次数达到命令配置的数值时，NQA 客户端会把探测成功的消息发送给外部特性，使外部特性利用 NQA 测试的结果进行相应处理。

外部特性调用 NQA 模板后进行相应的 NQA 测试，使用此命令可以设定节点有效的连续探测成功次数。

本命令与 **reaction trigger per-probe** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

【举例】

在 HTTP 类型的 NQA 模板视图下配置确定节点有效需要连续探测成功 5 次。当连续探测成功的次数达到 5 次时，NQA 客户端把探测成功的消息发送给外部特性，使外部特性能利用 NQA 测试的结果进行相应处理。

```
<Sysname> system-view
[Sysname] nqa template http httptplt
[Sysname-nqatplt-http-httptplt] reaction trigger probe-pass 5
```

【相关命令】

- **reaction trigger per-probe**
- **reaction trigger probe-fail**

1.1.72 request-method

request-method 命令用来配置 RTSP 模板测试请求方式。

undo request-method 命令用来恢复缺省情况。

【命令】

```
request-method { describe | options }
undo request-method
```

【缺省情况】

RTSP 模板测试请求方式为 **options**。

【视图】

RTSP 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

describe: Describe 方式，用于获取 URL 路径中指定对象的相关信息。

options: Options 方式，用于获取 RTSP 服务器提供的可用方法。

【使用指导】

配置探测请求方式为 Describe 方式时，必须通过 **url** 命令配置文件路径，NQA 客户端通过 **url** 命令指定的配置文件路径必须对应 RTSP 服务器上的文件路径。

【举例】

```
# 配置 RTSP 请求方式为 Describe 方式。
<Sysname> system-view
[Sysname] nqa template rtsp rtsptplt
[Sysname-nqatplt-rtsp-rtsptplt] request method describe
```

【相关命令】

- `url`

1.1.73 resolve-target

resolve-target 命令用来配置要解析的域名。

undo resolve-target 命令用来恢复缺省情况。

【命令】

```
resolve-target domain-name
undo resolve-target
```

【缺省情况】

未配置要解析的域名。

【视图】

DNS 测试类型视图

DNS 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

domain-name: 要解析的域名，由“.”分隔的字符串组成（如 aabbcc.com），每个字符串的长度不超过 63 个字符，包括“.”在内的总长度不超过 255 个字符，区分大小写。字符串中可以包含字母、数字、“-”及“_”，不能出现连续“.”。

【举例】

```
# 在 DNS 测试类型下配置 DNS 测试要解析的域名为 domain1。
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dns
[Sysname-nqa-admin-test-dns] resolve-target domain1
# 在 DNS 类型的 NQA 模板视图下配置测试要解析的域名为 domain1。
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] resolve-target domain1
```

1.1.74 resolve-type

resolve-type 命令用来配置域名解析类型。

undo resolve-type 命令用来恢复缺省情况。

【命令】

```
resolve-type { A | AAAA }  
undo resolve-type
```

【缺省情况】

域名解析类型为 **A** 类型。

【视图】

DNS 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

A: 域名解析类型为 A 类型请求，即将域名解析为 IPv4 地址。

AAAA: 域名解析类型为 AAAA 类型请求，即将域名解析为 IPv6 地址。

【举例】

在 DNS 类型的 NQA 模板视图下，配置测试的域名解析类型为 **A**。

```
<Sysname> system-view  
[Sysname] nqa template dns dnstplt  
[Sysname-nqatplt-dns-dnstplt] resolve-type A
```

1.1.75 resource-release { data-fill | hex-data-fill }

resource-release { data-fill | hex-data-fill } 命令用来配置向服务器发送的资源释放报文。

undo resource-release 命令用来恢复缺省情况。

【命令】

```
resource-release { data-fill | hex-data-fill } string  
undo resource-release
```

【缺省情况】

未配置向服务器发送的资源释放报文。

【视图】

TCP/UDP 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

data-fill: 表示使用文本格式的字符串来填充探测报文。

hex-data-fill: 表示使用十六进制字符串来填充探测报文。

string: 探测报文的填充内容。和 **data-fill** 关键字配合使用时，为 1~200 个字符的字符串，区分大小写；和 **hex-data-fill** 关键字配合使用时，为 2~200 个字符的字符串，字符串长度必须是偶数且不区分大小写。

【使用指导】

配置本命令后，设备会给服务器发送包含指定字符串的报文，用来通知服务器本次测试结束，要求服务器关闭连接并释放相应资源。

【举例】

在 TCP 类型的 NQA 模板视图下配置探测报文的填充字符串为 abcd。

```
<Sysname> system-view
[Sysname] nqa template tcp tcptplt
[Sysname-nqatplt-tcp-tcptplt] release-resource data-fill abcd
```

1.1.76 route-option bypass-route

route-option bypass-route 命令用来开启路由表旁路功能，探测直连目的地的连通情况。

undo route-option bypass-route 命令用来关闭路由表旁路功能。

【命令】

```
route-option bypass-route
undo route-option bypass-route
```

【缺省情况】

路由表旁路功能处于关闭状态。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图
DLSw/DNS/FTP/HTTP/SNMP 测试类型视图
UDP-tracert 测试类型视图
ICMP-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启该功能后，将不进行路由查找，而直接将报文发送到直连网络的目的地。

开启该功能后，设备转发探测报文可以经过的最大跳数为 1，**ttl** 命令设置的跳数不会生效。

测试目的端使用 IPv6 地址时，本命令配置无效。

【举例】

在 ICMP-echo 测试类型下开启路由旁路功能。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] route-option bypass-route
```

1.1.77 source interface

source interface 命令用来配置指定接口的 IP 地址作为探测报文的源 IP 地址。

undo source interface 命令用来恢复缺省情况。

【命令】

source interface *interface-type interface-number*

undo source interface

【缺省情况】

以报文发送接口的主 IP 地址作为探测报文中的源 IP 地址。

【视图】

ICMP-echo 测试类型视图

UDP-tracert 测试类型视图

ICMP 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type interface-number: 探测报文源接口的接口类型和接口编号。

【使用指导】

本命令指定的接口必须处于 UP 状态，否则探测将会失败。

对于 ICMP-echo 测试类型及 ICMP 类型的 NQA 模板，本命令与 **source ip**、**source ipv6** 命令作用相同，多次执行这三条命令时，最后一次执行的命令生效；对于 UDP-tracert 测试类型，本命令与 **source ip** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

【举例】

【相关命令】

- **source ip**
- **source ipv6**

1.1.78 source ip

source ip 命令用来配置探测报文的源 IPv4 地址。

undo source ip 命令用来恢复缺省情况。

【命令】

source ip *ip-address*

undo source ip

【缺省情况】

以报文发送接口的主 IP 地址作为探测报文中的源 IPv4 地址。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/FTP/HTTP/SNMP 测试类型视图

UDP-tracert 测试类型视图

ICMP-jitter/Path-jitter/UDP-jitter/Voice 测试类型视图

任意类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: 探测报文的源 IPv4 地址。

【使用指导】

source ip 命令配置的源 IP 地址必须是设备上接口的 IPv4 地址，且接口为 up 状态，否则测试将会失败。

对于 NQA 模板类型来说，当源地址类型和目的地址类型不一致时，以目的地址类型为准，进行该类型的报文探测，此时源地址的配置不生效。

对于 ICMP-echo/UDP-tracert 测试类型及 ICMP 类型的 NQA 模板，本命令和 **source interface** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

【举例】

在 ICMP-echo 测试类型下配置 ICMP-echo 探测报文中的源 IPv4 地址为 10.1.1.1。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] source ip 10.1.1.1
```

在 ICMP 类型的 NQA 模板视图下配置探测报文中的源 IPv4 地址为 10.1.1.1。

```
<Sysname> system-view
```

```
[Sysname] nqa template icmp icmptplt
```

```
[Sysname-nqatplt-icmp-icmptplt] source ip 10.1.1.1
```

【相关命令】

- **source interface**

1.1.79 source ipv6

source ipv6 命令用来配置探测报文的源 IPv6 地址。

undo source ipv6 命令用来恢复缺省情况。

【命令】

source ipv6 *ipv6-address*

undo source ipv6

【缺省情况】

以报文发送接口的 IPv6 地址作为探测报文中的源 IPv6 地址。

【视图】

ICMP-echo/TCP/UDP-echo/UDP-jitter 测试类型视图

DNS/FTP/HTTP/HTTPS/ICMP/IMAP/POP3/RADIUS 认证探测/RADIUS-ACCOUNT 计费探测/RTSP/SMTP/SNMP/SNMP-DCA/SSL/TCP/TCP Half Open/UDP/WAP 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address: 探测报文的源 IPv6 地址，不支持 IPv6 链路本地地址。

【使用指导】

source ipv6 命令配置的源 IPv6 地址必须是设备上接口的 IPv6 地址，且接口为 up 状态，否则测试将会失败。

对于 NQA 模板类型来说，当源地址类型和目的地址类型不一致时，以目的地址类型为准，进行该类型的报文探测，此时源地址的配置不生效。

对于 ICMP-echo 测试类型及 ICMP 类型的 NQA 模板，本命令和 **source interface** 命令作用相同，多次执行这两条命令时，最后一次执行的命令生效。

【举例】

在 ICMP-echo 测试类型下配置 ICMP-echo 探测报文中的源 IPv6 地址为 1::1。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source ipv6 1::1
```

在 ICMP 类型的 NQA 模板视图下配置探测报文中的源 IPv6 地址为 1::1。

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] source ipv6 1::1
```

【相关命令】

- **source interface**

1.1.80 source port

source port 命令用来配置探测报文的源端口号。

undo source port 命令用来恢复缺省情况。

【命令】

source port *port-number*

undo source port

【缺省情况】

未指定源端口号。

【视图】

UDP-echo 测试类型视图
SNMP 测试类型视图
UDP-tracert 测试类型视图
UDP-jitter/Voice 测试类型视图
DNS 类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

port-number: 探测报文的源端口号，取值范围为 1~65535。

【举例】

```
# 在 UDP-echo 测试类型下配置探测报文的源端口号为 8000。
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] source port 8000
# 在 DNS 类型的 NQA 模板视图下配置探测报文的源端口号为 8000。
<Sysname> system-view
[Sysname] nqa template dns dnstplt
[Sysname-nqatplt-dns-dnstplt] source port 8000
```

1.1.81 ssl-client-policy

ssl-client-policy 命令用来为 HTTPS/SSL 类型的 NQA 模板绑定 SSL 客户端策略。

undo ssl-client-policy 命令用来恢复缺省情况。

【命令】

```
ssl-client-policy policy-name
undo ssl-client-policy
```

【缺省情况】

未绑定 SSL 客户端策略。

【视图】

HTTPS/SSL 类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

policy-name: SSL 客户端策略名, 为 1~31 个字符的字符串, 不区分大小写。

【使用指导】

通过绑定 SSL 客户端策略与服务器建立 SSL 连接, 确认服务器业务的可用性。

【举例】

在 SSL 类型的 NQA 模板视图下配置 SSL 客户端策略为 *policy*。

```
<Sysname> system-view
[Sysname] nqa template ssl ssltplt
[Sysname-nqatplt-ssl-ssltplt] ssl-client-policy policy
```

1.1.82 statistics hold-time

statistics hold-time 命令用来配置统计组的保留时间。

undo statistics hold-time 命令用来恢复缺省情况。

【命令】

```
statistics hold-time hold-time
undo statistics hold-time
```

【缺省情况】

统计组的保留时间为 120 分钟。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图
DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图
ICMP-jitter/Path-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

hold-time: 统计组的保留时间, 取值范围为 1~1440, 单位为分钟。

【使用指导】

统计组具有老化功能。统计组保存一定时间后将被删除, 以便记录新的统计组信息。

【举例】

在 ICMP-echo 测试类型下配置统计组的保留时间为 3 分钟。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics hold-time 3
```

1.1.83 statistics interval

statistics interval 命令用来配置对测试结果进行统计的时间间隔。

undo statistics interval 命令用来恢复缺省情况。

【命令】

```
statistics interval interval  
undo statistics interval
```

【缺省情况】

对测试结果进行统计的时间间隔为 60 分钟。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图
DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图
ICMP-jitter/Path-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

network-admin
context-admin

【参数】

interval: 对测试结果进行统计的时间间隔，取值范围为 1～35791394，单位为分钟。

【使用指导】

NQA 将统计时间间隔内完成的 NQA 测试归为一组，计算该组测试结果的统计值，这些统计值构成一个统计组。通过 **display nqa statistics** 命令可以显示该统计组的信息。

【举例】

```
# 在 ICMP-echo 测试类型下配置对测试结果进行统计的时间间隔为 2 分钟。  
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type icmp-echo  
[Sysname-nqa-admin-test-icmp-echo] statistics interval 2
```

1.1.84 statistics max-group

statistics max-group 命令用来配置能够保留的最大统计组个数。

undo statistics max-group 命令用来恢复缺省情况。

【命令】

```
statistics max-group number  
undo statistics max-group
```

【缺省情况】

能够保留的最大统计组个数为 2。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

ICMP-jitter/Path-jitter/UDP-jitter/Voice 测试类型视图

【缺省用户角色】

network-admin

context-admin

【参数】

number: 能够保留的最大统计组个数，取值范围为 0~100。

【使用指导】

当保留的统计组数目达到最大值时，如果形成新的统计组，保存时间最久的统计组将被删除。

能够保留的最大统计组个数为 0 时，不进行统计。

【举例】

在 ICMP-echo 测试类型下配置能够保留的最大统计组个数为 5。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
```

```
[Sysname-nqa-admin-test-icmp-echo] statistics max-group 5
```

1.1.85 target-only

target-only 命令用来配置 Path-jitter 测试中仅针对到达目的地址的完整路径进行探测，不逐跳进行探测。

undo target-only 命令用来恢复缺省情况。

【命令】

target-only

undo target-only

【缺省情况】

Path-jitter 测试中会逐跳进行探测。

【视图】

Path-jitter 测试类型视图

【缺省用户角色】

network-admin

context-admin

【举例】

在 Path-jitter 测试类型下配置仅针对到达目的地址的完整路径进行探测。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type path-jitter
[Sysname-nqa-admin-test-path-jitter] target-only
```

1.1.86 tos

tos 命令用来配置 NQA 探测报文 IP 报文头中服务类型域的值。

undo tos 命令用来恢复缺省情况。

【命令】

tos *value*

undo tos

【缺省情况】

NQA 探测报文 IP 报文头中服务类型域的值 0。

【视图】

任意测试类型视图

DNS/FTP/HTTP/HTTPS/ICMP/IMAP/POP3/RADIUS 认证探测/RADIUS-ACCOUNT 计费探测
/RTSP/SIP/SMTP/SNMP/SNMP-DCA/SSL/TCP/TCP Half Open/UDP/WAP 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

value: 探测报文 IP 报文头中服务类型域的值，取值范围为 0~255。

【举例】

在 ICMP-echo 测试类型下配置探测报文 IP 报文头中服务类型域的值 1。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] tos 1
```

在 ICMP 类型的 NQA 模板视图下配置探测报文 IP 报文头中服务类型域的值 1。

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] tos 1
```

1.1.87 ttl

ttl 命令用来配置探测报文在网络中可以经过的最大跳数。

undo ttl 命令用来恢复缺省情况。

【命令】

ttl *value*

undo ttl

【缺省情况】

UDP-tracert 类型探测报文在网络中可以经过的最大跳数是 30 跳。其它测试类型下探测报文在网络中可以经过的最大跳数为 20 跳。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图

DLSw/DNS/FTP/HTTP/SNMP 测试类型视图

UDP-tracert 测试类型视图

ICMP-jitter/UDP-jitter/Voice 测试类型视图

DNS/FTP/HTTP/HTTPS/ICMP/IMAP/POP3/RADIUS 认证探测/RADIUS-ACCOUNT 计费探测/RTSP/SIP/SMTP/SNMP/SNMP-DCA/SSL/TCP/TCP Half Open/UDP/WAP 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

value: 对于 UDP-tracert 测试类型，表示允许探测报文填充的最大跳数值；对于其它测试类型，表示探测报文在网络中可以经过的最大跳数。取值范围为 1~255。

【使用指导】

配置 **route-option bypass-route** 命令后，探测报文在网络中可以经过的最大跳数为 1，**ttl** 命令不会生效。

配置 UDP-tracert 类型测试时，如果使用 **init-ttl** 命令配置的初始跳数值大于此值，测试将无法启动。

【举例】

在 ICMP-echo 测试类型下配置探测报文在网络中可以经过的最大跳数为 16 跳。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] ttl 16
```

在 ICMP 类型的 NQA 模板视图下配置探测报文在网络中可以经过的最大跳数为 16 跳。

```
<Sysname> system-view
[Sysname] nqa template icmp icmptplt
[Sysname-nqatplt-icmp-icmptplt] ttl 16
```

1.1.88 transport-protocol

transport-protocol 命令用来配置 SIP 测试使用的传输协议。

undo transport-protocol 命令用来恢复缺省情况。

【命令】

```
transport-protocol { tcp | udp }
undo transport-protocol
```

【缺省情况】

SIP 测试使用的传输协议为 UDP。

【视图】

SIP 类型的 NQA 模板视图

【缺省用户角色】

network-admin

context-admin

【参数】

tcp: 使用 TCP 连接发起 SIP 探测。

udp: 使用 UDP 连接发起 SIP 探测。

【使用指导】

修改 NQA 模板下 SIP 使用的传输协议后，系统将会停止使用该模板的已有 SIP 探测，并发起一个新的探测请求。

【举例】

配置 SIP 测试使用的传输协议为 TCP。

```
<Sysname> system-view
```

```
[Sysname] nqa template sip siptplt
```

```
[Sysname-nqatplt-sip-siptplt] transport-protocol tcp
```

1.1.89 type

type 命令用来配置当前测试组的测试类型，并进入测试组测试类型视图。

【命令】

```
type { dhcp | dlsw | dns | ftp | http | icmp-echo | icmp-jitter | path-jitter |  
snmp | tcp | udp-echo | udp-jitter | udp-tracert | voice }
```

【缺省情况】

未配置当前测试组的测试类型。

【视图】

NQA 测试组视图

【缺省用户角色】

network-admin

context-admin

【参数】

dhcp: 测试类型为 DHCP。

dlsw: 测试类型为 DLSw。

dns: 测试类型为 DNS。

ftp: 测试类型为 FTP。

http: 测试类型为 HTTP。

icmp-echo: 测试类型为 ICMP-echo。

icmp-jitter: 测试类型为 ICMP-jitter。

path-jitter: 测试类型为 Path-jitter。

snmp: 测试类型为 SNMP。

tcp: 测试类型为 TCP。

udp-echo: 测试类型为 UDP-echo。

udp-jitter: 测试类型为 UDP-jitter。

udp-tracert: 测试类型为 UDP-tracert。

voice: 测试类型为 Voice。

【使用指导】

一个 NQA 测试组对应一个 NQA 测试类型。当进入 NQA 测试组视图后，需要指定测试类型并配置测试类型相应的属性。当 NQA 测试组指定了一个测试类型后，测试组将与测试类型绑定，若需要重新指定测试类型，请在系统视图下删除测试组之后重新创建测试组并指定测试类型。

【举例】

配置测试组的测试类型为 FTP 测试，并进入测试组测试类型视图。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp]
```

1.1.90 url

url 命令用来配置测试访问的网址。

undo url 命令用来恢复缺省情况。

【命令】

```
url url
undo url
```

【缺省情况】

未配置测试访问的网址。

【视图】

FTP/HTTP 测试类型视图

FTP/HTTP/HTTPS/RTSP/WAP 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

url: 测试操作访问的目标资源地址，为 1~255 个字符的字符串，区分大小写。*url* 中的主机名部分，由“.”分隔的字符串组成（如 aabbcc.com），每个字符串的长度不超过 63 个字符，区分大小写；字符串中可以包含字母、数字、“-”及“_”，不能出现连续“.”。

- HTTP 测试类型时，*url* 格式为 *http://host/resource* 或 *http://host:port/resource*，缺省端口号为 80。
- HTTPS 测试类型时，*url* 格式为 *https://host/resource* 或 *https://host:port/resource*，缺省端口号为 443。
- FTP 测试类型时，*url* 格式为 *ftp://host/filename* 或 *ftp://host:port/filename*，缺省端口号为 21。
- RTSP 测试类型时，*url* 格式为 *rtsp://host/resource* 或 *rtsp://host:port/resource*，缺省端口号为 554。
- WAP 测试类型时，*url* 格式为 *http://host/filename*、*http://host:port/filename*、*https://host/resource* 或 *https://host:port/resource*。

filename 取值范围的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

【使用指导】

WAP 测试单独配置 URL 无效，需要配置 **expect data** 匹配期望测试成功的应答内容来判断探测是否成功。

【举例】

在 HTTP 测试类型下配置 HTTP 测试访问的网址为 *http://www.company.com/index.html*。

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type http
```

```
[Sysname-nqa-admin-test-http] url http://www.company.com/index.html
```

在 HTTP 类型的 NQA 模板视图下配置测试访问的网址为 *http://www.company.com/index.html*。

```
<Sysname> system-view
```

```
[Sysname] nqa template http httptplt
```

```
[Sysname-nqatplt-http-httptplt] url http://www.company.com/index.html
```

1.1.91 username

username 命令用来配置登录用户名。

undo username 命令用来恢复缺省情况。

【命令】

```
username username
```

```
undo username
```

【缺省情况】

未配置登录用户名。

【视图】

FTP/HTTP 测试类型视图

FTP/HTTP/HTTPS/IMAP/POP3/RADIUS 认证探测/RADIUS-ACCOUNT 计费探测类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

username: 测试使用的登录用户名，区分大小写。FTP、HTTP 或 HTTPS 登录用户名，为 1~32 个字符的字符串；POP3 或 IMAP 登录用户名，为 1~40 个字符的字符串，形如 user1@test.com；RADIUS 或 RADIUS-ACCOUNT 用户名，为 1~253 个字符的字符串。

【举例】

```
# 在 FTP 测试类型下配置 FTP 登录用户名为 administrator。
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] username administrator
# 在 FTP 类型的 NQA 模板视图下配置 FTP 登录用户名为 administrator。
<Sysname> system-view
[Sysname] nqa template ftp ftptplt
[Sysname-nqatplt-ftp-ftptplt] username administrator
```

【相关命令】

- **operation**
- **password**

1.1.92 version (HTTP/HTTPS test type view and HTTPS template view)

version 命令用来配置 HTTP/HTTPS 测试所使用的版本。

undo version 命令用来恢复缺省情况。

【命令】

```
version { v1.0 | v1.1 }
undo version
```

【缺省情况】

HTTP/HTTPS 测试所使用的版本为 1.0。

【视图】

HTTP 测试类型视图
HTTP/HTTPS 类型的 NQA 模板视图

【缺省用户角色】

network-admin
context-admin

【参数】

v1.0: 测试使用的版本为 1.0。

v1.1: 测试使用的版本为 1.1。

【举例】

在 HTTP 测试类型下配置 HTTP 测试使用的版本为 1.1。

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] version v1.1
```

1.1.93 version (SNMP-DCA template view)

version 命令用来配置 SNMP-DCA 测试所使用的 SNMP 版本。

undo version 命令用来恢复缺省情况。

【命令】

```
version { v1 | v2c }
undo version
```

【缺省情况】

SNMP-DCA 测试所使用的 SNMP 版本为 SNMPv1。

【视图】

SNMP-DCA 类型的 NQA 模板视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

v1: SNMPv1 版本。

v2c: SNMPv2c 版本。

【使用指导】

只有本命令配置的版本和测试的 SNMP Agent 使用的 SNMP 版本相同时，SNMP-DCA 才能正常工作。

【举例】

在 SNMP-DCA 类型的 NQA 模板视图下配置 SNMP-DCA 测试所使用的 SNMP 版本为 SNMPv2c。

```
<Sysname> system-view
[Sysname] nqa template snmpdca test
[Sysname-nqatplt-snmpdca-test] version v2c
```

1.1.94 vpn-instance

vpn-instance 命令用来指定测试操作所属的 VPN 实例。

undo vpn-instance 命令用来恢复缺省情况。

【命令】

```
vpn-instance vpn-instance-name  
undo vpn-instance
```

【缺省情况】

未指定测试操作所属的 VPN，NQA 用来测试公网的连通性。

【视图】

ICMP-echo/TCP/UDP-echo 测试类型视图
DHCP/DLSw/DNS/FTP/HTTP/SNMP 测试类型视图
UDP-tracert 测试类型视图
ICMP-jitter/Path-jitter/UDP-jitter/Voice 测试类型视图
任意类型的 NQA 模板视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

vpn-instance-name: VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

指定测试操作所属的 VPN 实例后，NQA 将测试指定 VPN 实例内隧道的连通情况。

【举例】

```
# 在 ICMP-echo 测试类型下指定测试操作所属的 VPN 实例为 vpn1。  
<Sysname> system-view  
[Sysname] nqa entry admin test  
[Sysname-nqa-admin-test] type icmp-echo  
[Sysname-nqa-admin-test-icmp-echo] vpn-instance vpn1  
# 在 FTP 类型的 NQA 模板视图下指定测试操作所属的 VPN 实例为 vpn1。  
<Sysname> system-view  
[Sysname] nqa template ftp ftptplt  
[Sysname-nqatplt-ftp-ftptplt] vpn-instance vpn1
```

1.2 NQA服务器端命令



说明

只有在测试类型为 UDP-jitter、TCP、UDP-echo 和 Voice 时，才需要配置 NQA 服务器。

1.2.1 display nqa server

display nqa server 命令用来显示 NQA 服务器的状态信息。

【命令】

display nqa server

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 显示 NQA 服务器的状态信息。
<Sysname> display nqa server
NQA server status: Enabled
TCP connect:
  IP address: 2.2.2.2
  Port: 2000
  ToS:200
  VPN instance: -
UDP echo:
  IP address: 3.3.3.3
  Port: 3000
  ToS: 255
  VPN instance: -
High performance mode: Enabled
```

表1-10 display nqa server 命令输出信息描述

字段	描述命令
NQA server status	NQA服务器状态，包括的取值如下： - Disabled: 未启用 NQA 服务器功能； - Enabled: 启用了 NQA 服务器功能；
TCP connect	NQA TCP测试中服务器的状态信息
UDP echo	NQA UDP测试中服务器的状态信息
IP address	NQA服务器TCP/UDP监听服务的IP地址
Port	NQA服务器TCP/UDP监听服务的端口号
ToS	NQA服务器TCP/UDP监听服务的回应报文携带的ToS值
VPN instance	NQA服务器监听的IP地址所属的VPN实例名称。如果NQA服务器监听的是公网IP地址，则显示为-
High performance mode	NQA服务器的高性能模式，包括的取值如下： - Disabled: 未开启 NQA 服务器高性能模式 - Enabled: 开启了 NQA 服务器高性能模式

【相关命令】

- **nqa server enable**
- **nqa server tcp-connect**
- **nqa server udp-echo**

1.2.2 nqa server enable

nqa server enable 命令用来开启 NQA 服务器功能。

undo nqa server enable 命令用来关闭 NQA 服务器功能。

【命令】

nqa server enable
undo nqa server enable

【缺省情况】

NQA 服务器功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 开启 NQA 服务器功能。
<Sysname> system-view
[Sysname] nqa server enable
```

【相关命令】

- **display nqa server**
- **nqa server tcp-connect**
- **nqa server udp-echo**

1.2.3 nqa server tcp-connect

nqa server tcp-connect 命令用来在 NQA 服务器上创建 TCP 监听服务。

undo nqa server tcp-connect 命令用来删除指定的 TCP 监听服务。

【命令】

```
nqa server tcp-connect { ipv4-address | ipv6 ipv6-address } port-number
[ vpn-instance vpn-instance-name ] [ tos tos ]
undo nqa server tcp-connect { ipv4-address | ipv6 ipv6-address } port-number
[ vpn-instance vpn-instance-name ]
```

【缺省情况】

不存在 TCP 监听服务

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-address: NQA 服务器 TCP 监听服务监听的 IPv4 地址。

ipv6-address: NQA 服务器 TCP 监听服务监听的 IPv6 地址。

port-number: NQA 服务器 TCP 监听服务监听的端口号，取值范围为 1~65535。

vpn-instance vpn-instance-name: NQA 服务器监听的 IP 地址所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果不指定本参数，则表示 TCP 监听的是公网 IP 地址。

tos tos: NQA 服务器应答报文中的 ToS 域的值。取值范围为 0~255，缺省值为 0。

【使用指导】

只有在测试类型为 TCP 时，才需在 NQA 服务器上配置此命令。

通过本命令可以指定发送应答 NQA 探测报文（TCP 报文）中携带的 ToS 值。

所配置的 IP 地址、端口号及 VPN 实例必须与 NQA 客户端的配置一致，且不能与已有的监听服务冲突。

所配置的 IP 地址必须是作为服务器的设备上的接口的 IP 地址，否则配置无效。

建议不要配置 1~1023 之间的端口（知名端口），否则可能导致 NQA 测试失败或该知名端口对应的服务不可用。

【举例】

创建 IP 地址为 169.254.10.2，端口号为 9000 的 TCP 监听服务。

```
<Sysname> system-view
```

```
[Sysname] nqa server tcp-connect 169.254.10.2 9000
```

【相关命令】

- **display nqa server**
- **nqa server enable**

1.2.4 nqa server udp-echo

nqa server udp-echo 命令用来在 NQA 服务器上创建 UDP 监听服务。

undo nqa server udp-echo 命令用来删除指定的 UDP 监听服务。

【命令】

```
nqa server udp-echo { ipv4-address | ipv6 ipv6-address } port-number  
[ vpn-instance vpn-instance-name ] [ high-performance-mode ] [ tos tos ]
```

```
undo nqa server udp-echo { ipv4-address | ipv6 ipv6-address } port-number  
[ vpn-instance vpn-instance-name ]
```

【缺省情况】

不存在 UDP 监听服务

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-address: NQA 服务器 UDP 监听服务监听的 IPv4 地址。

ipv6-address: NQA 服务器 UDP 监听服务监听的 IPv6 地址。

port-number: NQA 服务器 UDP 监听服务监听的端口号，取值范围为 1~65535。

vpn-instance vpn-instance-name: NQA 服务器监听的 IP 地址所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果不指定本参数，则表示 UDP 监听的是公网 IP 地址。

high-performance-mode: 开启 NQA 服务器端对于 UDP-jitter 测试的高性能模式。不指定本参数则 NQA 服务器对于 UDP-jitter 测试的高性能模式处于关闭状态。

tos tos: NQA 服务器应答报文中的 ToS 域的值。取值范围为 0~255，缺省值为 0。

【使用指导】

只有在测试类型为 UDP-jitter、UDP-echo 或 Voice 时，才需在 NQA 服务器上配置此命令。

通过本命令可以指定发送应答 NQA 探测报文（UDP 报文）中携带的 ToS 值。

配置的 IP 地址、端口号及 VPN 实例必须与 NQA 客户端的配置一致，且不能与已有的监听服务冲突。

所配置的 IP 地址必须是作为服务器的设备上的接口的 IP 地址，否则配置无效。

建议不要配置 1~1023 之间的端口（知名端口），否则可能导致 NQA 测试失败或该知名端口对应的服务不可用。

在高性能模式下，NQA 服务器将大大提升 UDP-jitter 测试的探测报文应答效率。此时 NQA 服务器端不能处理大于 100 字节的 NQA 报文，若客户端发送的报文长度大于 100 字节，可能导致 NQA 测试失败。

当有多个 UDP 监听服务对于 UDP-jitter 测试需要开启高性能模式时，可以通过 **nqa server udp-echo high-performance enable** 命令开启 NQA 服务器的所有 UDP 监听服务对于 UDP-jitter 测试的高性能模式。

【举例】

创建 IP 地址为 169.254.10.2、端口号为 9000 的 UDP 监听服务。

```
<Sysname> system-view
```

```
[Sysname] nqa server udp-echo 169.254.10.2 9000
```

【相关命令】

- **display nqa server**
- **nqa server enable**
- **nqa server udp-echo high-performance enable**

1.2.5 nqa server udp-echo high-performance enable

nqa server udp-echo high-performance enable 命令用来全局开启 NQA 服务器 UDP 监听服务对于 UDP-jitter 测试的高性能模式。

undo nqa server udp-echo high-performance enable 命令用来全局关闭 NQA 服务器 UDP 监听服务对于 UDP-jitter 测试的高性能模式。

【命令】

nqa server udp-echo high-performance enable
undo nqa server udp-echo high-performance enable

【缺省情况】

NQA 服务器 UDP 监听服务的高性能模式处于全局关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

用户可单独开启或全局开启 UDP 监听服务对于 UDP-jitter 测试的高性能模式。

- 全局开启即开启所有 UDP 监听服务对于 UDP-jitter 测试的高性能模式，单独开启则只能开启某个 UDP 监听服务对于 UDP-jitter 测试的高性能模式。
- 从全局开启和单独开启都能开启 UDP 监听服务对于 UDP-jitter 测试的高性能模式，但若关闭 UDP 监听服务对于 UDP-jitter 测试的高性能模式，则必须将全局和单独的 UDP 监听服务对于 UDP-jitter 测试的高性能模式都关闭。

在高性能模式下，NQA 服务器将大大提升 UDP-jitter 测试的探测报文应答效率。此时 NQA 服务器端不能处理大于 100 字节的 NQA 报文，若客户端发送的报文长度大于 100 字节，可能导致 NQA 测试失败。

【举例】

全局开启 NQA 服务器 UDP 监听服务对于 UDP-jitter 测试的高性能模式。

```
<Sysname> system-view
```

```
[Sysname] nqa server udp-echo high-performance enable
```

【相关命令】

- **nqa server udp-echo**

目 录

1 NTP	1-1
1.1 NTP配置命令	1-1
1.1.1 display ntp-service ipv6 sessions	1-1
1.1.2 display ntp-service sessions	1-5
1.1.3 display ntp-service status	1-9
1.1.4 display ntp-service trace	1-11
1.1.5 ntp-service acl	1-12
1.1.6 ntp-service authentication enable	1-13
1.1.7 ntp-service authentication-keyid	1-14
1.1.8 ntp-service broadcast-client	1-16
1.1.9 ntp-service broadcast-server	1-16
1.1.10 ntp-service dscp	1-17
1.1.11 ntp-service enable	1-18
1.1.12 ntp-service inbound enable	1-18
1.1.13 ntp-service ipv6 acl	1-19
1.1.14 ntp-service ipv6 dscp	1-20
1.1.15 ntp-service ipv6 inbound enable	1-21
1.1.16 ntp-service ipv6 multicast-client	1-21
1.1.17 ntp-service ipv6 multicast-server	1-22
1.1.18 ntp-service ipv6 source	1-23
1.1.19 ntp-service ipv6 unicast-peer	1-24
1.1.20 ntp-service ipv6 unicast-server	1-26
1.1.21 ntp-service max-dynamic-sessions	1-28
1.1.22 ntp-service multicast-client	1-29
1.1.23 ntp-service multicast-server	1-29
1.1.24 ntp-service refclock-master	1-30
1.1.25 ntp-service reliable authentication-keyid	1-31
1.1.26 ntp-service source	1-32
1.1.27 ntp-service time-offset-threshold	1-33
1.1.28 ntp-service unicast-peer	1-34
1.1.29 ntp-service unicast-server	1-36

2 SNTP	2-1
2.1 SNTP配置命令	2-1
2.1.1 display sntp ipv6 sessions	2-1
2.1.2 display sntp sessions	2-2
2.1.3 sntp authentication enable	2-2
2.1.4 sntp authentication-keyid	2-3
2.1.5 sntp enable	2-5
2.1.6 sntp ipv6 unicast-server	2-5
2.1.7 sntp reliable authentication-keyid	2-6
2.1.8 sntp time-offset-threshold	2-7
2.1.9 sntp unicast-server	2-8

1 NTP

1.1 NTP配置命令

支持 NTP 的接口均为三层接口，包括三层以太网接口/子接口、三层聚合接口/子接口、VLAN 接口等。

1.1.1 display ntp-service ipv6 sessions

display ntp-service ipv6 sessions 命令用来显示 NTP 服务的所有 IPv6 会话信息。

【命令】

display ntp-service ipv6 sessions [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

verbose: 显示 NTP 服务的所有 IPv6 会话的详细信息。如果不指定该参数，则只显示所有 IPv6 会话的简要信息。

【举例】

显示 NTP 服务的所有 IPv6 会话的简要信息。

```
<Sysname> display ntp-service ipv6 sessions
```

```
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
```

```
Source:    [125]3000::32
Reference: 127.127.1.0      Clock stratum: 2
Reachabilities: 1          Poll interval: 64
Last receive time: 6       Offset: -0.0
Roundtrip delay: 0.0       Dispersion: 0.0
```

```
Total sessions: 1
```

表1-1 display ntp-service ipv6 sessions 命令显示信息描述表

字段	描述
[12345]	五个数字所带表的字段含义如下： 1: 系统选中的时间服务器，即当前与设备进行时间同步的时间服务器 2: 该时间服务器的时钟层数小于等于 15 3: 该时间服务器的时钟通过了时钟选择算法 4: 该时间服务器的时钟为候选的时钟 5: 该时间服务器是通过配置命令指定的
Source	时间服务器的IPv6地址。若该字段显示为::, 表示时间服务器的IPv6地址尚未解析成功
Reference	时间服务器的参考时钟ID 当参考时钟为本地时钟时，本字段的显示情况和Clock stratum字段的取值有关： - 当 Clock stratum 字段为 0 或 1 时，本字段显示为 LOCL - 当 Clock stratum 字段为其他值时，本字段显示为 IPv6 地址前 32 位的 MD5 摘要值，摘要信息按照点分十进制形式显示 当参考时钟为网络中其他设备的时钟时，本字段显示为IPv6地址前32位的MD5摘要值，摘要信息按照点分十进制形式显示。若该字段显示为INIT，表示本地设备还未与时间服务器建立连接
Clock stratum	时间服务器的时钟层数 时钟层数决定了时钟的准确度，取值范围为1~16，层数取值越小，时钟的准确度最高，层数为16的时钟处于未同步状态
Reachabilities	时间服务器的可达性计数，0表示时间服务器不可达
Poll interval	轮询间隔，即两个连续NTP报文之间的时间间隔，单位为秒
Last receive time	最近一次接收到NTP报文或更新本地时间到当前时间的时间间隔 缺省单位为秒；如果时间间隔大于2048秒，则显示为分钟m；如果时间间隔大于300分钟，则显示为小时h；如果时间间隔大于96小时，则显示为天d；如果时间间隔大于999天，则显示为年y；如果最近一次接收到NTP报文或更新本地时间比当前时间晚，则显示为“-”
Offset	系统时钟相对于参考时钟的时钟偏移，单位为毫秒
Roundtrip delay	本地设备到时间服务器的往返时延，单位为毫秒
Dispersion	系统时钟相对于参考时钟的最大误差，单位为毫秒
Total sessions	总的会话数目

显示 NTP 服务的所有 IPv6 会话的详细信息。

```
<Sysname> display ntp-service ipv6 sessions verbose
```

```
Clock source: 1::1
Session ID: 36144
Clock stratum: 16
Clock status: configured, insane, valid, unsynced
Reference clock ID: INIT
VPN instance: Not specified
Local mode: sym_active, local poll interval: 6
```

Peer mode: unspec, peer poll interval: 10
Offset: 0.0000ms, roundtrip delay: 0.0000ms, dispersion: 15937ms
Root roundtrip delay: 0.0000ms, root dispersion: 0.0000ms
Reachabilities:0, sync distance: 15.938
Precision: 2^-18, version: 4, source interface: Not specified
Reftime: 00000000.00000000 Thu, Feb 7 2036 6:28:16.000
Orgtime: d17cbb21.0f318106 Tue, May 17 2011 9:15:13.059
Rcvtime: 00000000.00000000 Thu, Feb 7 2036 6:28:16.000
Xmttime: 00000000.00000000 Thu, Feb 7 2036 6:28:16.000
Roundtrip delay samples: 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000
Offset samples: 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
Filter order: 0 1 2 3 4 5 6 7

Total sessions: 1

表1-2 display ntp-service ipv6 sessions verbose 命令显示信息描述表

字段	描述
Clock source	时间服务器的IPv6地址。若该字段显示为::, 表示时间服务器的IPv6地址尚未解析成功
Session ID	会话ID
Clock stratum	时间服务器的时钟层数 时钟层数决定了时钟的准确度, 取值范围为1~16, 层数取值越小, 表示时钟的准确度最高, 层数为16的时钟处于未同步状态
Clock status	会话的状态, 该字段的取值及含义为: • configured: 表示该会话是配置命令所建立的 • dynamic: 表示该会话是动态生成的 • master: 表示该会话对应的时间服务器是当前系统的主时间服务器 • selected: 表示该会话对应时间服务器的时钟通过了时钟选择算法 • candidate: 表示该会话对应时间服务器的时钟为候选时钟 • sane: 表示该会话对应的时间服务器通过身份验证, 该时间服务器的时钟将作为参考时钟 • insane: 表示该会话对应的时间服务器未通过身份验证, 或该时间服务器通过身份验证但其时钟不作为参考时钟 • valid: 表示该会话对应的时间服务器是有效的(通过验证、处于同步状态、层数有效、根延时/离差未越界等) • invalid: 表示该会话对应的时间服务器是无效的 • unsynced: 表示该会话对应时间服务器的时钟未同步或层数非法
Reference clock ID	时间服务器的参考时钟ID 当参考时钟为本地时钟时, 本字段的显示情况和Clock stratum字段的取值有关: • 当 Clock stratum 字段为 0 或 1 时, 本字段显示为 LOCL • 当 Clock stratum 字段为其他值时, 本字段显示为 IPv6 地址前 32 位的 MD5 摘要值, 摘要信息按照点分十进制形式显示 当参考时钟为网络中其他设备的时钟时, 本字段显示为IPv6地址前32位的MD5摘要值, 摘要信息按照点分十进制形式显示。若该字段显示为INIT, 表示本地设备还未与时间服务器建立连接

字段	描述
VPN instance	时间服务器所属的VPN实例的名称，如果时间服务器位于公网，则显示为Not specified
Local mode	本地设备的工作模式，取值包括： • unspec: 未指定模式 • sym_active: 主动对等体模式 • sym_passive: 被动对等体模式 • client: 客户端模式 • server: 服务器模式 • broadcast: 广播服务器模式或组播服务器模式 • bclient: 广播客户端模式或组播客户端模式
local poll interval	本地设备的轮询间隔，显示的是2的次幂数，单位为秒，比如6表示轮询间隔为2的6次幂，即64s
Peer mode	对端设备的工作模式，取值包括： • unspec: 未指定模式 • sym_active: 主动对等体模式 • sym_passive: 被动对等体模式 • client: 客户端模式 • server: 服务器模式 • broadcast: 广播服务器模式或组播服务器模式 • bclient: 广播客户端模式或组播客户端模式
peer poll interval	对端设备的轮询间隔，显示的是2的次幂数，单位为秒，比如6表示轮询间隔为2的6次幂，即64s
Offset	系统时钟相对于参考时钟的时钟偏移，单位为毫秒
roundtrip delay	本地设备到时间服务器的往返时延，单位为毫秒
dispersion	系统时钟相对于参考时钟的最大误差，单位为毫秒
Root roundtrip delay	本地设备到主时间服务器的往返时延，单位为毫秒
root dispersion	系统时钟相对主参考时钟的最大误差，单位为毫秒
Reachabilities	时间服务器的可达性计数，0表示时间服务器不可达
sync distance	表示相对上一级时间服务器的同步距离，由误差disper和往返时延delay计算而来，单位为秒
Precision	系统时钟的精度
version	NTP版本，取值为1~4
source interface	源接口，未指定源接口时，此字段显示为Not specified
Reftime	NTP报文中的参考时间戳
Orgtime	NTP报文中的起始时间戳
Rcvtime	NTP报文的接收时间戳
Xmtime	NTP报文的发送时间戳

字段	描述
Roundtrip delay samples	本地设备到时间服务器往返时延的抽样值
Offset samples	相对于参考时钟的时钟偏移的抽样值
Filter order	样本信息排序
Reference clock status	本地时钟的工作状态，只有通过 ntp-service refclock-master 命令设置本地时钟作为参考时钟时，才会显示该字段 当本地时钟的reach值等于255时，该字段取值为working normally；否则，该字段取值为working abnormally
Total sessions	总的会话数目

1.1.2 display ntp-service sessions

display ntp-service sessions 命令用来显示 NTP 服务的所有 IPv4 会话信息。

【命令】

display ntp-service sessions [verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

verbose: 显示 NTP 服务的所有 IPv4 会话的详细信息。如果不指定该参数，则只显示所有会话的简要信息。

【使用指导】

设备作为 NTP 广播服务器或 NTP 组播服务器时，在设备上执行 **display ntp-service sessions** 命令不会显示与该广播服务器或组播服务器对应的 NTP 服务的 IPv4 会话信息，但是这些会话会统计在总的会话数中。

【举例】

显示 NTP 服务的所有 IPv4 会话的简要信息。

```
<Sysname> display ntp-service sessions
      source           reference      stra reach poll  now offset  delay disper
*****
[12345]LOCAL(0)        LOCL              0      1   64    - 0.0000 0.0000 7937.9
      [5]0.0.0.0        INIT              16     0   64    - 0.0000 0.0000 0.0000
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
Total sessions: 1
```

表1-3 display ntp-service sessions 命令显示信息描述表

字段	描述
source	参考时钟为本地时钟时，显示为LOCAL(<i>number</i>)，表示本地时钟的地址为127.127.1. <i>number</i> ，其中 <i>number</i> 为NTP的进程号，取值范围为0~3 参考时钟为网络中其他设备的时钟时，显示为时间服务器的IP地址。若该字段显示为0.0.0.0，表示时间服务器的IP地址尚未解析成功
reference	时间服务器的参考时钟ID 当参考时钟为本地时钟时，本字段的显示情况和stra字段的取值有关： - 当 stra 字段为 0 或 1 时，本字段将显示为 LOCL - 当 stra 字段为其他值时，本字段将显示为本地时钟的 IP 地址 当参考时钟为网络中其他设备的时钟时，本字段显示为该设备的IP地址，若该设备为IPv6设备，则本字段显示为该设备的IPv6地址前32位的MD5摘要值，摘要信息按照点分十进制形式显示。若该字段显示为INIT，表示本地设备还未与时间服务器建立连接
stra	时间服务器的时钟层数 时钟层数决定了时钟的准确度，取值范围为1~16，层数取值越小，表示时钟的准确度最高，层数为16的时钟处于未同步状态
reach	时间服务器的可达性计数，0表示时间服务器不可达
poll	轮询间隔，即两个连续NTP报文之间的时间间隔，单位为秒
now	最近一次接收到NTP报文或更新本地时间到当前时间的时间间隔 缺省单位为秒；如果时间间隔大于2048秒，则显示为分钟m；如果时间间隔大于300分钟，则显示为小时h；如果时间间隔大于96小时，则显示为天d；如果时间间隔大于999天，则显示为年y；如果最近一次接收到NTP报文或更新本地时间比当前时间晚，则显示为“-”
offset	系统时钟相对于参考时钟的时钟偏移，单位为毫秒
delay	本地设备到时间服务器的往返时延，单位为毫秒
disper	系统时钟相对于参考时钟的最大误差，单位为毫秒
[12345]	1: 系统选中的时间服务器，即当前与设备进行时间同步的时间服务器 2: 该时间服务器的时钟层数小于等于15 3: 该时间服务器的时钟通过了时钟选择算法 4: 该时间服务器的时钟为候选时钟 5: 该时间服务器的时钟是配置命令指定的
Total sessions	总的会话数目

显示 NTP 服务的所有 IPv4 会话的详细信息。

```
<Sysname> display ntp-service sessions verbose
Clock source: 192.168.1.40
Session ID: 35888
Clock stratum: 2
Clock status: configured, master, sane, valid
Reference clock ID: 127.127.1.0
VPN instance: Not specified
Local mode: client, local poll interval: 6
Peer mode: server, peer poll interval: 6
```



```

Offset: 0.2862ms, roundtrip delay: 3.2653ms, dispersion: 4.5166ms
Root roundtrip delay: 0.0000ms, root dispersion: 10.910ms
Reachabilities:31, sync distance: 0.0194
Precision: 2^-18, version: 3, source interface: Not specified
Reftime: d17cbb5.1473de1e Tue, May 17 2011 9:17:25.079
Orgtime: 00000000.00000000 Thu, Feb 7 2036 6:28:16.000
Rcvtime: d17cbbc0.b1959a30 Tue, May 17 2011 9:17:52.693
Xmttime: d17cbbc0.b1959a30 Tue, May 17 2011 9:17:52.693
Roundtrip delay samples: 0.007 0.010 0.006 0.011 0.010 0.005 0.007 0.003
Offset samples: 5629.55 3913.76 5247.27 6526.92 31.99 148.72 38.27 0.29
Filter order: 7      5      2      6      0      4      1      3

```

Total sessions: 1

表1-4 display ntp-service sessions verbose 命令显示信息描述表

字段	描述
Clock source	时间服务器的IP地址。若该字段显示为0.0.0.0，表示时间服务器的IP地址尚未解析成功
Session ID	会话ID
Clock stratum	时间服务器的时钟层数 时钟层数决定了时钟的准确度，取值范围为1~16，层数取值越小，表示时钟的准确度越高，层数为16的时钟处于未同步状态
Clock status	会话的状态，该字段的取值及含义为： - configured: 表示该会话是配置命令所建立的 - dynamic: 表示该会话是动态生成的 - master: 表示该会话对应的时间服务器是当前系统的主时间服务器 - selected: 表示该会话对应时间服务器的时钟通过了时钟选择算法 - candidate: 表示该会话对应时间服务器的时钟为候选时钟 - sane: 表示该会话对应的时间服务器通过身份验证，该时间服务器的时钟将作为参考时钟 - insane: 表示该会话对应的时间服务器未通过身份验证，或该时间服务器通过身份验证但其时钟不作为参考时钟 - valid: 表示该会话对应的时间服务器是有效的（通过验证、处于同步状态、层数有效、根延时/离差未越界等） - invalid: 表示该会话对应的时间服务器是无效的 - unsynced: 表示该会话对应时间服务器的时钟未同步或层数非法
Reference clock ID	时间服务器的参考时钟ID 当参考时钟为本地时钟时，本字段的显示情况和Clock stratum字段的取值有关： - 当 Clock stratum 字段取值为 0 或 1 时，本字段将显示为 LOCL； - 当 Clock stratum 字段取值为其他值时，本字段将显示为本地时钟的 IP 地址 当参考时钟为网络中其他设备的时钟时，本字段显示为该设备的IP地址，若该设备为IPv6设备，则本字段显示为该设备的IPv6地址前32位的MD5摘要值，摘要信息按照点分十进制形式显示。若该字段显示为INIT，表示本地设备还未与时间服务器建立连接
VPN instance	时间服务器所属的VPN实例的名称，如果时间服务器位于公网，则显示为Not specified

字段	描述
Local mode	本地设备的工作模式，取值包括： • unspec: 未指定模式 • sym_active: 主动对等体模式 • sym_passive: 被动对等体模式 • client: 客户端模式 • server: 服务器模式 • broadcast: 广播服务器模式或组播服务器模式 • bclient: 广播客户端模式或组播客户端模式
local poll interval	本地设备的轮询间隔，显示的是2的次幂数，单位为秒，比如6表示轮询间隔为2的6次幂，即64s
Peer mode	对端设备的工作模式，取值包括： • unspec: 未指定模式 • sym_active: 主动对等体模式 • sym_passive: 被动对等体模式 • client: 客户端模式 • server: 服务器模式 • broadcast: 广播服务器模式或组播服务器模式 • bclient: 广播客户端模式或组播客户端模式
peer poll interval	对端设备的轮询间隔，显示的是2的次幂数，单位为秒，比如6表示轮询间隔为2的6次幂，即64s
Offset	系统时钟相对于参考时钟的时钟偏移，单位为毫秒
roundtrip delay	本地设备到时间服务器的往返时延，单位为毫秒
dispersion	系统时钟相对于参考时钟的最大误差
Root roundtrip delay	本地设备到主时间服务器的往返时延，单位为毫秒
root dispersion	系统时钟相对主参考时钟的最大误差，单位为毫秒
Reachabilities	时间服务器的可达性计数，0表示时间服务器不可达
sync distance	表示相对上一级时间服务器的同步距离，由误差disper和往返时延delay计算而来，单位为秒
Precision	系统时钟的精度
version	NTP版本，取值为1~4
source interface	源接口，未指定源接口时，此字段显示为Not specified
Reftime	NTP报文中的参考时间戳
Orgtime	NTP报文中的起始时间戳
Rcvtime	NTP报文的接收时间戳
Xmttime	NTP报文的发送时间戳
Roundtrip delay samples	本地设备到时间服务器往返时延的抽样值

字段	描述
Offset samples	相对于参考时钟的时钟偏移的抽样值
Filter order	抽样信息排序
Reference clock status	本地时钟的工作状态，只有通过 ntp-service refclock-master 命令设置本地时钟作为参考时钟时，才会显示该字段 当本地时钟的reach值等于255时，该字段取值为working normally；否则，该字段取值为working abnormally
Total sessions	总的会话数目

1.1.3 display ntp-service status

display ntp-service status 命令用来显示 NTP 服务的状态信息。

【命令】

display ntp-service status

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

时间已同步时，显示 NTP 服务的状态信息。

```
<Sysname> display ntp-service status
Clock status: synchronized
Clock stratum: 2
System peer: LOCAL(0)
Local mode: client
Reference clock ID: 127.127.1.0
Leap indicator: 00
Clock jitter: 0.000977 s
Stability: 0.000 pps
Clock precision: 2^-18
Root delay: 0.000000 ms
Root dispersion: 3.96367 ms
Reference time: d0c5fc32.92c70b1e Wed, Dec 29 2010 18:28:02.573
System poll interval: 64 s
```

时间未同步时，显示 NTP 服务的状态信息。

```
<Sysname> display ntp-service status
Clock status: unsynchronized
Clock stratum: 16
```

Reference clock ID: none
Clock jitter: 0.000000 s
Stability: 0.000 pps
Clock precision: 2^-18
Root delay: 0.00000 ms
Root dispersion: 0.00002 ms
Reference time: d0c5fc32.92c70b1e Wed, Dec 29 2010 18:28:02.573
System poll interval: 8 s

表1-5 display ntp-service status 命令显示信息描述表

字段	描述
Clock status	系统时间的状态，取值为： - synchronized: 系统时间已同步 - unsynchronized: 系统时间未同步
Clock stratum	系统时钟的层数
System peer	系统时钟选中的时间服务器的IP地址
Local mode	相对于选中的时间服务器，本地设备的工作模式，取值包括： - unspec: 未指定模式 - sym_active: 主动对等体模式 - sym_passive: 被动对等体模式 - client: 客户端模式 - server: 服务器模式 - broadcast: 广播服务器模式或组播服务器模式 - bclient: 广播客户端模式或组播客户端模式
Reference clock ID	参考时钟ID 1. 对于 IPv4 NTP 服务器： 本地设备从远程时间服务器获取时间同步时，表示远程服务器的IP地址 本地设备从本地时钟获取时间同步时，表示本地时钟的标识： - 本地时钟的层数为 1 时，显示为 LOCL - 本地时钟的层数为其他值时，显示为本地时钟的 IP 地址 2. 对于 IPv6 NTP 服务器： 本地设备从远程时间服务器获取时间同步时，表示远程服务器的IPv6地址前 32位的MD5摘要值 本地设备从本地时钟获取时间同步时，表示本地时钟的标识： - 本地时钟的层数为 1 时，显示为 LOCL - 本地时钟的层数为其他值时，显示为本地时钟的 IPv6 地址前 32 位的 MD5 摘要值
Leap indicator	告警状态，取值包括： 00: 正常状态 01: 闰秒标志，表示一天中的最后一分钟有 61 秒 10: 闰秒标志，表示一天中的最后一分钟有 59 秒 11: 时间未被同步的告警状态

字段	描述
Clock jitter	系统时钟相对于参考时钟的偏移量，单位为秒
Stability	时钟频率的稳定性，取值越小，时钟频率越稳定
Clock precision	系统时钟的精度
Root delay	本地设备到主时间服务器的往返时延，单位为毫秒
Root dispersion	系统时钟相对主参考时钟的最大误差，单位为毫秒
Reference time	参考时间戳
System poll interval	系统轮询时间间隔，单位为秒

1.1.4 display ntp-service trace

display ntp-service trace 命令用来显示从本地设备回溯到主时间服务器的各个 NTP 时间服务器的简要信息。

【命令】

display ntp-service trace [*source interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

source interface-type interface-number: 指定回溯主时间服务器时发送 NTP 报文的源接口，*interface-type interface-number* 表示接口类型和接口编号。本地设备向时间服务器发送 NTP 报文时，报文的源地址为指定源接口的主 IPv4 地址或接口的 IPv6 地址；如果 NTP 时间服务器地址是链路本地地址时，报文的源地址为报文出接口的链路本地地址。如果不指定本参数，则以报文发送接口作为回溯主时间服务器时发送 NTP 报文的源接口。

【使用指导】

指定源接口回溯主时间服务器时，需要保证主时间服务器已及各个 NTP 时间服务器均和源接口之间路由可达，否则将导致回溯失败。

【举例】

显示从本地设备回溯到主时间服务器的各个 NTP 时间服务器的简要信息。

```
<Sysname> display ntp-service trace
Server      127.0.0.1
Stratum     3, jitter  0.000, synch distance 0.0000.
Server      3000::32
```

```
Stratum    2 , jitter 790.00, synch distance 0.0000.  
RefID      127.127.1.0
```

以上信息显示了服务器 127.0.0.1 的同步链：服务器 127.0.0.1 同步到服务器 3000::32，服务器 3000::32 从本地时钟得到同步。

表1-6 display ntp-service trace 命令显示信息描述表

字段	描述
Server	时间服务器的IP地址
Stratum	表示相应服务器的时钟层数
jitter	表示相对上一级时钟的时钟偏差的均方根，单位为秒
synch distance	表示相对上一级时间服务器的同步距离，由误差disper和往返时延delay计算而来，单位为秒
RefID	主时间服务器的标识，主参考时钟的层数为0时，显示为LOCL；为其他值时，显示为主参考时钟的IP地址

【相关命令】

- **ntp-service source**
- **ntp-service unicast-server**
- **ntp-service unicast-peer**
- **ntp-service ipv6 source**
- **ntp-service ipv6 unicast-server**
- **ntp-service ipv6 unicast-peer**

1.1.5 ntp-service acl

ntp-service acl 命令用来设置对端设备对本地设备 NTP 服务的访问控制权限。

undo ntp-service acl 命令用来取消设置的访问控制权限。

【命令】

```
ntp-service { peer | query | server | synchronization } acl ipv4-acl-number  
undo ntp-service { peer | query | server | synchronization } [ acl  
ipv4-acl-number ]
```

【缺省情况】

对端设备对本地设备 NTP 服务的访问控制权限为 **peer**。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

peer: 完全访问权限。该权限既允许对端设备向本地设备的时间同步, 对本地设备进行控制查询(查询 NTP 的一些状态, 比如告警信息、验证状态、时间服务器信息等), 同时本地设备也可以向对端设备的时间同步。

query: 仅具有控制查询的权限。该权限只允许对端设备对本地设备的 NTP 服务进行控制查询, 但是不能向本地设备的时间同步。

server: 服务器访问与查询权限。该权限允许对端设备向本地设备的时间同步, 对本地设备进行控制查询, 但本地设备不会向对端设备的时间同步。

synchronization: 仅具有访问服务器的权限。该权限只允许对端设备向本地设备的时间同步, 但不能进行控制查询。

ipv4-acl-number: 通过编号指定引用的 ACL (Access Control List, 访问控制列表)。通过 ACL 过滤的对端设备具有本命令中指定的访问控制权限。**ipv4-acl-number** 为 IPv4 基本或高级 ACL 的编号, 取值范围为 2000~2999 和 3000~3999。

【使用指导】

NTP 服务的访问控制权限从高到低依次为 **peer**、**server**、**synchronization**、**query**。当设备接收到一个 NTP 服务请求时, 会按照权限从高到低的顺序依次进行匹配, 第一个匹配的权限为此设备具有的访问控制权限。如果没有匹配的权限, 则不允许对端设备与本地设备进行时间同步、对本端进行控制查询, 也不允许本端设备与对端设备进行时间同步。

当引用的 ACL 不存在时, 任何设备都能访问本地 NTP 服务。当引用的 ACL 下没有配置规则时, 任何设备都不能访问本地 NTP 服务。

ntp-service acl 命令提供了一种最小限度的安全措施, 更安全的方法是进行身份验证。

【举例】

配置 10.10.0.0/16 网段的对端设备对本地设备具有完全访问权限。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ntp-service peer acl 2001
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.6 ntp-service authentication enable

ntp-service authentication enable 命令用来开启 NTP 身份验证功能。

undo ntp-service authentication enable 命令用来关闭 NTP 身份验证功能。

【命令】

```
ntp-service authentication enable
undo ntp-service authentication enable
```

【缺省情况】

NTP 身份验证功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

在一些对安全性要求较高的网络中，运行 NTP 协议时需要启用 NTP 身份验证功能。通过客户端和服务端端的身份验证，保证客户端只与通过验证的设备进行时间同步，避免客户端从非法的服务器获得错误的时间同步信息。

开启 NTP 身份验证功能后，还需要设置身份验证密钥，并将其设置为可信密钥，才能正确地进行身份验证。

【举例】

开启 NTP 身份验证功能。

```
<Sysname> system-view
```

```
[Sysname] ntp-service authentication enable
```

【相关命令】

- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.7 ntp-service authentication-keyid

ntp-service authentication-keyid 命令用来设置 NTP 身份验证密钥。

undo ntp-service authentication-keyid 命令用来删除指定的 NTP 身份验证密钥。

【命令】

```
ntp-service authentication-keyid keyid authentication-mode md5 { cipher | simple } string [ acl ipv4-acl-number | ipv6 acl ipv6-acl-number ] *
```

```
undo ntp-service authentication-keyid keyid
```

【缺省情况】

未设置 NTP 身份验证密钥。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

keyid: 密钥编号, 用来标识身份验证密钥, 取值范围为 1~4294967295。

authentication-mode md5: 表示采用 MD5 算法进行身份验证。

cipher: 以密文形式设置密钥。

simple: 以明文形式设置密钥, 该密钥将以密文形式存储。

string: 密钥字符串, 区分大小写。明文密钥为 1~32 个字符的字符串, 密文密钥为 1~73 个字符的字符串。

acl ipv4-acl-number: 对对端设备进行 ACL 过滤。通过 ACL 过滤的对端设备有权在本端使用该密钥 ID 进行身份验证。**ipv4-acl-number** 为 IPv4 基本 ACL 的编号, 取值范围为 2000~2999。

ipv6 acl ipv6-acl-number: 对对端设备进行 IPv6 ACL 过滤。通过 IPv6 ACL 过滤的对端设备有权在本端使用该密钥 ID 进行身份验证。**ipv6-acl-number** 为 IPv6 基本 ACL 的编号, 取值范围为 2000~2999。

【使用指导】

在一些对安全性要求较高的网络中, 运行 NTP 协议时需要启用身份验证功能。通过客户端和服务器的身份验证, 保证客户端只与通过验证的设备进行时间同步, 提高了时间同步的安全性。

NTP 协议采用哪个密钥对对端进行身份验证由对端报文中携带的密钥 ID 决定。这会导致如下安全问题: 对对端进行身份验证时只关心密钥是否正确而不关心对端是否有权使用该密钥 ID。**acl** 和 **ipv6 acl** 参数用于指定有权在本端使用该密钥 ID 进行身份验证的对端设备。需要注意的是:

- 当引用的 ACL 或 IPv6 ACL 不存在时, 任何设备都能在本端使用该密钥 ID 进行验证。
- 当引用的 ACL 或 IPv6 ACL 下没有配置规则时, 任何设备都不能在本端使用该密钥 ID 进行验证。

客户端和服务端需要配置相同的密钥 ID 及密钥值, 并且保证对端有权在本端使用该密钥 ID 进行身份验证, 否则无法实现时间同步。

配置 NTP 验证密钥后, 还需要通过 **ntp-service reliable authentication-keyid** 命令将该密钥设置为可信密钥。如果 NTP 验证密钥被指定为可信密钥, 删除密钥后, 该密钥将自动变为不可信密钥, 不必再执行 **undo ntp-service reliable authentication-keyid** 命令。通过重复执行本命令, 可以配置多个 NTP 身份验证密钥。设备上最多可以配置 128 个 NTP 身份验证密钥。

【举例】

设置 MD5 身份验证密钥, 密钥 ID 号为 10, 密钥为 BetterKey, 以明文形式输入。

```
<Sysname> system-view
```

```
[Sysname] ntp-service authentication enable
```

```
[Sysname] ntp-service authentication-keyid 10 authentication-mode md5 simple BetterKey
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service reliable authentication-keyid**

1.1.8 ntp-service broadcast-client

ntp-service broadcast-client 命令用来配置设备工作在 NTP 广播客户端模式，并使用当前接口接收 NTP 广播报文。

undo ntp-service broadcast-client 命令用来取消 NTP 广播客户端模式的配置。

【命令】

```
ntp-service broadcast-client
undo ntp-service broadcast-client
```

【缺省情况】

未配置 NTP 工作模式。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

配置设备工作在 NTP 广播客户端模式后，设备将在接口上监听 NTP 广播服务器发送的 NTP 广播报文，根据接收到的报文实现时间同步。

如果在接口上配置了设备工作在广播客户端模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 NTP 广播客户端配置。

【举例】

配置设备工作在广播客户端模式，在 GigabitEthernet1/0/1 接口上接收 NTP 广播报文。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntp-service broadcast-client
```

【相关命令】

- **ntp-service broadcast-server**

1.1.9 ntp-service broadcast-server

ntp-service broadcast-server 命令用来配置设备工作在 NTP 广播服务器模式，并使用当前接口发送 NTP 广播报文。

undo ntp-service broadcast-server 命令用来取消 NTP 广播服务器模式的配置。

【命令】

```
ntp-service broadcast-server [ authentication-keyid keyid | version number ]
*
undo ntp-service broadcast-server
```

【缺省情况】

未配置 NTP 工作模式。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

authentication-keyid keyid: 指定向广播客户端发送 NTP 报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1~4294967295。如果未指定本参数，则本端设备无法同步开启了身份验证功能的广播客户端。

version number: 指定 NTP 版本号。*number* 取值范围为 1~4，缺省值为 4。

【使用指导】

配置设备工作在 NTP 广播服务器模式后，设备将通过该接口周期性地向广播地址 255.255.255.255 发送 NTP 报文。

如果在接口上配置了设备工作在广播服务器模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 NTP 广播服务器配置。

【举例】

配置设备工作在广播服务器模式，在 GigabitEthernet1/0/1 接口上发送 NTP 广播报文，用 4 号密钥进行加密，设置 NTP 版本号为 4。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ntp-service broadcast-server authentication-keyid 4 version 4
```

【相关命令】

- **ntp-service broadcast-client**

1.1.10 ntp-service dscp

ntp-service dscp 命令用来配置 NTP 报文的 DSCP 优先级。

undo ntp-service dscp 命令用来恢复缺省情况。

【命令】

ntp-service dscp dscp-value

undo ntp-service dscp

【缺省情况】

NTP 报文的 DSCP 优先级为 48。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

dscp-value: NTP 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 NTP 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ntp-service dscp 30
```

1.1.11 ntp-service enable

ntp-service enable 命令用来开启 NTP 服务。

undo ntp-service enable 命令用来关闭 NTP 服务。

【命令】

```
ntp-service enable
undo ntp-service enable
```

【缺省情况】

NTP 服务处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【举例】

开启 NTP 服务。

```
<Sysname> system-view
[Sysname] ntp-service enable
```

1.1.12 ntp-service inbound enable

ntp-service inbound enable 命令用来开启接口接收 NTP 报文功能。

undo ntp-service inbound enable 命令用来关闭接口接收 NTP 报文功能。

【命令】

```
ntp-service inbound enable
undo ntp-service inbound enable
```

【缺省情况】

接口接收 NTP 报文功能处于开启状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

如果不允许设备为某个接口对应网段内的对端设备提供时间同步，或不允许设备从某个接口对应网段内的对端设备获得时间同步，则可以在该接口上执行 **undo ntp-service inbound enable** 命令，使该接口关闭接收 NTP 报文功能。

【举例】

```
# 关闭 GigabitEthernet1/0/1 接口接收 NTP 报文功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo ntp-service inbound enable
```

1.1.13 ntp-service ipv6 acl

ntp-service ipv6 acl 命令用来设置对端设备对本地设备 IPv6 NTP 服务的访问控制权限。

undo ntp-service ipv6 acl 命令用来取消设置的访问控制权限。

【命令】

```
ntp-service ipv6 { peer | query | server | synchronization } acl
ipv6-acl-number
undo ntp-service ipv6 { peer | query | server | synchronization } [ acl
ipv6-acl-number ]
```

【缺省情况】

对端设备对本地设备 IPv6 NTP 服务的访问控制权限为 **peer**。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

peer: 完全访问权限。该权限既允许对端设备向本地设备的时间同步，对本地设备进行控制查询（查询 NTP 的一些状态，比如告警信息、验证状态、时间服务器信息等），同时本地设备也可以向对端设备的时间同步。

query: 仅具有控制查询的权限。该权限只允许对端设备对本地设备的 NTP 服务进行控制查询，但是不能向本地设备的时间同步。

server: 服务器访问与查询权限。该权限允许对端设备向本地设备的时间同步，对本地设备进行控制查询，但本地设备不会向对端设备的时间同步。

synchronization: 仅具有访问服务器的权限。该权限只允许对端设备向本地设备的时间同步，但不能进行控制查询。

ipv6-acl-number: 通过编号指定应用的 IPv6 ACL（Access Control List，访问控制列表）。通过 IPv6 ACL 过滤的对端设备具有本命令中指定的访问控制权限。**ipv6-acl-number** 为 IPv6 基本或高级 ACL 的编号，取值范围为 2000～2999 和 3000～3999。

【使用指导】

IPv6 NTP 服务的访问控制权限从高到低依次为 **peer**、**server**、**synchronization**、**query**。当设备接收到一个 IPv6 NTP 服务请求时，会按照权限从高到低的顺序依次进行匹配，第一个匹配的权限为此设备具有的访问控制权限。如果没有匹配的权限，则不允许对端设备与本地设备进行时间同步、对本端进行控制查询，也不允许本端设备与对端设备进行时间同步。

当引用的 IPv6 ACL 不存在时，任何设备都能访问本地 IPv6 NTP 服务。当引用的 IPv6 ACL 下没有配置规则时，任何设备都不能访问本地 IPv6 NTP 服务。

ntp-service ipv6 acl 命令提供了一种最小限度的安全措施，更安全的方法是进行身份验证。

【举例】

```
# 配置 2001::1 网段的对端设备对本地设备具有完全访问权限。
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2001::1 64
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] ntp-service ipv6 peer acl 2001
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.14 ntp-service ipv6 dscp

ntp-service ipv6 dscp 命令用来配置 IPv6 NTP 报文的 DSCP 优先级。

undo ntp-service ipv6 dscp 命令用来恢复缺省情况。

【命令】

```
ntp-service ipv6 dscp dscp-value
undo ntp-service ipv6 dscp
```

【缺省情况】

IPv6 NTP 报文的 DSCP 优先级为 56。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

dscp-value: IPv6 NTP 报文的 DSCP 优先级，取值范围为 0~63。

【使用指导】

DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 IPv6 NTP 报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ntp-service ipv6 dscp 30
```

1.1.15 ntp-service ipv6 inbound enable

ntp-service ipv6 inbound enable 命令用来开启接口接收 IPv6 NTP 报文功能。

undo ntp-service ipv6 inbound enable 命令用来关闭接口接收 IPv6 NTP 报文功能。

【命令】

```
ntp-service ipv6 inbound enable
undo ntp-service ipv6 inbound enable
```

【缺省情况】

接口接收 IPv6 NTP 报文功能处于开启状态。

【视图】

接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

如果不允许设备为某个接口对应网段内的对端设备提供时间同步，或不允许设备从某个接口对应网段内的对端设备获得时间同步，则可以在该接口上执行 **undo ntp-service ipv6 inbound enable** 命令，使该接口关闭接收 IPv6 NTP 报文功能。

【举例】

关闭 GigabitEthernet1/0/1 接口接收 IPv6 NTP 报文功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo ntp-service ipv6 inbound enable
```

1.1.16 ntp-service ipv6 multicast-client

ntp-service ipv6 multicast-client 命令用来配置设备工作在 IPv6 NTP 组播客户端模式，并使用当前接口接收 IPv6 NTP 组播报文。

undo ntp-service ipv6 multicast-client 命令用来取消 IPv6 NTP 组播客户端模式的配置。

【命令】

```
ntp-service ipv6 multicast-client ipv6-address  
undo ntp-service ipv6 multicast-client ipv6-address
```

【缺省情况】

未配置 NTP 工作模式。

【视图】

接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

ipv6-address: NTP 报文的 IPv6 组播地址。IPv6 组播客户端和 IPv6 组播服务器上配置的组播地址必须相同。

【使用指导】

配置设备工作在 IPv6 NTP 组播客户端模式后，设备将在接口上监听目的地址为指定 IPv6 组播地址的 IPv6 NTP 报文，根据接收到的报文实现时间同步。

如果在接口上配置了设备工作在 IPv6 组播客户端模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 IPv6 NTP 组播客户端配置。

【举例】

配置设备工作在 IPv6 组播客户端模式，在 GigabitEthernet1/0/1 接口上接收目的地址为组播地址 FF21::1 的 NTP 报文。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ntp-service ipv6 multicast-client ff21::1
```

【相关命令】

- **ntp-service ipv6 multicast-server**

1.1.17 ntp-service ipv6 multicast-server

ntp-service ipv6 multicast-server 命令用来配置设备工作在 IPv6 NTP 组播服务器模式，并使用当前接口发送 IPv6 NTP 组播报文。

undo ntp-service ipv6 multicast-server 命令用来取消 IPv6 NTP 组播服务器模式的配置。

【命令】

```
ntp-service ipv6 multicast-server ipv6-address [ authentication-keyid keyid  
| ttl ttl-number ] *  
undo ntp-service ipv6 multicast-server ipv6-address
```


【缺省情况】

未配置 NTP 工作模式。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-address: NTP 报文的 IPv6 组播地址。IPv6 组播客户端和 IPv6 组播服务器上配置的组播地址必须相同。

authentication-keyid keyid: 指定向组播客户端发送 NTP 报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1~4294967295。如果未指定本参数，则本端设备无法同步开启了身份验证功能的组播客户端。

ttl ttl-number: 指定组播报文的生存期。*ttl-number* 取值范围为 1~255，缺省值为 16。

【使用指导】

配置设备工作在 IPv6 NTP 组播服务器模式后，设备将通过该接口周期性地向指定的 IPv6 组播地址发送 NTP 报文。

如果在接口上配置了设备工作在 IPv6 组播服务器模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 IPv6 NTP 组播服务器配置。

【举例】

配置设备工作在 IPv6 组播服务器模式，在 GigabitEthernet1/0/1 接口上向 IPv6 组播地址 FF21::1 发送 NTP 报文，用 4 号密钥加密 NTP 报文。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntp-service ipv6 multicast-server ff21::1
authentication-keyid 4
```

【相关命令】

- **ntp-service ipv6 multicast-client**

1.1.18 ntp-service ipv6 source

ntp-service ipv6 source 命令用来指定 IPv6 NTP 报文的源接口。

undo ntp-service ipv6 source 命令用来恢复缺省情况。

【命令】

```
ntp-service ipv6 source interface-type interface-number
undo ntp-service ipv6 source
```

【缺省情况】

未指定 IPv6 NTP 报文的源接口，设备自动选择报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type interface-number: 接口类型和接口编号。

【使用指导】

如果指定了 IPv6 NTP 报文的源接口，则设备在主动发送 IPv6 NTP 报文时，将采用源接口的 IPv6 地址作为发送报文的源 IPv6 地址，从而保证 IPv6 NTP 应答报文的目地址均为此地址。

设备对接收到的 IPv6 NTP 请求报文进行应答时，应答报文的源 IPv6 地址始终为接收到 IPv6 NTP 请求报文的目 IPv6 地址。

如果不想让本地设备上其他接口的 IPv6 地址成为应答报文的目地址，可以使用本命令。

使用本命令指定 IPv6 NTP 报文的源接口时，需要注意：

- 当 NTP 工作在客户端/服务器模式时，如果在命令 **ntp-service ipv6 unicast-server** 中指定了 IPv6 NTP 报文的源接口，则以 **ntp-service ipv6 unicast-server** 命令指定源接口的为准。
- 当 NTP 工作在对等体模式时，如果在命令 **ntp-service ipv6 unicast-peer** 中指定了 IPv6 NTP 报文的源接口，则以 **ntp-service ipv6 unicast-peer** 命令指定源接口的为准。
- 当 NTP 工作在组播模式时，如果在接口视图下配置了 **ntp-service ipv6 multicast-server** 命令，则 NTP 组播报文的源接口为配置了 **ntp-service ipv6 multicast-server** 命令的接口。
- 如果指定的 NTP 源接口处于 down 状态，则设备不再发送 IPv6 NTP 报文。

【举例】

配置 IPv6 NTP 报文的源接口为接口 GigabitEthernet1/0/1。

```
<Sysname> system-view
```

```
[Sysname] ntp-service ipv6 source gigabitethernet 1/0/1
```

1.1.19 ntp-service ipv6 unicast-peer

ntp-service ipv6 unicast-peer 命令用来为设备指定 IPv6 被动对等体。

undo ntp-service ipv6 unicast-peer 命令用来删除为设备指定的 IPv6 被动对等体。

【命令】

```
ntp-service ipv6 unicast-peer { peer-name | ipv6-address } [ vpn-instance vpn-instance-name ] [ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number ] *
```

```
undo ntp-service ipv6 unicast-peer { peer-name | ipv6-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未指定 IPv6 被动对等体。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

peer-name: 被动对等体的主机名，为 1~253 个字符的字符串，不区分大小写，字符串中只能包含字母、数字、“-”、“_”和“.”。

ipv6-address: 被动对等体的 IPv6 地址。该地址只能是一个单播地址，不能为组播地址。

vpn-instance vpn-instance-name: 指定 NTP 被动对等体所属的 VPN 实例，**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 NTP 被动对等体位于公网中。

authentication-keyid keyid: 指定向对等体发送 NTP 报文时，使用指定的密钥计算报文的摘要。**keyid** 取值范围为 1~4294967295。如果未指定本参数，则本端设备与对等体之间不会进行身份验证。

maxpoll maxpoll-interval: 用来配置最大轮询时间间隔。**maxpoll-interval** 取值范围为 4~17，最大轮询时间间隔为 2 的 **maxpoll-interval** 次幂，对应的最大轮询时间间隔的取值范围为 $2^4 \sim 2^{17}$ （即 16~131072）秒。本参数的缺省值为 6，即最大轮询时间间隔为 64 秒。

minpoll minpoll-interval: 用来配置最小轮询时间间隔，**minpoll-interval** 取值范围为 4~17，最大轮询时间间隔为 2 的 **maxpoll-interval** 次幂，对应的最大轮询时间间隔的取值范围为 $2^4 \sim 2^{17}$ （即 16~131072）秒。本参数的缺省值为 6，即最小轮询时间间隔为 64 秒。

priority: 在同等条件下，优先选择 **ipv6-address** 或 **peer-name** 指定的对等体为同步对等体。

source interface-type interface-number: 指定 IPv6 NTP 报文的源接口。如果指定的被动对等体地址不是链路本地地址，则本地设备给对端发送 IPv6 NTP 报文时，报文的源 IPv6 地址为指定源接口的 IPv6 地址。如果指定的被动对等体地址是链路本地地址，则 IPv6 NTP 报文从指定的源接口发送，并且报文的源地址为该接口的链路本地地址。**interface-type interface-number** 为接口类型和接口编号。如果未指定本参数，则设备自动选择报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【使用指导】

为设备指定 IPv6 被动对等体后，主动对等体和被动对等体的时间可以互相同步。如果双方的时钟都处于同步状态，则层数大的时钟与层数小的时钟的时间同步。

配置 PE 向某个 VPN 实例内的其他 PE 或 CE 同步时，需要指定 **vpn-instance vpn-instance-name** 参数。

在执行 **undo ntp-service ipv6 unicast-peer** 命令时，如果指定 **vpn-instance vpn-instance-name** 参数，则取消指定 VPN 实例内 IPv6 地址为 **ipv6-address** 的 NTP 被动

对等体配置；如果未指定 **vpn-instance vpn-instance-name** 参数，则取消公网中 IPv6 地址为 **ipv6-address** 的 NTP 被动对等体配置。

被动对等体的 IPv6 地址为链路本地地址时，必须指定报文的源接口，并且不能指定被动对等体所属的 VPN 实例。

主动对等体会按周期与被动对等体进行时间同步，该过程称为轮询。本命令的 **maxpoll** 和 **minpoll** 参数分别用来配置 NTP 对等体模式系统轮询时间间隔的最大值和最小值。选定对等体之后，设备将使用最小轮询间隔进行轮询。当同步时间误差在系统可接受范围内且趋于稳定之后，轮询间隔会逐渐增大直到最大值。当同步时间误差连续超出系统可接受范围多次时，轮询间隔将会减小。

修改轮询间隔不会立即生效，在下次轮询时生效。

【举例】

配置设备工作在主动对等体模式，被动对等体的 IPv6 地址为 2001::1，NTP 报文的源接口为接口 GigabitEthernet1/0/1。

```
<Sysname> system-view
```

```
[Sysname] ntp-service ipv6 unicast-peer 2001::1 source gigabitethernet 1/0/1
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.20 ntp-service ipv6 unicast-server

ntp-service ipv6 unicast-server 命令用来为设备指定 IPv6 NTP 服务器。

undo ntp-service ipv6 unicast-server 命令用来删除为设备指定的 IPv6 NTP 服务器。

【命令】

```
ntp-service ipv6 unicast-server { server-name | ipv6-address }  
[ vpn-instance vpn-instance-name ] [ authentication-keyid keyid | maxpoll  
maxpoll-interval | minpoll minpoll-interval | priority | source  
interface-type interface-number ] *
```

```
undo ntp-service ipv6 unicast-server { server-name | ipv6-address }  
[ vpn-instance vpn-instance-name ]
```

【缺省情况】

未指定 IPv6 NTP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

server-name: NTP 服务器的主机名，为 1~253 个字符的字符串，不区分大小写，字符串中只能包含字母、数字、“-”、“_”和“.”。

ipv6-address: NTP 服务器的 IPv6 地址。该地址只能是一个单播地址，不能为组播地址。

vpn-instance vpn-instance-name: 指定 NTP 服务器所属的 VPN 实例，**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 NTP 服务器位于公网中。

authentication-keyid keyid: 指定向 NTP 服务器发送报文时，使用指定的密钥计算报文的摘要。**keyid** 取值范围为 1~4294967295。如果未指定本参数，则本端设备与 NTP 服务器之间不会进行身份验证。

maxpoll maxpoll-interval: 用来配置最大轮询时间间隔。**maxpoll-interval** 取值范围为 4~17，最大轮询时间间隔为 2 的 **maxpoll-interval** 次幂，对应的最大轮询时间间隔的取值范围为 $2^4 \sim 2^{17}$ （即 16~131072）秒。本参数的缺省值为 6，即最大轮询时间间隔为 64 秒。

minpoll minpoll-interval: 用来配置最小轮询时间间隔，**minpoll-interval** 取值范围为 4~17，最大轮询时间间隔为 2 的 **maxpoll-interval** 次幂，对应的最大轮询时间间隔的取值范围为 $2^4 \sim 2^{17}$ （即 16~131072）秒。本参数的缺省值为 6，即最小轮询时间间隔为 64 秒。

priority: 指定在同等条件下，优先选择该服务器。

source interface-type interface-number: 指定 IPv6 NTP 报文的源接口。如果指定的 IPv6 NTP 服务器地址不是链路本地地址，则本地设备给服务器发送 IPv6 NTP 报文时，报文的源 IPv6 地址为指定源接口的 IPv6 地址。如果指定的 IPv6 NTP 服务器地址是链路本地地址，则 IPv6 NTP 报文从指定的源接口发送，并且报文的源地址为该接口的链路本地地址。**interface-type interface-number** 为接口类型和接口编号。如果未指定本参数，则设备自动选择报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【使用指导】

为设备指定 IPv6 NTP 服务器后，设备可以与该服务器的时间同步，但是服务器不会与设备的时间同步。

配置 PE 向某个 VPN 实例内的其他 PE 或 CE 同步时，需要指定 **vpn-instance vpn-instance-name** 参数。

在执行 **undo ntp-service ipv6 unicast-server** 命令时，如果指定 **vpn-instance vpn-instance-name** 参数，则取消指定 VPN 实例内 IPv6 地址为 **ipv6-address** 的 NTP 被动对等体配置；如果没有指定 **vpn-instance vpn-instance-name** 参数，则取消公网中 IPv6 地址为 **ipv6-address** 的 NTP 被动对等体配置。

NTP 服务器的 IPv6 地址为链路本地地址时，必须指定报文的源接口，并且不能指定 NTP 服务器所属的 VPN 实例。

NTP 客户端会按周期向 NTP 服务器同步时间，该过程称为轮询。本命令的 **maxpoll** 和 **minpoll** 参数分别用来配置 NTP 客户端服务器模式系统轮询时间间隔的最大值和最小值。选定 NTP 服务器之后，设备将使用最小轮询间隔进行轮询。当同步时间误差在系统可接受范围内且趋于稳定之后，轮询间隔会逐渐增大直到最大值。当同步时间误差连续超出系统可接受范围多次时，轮询间隔将会减小。

修改轮询间隔不会立即生效，在下次轮询时生效。

【举例】

```
# 配置设备的 IPv6 NTP 服务器为 2001::1。  
<Sysname> system-view  
[Sysname] ntp-service ipv6 unicast-server 2001::1
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.21 ntp-service max-dynamic-sessions

ntp-service max-dynamic-sessions 命令用来配置 NTP 动态会话的最大数目。

undo ntp-service max-dynamic-sessions 命令用来恢复缺省情况。

【命令】

```
ntp-service max-dynamic-sessions number  
undo ntp-service max-dynamic-sessions
```

【缺省情况】

NTP 动态会话的最大数目为 100。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

number: NTP 动态会话的最大数目，取值范围为 0~100。

【使用指导】

同一设备同一时间内存在的会话数目最多为 128 个，其中包括静态会话数和动态会话数。静态会话是用户手动配置 NTP 相关命令而建立的会话；动态会话是 NTP 运行过程中建立的临时会话。

本配置用来限制动态会话的数目，以避免设备上维护过多的动态会话，占用过多的系统资源。

【举例】

```
# 设置 NTP 动态会话的最大数目为 50 个。  
<Sysname> system-view  
[Sysname] ntp-service max-dynamic-sessions 50
```

【相关命令】

- **display ntp-service sessions**

1.1.22 ntp-service multicast-client

ntp-service multicast-client 命令用来配置设备工作在 NTP 组播客户端模式，并使用当前接口接收 NTP 组播报文。

undo ntp-service multicast-client 命令用来取消 NTP 组播客户端模式的配置。

【命令】

```
ntp-service multicast-client [ ip-address ]  
undo ntp-service multicast-client [ ip-address ]
```

【缺省情况】

未配置 NTP 工作模式。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

ip-address: NTP 报文的组播 IP 地址，缺省值为 224.0.1.1。组播客户端和组播服务器上配置的组播地址必须相同。

【使用指导】

配置设备工作在 NTP 组播客户端模式后，设备将在接口上监听目的地址为指定组播地址的 NTP 报文，根据接收到的报文实现时间同步。

如果在接口上配置了设备工作在组播客户端模式，则建议不要将该接口加入聚合组。如果要接口加入聚合组，则建议先取消 NTP 组播客户端配置。

【举例】

配置设备工作在组播客户端模式，在 GigabitEthernet1/0/1 接口上接收目的地址为 224.0.1.1 的 NTP 报文。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ntp-service multicast-client 224.0.1.1
```

【相关命令】

- **ntp-service multicast-server**

1.1.23 ntp-service multicast-server

ntp-service multicast-server 命令用来配置设备工作在 NTP 组播服务器模式，并使用当前接口发送 NTP 组播报文。

undo ntp-service multicast-server 命令用来取消 NTP 组播服务器模式的配置。

【命令】

```
ntp-service multicast-server [ ip-address ] [ authentication-keyid keyid |  
ttl ttl-number | version number ] *  
undo ntp-service multicast-server [ ip-address ]
```

【缺省情况】

未配置 NTP 工作模式。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ip-address: NTP 报文的组播 IP 地址，缺省值为 224.0.1.1。组播客户端和组播服务器上配置的组播地址必须相同。

authentication-keyid keyid: 指定向组播客户端发送 NTP 报文时，使用指定的密钥计算报文的摘要。**keyid** 取值范围为 1~4294967295。如果未指定本参数，则本端设备无法同步开启了身份验证功能的组播客户端。

ttl ttl-number: 指定组播报文的生存期。**ttl-number** 取值范围为 1~255，缺省值为 16。

version number: 指定 NTP 版本号。**number** 取值范围为 1~4，缺省值为 4。

【使用指导】

配置设备工作在 NTP 组播服务器模式后，设备将通过该接口周期性地向指定的组播地址发送 NTP 报文。

如果在接口上配置了设备工作在组播服务器模式，则建议不要将该接口加入聚合组。如果要将接口加入聚合组，则建议先取消 NTP 组播服务器配置。

【举例】

配置设备工作在组播服务器模式，在 GigabitEthernet1/0/1 接口上发送 NTP 报文，NTP 报文的地址为组播地址 224.0.1.1，用 4 号密钥加密 NTP 报文，并设置 NTP 版本号为 4。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] ntp-service multicast-server 224.0.1.1 version 4  
authentication-keyid 4
```

【相关命令】

- **ntp-service multicast-client**

1.1.24 ntp-service refclock-master

ntp-service refclock-master 命令用来设置本地时钟作为参考时钟。

undo ntp-service refclock-master 命令用来取消本地时钟作为参考时钟。

【命令】

```
ntp-service refclock-master [ ip-address ] [ stratum ]  
undo ntp-service refclock-master [ ip-address ]
```

【缺省情况】

设备未采用本地时钟作为参考时钟。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

ip-address: 本地时钟的 IP 地址 127.127.1.u。u 的取值范围为 0~3，表示 NTP 的进程号。如果不指定 **ip-address**，则系统默认值是 127.127.1.0。

stratum: 本地时钟所处的层数，取值范围为 1~15，缺省值为 8。时钟的层数定义了时钟的准确度，层数取值越小，时钟的准确度越高。

【使用指导】

实际网络中，通常将从权威时钟（如原子时钟）获得时间同步的 NTP 服务器的层数设置为 1，并将其作为主时间服务器同步网络中其他设备的时钟。网络中的设备与主时间服务器的 NTP 距离，即 NTP 同步链上 NTP 服务器的数目，决定了设备上时钟的层数。

在某些网络中，例如无法与外界通信的孤立网络，网络中的设备无法与权威时钟进行时间同步。此时，可以从该网络中选择一台时钟较为准确的设备，指定该设备与本地时钟进行时间同步，即采用本地时钟作为参考时钟，使得该设备的时钟处于同步状态。该设备作为时间服务器为网络中的其他设备提供时间同步，从而实现整个网络的时间同步。

请谨慎使用本配置，以免导致网络中设备的时间错误。在执行本命令之前，建议先调整本地系统时间。

【举例】

```
# 设置本地设备时钟作为参考时钟，层数为 2。  
<Sysname> system-view  
[Sysname] ntp-service refclock-master 2
```

1.1.25 ntp-service reliable authentication-keyid

ntp-service reliable authentication-keyid 命令用来指定已创建的密钥是可信的。

undo ntp-service reliable authentication-keyid 命令用来取消可信密钥。

【命令】

```
ntp-service reliable authentication-keyid keyid  
undo ntp-service reliable authentication-keyid keyid
```

【缺省情况】

未指定可信密钥。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

keyid: 密钥编号，取值范围为 1～4294967295。

【使用指导】

开启身份验证功能后，客户端只会与提供可信密钥的服务器进行时间同步；如果服务器提供的密钥不是可信的，那么客户端不会与其同步。

配置本命令前，请确认证开关已经打开并且配置了密钥，即保证该密钥的存在性后才能设定它是否可信。如果 NTP 验证密钥被指定为可信密钥，删除密钥后，该密钥将自动变为不可信密钥，不必再执行 **undo ntp-service reliable authentication-keyid** 命令。

本命令可以多次配置，最多可以配置 128 个可信密钥。

【举例】

开启 NTP 身份验证功能，配置编号为 37 的密钥采用 MD5 算法进行身份验证，密钥值为 BetterKey。

```
<Sysname> system-view
```

```
[Sysname] ntp-service authentication enable
```

```
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 simple BetterKey
```

指定该密钥为可信密钥。

```
[Sysname] ntp-service reliable authentication-keyid 37
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**

1.1.26 ntp-service source

ntp-service source 命令用来指定 NTP 报文的源接口。

undo ntp-service source 命令用来恢复缺省情况。

【命令】

ntp-service source *interface-type interface-number*

undo ntp-service source

【缺省情况】

未指定 NTP 报文的源接口，设备根据路由表查找报文的出接口，并采用出接口的主 IP 地址作为 NTP 报文的源 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type interface-number: 接口类型及接口编号。

【使用指导】

如果指定了 NTP 报文的源接口，则设备在主动发送 NTP 报文时，将报文的源 IP 地址设置为指定接口的主 IP 地址，从而保证 NTP 应答报文的目地址均为此地址。

设备对接收到的 NTP 请求报文进行应答时，应答报文的源地址始终为接收到 NTP 请求报文的目地址。

如果不想让本地设备上其他接口的 IP 地址成为应答报文的目地址，可以使用本命令。

使用本命令指定 NTP 报文的源接口时，需要注意：

- 当 NTP 工作在客户端/服务器模式时，如果在命令 **ntp-service unicast-server** 中指定了 NTP 报文的源接口，则以 **ntp-service unicast-server** 命令指定的源接口为准。
- 当 NTP 工作在对等体模式时，如果在命令 **ntp-service unicast-peer** 中指定了 NTP 报文的源接口，则以 **ntp-service unicast-peer** 命令指定源接口的为准。
- 当 NTP 工作在组播模式时，如果在接口视图下配置了 **ntp-service multicast-server** 命令，则 NTP 组播报文的源接口为配置了 **ntp-service multicast-server** 命令的接口。
- 当 NTP 工作在广播模式时，如果在接口视图下配置了 **ntp-service broadcast-server** 命令，则 NTP 广播报文的源接口为配置了 **ntp-service broadcast-server** 命令的接口。
- 如果指定的 NTP 源接口处于 down 状态，则设备不再发送 NTP 报文。

【举例】

配置 NTP 报文的源接口为接口 GigabitEthernet1/0/1。

```
<Sysname> system-view
```

```
[Sysname] ntp-service source gigabitethernet 1/0/1
```

1.1.27 ntp-service time-offset-threshold

ntp-service time-offset-threshold 命令用来配置 NTP 时间同步过程中，打印日志和告警信息的时间偏移阈值。

undo ntp-service time-offset-threshold 命令用来恢复缺省情况。

【命令】

```
ntp-service time-offset-threshold { log log-threshold | trap  
trap-threshold } *
```

```
undo ntp-service time-offset-threshold
```

【缺省情况】

未配置打印日志和告警信息的时间偏移阈值。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

log *log-threshold*: 表示 NTP 时间同步过程中，打印日志信息的时间偏移阈值。
log-threshold 取值范围为 128~60000，单位为毫秒。

trap *trap-threshold*: 表示 NTP 时间同步过程中，打印告警信息的时间偏移阈值。
trap-threshold 取值范围为 128~60000，单位为毫秒。

【使用指导】

缺省情况下，NTP 客户端与服务器端的时间差经过多次采样得到的时间偏移超过 128ms 时，客户端将进行一次时间同步，并打印日志信息和告警信息。配置本命令后，NTP 客户端与服务器端的时间差经过多次采样得到的时间偏移超过 128ms 时，客户端将进行一次时间同步，但是时间偏移大于阈值时，才会打印日志；时间偏移大于阈值时，才会打印告警信息。

【举例】

配置 NTP 时间同步过程中，打印日志和告警信息的时间偏移阈值为 500ms 和 600ms。

```
<Sysname> system-view
```

```
[Sysname] ntp-service time-offset-threshold log 500 trap 600
```

1.1.28 ntp-service unicast-peer

ntp-service unicast-peer 命令用来为设备指定被动对等体。

undo ntp-service unicast-peer 命令用来删除为设备指定的被动对等体。

【命令】

```
ntp-service unicast-peer { peer-name | ip-address } [ vpn-instance vpn-instance-name ] [ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number | version number ] *
```

```
undo ntp-service unicast-peer { peer-name | ip-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未指定被动对等体。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

peer-name: 被动对等体的主机名，为 1~253 个字符的字符串，不区分大小写，字符串中只能包含字母、数字、“-”、“_”和“.”。

ip-address: 被动对等体的 IP 地址。该地址只能是一个单播地址，不能为广播地址、组播地址或本地时钟的 IP 地址。

vpn-instance vpn-instance-name: 指定被动对等体所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示被动对等体位于公网中。

authentication-keyid keyid: 指定向对等体发送 NTP 报文时，使用指定的密钥计算报文的摘要。**keyid** 取值范围为 1~4294967295。如果未指定本参数，则本端设备与对等体之间不会进行身份验证。

maxpoll maxpoll-interval: 用来配置最大轮询时间间隔。**maxpoll-interval** 取值范围为 4~17，最大轮询时间间隔为 2 的 **maxpoll-interval** 次幂，对应的最大轮询时间间隔的取值范围为 $2^4 \sim 2^{17}$ （即 16~131072）秒。本参数的缺省值为 6，即最大轮询时间间隔为 64 秒。

minpoll minpoll-interval: 用来配置最小轮询时间间隔，**minpoll-interval** 取值范围为 4~17，最大轮询时间间隔为 2 的 **maxpoll-interval** 次幂，对应的最大轮询时间间隔的取值范围为 $2^4 \sim 2^{17}$ （即 16~131072）秒。本参数的缺省值为 6，即最小轮询时间间隔为 64 秒。

priority: 在同等条件下，优先选择 **ip-address** 或 **peer-name** 指定的对等体为同步对等体。

source interface-type interface-number: 指定 NTP 报文的源接口。本地设备给对端发送 NTP 报文时，报文的源地址为指定源接口的主 IP 地址。**interface-type interface-number** 为接口类型和接口编号。如果未指定本参数，则根据路由表查找报文的出接口，并采用出接口的主 IP 地址作为 NTP 报文的源 IP 地址。

version number: 指定 NTP 版本号。**number** 取值范围为 1~4，缺省值为 4。

【使用指导】

为设备指定被动对等体后，主动对等体和被动对等体的时间可以互相同步。如果双方的时钟都处于同步状态，则层数大的时钟与层数小的时钟的时间同步。

配置 PE 向某个 VPN 实例内的其他 PE 或 CE 同步时，需要指定 **vpn-instance vpn-instance-name** 参数。

在执行 **undo ntp-service unicast-peer** 命令时，如果指定 **vpn-instance vpn-instance-name** 参数，则取消指定 VPN 实例内 IP 地址为 **ip-address** 的 NTP 被动对等体配置；如果没有指定 **vpn-instance vpn-instance-name** 参数，则取消公网中 IP 地址为 **ip-address** 的 NTP 被动对等体配置。

主动对等体会按周期与被动对等体进行时间同步，该过程称为轮询。本命令的 **maxpoll** 和 **minpoll** 参数分别用来配置 NTP 对等体模式系统轮询时间间隔的最大值和最小值。选定对等体之后，设备将使用最小轮询间隔进行轮询。当同步时间误差在系统可接受范围内且趋于稳定时，轮询间隔会逐渐增大直到最大值。当同步时间误差连续超出系统可接受范围多次时，轮询间隔将会减小。

修改轮询间隔不会立即生效，在下次轮询时生效。

【举例】

配置设备工作在主动对等体模式，被动对等体的 IP 地址为 10.1.1.1，NTP 版本号为 4，NTP 报文的源接口为接口 GigabitEthernet1/0/1。

```
<Sysname> system-view
```

```
[Sysname] ntp-service unicast-peer 10.1.1.1 version 4 source gigabitethernet 1/0/1
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

1.1.29 ntp-service unicast-server

ntp-service unicast-server 命令用来为设备指定 NTP 服务器。

undo ntp-service unicast-server 命令用来删除为设备指定的 NTP 服务器。

【命令】

```
ntp-service unicast-server { server-name | ip-address } [ vpn-instance vpn-instance-name ] [ authentication-keyid keyid | maxpoll maxpoll-interval | minpoll minpoll-interval | priority | source interface-type interface-number | version number ] *
```

```
undo ntp-service unicast-server { server-name | ip-address } [ vpn-instance vpn-instance-name ]
```

【缺省情况】

未指定 NTP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

server-name: NTP 服务器的主机名，为 1~253 个字符的字符串，不区分大小写，字符串中只能包含字母、数字、“-”、“_”和“.”。

ip-address: NTP 服务器的 IP 地址。该地址只能是一个单播地址，不能为广播地址、组播地址或本地时钟的 IP 地址。

vpn-instance *vpn-instance-name*: 指定 NTP 服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 NTP 服务器位于公网中。

authentication-keyid *keyid*: 指定向 NTP 服务器发送报文时，使用指定的密钥计算报文的摘要。*keyid* 取值范围为 1~4294967295。如果未指定本参数，则本端设备与 NTP 服务器之间不会进行身份验证。

maxpoll *maxpoll-interval*: 用来配置最大轮询时间间隔。*maxpoll-interval* 取值范围为 4~17, 最大轮询时间间隔为 2 的 *maxpoll-interval* 次幂, 对应的最大轮询时间间隔的取值范围为 $2^4 \sim 2^{17}$ (即 16~131072) 秒。本参数的缺省值为 6, 即最大轮询时间间隔为 64 秒。

minpoll *minpoll-interval*: 用来配置最小轮询时间间隔, *minpoll-interval* 取值范围为 4~17, 最大轮询时间间隔为 2 的 *maxpoll-interval* 次幂, 对应的最大轮询时间间隔的取值范围为 $2^4 \sim 2^{17}$ (即 16~131072) 秒。本参数的缺省值为 6, 即最小轮询时间间隔为 64 秒。

priority: 指定在同等条件下, 优先选择该服务器。

source interface-type interface-number: 指定 NTP 报文的源接口。本地设备给服务器发送 NTP 报文时, 报文的源地址为指定源接口的主 IP 地址。*interface-type interface-number* 为接口类型和接口编号。如果未指定本参数, 则根据路由表查找报文的出接口, 并采用出接口的主 IP 地址作为 NTP 报文的源 IP 地址。

version number: 指定 NTP 版本号。*number* 取值范围为 1~4, 缺省值为 4。

【使用指导】

为设备指定 NTP 服务器后, 设备可以与该服务器的时间同步, 但是服务器不会与设备的时间同步。

配置 PE 向某个 VPN 实例内的其他 PE 或 CE 同步时, 需要指定 **vpn-instance vpn-instance-name** 参数。

在执行 **undo ntp-service unicast-server** 命令时, 如果指定 **vpn-instance vpn-instance-name** 参数, 则取消指定 VPN 实例内 IP 地址为 *ip-address* 的 NTP 服务器配置; 如果没有指定 **vpn-instance vpn-instance-name** 参数, 则取消公网中 IP 地址为 *ip-address* 的 NTP 服务器配置。

NTP 客户端会按周期向 NTP 服务器同步时间, 该过程称为轮询。本命令的 **maxpoll** 和 **minpoll** 参数分别用来配置 NTP 客户端服务器模式系统轮询时间间隔的最大值和最小值。选定 NTP 服务器之后, 设备将使用最小轮询间隔进行轮询。当同步时间误差在系统可接受范围内且趋于稳定之后, 轮询间隔会逐渐增大直到最大值。当同步时间误差连续超出系统可接受范围多次时, 轮询间隔将会减小。

修改轮询间隔不会立即生效, 在下次轮询时生效。

【举例】

配置设备的 NTP 服务器为 10.1.1.1, 版本号为 4。

```
<Sysname> system-view
```

```
[Sysname] ntp-service unicast-server 10.1.1.1 version 4
```

【相关命令】

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

2 SNTP

2.1 SNTP配置命令

2.1.1 display sntp ipv6 sessions

display sntp ipv6 sessions 命令用来显示 SNTP 服务的所有 IPv6 会话信息。

【命令】

display sntp ipv6 sessions

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 IPv6 SNTP 服务的所有 IPv6 会话信息。

```
<Sysname> display sntp ipv6 sessions
SNTP server: 2001::1
Stratum: 16
Version: 4
Last receive time: No packet was received.

SNTP server: 2001::100
Stratum: 3
Version: 4
Last receive time: Fri, Oct 21 2011 11:28:28.058 (Synced)
```

表2-1 display sntp ipv6 sessions 命令显示信息描述表

字段	描述
SNTP server	SNTP服务器，即NTP服务器。若该字段显示为::，表示NTP服务器的IPv6地址尚未解析成功
Stratum	时钟的层数 时钟层数决定了时钟的准确度，取值范围为1~16，层数取值越小，表示时钟的准确度越高，层数为16的时钟处于未同步状态
Version	版本号

字段	描述
Last receive time	最后一次接收到SNTP会话消息的时间 - Synced 表示设备的本地时钟从该服务器获得同步 - No packet was received.表示设备未从该服务器接收到 SNTP 会话消息

2.1.2 display sntp sessions

display sntp sessions 命令用来显示 SNTP 服务的所有 IPv4 会话信息。

【命令】

display sntp sessions

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 SNTP 服务的所有 IPv4 会话信息。

```
<Sysname> display sntp sessions
```

```
SNTP server      Stratum   Version   Last receive time
1.0.1.11         2         4         Tue, May 17 2011  9:11:20.833 (Synced)
```

表2-2 display sntp sessions 命令显示信息描述表

字段	描述
SNTP server	SNTP服务器，即NTP服务器。若该字段显示为0.0.0.0，表示NTP服务器的IP地址尚未解析成功
Stratum	时钟的层数 时钟层数决定了时钟的准确度，取值范围为1~16，层数取值越小，表示时钟的准确度越高，层数为16的时钟处于未同步状态
Version	SNTP版本号
Last receive time	上一次接收到消息的时间，Synced标识本地时钟从该服务器获得同步

2.1.3 sntp authentication enable

sntp authentication enable 命令用来开启 SNTP 身份验证功能。

undo sntp authentication enable 命令用来关闭 SNTP 身份验证功能。

【命令】

```
sntp authentication enable
undo sntp authentication enable
```

【缺省情况】

SNTP 身份验证功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

在一些对安全性要求较高的网络中，运行 SNTP 协议时需要启用身份验证功能。通过客户端和服务器的身份验证，保证客户端只与通过验证的服务器进行时间同步，避免客户端从非法的服务器获得错误的时间同步信息。

开启 SNTP 身份验证功能后，还需要设置身份验证密钥，并将其设置为可信密钥，才能正确地进行身份验证。

【举例】

```
# 开启 SNTP 身份验证功能。
<Sysname> system-view
[Sysname] sntp authentication enable
```

【相关命令】

- **sntp authentication-keyid**
- **sntp reliable authentication-keyid**

2.1.4 sntp authentication-keyid

sntp authentication-keyid 命令用来设置 SNTP 身份验证密钥。

undo sntp authentication-keyid 命令用来删除指定的 SNTP 身份验证密钥。

【命令】

```
sntp authentication-keyid keyid authentication-mode md5 { cipher | simple }
string [ acl ipv4-acl-number | ipv6 acl ipv6-acl-number ] *
undo sntp authentication-keyid keyid
```

【缺省情况】

未设置 SNTP 身份验证密钥。

【视图】

系统视图

【缺省用户角色】

```
network-admin
```

context-admin

【参数】

keyid: 密钥编号，用来标识身份验证密钥，取值范围为 1~4294967295。

authentication-mode md5: 表示采用 MD5 算法进行身份验证。

cipher: 以密文形式设置密钥。

simple: 以明文形式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~32 个字符的字符串，密文密钥为 1~73 个字符的字符串。

acl ipv4-acl-number: 对对端设备进行 ACL 过滤。通过 ACL 过滤的对端设备有权在本端使用该密钥 ID 进行身份验证。**ipv4-acl-number** 为 IPv4 基本 ACL 的编号，取值范围为 2000~2999。

ipv6 acl ipv6-acl-number: 对对端设备进行 IPv6 ACL 过滤。通过 IPv6 ACL 过滤的对端设备有权在本端使用该密钥 ID 进行身份验证。**ipv6-acl-number** 为 IPv6 基本 ACL 的编号，取值范围为 2000~2999。

【使用指导】

在一些对安全性要求较高的网络中，运行 SNTP 协议时需要启用身份验证功能。通过客户端和服务器的身份验证，保证客户端只与通过验证的服务器进行同步，提高了网络安全性。

SNTP 协议采用哪个密钥对对端进行身份验证由对端报文中携带的密钥 ID 决定。这会导致如下安全问题：对对端进行身份验证时只关心密钥是否正确而不关心对端是否有权使用该密钥 ID。**acl** 和 **ipv6 acl** 参数用于指定有权在本端使用该密钥 ID 进行身份验证的对端设备。需要注意的是：

- 当引用的 ACL 或 IPv6 ACL 不存在时，任何设备都能在本端使用该密钥 ID 进行验证。
- 当引用的 ACL 或 IPv6 ACL 下没有配置规则时，任何设备都不能在本端使用该密钥 ID 进行验证。

客户端和服务端上需要配置相同的密钥 ID 及密钥值，并且保证对端有权在本端使用该密钥 ID 进行身份验证，否则无法实现时间同步。

配置 SNTP 验证密钥后，还需要通过 **sntp reliable authentication-keyid** 命令将该密钥设置为可信密钥。如果 SNTP 验证密钥被指定为可信密钥，删除密钥后，该密钥将自动变为不可信密钥，不必再执行 **undo sntp reliable authentication-keyid** 命令。

通过重复执行本命令，可以配置多个 SNTP 身份验证密钥。设备上最多可以配置 128 个 SNTP 身份验证密钥。

【举例】

设置 MD5 身份验证密钥，密钥 ID 号为 10，密钥为 BetterKey，以明文形式输入。

```
<Sysname> system-view
```

```
[Sysname] sntp authentication enable
```

```
[Sysname] sntp authentication-keyid 10 authentication-mode md5 simple BetterKey
```

【相关命令】

- **sntp authentication enable**
- **sntp reliable authentication-keyid**

2.1.5 sntp enable

sntp enable 命令用来开启 SNTP 服务。

undo sntp enable 命令用来关闭 SNTP 服务。

【命令】

```
sntp enable
undo sntp enable
```

【缺省情况】

SNTP 服务处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

```
# 开启 SNTP 服务。
<Sysname> system-view
[Sysname] sntp enable
```

2.1.6 sntp ipv6 unicast-server

sntp ipv6 unicast-server 命令用来为设备指定 IPv6 NTP 服务器。

undo sntp ipv6 unicast-server 命令用来删除为设备指定的 IPv6 NTP 服务器。

【命令】

```
sntp ipv6 unicast-server { server-name | ipv6-address } [ vpn-instance
vpn-instance-name ] [ authentication-keyid keyid | source interface-type
interface-number ] *
undo sntp ipv6 unicast-server { server-name | ipv6-address } [ vpn-instance
vpn-instance-name ]
```

【缺省情况】

未指定 IPv6 NTP 服务器。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

server-name: NTP 服务器的主机名, 为 1~253 个字符的字符串, 不区分大小写, 字符串中只能包含字母、数字、“-”、“_”和“.”。

ipv6-address: NTP 服务器的 IPv6 地址。

vpn-instance vpn-instance-name: 指定 IPv6 NTP 服务器所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示 IPv6 NTP 服务器位于公网中。

authentication-keyid keyid: 指定向 NTP 服务器发送报文时, 使用指定的密钥计算报文的摘要。**keyid** 取值范围为 1~4294967295。如果未指定本参数, 则本端设备与 NTP 服务器之间不会进行身份验证。

source interface-type interface-number: 指定 IPv6 NTP 报文的源接口。如果指定的 IPv6 NTP 服务器地址不是链路本地地址, 则本地设备给服务器发送 IPv6 NTP 报文时, 报文的源 IPv6 地址为指定源接口的 IPv6 地址。如果指定的 IPv6 NTP 服务器地址是链路本地地址, 则 IPv6 NTP 报文从指定的源接口发送, 并且报文的源地址为该接口的链路本地地址。**interface-type interface-number** 为接口类型和接口编号。如果未指定本参数, 则设备自动选择报文的源 IPv6 地址, 具体选择原则请参见 RFC 3484。

【使用指导】

为设备指定 IPv6 NTP 服务器后, 设备可以与该服务器进行时间同步。设备的时间获得同步后, 不能作为服务器为其他设备提供时间同步。

配置 PE 向某个 VPN 实例内的其他 PE 或 CE 同步时, 需要指定 **vpn-instance vpn-instance-name** 参数。

在执行 **undo sntp unicast-server** 命令时, 如果指定 **vpn-instance vpn-instance-name** 参数, 则取消指定 VPN 实例内 IPv6 地址为 **ipv6-address** 的 NTP 服务器配置; 如果没有指定 **vpn-instance vpn-instance-name** 参数, 则取消公网中 IPv6 地址为 **ipv6-address** 的 NTP 服务器配置。

NTP 服务器的 IPv6 地址为链路本地地址时, 必须指定报文的源接口, 并且不能指定 NTP 服务器所属的 VPN 实例。

【举例】

```
# 配置设备的 NTP 服务器为 2001::1。  
<Sysname> system-view  
[Sysname] sntp ipv6 unicast-server 2001::1
```

【相关命令】

- **sntp authentication enable**
- **sntp authentication-keyid**
- **sntp reliable authentication-keyid**

2.1.7 sntp reliable authentication-keyid

sntp reliable authentication-keyid 命令用来配置可信密钥。

undo sntp reliable authentication-keyid 命令用来取消可信密钥。

【命令】

```
sntp reliable authentication-keyid keyid  
undo sntp reliable authentication-keyid keyid
```

【缺省情况】

未指定可信密钥。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

keyid: 密钥编号，取值范围为 1~4294967295。

【使用指导】

开启身份验证功能后，客户端只会同步到提供可信密钥的服务器；如果服务器提供的密钥不是可信的，那么客户端不会与其同步。

本命令的使用前提是认证开关已经打开并且配置了密钥，即保证该密钥的存在性后才能设定它是否可信。如果 SNTP 验证密钥被指定为可信密钥，删除密钥后，该密钥将自动变为不可信密钥，不必再执行 **undo sntp reliable authentication-keyid** 命令。

【举例】

```
# 开启 SNTP 身份验证功能,配置编号为37的密钥采用 MD5算法进行身份验证,密钥值为 BetterKey。  
<Sysname> system-view  
[Sysname] sntp authentication enable  
[Sysname] sntp authentication-keyid 37 authentication-mode md5 simple BetterKey  
# 指定该密钥为可信密钥。  
[Sysname] sntp reliable authentication-keyid 37
```

【相关命令】

- **sntp authentication-keyid**
- **sntp authentication enable**

2.1.8 sntp time-offset-threshold

sntp time-offset-threshold 命令用来配置 SNTP 时间同步过程中，打印日志和告警信息的时间偏移阈值。

undo sntp time-offset-threshold 命令用来恢复缺省情况。

【命令】

```
sntp time-offset-threshold { log log-threshold | trap trap-threshold } *  
undo sntp time-offset-threshold
```

【缺省情况】

未配置打印日志和告警信息的时间偏移阈值。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

log log-threshold: 表示 SNTP 时间同步过程中，打印日志信息的时间偏移阈值。
log-threshold 取值范围为 128~60000，单位为毫秒。

trap trap-threshold: 表示 SNTP 时间同步过程中，打印告警信息的时间偏移阈值。
trap-threshold 取值范围为 128~60000，单位为毫秒。

【使用指导】

缺省情况下，SNTP 客户端与服务器端的时间差经过多次采样得到的时间偏移超过 128ms 时，客户端将进行一次时间同步，并打印日志信息和告警信息。配置本命令后，SNTP 客户端与服务器端的时间差经过多次采样得到的时间偏移超过 128ms 时，客户端将进行一次时间同步，但是时间偏移大于阈值时，才会打印日志；时间偏移大于阈值时，才会打印告警信息。

【举例】

配置 SNTP 时间同步过程中，打印日志和告警信息的时间偏移阈值为 500ms 和 600ms。

```
<Sysname> system-view
```

```
[Sysname] sntp time-offset-threshold log 500 trap 600
```

2.1.9 sntp unicast-server

sntp unicast-server 命令用来为设备指定 NTP 服务器。

undo sntp unicast-server 命令用来删除为设备指定的 NTP 服务器。

【命令】

```
sntp unicast-server { server-name | ip-address } [ vpn-instance  
vpn-instance-name ] [ authentication-keyid keyid | source interface-type  
interface-number | version number ] *
```

```
undo sntp unicast-server { server-name | ip-address } [ vpn-instance  
vpn-instance-name ]
```

【缺省情况】

未指定 NTP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

server-name: NTP 服务器的主机名, 为 1~253 个字符的字符串, 不区分大小写, 字符串中只能包含字母、数字、“-”、“_”和“.”。

ip-address: NTP 服务器的 IP 地址。该地址只能是一个单播地址, 不能为广播地址、组播地址或本地时钟的 IP 地址。

vpn-instance vpn-instance-name: 指定 NTP 服务器所属的 VPN 实例。
vpn-instance-name 表示 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示 NTP 服务器位于公网中。

authentication-keyid keyid: 指定向 NTP 服务器发送报文时, 使用指定的密钥计算报文的摘要。**keyid** 取值范围为 1~4294967295。如果未指定本参数, 则本端设备与 NTP 服务器之间不会进行身份验证。

source interface-type interface-number: 指定 NTP 报文的源接口。本地设备给服务器发送 NTP 报文时, 报文的源地址为指定源接口的主 IP 地址。**interface-type interface-number** 为接口类型和接口编号。如果未指定本参数, 则根据路由表查找报文的出接口, 并采用出接口的主 IP 地址作为 NTP 报文的源 IP 地址。

version number: 指定 NTP 版本号。**number** 取值范围为 1~4, 缺省值为 4。

【使用指导】

为设备指定 NTP 服务器后, 设备可以与该服务器进行时间同步。设备的时间获得同步后, 不能作为服务器为其他设备提供时间同步。

配置 PE 向某个 VPN 实例内的其他 PE 或 CE 同步时, 需要指定 **vpn-instance vpn-instance-name** 参数。

在执行 **undo sntp unicast-server** 命令时, 如果指定 **vpn-instance vpn-instance-name** 参数, 则取消指定 VPN 实例内 IP 地址为 **ip-address** 的 NTP 服务器配置; 如果没有指定 **vpn-instance vpn-instance-name** 参数, 则取消公网中 IP 地址为 **ip-address** 的 NTP 服务器配置。

【举例】

配置设备的 NTP 服务器为 10.1.1.1, 版本号为 4。

```
<Sysname> system-view
```

```
[Sysname] sntp unicast-server 10.1.1.1 version 4
```

【相关命令】

- **sntp authentication enable**
- **sntp authentication-keyid**
- **sntp reliable authentication-keyid**

目 录

1 SNMP	1-1
1.1 SNMP配置命令	1-1
1.1.1 display snmp-agent community	1-1
1.1.2 display snmp-agent context	1-3
1.1.3 display snmp-agent group	1-3
1.1.4 display snmp-agent local-engineid	1-4
1.1.5 display snmp-agent mib-node	1-5
1.1.6 display snmp-agent mib-view	1-9
1.1.7 display snmp-agent remote	1-11
1.1.8 display snmp-agent statistics	1-12
1.1.9 display snmp-agent sys-info	1-14
1.1.10 display snmp-agent trap queue	1-15
1.1.11 display snmp-agent trap-list	1-15
1.1.12 display snmp-agent usm-user	1-16
1.1.13 enable snmp trap updown	1-18
1.1.14 snmp-agent	1-19
1.1.15 snmp-agent { inform trap } source	1-20
1.1.16 snmp-agent calculate-password	1-21
1.1.17 snmp-agent community	1-22
1.1.18 snmp-agent community-map	1-24
1.1.19 snmp-agent context	1-25
1.1.20 snmp-agent group	1-26
1.1.21 snmp-agent local-engineid	1-28
1.1.22 snmp-agent log	1-29
1.1.23 snmp-agent mib-view	1-30
1.1.24 snmp-agent packet max-size	1-31
1.1.25 snmp-agent port	1-31
1.1.26 snmp-agent remote	1-32
1.1.27 snmp-agent sys-info contact	1-33
1.1.28 snmp-agent sys-info location	1-34
1.1.29 snmp-agent sys-info version	1-34
1.1.30 snmp-agent target-host	1-35
1.1.31 snmp-agent trap enable	1-37
1.1.32 snmp-agent trap if-mib link extended	1-38

1.1.33 snmp-agent trap life	1-39
1.1.34 snmp-agent trap log	1-39
1.1.35 snmp-agent trap queue-size	1-40
1.1.36 snmp-agent usm-user { v1 v2c }	1-41
1.1.37 snmp-agent usm-user v3	1-43
1.1.38 snmp-agent usm-user v3 user-role	1-46

1 SNMP

1.1 SNMP配置命令

SNMP 告警信息包括 SNMP Trap 和 Inform 报文，用来告知 NMS 设备上发生了重要事件，比如，用户的登录/退出，接口状态变成 up/down 等。如无特殊说明，本文中的告警信息均指 Trap 和 Inform 两种信息。

1.1.1 display snmp-agent community

display snmp-agent community 命令用来显示 SNMPv1 或 SNMPv2c 的团体信息。

【命令】

display snmp-agent community [read | write]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

read: 显示只读访问权限的团体信息。

write: 显示读写访问权限的团体信息。

【使用指导】

不带参数时，显示所有 SNMP 团体的信息。

用户有两种方式创建团体：

- 使用 **snmp-agent community** 命令来创建团体。
- 配置 **snmp-agent usm-user { v1 | v2c }** 和 **snmp-agent group { v1 | v2c }** 命令成功创建 SNMPv1 或 SNMPv2c 用户以及相应的组后，系统会以用户名为团体名自动创建一个团体。

display snmp-agent community 会显示这两种方式创建的、以明文方式配置并以明文方式保存到配置文件中的团体的信息。

【举例】

显示设备当前所有已配置的团体信息。

```
<Sysname> display snmp-agent community
Community name: aa
Group name: aa
ACL:2001
Storage-type: nonVolatile
```

Context name: con1

Community name: bb

Role name: bb

Storage-type: nonVolatile

Community name: userv1

Group name: testv1

Storage-type: nonVolatile

Community name: cc

Group name: cc

ACL name: testacl

Storage-type: nonVolatile

表1-1 display snmp-agent community 命令显示信息描述表

字段	描述
Community name	团体名： - 如果团体名是通过 snmp-agent community 命令创建的，则显示的是团体名 - 如果团体名是通过 snmp-agent usm-user { v1 v2c } 命令创建的，则显示的是用户名
Group name	组名： - 如果团体名是通过 snmp-agent community 命令的 VACM 方式创建的，则组名和团体名相同 - 如果团体名是通过 snmp-agent usm-user { v1 v2c } 命令创建的，则显示用户所在的组名
Role name	SNMP用户所在团体绑定的角色名： 通过 snmp-agent community 命令的RBAC方式创建的团体名可绑定用户角色
ACL	使用的ACL列表的编号（该字段仅在团体名与ACL编号绑定后显示）
ACL name	使用的ACL列表的名称（该字段仅在团体名与ACL名称绑定后显示）
IPV6 ACL	使用的IPv6 ACL列表的编号（该字段仅在团体名与IPv6 ACL编号绑定后显示）
IPV6 ACL name	使用的IPv6 ACL列表的名称（该字段仅在团体名与IPv6 ACL名称绑定后显示）
Storage-type	表示存储方式，分为以下几种： volatile: 重启后信息丢失 nonVolatile: 重启后信息仍保存 permanent: 重启后信息仍保存，允许更改，但不许删除 readOnly: 重启后信息仍保存，既不允许更改，也不许删除 other: 其他
Context name	SNMP上下文： - 如果此团体名配置了对应的上下文映射，则显示对应的上下文 - 如果此团体名未配置对应的上下文映射，该字段显示为空

【相关命令】

- **snmp-agent community**
- **snmp-agent usm-user { v1 | v2c }**

1.1.2 display snmp-agent context

display snmp-agent context 命令用来显示 SNMP 上下文。

【命令】

display snmp-agent context [*context-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

context-name: 显示指定的 SNMP 上下文，为 1~32 个字符的字符串，区分大小写。不指定该参数时，显示设备上所有已创建的 SNMP 上下文。

【举例】

显示设备上所有已创建的 SNMP 上下文。

```
<Sysname> display snmp-agent context  
testcontext
```

【相关命令】

- **snmp-agent context**

1.1.3 display snmp-agent group

display snmp-agent group 命令用来显示 SNMP 组信息。

【命令】

display snmp-agent group [*group-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

group-name: 指定要显示信息的 SNMPv1、SNMPv2c 或 SNMPv3 组的名称。取值范围为 1~32 个字符的字符串，区分大小写。不指定该参数时，显示设备上所有已创建的 SNMP 组的信息。

【举例】

```
# 显示所有 SNMP 组的信息。
<Sysname> display snmp-agent group
  Group name: groupv3
    Security model: v3 noAuthnoPriv
    Readview: ViewDefault
    Writeview: <no specified>
    Notifyview: <no specified>
    Storage-type: nonVolatile
    ACL name: testacl
```

表1-2 display snmp-agent group 命令显示信息描述表

字段	描述
Group name	SNMP组名
Security model	SNMP组配置的安全模式，包括版本信息和安全模式，以空格分隔： - 对于 SNMPv1 和 SNMPv2c 版本，认证加密级别只能为 noAuthNoPriv（无认证无加密） - 对于 SNMPv3 版本，安全模式分为三种：authPriv（既认证又加密）、authNoPriv（只认证不加密）、noAuthNoPriv（不认证不加密）
Readview	SNMP组对应的只读的MIB视图名
Writeview	SNMP组对应的可写的MIB视图名
Notifyview	SNMP组对应的可以发Trap和Inform报文的MIB视图名
Storage-type	存储方式，分为以下几种：volatile、nonVolatile、permanent、readOnly、other，具体描述请参见 表1-1
ACL	使用的IPv4 ACL列表的编号（该字段仅在SNMP组与IPv4 ACL编号绑定后显示）
ACL name	使用的ACL列表的名称（该字段仅在SNMP组与ACL名称绑定后显示）
IPV6 ACL	使用的IPv6 ACL列表的编号（该字段仅在SNMP组与IPv6 ACL编号绑定后显示）
IPV6 ACL name	使用的IPv6 ACL列表的名称（该字段仅在SNMP组与IPv6 ACL名称绑定后显示）

【相关命令】

- snmp-agent group

1.1.4 display snmp-agent local-engineid

display snmp-agent local-engineid 命令用来显示本设备的 SNMP 引擎 ID。

【命令】

```
display snmp-agent local-engineid
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

SNMP 引擎 ID 是 SNMP 实体的唯一标识,它在一个 SNMP 管理域内是唯一的。SNMP 引擎是 SNMP 实体的重要组成部分,完成 SNMP 信息的信息调度、信息处理、安全验证、访问控制等功能。

【举例】

```
# 显示本设备的 SNMP 引擎 ID。  
<Sysname> display snmp-agent local-engineid  
SNMP local engine ID: 800063A2800084E52BED7900000001
```

【相关命令】

- **snmp-agent local-engineid**

1.1.5 display snmp-agent mib-node

display snmp-agent mib-node 命令用来显示 SNMP 支持的 MIB 节点信息。

【命令】

display snmp-agent mib-node [details | index-node | trap-node | verbose]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

details: 表示显示 SNMP 支持的 MIB 节点细节信息,包括节点名、OID 末位、下一个叶子节点名。

index-node: 显示 SNMP 支持的 MIB 表、节点名及索引节点 OID。

trap-node: 显示 SNMP 支持的 MIB 告警节点名及对应的 OID、告警绑定变量节点名及对应的 OID。

verbose: 显示 SNMP 支持的 MIB 节点详细信息,包括节点名、OID、节点类型、访问权限、数据类型,对应 MOR (Managed Object Repository, 管理对象库) 定义、父子兄弟节点信息等。

【使用指导】

未指定任何参数时,显示 SNMP 支持的 MIB 节点信息,包括节点名、OID 和节点访问权限。

特性包中可以包含不同的 MIB 插件，设备根据加载特性包的不同，支持的 MIB 不相同。

【举例】

显示 SNMP 支持 MIB 节点信息。

<Sysname> display snmp-agent mib-node

```
iso<1>(NA)
  |-std<1.0>(NA)
    |-iso8802<1.0.8802>(NA)
      |-ieee802dot1<1.0.8802.1>(NA)
        |-ieee802dot1mibs<1.0.8802.1.1>(NA)
```

其它显示信息略……

表1-3 display snmp-agent mib-node 命令显示信息描述表

字段	描述
-std	MIB节点名
<1.0>	MIB节点对应的OID
(NA)	MIB节点访问权限，取值为： • NA：表示节点不可访问 • NF：表示节点支持告警 • RO：表示节点支持只读访问 • RW：表示节点支持读写访问 • RC：表示节点支持读写创建访问 • WO：表示节点支持只写访问
*	表示叶子节点或表节点

显示 SNMP 支持 MIB 节点细节信息。

<Sysname> display snmp-agent mib-node details

```
iso(1)(dot1xPaeSystemAuthControl)
  |-std(0)(dot1xPaeSystemAuthControl)
    |-iso8802(8802)(dot1xPaeSystemAuthControl)
      |-ieee802dot1(1)(dot1xPaeSystemAuthControl)
        |-ieee802dot1mibs(1)(dot1xPaeSystemAuthControl)
```

其它显示信息略……

表1-4 display snmp-agent mib-node details 命令显示信息描述表

字段	描述
-std	MIB节点名
(0)	MIB节点对应OID末位
(lldpMessageTxInterval)	MIB节点下一个叶子节点名
*	表示叶子节点或表节点

显示 SNMP 支持的 MIB 表名、索引节点名及对应的 OID。

<Sysname> display snmp-agent mib-node index-node

```
Table          |dot1xPaePortTable
Index          ||dot1xPaePortNumber
OID            ||| 1.0.8802.1.1.1.1.2.1.1
```

其它显示信息略……

表1-5 display snmp-agent mib-node index-node 命令显示信息描述表

字段	描述
Table	MIB表名
Index	MIB索引节点名
OID	MIB索引节点对应的OID

显示 SNMP 支持的 MIB 告警节点名及对应的 OID、告警绑定变量节点名及对应的 OID。

<Sysname> display snmp-agent mib-node trap-node

```
Name          |lldpRemTablesChange
OID           ||1.0.8802.1.1.2.0.0.1
Trap Object
Name          |||lldpStatsRemTablesInserts
OID           |||1.0.8802.1.1.2.1.2.2
Name          |||lldpStatsRemTablesDeletes
OID           |||1.0.8802.1.1.2.1.2.3
Name          |||lldpStatsRemTablesDrops
OID           |||1.0.8802.1.1.2.1.2.4
Name          |||lldpStatsRemTablesAgeouts
OID           |||1.0.8802.1.1.2.1.2.5
```

其它显示信息略……

表1-6 display snmp-agent mib-node trap-node 命令显示信息描述表

字段	描述
Name	MIB告警节点名
OID	MIB告警节点对应的OID
Trap Object	MIB告警绑定变量节点相关信息（其中Name表示告警绑定变量节点名，OID表示变量名节点对应的OID）

显示 SNMP 支持的 MIB 节点详细信息，包括节点名、OID、节点类型、访问权限、数据类型，对应 MOR 定义、父子兄弟节点信息等。

<Sysname> display snmp-agent mib-node verbose

```
Name          |iso
```

```
OID          ||1
Properties    ||NodeType:   Other
              ||AccessType: NA
              ||DataType:   NA
              ||MOR:        0x00000000
Parent        ||
First child   ||std
Next leaf     ||dot1xPaeSystemAuthControl
Next sibling   ||
其它显示信息略……
```

表1-7 display snmp-agent mib-node verbose 命令显示信息描述表

字段	描述
Name	MIB节点名
OID	MIB节点对应的OID
Properties	MIB节点的属性
NodeType	MIB节点类型，取值为： • Table: 表节点 • Row: 表中行节点 • Column: 表中列节点 • Leaf: 叶子节点 • Group: 组节点（叶子节点的父节点） • Trapnode: 告警节点 • Other: 其他类型
AccessType	MIB节点访问权限，取值为： • NA: 表示节点不可访问 • NF: 表示节点支持告警 • RO: 表示节点支持只读访问 • RW: 表示节点支持读写访问 • RC: 表示节点支持读写创建访问 • WO: 表示节点支持只写访问

字段	描述
DataType	MIB节点数据类型，取值为： - Integer: 整数 - Integer32: 32 位整数 - Unsigned32: 32 位无符号整数 - Gauge: 可增可减的非负整数 - Gauge32: 32 位可增可减的非负整数 - Counter: 可增不可减的非负整数 - Counter32: 32 位可增不可减的非负整数 - Counter64: 64 位可增不可减的非负整数 - Timeticks: 用于计时的非负整数 - Octstring: 八进制字符串 - OID: 对象标识符 - IPAddress: 用于 IP 规范格式的 32 位地址 - Networkaddress: 网络 IP 地址 - Opaque: 任意数据 - Userdefined: 用户类型 - BITS: 所述位枚举 - NA: 其他类型节点
MOR	MIB节点对应的MOR定义
Parent	父节点名
First child	第一个子节点名
Next leaf	下一个叶子节点名
Next sibling	右兄弟节点名
Allow	允许的操作类型，取值包括如下： - get/set/getnext: 允许所有操作 - get: 只允许 Get 操作 - set: 只允许 Set 操作 - getnext: 只允许 GetNext 操作
Value range	节点的取值范围
Index	表索引，仅表节点显示此字段

1.1.6 display snmp-agent mib-view

display snmp-agent mib-view 命令用来显示 MIB 视图的信息。

【命令】

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

exclude: 显示属性为 **exclude** 的 MIB 视图的信息。

include: 显示属性为 **include** 的 MIB 视图的信息。

viewname view-name: 显示指定名称 MIB 视图的信息，*view-name* 为视图的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

不指定参数时，显示所有 MIB 视图的信息。

【举例】

显示设备的所有 MIB 视图。

```
<Sysname> display snmp-agent mib-view
```

```
View name: ViewDefault
MIB Subtree: iso
Subtree mask:
Storage-type: nonVolatile
View Type: included
View status: active
```

```
View name: ViewDefault
MIB Subtree: snmpUsmMIB
Subtree mask:
Storage-type: nonVolatile
View Type: excluded
View status: active
```

```
View name: ViewDefault
MIB Subtree: snmpVacmMIB
Subtree mask:
Storage-type: nonVolatile
View Type: excluded
View status: active
```

```
View name: ViewDefault
MIB Subtree: snmpModules.18
Subtree mask:
Storage-type: nonVolatile
View Type: excluded
View status: active
```

以上信息表明，设备上当前有四个 MIB 视图，名称均为 ViewDefault。使用 ViewDefault 视图名限制 NMS 访问时，除了 snmpUsmMIB、snmpVacmMIB、snmpModules.18 子树下的 MIB 对象，NMS 可以访问 iso 子树下其它所有 MIB 对象。

表1-8 display snmp-agent mib-view 命令显示信息描述表

字段	描述
View name	视图名
MIB Subtree	MIB视图对应的MIB子树
Subtree mask	MIB子树的掩码
Storage-type	存储方式，分为以下几种：volatile、nonVolatile、permanent、readOnly、other，具体请参见 表1-1
View Type	MIB视图的类型（即该视图与MIB子树的关系），包括included和excluded两种： - included 表示当前视图包括该子树的所有节点，即可以访问子树内的所有 MIB 对象 - excluded 表示当前视图不包括该子树的任意节点，即子树内的所有 MIB 对象都不能被访问
View status	MIB视图的状态，包括： - active 表示 MIB 视图可用 - inactive 表示 MIB 视图不可用。用户不能对处于该状态的 MIB 视图中的节点执行读写操作，但允许 MIB 视图中的节点发送 Trap 和 Inform 消息

【相关命令】

- **snmp-agent mib-view**

1.1.7 display snmp-agent remote

display snmp-agent remote 命令用来显示远端 SNMP 实体的引擎 ID。

【命令】

```
display snmp-agent remote [ { ipv4-address | ipv6 ipv6-address }
[ vpn-instance vpn-instance-name ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

ipv4-address：显示指定 IPv4 地址的远端 SNMP 实体的引擎 ID。**ipv4-address** 表示远端 SNMP 实体的 IPv4 地址。

ipv6 ipv6-address: 显示指定 IPv6 地址的远端 SNMP 实体的引擎 ID。*ipv6-address* 表示远端 SNMP 实体的 IPv6 地址。

vpn-instance vpn-instance-name : 指定远端 SNMP 实体所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示远端 SNMP 实体位于公网中。

【使用指导】

SNMP 实体引擎 ID 是 SNMP 实体的唯一标识，它在一个 SNMP 管理域内是唯一的。SNMP 实体引擎是 SNMP 实体的重要组成部分，完成 SNMP 信息的信息调度、信息处理、安全验证、访问控制等功能。

如果未指定远端 SNMP 实体的 IP 地址，则会显示设备上配置的所有远端 SNMP 实体的引擎 ID。

【举例】

```
# 显示设备上配置的所有远端 SNMP 实体的引擎 ID。
<Sysname> display snmp-agent remote
    Remote engineID: 800063A28000A0FC00580400000001
    IPv4 address: 1.1.1.1
    VPN instance: vpn1
```

表1-9 display snmp-agent remote 命令显示信息描述表

字段	描述
Remote engineID	远端SNMP实体的引擎，可通过 snmp-agent remote 命令配置
IPv4 address	远端SNMP实体的IPv4地址
IPv6 address	远端SNMP实体的IPv6地址。当配置 snmp-agent remote 命令时绑定的是IPv6地址时，显示该信息
VPN instance	远端SNMP实体所属的VPN实例。只有配置 snmp-agent remote 命令且绑定了VPN实例时，才显示该信息

【相关命令】

- **snmp-agent remote**

1.1.8 display snmp-agent statistics

display snmp-agent statistics 命令用来显示 SNMP 报文的统计信息。

【命令】

display snmp-agent statistics

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【举例】

显示 SNMP 报文的统计信息。

```
<Sysname> display snmp-agent statistics
1684 messages delivered to the SNMP entity.
5 messages were for an unsupported version.
0 messages used an unknown SNMP community name.
0 messages represented an illegal operation for the community supplied.
0 ASN.1 or BER errors in the process of decoding.
1679 messages passed from the SNMP entity.
0 SNMP PDUs had badValue error-status.
0 SNMP PDUs had genErr error-status.
0 SNMP PDUs had noSuchName error-status.
0 SNMP PDUs had tooBig error-status (Maximum packet size 1500).
16544 MIB objects retrieved successfully.
2 MIB objects altered successfully.
7 GetRequest-PDU accepted and processed.
7 GetNextRequest-PDU accepted and processed.
1653 GetBulkRequest-PDU accepted and processed.
1669 GetResponse-PDU accepted and processed.
2 SetRequest-PDU accepted and processed.
0 Trap PDUs accepted and processed.
0 alternate Response Class PDUs dropped silently.
0 forwarded Confirmed Class PDUs dropped silently.
```

表1-10 display snmp-agent statistics 命令显示信息描述表

字段	描述
messages delivered to the SNMP entity	Agent收到的数据报文个数
messages were for an unsupported version	版本不支持的数据报文个数
messages used an unknown SNMP community name	使用了非法团体名的数据报文个数
messages represented an illegal operation for the community supplied	包含了超出团体名权限的操作的数据报文个数
ASN.1 or BER errors in the process of decoding	在解码过程中发生ASN.1（Abstract Syntax Notation dot one，抽象记法1）或BER（Basic Encoding Rules，基本编码规则）错误的数据报文个数
messages passed from the SNMP entity	Agent发送给别的SNMP实体的数据报文个数
SNMP PDUs had badValue error-status	错误类型为BadValues的数据报文个数
SNMP PDUs had genErr error-status	genErr错误的数据报文个数
SNMP PDUs had noSuchName error-status	NoSuchName错误的数据报文个数
SNMP PDUs had tooBig error-status	TooBig错误的数据报文个数（设备允许通过的最大SNMP PDU为1500字节）
MIB objects retrieved successfully	已成功获取的MIB对象个数
MIB objects altered successfully	已成功修改的MIB对象个数

字段	描述
GetRequest-PDU accepted and processed	已接收并处理的Get请求的个数
GetNextRequest-PDU accepted and processed	已接收并处理的GetNext请求的个数
GetBulkRequest-PDU accepted and processed	已接收并处理的GetBulk请求的个数
GetResponse-PDU accepted and processed	已接收并处理的Get响应的个数
SetRequest-PDU accepted and processed	已接收并处理的Set请求的个数
Trap PDUs accepted and processed	已接收并处理的Trap和Inform报文的个数
alternate Response Class PDUs dropped silently	被丢弃的响应数据报文个数
forwarded Confirmed Class PDUs dropped silently	被丢弃的转发数据报文个数

1.1.9 display snmp-agent sys-info

display snmp-agent sys-info 命令用来显示 SNMP 设备的系统信息。

【命令】

display snmp-agent sys-info [contact | location | version] *

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

contact: 显示当前设备维护者的联系信息。
location: 显示当前设备的物理位置信息。
version: 显示当前设备中运行的 SNMP 版本号。

【使用指导】

不指定参数时，显示设备的全部系统信息。

【举例】

```
# 显示设备系统信息。
<Sysname> display snmp-agent sys-info
  The contact information of the agent:
    Beijing UNIS Hengyue Technologies Co., Ltd.

  The location information of the agent:
    Beijing, China

  The SNMP version of the agent:
```


【相关命令】

- **snmp-agent sys-info**

1.1.10 display snmp-agent trap queue

display snmp-agent trap queue 命令用来显示告警信息队列的基本信息。

【命令】

display snmp-agent trap queue

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示当前告警信息队列的配置及使用情况。

```
<Sysname> display snmp-agent trap queue
```

```
Queue size: 100
```

```
Message number: 6
```

表1-11 display snmp-agent trap queue 命令显示信息描述表

字段	描述
Queue size	告警信息队列长度
Message number	告警信息队列中当前告警信息的个数

【相关命令】

- **snmp-agent trap life**
- **snmp-agent trap queue-size**

1.1.11 display snmp-agent trap-list

display snmp-agent trap-list 命令用来显示 SNMP 告警功能的开启状态。

【命令】

display snmp-agent trap-list

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context-operator

【使用指导】

如果一个模块包含多个子模块，只要有任何一个子模块的告警信息是使能的，就显示整个模块是使能的。

业务模块是否支持 SNMP 告警功能请通过执行 **snmp-agent trap enable ?** 命令来获知。本命令的显示信息和 **snmp-agent trap enable** 命令以及业务模块的配置相关。

【举例】

显示 SNMP 告警功能的开启状态。

```
<Sysname> display snmp-agent trap-list
arp notification is disabled.
configuration notification is enabled.
l3vpn notification is enabled.
mac-address notification is enabled.
ospf notification is enabled.
radius notification is disabled.
rddc notification is enabled.
standard notification is enabled.
syslog notification is disabled.
system notification is enabled.

Enabled notifications: 7; Disabled notifications: 3
```

【相关命令】

- **snmp-agent trap enable**

1.1.12 display snmp-agent usm-user

display snmp-agent usm-user 命令用来显示 SNMPv3 用户信息。

【命令】

display snmp-agent usm-user [engineid *engineid* | group *group-name* | username *user-name*] *

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

engineid engineid: 显示指定引擎 ID 的 SNMPv3 用户信息, *engineid* 表示 SNMP 引擎 ID, 不区分大小写。SNMPv3 用户创建的时候, 系统会记录当时设备的 SNMP 实体引擎 ID, 如果设备的引擎 ID 被修改, 则被创建的 SNMPv3 用户将暂时无效, 只有引擎 ID 恢复后, 才能继续生效。

group group-name: 显示属于指定 SNMP 组的 SNMPv3 用户信息, 区分大小写。

username user-name: 显示指定名称的 SNMPv3 用户信息, 区分大小写。

【使用指导】

使用 **snmp-agent usm-user** 命令可以创建 SNMPv1/v2c/v3 用户, 如果创建的是 SNMPv1/v2c 用户, 系统自动添加一个新的同名的团体名, 并将这个用户当成 SNMPv1/v2c 团体来处理。所以, 不能通过 **display snmp-agent usm-user** 命令来查看 SNMPv1/v2c 用户的信息, 能通过 **display snmp-agent community** 查看 SNMPv1/v2c 用户对应的团体的信息。

【举例】

显示设备上已创建的所有 SNMPv3 用户的信息。

```
<Sysname> display snmp-agent usm-user
  Username: userv3
  Group name: mygroupv3
    Engine ID: 800063A203000FE240A1A6
    Storage-type: nonVolatile
    UserStatus: active
    ACL: 2000

  Username: userv3
  Group name: mygroupv3
    Engine ID: 8000259503000BB3100A508
    Storage-type: nonVolatile
    UserStatus: active
    ACL name: testacl

  Username: userv3code
  Role name: groupv3code
    network-operator
    Engine ID: 800063A203000FE240A1A6
    Storage-type: nonVolatile
    UserStatus: active

  Username: userv3code
  Role name: snmprole
    network-operator
    Engine ID: 800063A280000002BB0001
    Storage-type: nonVolatile
    UserStatus: active
```

表1-12 display snmp-agent usm-user 命令显示信息描述表

字段	描述
Username	SNMP用户的用户名

字段	描述
Group name	SNMP用户所在组的组名
Role name	SNMP用户的角色名称
Engine ID	SNMP用户创建时使用的SNMP实体引擎ID
Storage-type	存储方式，分为以下几种：volatile、nonVolatile、permanent、readOnly、other，具体请参见 表1-1
UserStatus	SNMP用户的状态，分为以下几种： - active：有效 - notInService：当前不可用 - notReady：未配置完成 - other：其他
ACL	使用的ACL列表的编号（该字段仅在用户与ACL编号绑定后显示）
ACL name	使用的ACL列表的名称（该字段仅在用户与ACL名称绑定后显示）
IPV6 ACL	使用的IPv6 ACL列表的编号（该字段仅在用户与IPv6 ACL编号绑定后显示）
IPV6 ACL name	使用的IPv6 ACL列表的名称（该字段仅在用户与IPv6 ACL名称绑定后显示）

【相关命令】

- **snmp-agent usm-user v3**

1.1.13 enable snmp trap updown

enable snmp trap updown 命令用来开启接口状态变化的告警功能。

undo enable snmp trap updown 命令用来关闭接口状态变化的告警功能。

【命令】

enable snmp trap updown

undo enable snmp trap updown

【缺省情况】

接口状态变化的告警功能处于开启状态。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

需要注意的是，如果要求接口在状态发生改变时生成接口状态变化的告警信息，需要开启全局告警功能并在接口开启接口状态变化的告警功能。接口下开启请使用命令 **enable snmp trap updown**，全局下开启请使用命令 **snmp-agent trap enable standard [linkdown | linkup] ***。

【举例】

允许发送端口 GigabitEthernet1/0/1 的 linkUp/linkDown 的 SNMP 告警，使用团体名 public，向 IP 地址为 10.1.1.1 的目的主机发送 Trap 报文。

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] enable snmp trap updown
```

【相关命令】

- **snmp-agent target-host**
- **snmp-agent trap enable**

1.1.14 snmp-agent

snmp-agent 命令用来开启 SNMP Agent 功能。

undo snmp-agent 命令用来关闭 SNMP Agent 功能。

【命令】

```
snmp-agent
undo snmp-agent
```

【缺省情况】

SNMP Agent 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

执行除 **snmp-agent calculate-password** 外任何以 **snmp-agent** 开头的命令都可以开启 SNMP Agent 功能。

当 SNMP 侦听端口被设备上的其他服务占用时，会导致 SNMP 功能启动失败。SNMP 侦听端口可通过 **snmp-agent port** 命令配置，用户可使用 **display udp verbose** 命令查看设备上 UDP 端口的使用情况。

【举例】

开启设备的 SNMP Agent 功能。

```
<Sysname> system-view
[Sysname] snmp-agent
```

【相关命令】

- **display udp verbose**（三层技术-IP 业务/IP 性能优化）
- **snmp-agent port**

1.1.15 snmp-agent { inform | trap } source

snmp-agent { inform | trap } source 命令用来配置发送的告警信息的源 IP 地址。

undo snmp-agent { inform | trap } source 命令用来恢复缺省情况。

【命令】

snmp-agent { inform | trap } source *interface-type* { *interface-number* | *interface-number.subnumber* }
undo snmp-agent { inform | trap } source

【缺省情况】

使用出接口的 IP 地址作为告警信息的源 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

inform: 用来指定 Inform 报文中的源 IP 地址。

trap: 用来指定 Trap 报文中的源 IP 地址。

***interface-type* { *interface-number* | *interface-number.subnumber* }**: 指定三层接口类型与接口编号。其中 *interface-number* 为主接口编号；*subnumber* 为子接口编号，取值范围为 1~4094。

【使用指导】

执行该命令后，系统会使用指定接口的主 IP 地址作为发送出去的告警信息的源 IP 地址。这样，在 NMS 上就可以使用该 IP 地址唯一标志 Agent。即便 Agent 使用不同的出接口发送告警信息，NMS 都可以使用该 IP 地址来过滤 Agent 发送的所有告警信息。

在将某个接口配置为获取告警信息的源地址接口之前需要注意的是：

- 如果配置的接口已存在，并且配置了合法的 IP 地址，则该 IP 地址将作为告警信息的源地址；
- 如果配置的接口不存在，则该命令会配置失败；
- 如果配置的接口已存在，但未配置合法的 IP 地址，则该命令不生效，在接口配置了合法 IP 地址后，该命令会自动生效。

【举例】

配置 Trap 报文的源地址为以太网接口 GigabitEthernet1/0/1 上的接口主 IP 地址。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent trap source gigabitethernet 1/0/1
```

配置 Inform 报文的源地址为以太网接口 GigabitEthernet1/0/2 上的接口主 IP 地址。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent inform source gigabitethernet 1/0/2
```

【相关命令】

- **snmp-agent trap enable**
- **snmp-agent target-host**

1.1.16 snmp-agent calculate-password

snmp-agent calculate-password 命令用来为明文密码计算对应的密文密码。

【命令】

```
snmp-agent calculate-password plain-password mode { 3desmd5 | 3dessha | md5 | sha } { local-engineid | specified-engineid engineid }
```

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

plain-password: 表示明文密码，为 1~64 个字符的字符串，区分大小写。

mode: 指定认证算法和加密算法。设备支持的认证算法有 HMAC-MD5 和 HMAC-SHA1，其中 HMAC-MD5 的计算速度比 HMAC-SHA1 快，而 HMAC-SHA1 的安全强度比 HMAC-MD5 高；设备支持的加密算法安全性由高到低依次是：AES、3DES、DES，安全性高的加密算法实现机制复杂，运算速度慢。对于普通的安全要求，DES 算法就可以满足需要。

- **3desmd5**: 用于计算密文加密密码，此时对应的认证算法必须为 HMAC-MD5，加密算法必须为 3DES。
- **3dessha**: 用于计算密文加密密码，此时对应的认证算法必须为 HMAC-SHA1，加密算法必须为 3DES。
- **md5**: 用于计算密文认证密码和密文加密密码。用于计算密文认证密码时，认证算法必须为 HMAC-MD5；用于计算密文加密密码时，认证算法必须为 HMAC-MD5，加密算法可以为 AES 或者 DES。因为当认证算法为 HMAC-MD5 时，相同的明文密码，各自计算出来的密文认证密码和密文加密密码均相同。
- **sha**: 用于计算密文认证密码和密文加密密码。用于计算密文认证密码时，认证算法必须为 HMAC-SHA1；用于计算密文加密密码时，认证算法必须为 HMAC-SHA1，加密算法可以为 AES 或者 DES。因为当认证算法为 HMAC-SHA1 时，相同的明文密码，各自计算出来的密文认证密码和密文加密密码均相同。

local-engineid: 使用本地引擎 ID 计算密文密码，引擎 ID 的相关描述与配置可参考命令 **snmp-agent local-engineid**。

specified-engineid: 使用用户指定的引擎 ID 计算密文密码。

engineid: 引擎 ID，必须为偶数个十六进制数，偶数的取值范围为 10~64，不区分大小写。全 0 和全 F 均被认为是无效参数。

【使用指导】

执行本命令前，必须先开启设备的 SNMP Agent 功能。

在创建 SNMPv3 用户时，如果指明认证或者加密密码采用密文配置方式，则可以输入该命令生成的密文密码来代替明文密码，从而避免在非安全环境直接输入明文密码造成的安全隐患。

生成的密码是和引擎 ID 相关联的，在某一引擎 ID 下生成的密码，也只在此引擎 ID 下生效。

【举例】

```
# 使用本地引擎 ID 和 HMAC-SHA1 算法计算明文认证密码 authkey 的密文密码。
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode sha local-engineid
The encrypted key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

【相关命令】

- **snmp-agent local-engineid**
- **snmp-agent usm-user v3**

1.1.17 snmp-agent community

snmp-agent community 命令用来创建 SNMP 团体。

undo snmp-agent community 命令用来删除 SNMP 团体。

【命令】

VACM 方式:

```
snmp-agent community { read | write } [ simple | cipher ] community-name
[ mib-view view-name ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6
{ ipv6-acl-number | name ipv6-acl-name } ] *
undo snmp-agent community [ cipher ] community-name
```

RBAC 方式:

```
snmp-agent community [ simple | cipher ] community-name user-role role-name
[ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number |
name ipv6-acl-name } ] *
undo snmp-agent community [ cipher ] community-name
```

【缺省情况】

不存在 SNMP 团体。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

read: 表示对 MIB 对象的访问权限为只读。NMS 使用该团体名访问 Agent 时只能执行读操作。

write: 表示对 MIB 对象的访问权限为读写。NMS 使用该团体名访问 Agent 时可以执行读、写操作。

simple: 表示以明文方式配置团体名并以密文方式保存到配置文件中。

cipher: 表示以密文方式配置团体名并以密文方式保存到配置文件中。

community-name: 配置明文团体名或密文团体名，是限制 NMS 访问 Agent 时所使用的团体名。区分大小写，需要转义的字符请加“\”后输入。当以明文方式配置时，团体名为 1~32 个字符的字符串；当以密文方式配置时，团体名为 33~73 个字符的字符串。

mib-view view-name: 用来指定 NMS 可以访问的 MIB 对象的范围, **view-name** 表示 MIB 视图名, 为 1~32 个字符的字符串, 区分大小写。不指定参数时, 缺省视图为 ViewDefault。

user-role role-name: 该团体对应的角色名称, **role-name** 为 1~63 个字符的字符串, 区分大小写。

acl: 将团体名与基本/高级 IPv4 ACL 绑定。

ipv4-acl-number: 表示基本或高级 IPv4 ACL 的编号, 其中基本 IPv4 ACL 的取值范围为 2000~2999, 高级 IPv4 ACL 的取值范围为 3000~3999。

name ipv4-acl-name: 表示基本或高级 IPv4 ACL 的名称, 为 1~63 个字符的字符串, 不区分大小写。

acl ipv6: 将团体名与基本/高级 IPv6 ACL 绑定。

ipv6-acl-number: 表示基本或高级 IPv6 ACL 的编号, 其中基本 IPv6 ACL 的取值范围为 2000~2999, 高级 IPv6 ACL 的取值范围为 3000~3999。

name ipv6-acl-name: 表示基本或高级 IPv6 ACL 的名称, 为 1~63 个字符的字符串, 不区分大小写。

【使用指导】

为了安全起见, 只有具有 **network-admin**、**context-admin** 或者 **level-15** 用户角色的用户登录设备后才能执行本命令。其它角色的用户, 即使授权了 SNMP 特性或本命令的操作权限, 也不能执行本命令。

该命令用于 SNMPv1 和 SNMPv2c 组网环境。

团体是 NMS 和 Agent 的集合, 用团体名来标志。团体名相当于密码, 团体内的设备通信使用团体名来进行认证。只有 NMS 和 Agent 上配置的团体名相同时, 才能互相访问。通常情况下, “**public**” 被用来作为读权限团体名、“**private**” 被用来作为写权限团体名。为了增强安全性, 网络管理员也可以配置其它团体名。

用户有两种方式创建团体:

- 使用 **snmp-agent community** 命令来创建团体。
- 配置 **snmp-agent usm-user { v1 | v2c }** 和 **snmp-agent group { v1 | v2c }** 命令成功创建 SNMPv1 或 SNMPv2c 用户以及相应的组后, 系统会以用户名为团体名自动创建一个团体。

display snmp-agent community 会显示这两种方式创建的、以明文方式配置并以明文方式保存到配置文件中的团体的信息。

使用 **snmp-agent community** 命令创建团体时, 可以通过两种配置方式来控制团体的访问:

- VACM (View-based Access Control Model, 基于视图的访问控制模型) 的配置方式: 该方式通过指定 MIB 视图来限定 NMS 可以访问的 MIB 节点, 访问的动作包括只读和读写两种。
- RBAC (Role Based Access Control, 基于角色的访问控制) 的配置方式: 该方式使用用户角色来限定 NMS 的访问权限。缺省情况下, 用户角色 **network-admin**、**context-admin** 和 **level-15** 可以读写所有的 MIB 节点, **network-operator** 和 **context-operator** 可以只读所有的 MIB 节点。有关用户角色的详细信息, 请参见“基础配置指导”中的“RBAC”。

推荐使用 RBAC 配置方式, 安全性更高。

多次执行本命令最多可创建 10 个团体名。

多次执行该命令, 指定的团体名相同, 其它参数不同时, 新配置生效。

不指定 **simple** 和 **cipher** 参数时, 表示以明文方式配置团体名, 并以明文方式保存到配置文件。

使用 **acl** 参数可以限制非法 NMS 访问设备：

- 当未引用 **ACL**、引用的 **ACL** 不存在、或者引用的 **ACL** 下没有配置规则时，允许所有 NMS 访问设备。
- 当引用的 **ACL** 下配置了规则时，则只有规则中 **permit** 的 NMS 才能访问设备，其他 NMS 不允许访问设备。

【举例】

以明文方式创建 **SNMP** 团体 **readaccess**，并且允许 NMS 使用该团体名对设备上缺省视图内的 **MIB** 对象进行只读访问。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent community read simple readaccess
```

以明文方式配置团体名 **writeaccess**，并且只允许 IP 地址为 **1.1.1.1** 的 NMS 使用该团体名对设备上缺省视图内的 **MIB** 对象进行读写操作，禁止其它 NMS 使用该团体名执行写操作。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write simple writeaccess acl 2001
```

以明文方式配置团体名 **writeaccess**，并且只允许 IP 地址为 **1.1.1.2** 的 NMS 使用该团体名对设备上缺省视图内的 **MIB** 对象进行读写操作，禁止其它 NMS 使用该团体名执行写操作。

```
<Sysname> system-view
[Sysname] acl basic name testacl
[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Sysname-acl-ipv4-basic-testacl] rule deny source any
[Sysname-acl-ipv4-basic-testacl] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write simple writeaccess acl name testacl
```

以明文方式创建团体名 **wr-sys-acc**，使用该团体名访问设备时只能对 **system** (OID 为 **1.3.6.1.2.1.1**) 子树下的 **MIB** 对象执行写操作。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] undo snmp-agent mib-view ViewDefault
[Sysname] snmp-agent mib-view included test system
[Sysname] snmp-agent community write simple wr-sys-acc mib-view test
```

【相关命令】

- **display snmp-agent community**
- **snmp-agent mib-view**

1.1.18 snmp-agent community-map

snmp-agent community-map 命令用来创建团体名到 **SNMP** 上下文的映射。

undo snmp-agent community-map 命令用来删除团体名到 **SNMP** 上下文的映射。

【命令】

```
snmp-agent community-map community-name context context-name  
undo snmp-agent community-map community-name context context-name
```

【缺省情况】

不存在团体名到 SNMP 上下文的映射。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

community-name: 团体名，为 1~32 个字符的字符串，区分大小写。
context-name: SNMP 上下文。为 1~32 个字符的字符串，区分大小写。

【使用指导】

用户配置成功后，使用 SNMP v1/v2 版本连接 SNMP Agent 时，SNMP 插件端所获取的上下文，是此时 NMS 访问 Agent，使用的团体名映射的上下文。如团体名未配置上下文映射，则获取不到。系统中可配置的映射最多为 10 个。

【举例】

```
# 配置一个团体名到 SNMP 上下文的映射。  
<Sysname> system-view  
[Sysname] snmp-agent community-map private context testcontext
```

【相关命令】

- **display snmp-agent community**

1.1.19 snmp-agent context

snmp-agent context 命令用来创建 SNMP 上下文。
undo snmp-agent context 命令用来删除 SNMP 上下文。

【命令】

```
snmp-agent context context-name  
undo snmp-agent context context-name
```

【缺省情况】

不存在 SNMP 上下文。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

context-name: SNMP 上下文, 为 1~32 个字符的字符串, 区分大小写。

【使用指导】

NMS 未配置上下文, 或 NMS 与 Agent 配置为相同的上下文时, 两者可以连接成功, 否则返回超时。
系统中可配置的 SNMP 上下文最多为 20 个。

【举例】

```
# 创建一个新的 context。  
<Sysname> system-view  
[Sysname] snmp-agent context testcontext
```

【相关命令】

- **display snmp-agent context**

1.1.20 snmp-agent group

snmp-agent group 命令用来创建 SNMP 组。

undo snmp-agent group 命令用来删除 SNMP 组。

【命令】

- SNMPv1 和 SNMPv2c 版本下的命令格式是:
snmp-agent group { v1 | v2c } group-name [notify-view view-name | read-view view-name | write-view view-name] * [acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name }] *
undo snmp-agent group { v1 | v2c } group-name
- SNMPv3 版本下的命令格式是:
snmp-agent group v3 group-name [authentication | privacy] [notify-view view-name | read-view view-name | write-view view-name] * [acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name }] *
undo snmp-agent group v3 group-name [authentication | privacy]

【缺省情况】

不存在 SNMP 组。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

v1: SNMPv1 版本。
v2c: SNMPv2c 版本。

v3: SNMPv3 版本。

group-name: SNMP 组的名称，取值范围为 1~32 个字符的字符串，区分大小写。

authentication: 表示对报文进行认证但不加密。

privacy: 表示对报文进行认证和加密。

notify-view view-name: 可以发告警信息的视图名，为 1~32 个字符的字符串，区分大小写。缺省情况下，未配置告警信息视图。

read-view view-name: 只读视图名，为 1~32 个字符的字符串，区分大小写。缺省值为 ViewDefault。

write-view view-name: 读写视图名，为 1~32 个字符的字符串，区分大小写。缺省情况下，未配置读写视图，即 NMS 不能对设备的所有 MIB 对象进行写操作。

acl: 将组与基本/高级 IPv4 ACL 绑定。

ipv4-acl-number: 表示基本或高级 IPv4 ACL 的编号，其中基本 IPv4 ACL 编号的取值范围为 2000~2999，高级 IPv4 ACL 编号的取值范围为 3000~3999。

name ipv4-acl-name: 表示基本或高级 IPv4 ACL 的名称，为 1~63 个字符的字符串，不区分大小写。

acl ipv6: 将组与基本/高级 IPv6 ACL 绑定。

ipv6-acl-number: 表示基本或高级 IPv6 ACL 的编号，其中基本 IPv6 ACL 编号的取值范围为 2000~2999，高级 IPv6 ACL 编号的取值范围为 3000~3999。

name ipv6-acl-name: 表示基本或高级 IPv6 ACL 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

为了安全起见，只有具有 network-admin、context-admin 或者 level-15 用户角色的用户登录设备后才能执行本命令。其它角色的用户，即使授权了 SNMP 特性或本命令的操作权限，也不能执行本命令。

SNMP 组可以定义安全模式、视图权限等信息，配置在此组内的用户都具有这些公共属性。

系统中可配置的 SNMP 组最多为 20 个。

是否指定 **authentication** 和 **privacy** 参数存在如下情况：

- 当不指定 **authentication** 和 **privacy** 时，表示不认证不加密。此时，使用与该组绑定的用户名建立 SNMP 连接时，均不认证不加密。即使用户配置了认证密码/加密密码，认证密码/加密密码也不生效。
- 当指定 **authentication** 时，表示认证不加密。此时，使用与该组绑定的用户名建立 SNMP 连接时，均认证不加密。即使用户配置了加密密码，加密密码也不生效。
- 当指定 **privacy** 时，表示认证加密。此时，使用与该组绑定的用户名建立 SNMP 连接时，均认证加密。该组内的用户必须配置认证密码和加密密码，否则，不能建立 SNMP 连接。

创建 SNMP 组和用户的时候都可以使用 **acl** 参数限制非法 NMS 访问设备，只有两个 ACL 均允许的 NMS 才能访问设备。在创建组或用户时，ACL 均遵循以下规则：

- 当未引用 ACL、引用的 ACL 不存在、或者引用的 ACL 下没有配置规则时，允许所有 NMS 访问设备。
- 当引用的 ACL 下配置了规则时，则只有规则中 **permit** 的 NMS 才能访问设备，其他 NMS 不允许访问设备。

【举例】

```
# 在运行 SNMPv3 版本的设备上创建一个 SNMP 组 group1。
<Sysname> system-view
[Sysname] snmp-agent group v3 group1
```

【相关命令】

- **display snmp-agent group**
- **snmp-agent mib-view**
- **snmp-agent usm-user**

1.1.21 snmp-agent local-engineid

snmp-agent local-engineid 命令用来配置本设备的 SNMP 引擎 ID。

undo snmp-agent local-engineid 命令用来恢复缺省情况。

【命令】

```
snmp-agent local-engineid engineid
undo snmp-agent local-engineid
```

【缺省情况】

设备引擎 ID 为“公司的企业号+设备信息”。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

engineid: SNMP 引擎 ID，必须为偶数个十六进制数，偶数的取值范围为 10~64，不区分大小写。全 0 和全 F 均被认为是无效参数。

【使用指导】

SNMP 引擎 ID 有两个作用：

- 在 NMS 管理的所有设备中，每一台设备都需要用一个唯一的引擎 ID 来标识 Agent，缺省情况下每个设备有一个缺省的引擎 ID，网络管理员需要确保管理域内不能有重复的引擎 ID。
- SNMPv3 版本的用户名、密文密码等都和引擎 ID 相关联，如果更改了引擎 ID，则原引擎 ID 下配置的用户名、密码失效。

通常情况下，使用设备的缺省引擎 ID 即可，用户也可以根据网络整体规划给设备配置方便记忆的引擎 ID，比如 A 栋一楼的一号设备可以将它的引擎 ID 设置为 000Af0010001，二号设备可以配置为 000Af0010002。

【举例】

```
# 配置本设备的 SNMP 引擎 ID 为 123456789A。
<Sysname> system-view
[Sysname] snmp-agent local-engineid 123456789A
```

【相关命令】

- **display snmp-agent local-engineid**
- **snmp-agent usm-user**

1.1.22 snmp-agent log

snmp-agent log 命令用来开启 SNMP 日志功能。

undo snmp-agent log 命令用来关闭 SNMP 日志功能。

【命令】

```
snmp-agent log { all | authfail | get-operation | set-operation }  
undo snmp-agent log { all | authfail | get-operation | set-operation }
```

【缺省情况】

SNMP 日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

all: 表示 SNMP Get 操作、Set 操作和 SNMP 认证失败的日志开关。

authfail: 表示 SNMP 认证失败的日志开关。

get-operation: 表示 SNMP Get 操作的日志开关。

set-operation: 表示 SNMP Set 操作的日志开关。

【使用指导】

当打开 SNMP Get 或者 Set 操作的日志开关，NMS 对 Agent 执行指定的操作时，Agent 会记录与该操作相关信息并保存到设备的信息中心。当打开 SNMP 认证失败的日志开关时，如果 Agent 收到来自 NMS 的 SNMP 请求但是没有通过认证，Agent 会记录相关信息并保存到设备的信息中心。保存的相关信息将通过信息中心的参数配置，最终决定 SNMP 日志的输出规则（即是否允许输出以及输出方向）。

【举例】

```
# 打开 SNMP Get 操作的日志开关。  
<Sysname> system-view  
[Sysname] snmp-agent log get-operation  
# 打开 SNMP Set 操作的日志开关。  
<Sysname> system-view  
[Sysname] snmp-agent log set-operation  
# 打开 SNMP 认证失败的日志开关。  
<Sysname> system-view  
[Sysname] snmp-agent log authfail
```


1.1.23 snmp-agent mib-view

snmp-agent mib-view 命令用来创建或者更新 MIB 视图。

undo snmp-agent mib-view 命令用来删除 MIB 视图。

【命令】

```
snmp-agent mib-view { excluded | included } view-name oid-tree [ mask  
mask-value ]
```

```
undo snmp-agent mib-view view-name
```

【缺省情况】

存在四个 MIB 视图，名称均为 ViewDefault:

- 视图一包含 MIB 子树 iso;
- 视图二不包含子树 snmpUsmMIB;
- 视图三不包含子树 snmpVacmMIB;
- 视图四不包含子树 snmpModules.18。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

excluded: 表示当前视图不包括该 MIB 子树的任何节点（即禁止访问 MIB 子树的所有节点）。

included: 表示当前视图包括该 MIB 子树的所有节点（即允许访问 MIB 子树的所有节点）。

view-name: 视图名，为 1~32 个字符的字符串，区分大小写。

oid-tree: MIB 子树，用子树根节点的 OID（如“1.3.6.1.2.1.1”）或名称（如“system”）表示，为 1~255 个字符的字符串，区分大小写。OID 是由一系列的整数组成，标明节点在 MIB 树中的位置，它能唯一地标识一个 MIB 库中的对象。

mask mask-value: 对象子树的掩码，必须为偶数个十六进制数，偶数的取值范围为 1~32，不区分大小写。

【使用指导】

MIB 视图是 MIB 的子集，由视图名和 MIB 子树来唯一确定一个 MIB 视图。视图名相同但包含的子树不同，则认为不同的视图。

缺省视图可以通过 **display snmp-agent mib-view** 命令来查看。如果使用缺省视图限制 NMS 的访问权限时，除了 snmpUsmMIB、snmpVacmMIB、snmpModules.18 子树下的 MIB 对象，NMS 可以访问 iso 子树下其它所有 MIB 对象。缺省视图可以通过 **undo snmp-agent mib-view** 命令删除，但是删除以后，可能导致不能对 Agent 的所有 MIB 节点执行读写操作，除非另外手工配置视图。

【举例】

创建并更新 MIB 视图信息，视图名称为 mibtest，先创建一个包含 mib-2 子树(OID 为“1.3.6.1.2.1”)所有对象的 MIB 视图，再更新为不包含“system”子树(OID 为“1.3.6.1.2.1.1”)所有对象的 MIB 视图。

```
<Sysname> system-view
```



```
[Sysname] snmp-agent sys-info version v1
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1.2.1
[Sysname] snmp-agent mib-view excluded mibtest system
[Sysname] snmp-agent community read public mib-view mibtest
```

以上配置成功后，当 NMS 使用 SNMPv1 版本，public 团体名访问设备时，不能查询 system 子树的所有对象（比如 sysDescr 和 sysObjectID 等节点），可以查询 mib-2 子树下的其它所有对象。

【相关命令】

- **display snmp-agent mib-view**
- **snmp-agent group**

1.1.24 snmp-agent packet max-size

snmp-agent packet max-size 命令用来配置 Agent 能接收或发送的 SNMP 报文的最大长度。

undo snmp-agent packet max-size 命令用来恢复缺省情况。

【命令】

```
snmp-agent packet max-size byte-count
undo snmp-agent packet max-size
```

【缺省情况】

Agent 能处理的 SNMP 报文的最大长度为 1500。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

byte-count：Agent 能接收/发送的 SNMP 报文的最大长度，取值范围为 484~17940，单位为字节。

【使用指导】

配置报文的最大长度是为了防止网络中存在不支持分片的主机，而导致超长数据被丢弃。通常情况下，使用缺省值即可。

【举例】

```
# 配置 Agent 能接收/发送的 SNMP 报文的最大长度为 1024 字节。
<Sysname> system-view
[Sysname] snmp-agent packet max-size 1024
```

1.1.25 snmp-agent port

snmp-agent port 命令用来配置 SNMP 服务的侦听端口号。

undo snmp-agent port 命令用来恢复缺省情况。

【命令】

```
snmp-agent port port-number
```

undo snmp-agent port

【缺省情况】

SNMP 服务的侦听端口号是 161。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

port-number: SNMP 服务的侦听端口号，取值范围为 1~65535，缺省值为 161。

【使用指导】

当开启 SNMP Agent 功能时，如果 SNMP 侦听端口正被设备上的其它服务占用，会导致 SNMP 功能启动失败。此时，可使用本命令修改 SNMP 侦听端口。如果指定的新端口仍被其它服务占用，则新端口配置失败。建议修改前使用 **display udp verbose** 命令查看设备上 UDP 端口的使用情况。

本命令配置成功后，NMS 需要使用新端口重新连接设备后，才能进行 Get/Set 等操作。

【举例】

配置 SNMP 服务的侦听端口号为 5555。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent port 5555
```

【相关命令】

- **display udp verbose**（三层技术-IP 业务/IP 性能优化）

1.1.26 snmp-agent remote

snmp-agent remote 命令用来配置远端 SNMP 实体的引擎 ID。

undo snmp-agent remote 命令用来取消已配置的远端 SNMP 实体的引擎 ID。

【命令】

```
snmp-agent remote { ipv4-address | ipv6 ipv6-address } [ vpn-instance  
vpn-instance-name ] engineid engineid
```

```
undo snmp-agent remote ip-address
```

【缺省情况】

未配置远端 SNMP 实体的引擎 ID。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-address: 远端 SNMP 实体的 IP 地址。

ipv6 ipv6-address: 远端 SNMP 实体的 IPv6 地址。

vpn-instance vpn-instance-name: 指定远端 SNMP 实体所属的 VPN 实例。
vpn-instance-name 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示远端 SNMP 实体位于公网中。

engineid: 引擎 ID, 必须为偶数个十六进制数, 偶数的取值范围为 10~64, 不区分大小写。全 0 和全 F 均被认为是无效参数。

【使用指导】

当设备需要向 NMS 发送 SNMPv3 Inform 报文时, 必须配置该命令, 并将 **ip-address** 配置为 NMS 的 IP 地址, **engineid** 配置为 NMS 的引擎 ID。因为协议要求 SNMPv3 Inform 报文中必须携带一个权威引擎 ID, NMS 收到该报文后, 会用自己的引擎 ID 和这个权威引擎 ID 比较, 如果相同, 才能接收。

用户最多可以配置 20 个远端 SNMP 实体引擎 ID。

【举例】

配置 IP 地址为 10.1.1.1 的 SNMP 实体的引擎 ID 为 123456789A。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A
```

【相关命令】

- **display snmp-agent remote**

1.1.27 snmp-agent sys-info contact

snmp-agent sys-info contact 命令用来配置设备的维护联系信息。

undo snmp-agent sys-info contact 命令用来恢复缺省情况。

【命令】

snmp-agent sys-info contact sys-contact

undo snmp-agent sys-info contact

【缺省情况】

设备的维护联系信息为 Beijing UNIS Hengyue Technologies Co., Ltd.

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

sys-contact: 描述系统维护联系信息, 为 1~255 个字符的字符串, 区分大小写。

【使用指导】

如果设备发生故障, 设备维护人员可以利用系统维护联系信息, 及时与设备生产厂商取得联系。

【举例】

```
# 配置设备的维护联系信息为 Dial System Operator # 27345。
<Sysname> system-view
[Sysname] snmp-agent sys-info contact Dial System Operator # 27345
```

【相关命令】

- **display snmp-agent sys-info**

1.1.28 snmp-agent sys-info location

snmp-agent sys-info location 命令用来配置设备的物理位置信息。

undo snmp-agent sys-info location 命令用来恢复缺省情况。

【命令】

```
snmp-agent sys-info location sys-location
undo snmp-agent sys-info location
```

【缺省情况】

物理位置信息为 Beijing, China。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

sys-location: 设备的物理位置信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

为便于识别和管理设备，请使用该命令将设备所处的物理位置记录在设备中。

【举例】

```
# 配置设备的物理位置信息为 Room524-row1-3。
<Sysname> system-view
[Sysname] snmp-agent sys-info location Room524-row1-3
```

【相关命令】

- **display snmp-agent sys-info**

1.1.29 snmp-agent sys-info version

snmp-agent sys-info version 命令用来配置设备支持的 SNMP 版本。

undo snmp-agent sys-info version 命令用来取消对指定 SNMP 版本的支持。

【命令】

```
snmp-agent sys-info version { all | { v1 | v2c | v3 } * }
undo snmp-agent sys-info version { all | { v1 | v2c | v3 } * }
```

【缺省情况】

启用 SNMPv3 版本。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

all: 支持 SNMPv1、SNMPv2c 和 SNMPv3 版本。

v1: 支持 SNMPv1 版本。

v2c: 支持 SNMPv2c 版本。

v3: 支持 SNMPv3 版本。

【使用指导】

支持指定的 SNMP 版本后，设备才能收发该版本的 SNMP 报文。只有 NMS 和 Agent 使用的 SNMP 版本相同，NMS 才能和 Agent 建立连接。

如果在 IPv6 环境下，要使用 SNMP 告警功能，请将 SNMP 版本号配置为 **v2c** 或者 **v3**。

【举例】

配置设备支持 SNMPv3 版本。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent sys-info version v3
```

【相关命令】

- **display snmp-agent sys-info**

1.1.30 snmp-agent target-host

snmp-agent target-host 命令用来配置接收 SNMP 告警信息的目的主机（能够解析 Trap 和 Inform 报文的设备，通常为 NMS）的属性。

undo snmp-agent target-host 命令用来取消目的主机配置。

【命令】

```
snmp-agent target-host inform address udp-domain { ipv4-target-host | ipv6 ipv6-target-host } [udp-port port-number] [vpn-instance vpn-instance-name] params securityname security-string { v2c | v3 [authentication | privacy] }  
snmp-agent target-host trap address udp-domain { ipv4-target-host | ipv6 ipv6-target-host } [udp-port port-number] [vpn-instance vpn-instance-name] params securityname security-string [v1 | v2c | v3 [authentication | privacy]]  
undo snmp-agent target-host { trap | inform } address udp-domain { ipv4-target-host | ipv6 ipv6-address } params securityname security-string [vpn-instance vpn-instance-name]
```

【缺省情况】

未配置告警主机。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

inform: 配置接收 Inform 报文的目的主机的参数。

trap: 配置接收 Trap 报文的目的主机的参数。

address: 指定接收告警信息的目的主机的地址。

udp-domain: 指定使用 UDP 协议来传输 SNMP 告警信息。

ipv4-target-host: 接收告警信息的目的主机的 IPv4 地址或主机名，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。若使用主机名配置，发送时将获取主机名对应的 IPv4 地址，向对应的主机发送告警信息。

ipv6 ipv6-target-host: 接收告警信息的目的主机的 IPv6 地址或主机名，主机名为 1~253 个字符的字符串，不区分大小写，字符串仅可包含字母、数字、“-”、“_”或“.”。若使用主机名配置，发送时将获取主机名对应的 IPv6 地址，向对应的主机发送告警信息。若使用 IPv6 地址配置，则不能为链路本地地址。

udp-port port-number: 指定目的主机上用来接收告警信息的端口号，缺省值为 162。

vpn-instance vpn-instance-name: 指定目的主机所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示目的主机位于公网中。

params securityname security-string: 指定认证的参数，*security-string* 为 SNMPv1、SNMPv2c 的团体名或 SNMPv3 的用户名，为 1~32 个字符的字符串，区分大小写。

v1: SNMPv1 版本。

v2c: SNMPv2c 版本。

v3: SNMPv3 版本。

authentication: 指明对报文进行认证但不加密。认证功能用来验证报文的完整性或报文是否被篡改等，认证密码在创建 SNMPv3 用户时配置。

privacy: 指明对报文进行认证和加密。加密是对报文的数据部分进行加密处理以防信息被窃取，认证密码和加密密码在创建 SNMPv3 用户时配置。

【使用指导】

根据实际组网需要，用户可以多次使用该命令配置不同的目的主机的属性，使得设备可以向多个 NMS 发送告警信息。

不指定 **udp-port port-number** 参数时，使用的端口号为 162。162 是 SNMP 协议规定的 NMS 接收告警信息的端口，通常情况下（比如使用 iMC 或者 MIB Browser 作为 NMS 时），使用该缺省值即可。如果要将该参数修改为其它值，则必须和 NMS 上的配置保持一致。

不指定 **v1**、**v2c**、**v3** 版本参数时，使用的版本是 v1。设备配置的 SNMP 版本必须和 NMS 上运行的 SNMP 版本一致，否则，NMS 将收不到告警信息。

不指定 **authentication** 和 **privacy** 参数时，使用的是不认证不加密的安全级别。

【举例】

允许向 10.1.1.1 发送 SNMPv3 Trap 报文，用户名为 public。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent trap enable standard
```

```
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public v3
```

【相关命令】

- **snmp-agent { inform | trap } source**
- **snmp-agent trap enable**
- **snmp-agent trap life**

1.1.31 snmp-agent trap enable

snmp-agent trap enable 命令用来开启 SNMP 告警功能。

undo snmp-agent trap enable 命令用来关闭 SNMP 告警功能。

【命令】

```
snmp-agent trap enable [ configuration | protocol | standard [ authentication  
| coldstart | linkdown | linkup | warmstart ] * | system ]
```

```
undo snmp-agent trap enable [ configuration | protocol | standard  
[ authentication | coldstart | linkdown | linkup | warmstart ] * | system ]
```

【缺省情况】

SNMP 配置告警、标准告警和系统告警功能处于开启状态，其他各模块告警功能是否开启请参见各模块手册。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

configuration: SNMP 配置告警信息。配置该参数后，系统会以 10 分钟为周期，查看周期内当前运行配置或者启动配置是否被修改，以及是否有用户对启动配置文件进行修改，并将最后一次修改形成一条告警输出。

protocol: 开启指定协议模块的 SNMP 告警功能。用户可通过执行 **snmp-agent trap enable ?** 命令来获取该参数的取值，有关此参数的详细介绍，请参见各模块的命令手册。

standard: SNMP 标准告警信息。包括以下五种：

- **authentication:** NMS 访问设备时认证失败，输出 SNMP 认证失败的告警信息。
- **coldstart:** 当设备重新启动时，输出设备冷启动告警信息。
- **linkdown:** 当接口的链路 down 时，输出 linkDown 告警信息。
- **linkup:** 当接口的链路 up 时，输出 linkUp 告警信息。

- **warmstart:** 当 SNMP 模块重新启动时，输出热启动告警信息。
- system:** SNMP 系统告警信息。配置该参数后，如果系统时间被修改、系统重启或系统主用启动软件包不可用，均会生成告警信息。

【使用指导】

对于协议模块的 SNMP 告警功能，需要先使能相关协议，本命令才能配置成功。

如果在 IPv6 环境下，要使用 SNMP 告警功能，请将 SNMP 版本号配置为 **v2c** 或者 **v3**。

开启指定协议模块的告警功能后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

不指定可选参数时，表示在全局下开启/关闭所有可选模块的告警功能。

【举例】

开启 SNMP 认证失败的告警功能。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent trap enable standard authentication
```

【相关命令】

- **snmp-agent target-host**
- **snmp-agent sys-info version**

1.1.32 snmp-agent trap if-mib link extended

snmp-agent trap if-mib link extended 命令用来对标准格式的 linkUp 或 linkDown 告警信息进行私有扩展。

undo snmp-agent trap if-mib link extended 命令用来恢复缺省情况。

【命令】

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

【缺省情况】

系统发送的 linkUp/linkDown 告警信息的格式为标准格式，不对其进行私有扩展。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

扩展格式的 linkUp/linkDown 告警信息由标准格式的 linkUp/linkDown 告警信息后增加接口描述和接口类型信息构成，使用扩展格式的告警信息有助于网络管理员快速定位问题。

需要注意的是，配置该命令后，设备发送的 linkUp/linkDown 告警信息为扩展格式的信息。如果 NMS 不支持扩展格式，可能会无法解析信息。

【举例】

```
# 对标准格式的 linkUp/linkDown 告警信息进行私有扩展。  
<Sysname> system-view  
[Sysname] snmp-agent trap if-mib link extended
```

1.1.33 snmp-agent trap life

snmp-agent trap life 命令用来配置告警信息的保存时间。

undo snmp-agent trap life 命令用来恢复缺省情况。

【命令】

```
snmp-agent trap life seconds  
undo snmp-agent trap life
```

【缺省情况】

SNMP 告警信息的保存时间为 120 秒。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

seconds: 超时时间，取值范围为 1～2592000，单位为秒。

【使用指导】

SNMP 模块使用队列来发送告警信息，告警信息进入消息发送队列时会启动一个存活定时器。如果直到定时器超时（即达到 **snmp-agent trap life** 命令配置的时间），告警信息还没有被发送出去，系统就会将该告警信息从发送队列中删除。

【举例】

```
# 配置告警信息的保存时间为 60 秒。  
<Sysname> system-view  
[Sysname] snmp-agent trap life 60
```

【相关命令】

- **snmp-agent trap enable**
- **snmp-agent target-host**
- **snmp-agent trap queue-size**

1.1.34 snmp-agent trap log

snmp-agent trap log 命令用来开启 SNMP 告警日志功能。

undo snmp-agent trap log 命令用来关闭 SNMP 告警日志功能。

【命令】

```
snmp-agent trap log
```

undo snmp-agent trap log

【缺省情况】

SNMP 告警日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

打开 SNMP 告警日志开关，Agent 向 NMS 发送告警时，Agent 会向信息中心模块发送一条日志来记录该告警相关的信息。通过配置信息中心的参数，最终决定 SNMP 告警日志的输出规则（即是否允许输出以及输出方向）。

【举例】

```
# 开启 SNMP 告警日志功能。  
<Sysname> system-view  
[Sysname] snmp-agent trap log
```

1.1.35 snmp-agent trap queue-size

snmp-agent trap queue-size 命令用来配置告警信息发送队列的长度。

undo snmp-agent trap queue-size 命令用来恢复缺省情况。

【命令】

snmp-agent trap queue-size size

undo snmp-agent trap queue-size

【缺省情况】

告警信息的发送队列最多可以存储 100 条告警信息。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

size：消息队列中可以存储的告警信息的数目，取值范围 1~1000。

【使用指导】

告警信息产生后，会进入告警信息消息队列进行发送，告警信息消息队列的长度决定了队列最多可以存储的告警信息的数目。

如果在告警信息发送队列满时系统又收到了新的告警信息，则系统会丢弃新收到的告警信息。

如果用户修改队列长度，导致队列中告警信息数量超过告警信息发送队列的长度，系统会丢弃较老的告警信息。

【举例】

```
# 配置发送告警信息的消息队列最多可以存储 200 条告警信息。
<Sysname> system-view
[Sysname] snmp-agent trap queue-size 200
```

【相关命令】

- **snmp-agent trap enable**
- **snmp-agent target-host**
- **snmp-agent trap life**

1.1.36 snmp-agent usm-user { v1 | v2c }

snmp-agent usm-user { v1 | v2c } 命令用来创建 SNMPv1 或 SNMPv2c 用户。
undo snmp-agent usm-user { v1 | v2c } 命令用来删除 SNMPv1 或 SNMPv2c 用户。

【命令】

```
snmp-agent usm-user { v1 | v2c } user-name group-name [ acl { ipv4-acl-number |
name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *
undo snmp-agent usm-user { v1 | v2c } user-name
```

【缺省情况】

不存在 SNMP 用户。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

v1: 表示配置的用户名适用于 SNMPv1 组网环境。

v2c: 表示配置的用户名适用于 SNMPv2c 组网环境。

user-name: 用户名，为 1~32 个字符的字符串，区分大小写。

group-name: 该用户对应组的名称，取值范围为 1~32 个字符的字符串，区分大小写。创建用户时，组可以不存在。但要使创建的用户生效，必须先创建组。

acl: 将用户名与基本/高级 IPv4 ACL 绑定。

ipv4-acl-number: 表示基本或高级 IPv4 ACL 的编号，其中基本 IPv4 ACL 的取值范围为 2000~2999，高级 IPv4 ACL 的取值范围为 3000~3999。

name ipv4-acl-name: 表示基本或高级 IPv4 ACL 的名称，为 1~63 个字符的字符串，不区分大小写。

acl ipv6: 将用户名与基本/高级 IPv6 ACL 绑定。

ipv6-acl-number: 表示基本或高级 IPv6 ACL 的编号，其中基本 IPv6 ACL 的取值范围为 2000~2999，高级 IPv6 ACL 的取值范围为 3000~3999。

name ipv6-acl-name: 表示基本或高级 IPv6 ACL 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

为了安全起见，只有具有 **network-admin**、**context-admin** 或者 **level-15** 用户角色的用户登录设备后才能执行本命令。其它角色的用户，即使授权了 **SNMP** 特性或本命令的操作权限，也不能执行本命令。

SNMPv1 和 **SNMPv2c** 组网应用中 **NMS** 和 **Agent** 之间使用团体名来认证，**SNMPv3** 组网应用中使用用户名来认证。

用户有两种方式创建团体：

- 使用 **snmp-agent community** 命令来创建团体。
- 配置 **snmp-agent usm-user { v1 | v2c }** 和 **snmp-agent group { v1 | v2c }** 命令成功创建 **SNMPv1** 或 **SNMPv2c** 用户以及相应的组后，系统会以用户名为团体名自动创建一个团体。该团体的访问权限可通过 **snmp-agent community** 或 **snmp-agent group { v1 | v2c }** 命令来修改，最后一次执行的命令生效。

display snmp-agent community 会显示这两种方式创建的、以明文方式配置并以明文方式保存到配置文件中的团体的信息。

创建 **SNMP** 组和用户的时候都可以使用 **acl** 参数限制非法 **NMS** 访问设备，只有两个 **ACL** 均允许的 **NMS** 才能访问设备。在创建组或用户时，**ACL** 均遵循以下规则：

- 当未引用 **ACL**、引用的 **ACL** 不存在、或者引用的 **ACL** 下没有配置规则时，允许所有 **NMS** 访问设备。
- 当引用的 **ACL** 下配置了规则时，则只有规则中 **permit** 的 **NMS** 才能访问设备，其他 **NMS** 不允许访问设备。

【举例】

在 **SNMP** 组 **readCom** 里创建 **SNMPv2c** 用户 **userv2c**。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom
```

如果 **NMS** 需要访问 **Agent**，则应将 **NMS** 的版本号指定为 **SNMPv2c**，**Read community** 选项填写为 **userv2c**。

在 **SNMP** 组 **readCom** 里创建 **SNMPv2c** 用户 **userv2c**，并且只允许 IP 地址为 **1.1.1.1** 的 **NMS** 使用该用户名访问 **Agent**，禁止其它 **NMS** 使用该用户名访问。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl 2001
```

在 **SNMP** 组 **readCom** 里创建 **SNMPv2c** 用户 **userv2c**，并且只允许 IP 地址为 **1.1.1.2** 的 **NMS** 使用该用户名访问 **Agent**，禁止其它 **NMS** 使用该用户名访问。

```
[Sysname] acl basic name testacl
[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0
[Sysname-acl-ipv4-basic-testacl] rule deny source any
[Sysname-acl-ipv4-basic-testacl] quit
```

```
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl name testacl
```

【相关命令】

- **snmp-agent group**
- **snmp-agent community**
- **display snmp-agent community**

1.1.37 snmp-agent usm-user v3

snmp-agent usm-user v3 命令用来创建 SNMPv3 用户。

undo snmp-agent usm-user v3 命令用来删除 SNMPv3 用户。

【命令】

- VACM 方式:

```
snmp-agent usm-user v3 user-name group-name [ remote { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] ] [ { cipher | simple } authentication-mode { md5 | sha } auth-password [ privacy-mode { 3des | aes128 | des56 } priv-password ] ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *  

undo snmp-agent usm-user v3 user-name { local | engineid engineid-string | remote { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] }
```
- RBAC 方式:

```
snmp-agent usm-user v3 user-name user-role role-name [ remote { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] ] [ { cipher | simple } authentication-mode { md5 | sha } auth-password [ privacy-mode { 3des | aes128 | des56 } priv-password ] ] [ acl { ipv4-acl-number | name ipv4-acl-name } | acl ipv6 { ipv6-acl-number | name ipv6-acl-name } ] *  

undo snmp-agent usm-user v3 user-name { local | engineid engineid-string | remote { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ] }
```

【缺省情况】

不存在 SNMPv3 用户。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

user-name: 用户名，为 1~32 个字符的字符串，区分大小写。

group-name: 该用户对应组的名称, 取值范围为 1~32 个字符的字符串, 区分大小写。创建用户时, 组可以不存在。但要使创建的用户生效, 必须先创建组。

user-role role-name: 该用户对应的角色名称, **role-name** 为 1~63 个字符的字符串, 区分大小写。

remote { ipv4-address | ipv6 ipv6-address }: 接收 Inform 报文的目的主机的 IPv4 地址或者 IPv6 地址, 通常为 NMS 的 IPv4 地址或者 IPv6 地址。当设备需要向目的主机发送 SNMPv3 Inform 报文时, 该参数必须配置, 还需要使用 **snmp-agent remote** 命令将目的主机的 IPv4 地址或者 IPv6 地址和引擎 ID 绑定。

vpn-instance vpn-instance-name: 目的主机所属的 VPN 实例。**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示目的主机位于公网中。

cipher: 以密文方式配置认证密码和加密密码。该密码将转换成对应的密文摘要存储在设备中。

simple: 以明文方式配置认证密码和加密密码。该密码将转换成对应的密文摘要存储在设备中。

authentication-mode: 指定认证算法。不指定该参数时, 表示不认证。取值为:

- **md5**: 采用 HMAC-MD5 算法。
- **sha**: 采用 HMAC-SHA1 算法。

auth-password: 表示认证密码, 区分大小写, 具体要求如下:

- 以明文方式配置时, **auth-password** 表示明文认证密码。认证密码的长度范围是 1~64 个字符。
- 以密文方式配置时, **auth-password** 表示密文认证密码, 该密码可通过 **snmp-agent calculate-password** 命令计算获得。

privacy-mode: 指定加密算法。不指定该参数时, 表示不加密。取值为:

- **3des**: 采用 3DES (Triple Data Encryption Standard, 三重数据加密标准) 算法, 密钥长度为 168 比特。
- **aes128**: 采用 AES (Advanced Encryption Standard, 高级加密标准) 算法, 密钥长度为 128 比特。
- **des56**: 采用 DES (Data Encryption Standard, 数据加密标准) 算法, 密钥长度为 56 比特。

priv-password: 表示加密密码, 区分大小写, 具体要求如下:

- 以明文方式配置时, **auth-password** 表示明文加密密码。密码的长度范围是 1~64 个字符。
- 以密文方式配置时, **auth-password** 表示密文加密密码, 该密码可通过 **snmp-agent calculate-password** 命令计算获得。

acl: 将用户名与基本/高级 IPv4 ACL 绑定。

ipv4-acl-number: 表示基本或高级 IPv4 ACL 的编号, 其中基本 IPv4 ACL 的取值范围为 2000~2999, 高级 IPv4 ACL 的取值范围为 3000~3999。

name ipv4-acl-name: 表示基本或高级 IPv4 ACL 的名称, 为 1~63 个字符的字符串, 不区分大小写。

acl ipv6: 将用户名与基本/高级 IPv6 ACL 绑定。

ipv6-acl-number: 表示基本或高级 IPv6 ACL 的编号, 其中基本 IPv6 ACL 的取值范围为 2000~2999, 高级 IPv6 ACL 的取值范围为 3000~3999。

name ipv6-acl-name: 表示基本或高级 IPv6 ACL 的名称, 为 1~63 个字符的字符串, 不区分大小写。

local: 表示本地实体引擎 ID。缺省情况下, 创建的 SNMPv3 用户与本地 SNMP 实体引擎相关联。

engineid engineid-string: 指定与该用户相关联的引擎 ID 字符串, 必须为偶数个十六进制数, 偶数的取值范围为 10~64, 不区分大小写。全 0 和全 F 均被认为是无效参数。由于 SNMPv3 版本的用户名、密文密码等都和引擎 ID 相关联, 如果更改了引擎 ID, 则原引擎 ID 下配置的用户名、密码失效, 更改后可以使用该参数将 **engineid-string** 指定为创建该用户时的本地引擎 ID 来删除失效用户名。

【使用指导】

为了安全起见, 只有具有 **network-admin**、**context-admin** 或者 **level-15** 用户角色的用户登录设备后才能执行本命令。其它角色的用户, 即使授权了 SNMP 特性或本命令的操作权限, 也不能执行本命令。

创建 SNMPv3 用户时, 可以通过两种配置方式来控制用户访问的权限:

- 通过 VACM 方式配置的 SNMP 用户依附于 SNMP 组, 创建用户时, 请先创建组。否则, 用户能够创建成功但是不生效。一个组可以包含多个用户。组定义了用户能够访问的 SNMP 对象 (通过 MIB 视图来限定) 以及是否进行认证和加密等, 而认证和加密的具体算法和密码则是在创建用户时定义。
- 通过 RBAC 方式配置的 SNMP 用户依附于用户角色, 创建用户时, 通过 **user-role role-name** 参数配置用户的角色。用户角色定义了 SNMP 用户能够访问的 SNMP 对象以及操作类型 (通过 **rule** 规则来限定)。使用 RBAC 方式创建 SNMP v3 用户后, 还可以使用 **snmp-agent usm-user v3 user-role** 命令为该用户绑定更多的用户角色, 最多可绑定 64 个用户角色。

推荐使用 RBAC 配置方式, 安全性更高。

通过 VACM 和 RBAC 方式配置 SNMP 用户时, 需要注意:

- 通过 VACM 方式配置 SNMP 用户时, 当用户名相同, 多次执行本命令, 最后一次执行的命令生效。
- 通过 RBAC 方式配置 SNMP 用户时, 可以多次使用本命令为已创建的 SNMPv3 用户添加角色, 若未配置其他参数, 则其他配置不变, 只添加角色; 若同时配置其他参数 (如认证方式), 则为用户添加角色, 同时修改其他配置。

创建 SNMP 组和用户的时候都可以使用 **acl** 参数限制非法 NMS 访问设备, 只有两个 ACL 均允许的 NMS 才能访问设备。在创建组或用户时, ACL 均遵循以下规则:

- 当未引用 ACL、引用的 ACL 不存在、或者引用的 ACL 下没有配置规则时, 允许所有 NMS 访问设备。
- 当引用的 ACL 下配置了规则时, 则只有规则中 **permit** 的 NMS 才能访问设备, 其他 NMS 不允许访问设备。

【举例】

VACM 方式: 为 v3 组 testGroup 加入一个用户 testUser, 安全级别为只认证不加密, 认证算法为 HMAC-SHA1, 认证密码为明文 123456TESTplat&!。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent group v3 testGroup authentication
```

```
[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha 123456TESTplat&!
```

在 NMS 上配置: 版本号为 SNMPv3, 用户名为 testUser, 认证算法为 HMAC-SHA1, 认证密码为 123456TESTplat&!, 建立连接, 就可以对设备上缺省视图内的 MIB 对象进行访问了。

VACM 方式：为 v3 组 testGroup 加入一个用户 testUser，安全级别为认证和加密，认证算法为 HMAC-SHA1、加密算法为 AES，认证密码为明文 123456TESTauth&！，加密密码为明文 123456TESTencr&！。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent group v3 testGroup privacy
```

```
[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha 123456TESTauth&！ privacy-mode aes128 123456TESTencr&！
```

在 NMS 上配置：版本号为 SNMPv3，用户名为 testUser，认证算法为 HMAC-SHA1，认证密码为 123456TESTauth&！，加密算法为 AES，加密密码为 123456TESTencr&！，建立连接，就可以对设备上缺省视图内的 MIB 对象进行访问了。

VACM 方式：为 v3 组 testGroup 加入一个与 IP 为 10.1.1.1 的远端 SNMP 实体引擎相关联的 SNMPv3 用户 remoteUser，安全级别为认证和加密，认证算法为 HMAC-SHA1、加密算法为 AES，认证密码为明文 123456TESTauth&！，加密密码为明文 123456TESTencr&！。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A
```

```
[Sysname] snmp-agent group v3 testGroup privacy
```

```
[Sysname] snmp-agent usm-user v3 remoteUser testGroup remote 10.1.1.1 simple authentication-mode sha 123456TESTauth&！ privacy-mode aes128 123456TESTencr&！
```

RBAC 方式：创建一个新的 SNMPv3 用户 testUser，角色为 network-operator，安全级别为只认证不加密，认证算法为 HMAC-SHA1，认证密码为明文 123456TESTplat&！。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent usm-user v3 testUser user-role network-operator simple authentication-mode sha 123456TESTplat&！
```

在 NMS 上配置：版本号为 SNMPv3，用户名为 testUser，认证算法为 HMAC-SHA1，认证密码为 123456TESTplat&！，建立连接，就可以对设备上所有 MIB 对象进行只读操作。

【相关命令】

- **display snmp-agent usm-user**
- **snmp-agent group**
- **snmp-agent calculate-password**
- **snmp-agent remote**
- **snmp-agent usm-user v3 user-role**

1.1.38 snmp-agent usm-user v3 user-role

snmp-agent usm-user v3 user-role 命令用来为通过 RBAC 方式创建的 SNMPv3 用户添加角色。

undo snmp-agent usm-user user-role 命令用来为 SNMPv3 用户删除角色。

【命令】

```
snmp-agent usm-user v3 user-name user-role role-name
```

```
undo snmp-agent usm-user v3 user-name user-role role-name
```

【缺省情况】

使用创建 SNMPv3 用户时指定的角色。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

user-name: 用户名，为 1~32 个字符的字符串，区分大小写。

user-role role-name: 该用户对应的角色名称，**role-name** 为 1~63 个字符的字符串，区分大小写。

【使用指导】

一个 RBAC 方式配置的 SNMPv3 用户可配置多个用户角色。用户可以通过本命令来为通过 RBAC 方式创建的 SNMPv3 用户添加与删除角色，最多可以配置 64 个有效的用户角色且至少保留一个用户角色。

【举例】

已创建 SNMPv3 用户 testUser 拥有 network-operato 用户角色，现为用户 testUser 添加 network-admin 用户角色。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent usm-user v3 testUser user-role network-admin
```

【相关命令】

- **snmp-agent usm-user v3**

目 录

1 RMON.....	1-1
1.1 RMON配置命令	1-1
1.1.1 display rmon alarm.....	1-1
1.1.2 display rmon event.....	1-2
1.1.3 display rmon eventlog.....	1-3
1.1.4 display rmon history	1-5
1.1.5 display rmon prialarm	1-7
1.1.6 display rmon statistics.....	1-8
1.1.7 rmon alarm.....	1-10
1.1.8 rmon event.....	1-12
1.1.9 rmon history	1-13
1.1.10 rmon prialarm.....	1-14
1.1.11 rmon statistics	1-16

1 RMON

1.1 RMON配置命令

1.1.1 display rmon alarm

display rmon alarm 命令用来显示 RMON 告警表项的相关信息。

【命令】

display rmon alarm [*entry-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

entry-number: 告警表项的索引号，取值范围为 1~65535。如果不指定索引号，则显示所有告警表项的相关信息。

【举例】

```
# 显示所有 RMON 告警表项的相关信息。
<Sysname> display rmon alarm
AlarmEntry 1 owned by user1 is VALID.
  Sample type           : absolute
  Sampled variable      : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval (in seconds) : 10
  Rising threshold      : 50(associated with event 1)
  Falling threshold     : 5(associated with event 2)
  Alarm sent upon entry startup : risingOrFallingAlarm
  Latest value          : 0
```

表1-1 display rmon alarm 命令显示信息描述表

字段	描述
AlarmEntry <i>entry-number</i> owned by <i>owner</i> is <i>status</i> .	<i>owner</i>创建的告警表项<i>entry-number</i>的当前状态为<i>status</i> <i>entry-number</i>: 告警表项 <i>owner</i>: 该表项创建者 <i>status</i>: 与该索引对应的告警表项的状态（VALID 表示有效，UNDERCREATION 表示无效。处于无效状态的表项使用 display rmon alarm 命令可以查看到，但使用 display current-configuration 和 display this 看不到对应的 rmon alarm 配置命令）。命令行配置告警表项时不可配且缺省为 VALID

字段	描述
Sample type	采样类型，取值为： absolute: 绝对值采样 delta: 变化值采样
Sampled variable	告警变量，即被监控的MIB节点
Sampling interval	采样的时间间隔，单位为秒
Rising threshold	上限阈值（当采样值大于等于该值时引发上限告警）
associated with event	告警对应的事件索引
Falling threshold	下限阈值（当采样值小于等于该值时引发下限告警）
Alarm sent upon entry startup	初次触发告警类型： risingAlarm: 表示触发上限告警 fallingAlarm: 表示触发下限告警 risingorFallingAlarm: 表示触发上限或下限告警 缺省情况下，触发risingorFallingAlarm类型告警
Latest value	最近一次采样值

【相关命令】

- rmon alarm**

1.1.1.2 display rmon event

display rmon event 命令用来显示 RMON 事件表项相关信息。

【命令】

display rmon event [*entry-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

entry-number: 事件表项的索引号，取值范围为 1~65535。如果不指定索引号，则显示所有事件表项的相关信息。

【使用指导】

显示信息包括：事件表中的事件索引、事件的所有者、对事件的描述、事件引发的动作（日志或告警信息）、最近一次事件发生的时刻（此时间是以系统初始化/启动以来的秒数计算的）等。

【举例】

显示所有 RMON 事件表项相关信息。

```
<Sysname> display rmon event
```

EventEntry 1 owned by user1 is VALID.

Description: N/A

Community: Security

Take the action log-trap when triggered, last triggered at 0days 00h:02m:27s uptime.

表1-2 display rmon event 命令显示信息描述表

字段	描述
EventEntry <i>entry-number</i> owned by <i>owner</i> is <i>status</i> .	Owner创建的事件表项<i>entry-number</i>的当前状态为<i>status</i> • <i>entry-number</i>: 事件表项 • <i>owner</i>: 该表项创建者 • <i>status</i>: 与该索引对应的事件表项的状态 (VALID 表示有效, UNDERCREATION 表示无效。处于无效状态的表项使用 display rmon event 命令可以查看到, 但使用 display current-configuration 和 display this 看不到对应的 rmon event 配置命令)。命令行配置 event 表项时不可配且默认为 VALID
Description	该事件表项的描述
Community	接收告警信息的网管站的团体名
Take the action <i>action</i> when triggered	事件触发时采取的动作: • none: 表示不采取任何措施 • log: 表示事件被触发时会记录日志 • trap: 表示事件被触发时会生成告警信息发送给设备的 SNMP 模块 • log-trap: 表示事件被触发时既会记录日志又会生成告警信息发送给设备的 SNMP 模块
last triggered at <i>time</i> uptime	最近一次事件发生的时间 (设备启动以来的时间)

【相关命令】

- **rmon event**

1.1.3 display rmon eventlog

display rmon eventlog 命令用来显示事件日志表项的相关信息。

【命令】

```
display rmon eventlog [entry-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

entry-number: 事件表项的索引号, 取值范围为 1~65535。如果不指定索引号, 则显示所有事件的日志表项的相关信息。

【使用指导】

如果使用 **rmon event** 命令指定某表项的动作包括记录日志, 当该事件被触发时, 就会在 RMON 事件日志表中记录一条该事件的日志。通过该命令可以显示事件日志表的具体内容: 事件表中的事件索引及事件当前的状态、事件产生日志的时刻 (此时间是以系统初始化/启动以来的秒数计算的) 以及事件的描述等。

每个事件最多有 10 条日志。超过 10 条日志后, 新日志将覆盖最早的日志。

【举例】

查看由告警表产生的 RMON 事件 99 的日志。

```
<Sysname> display rmon eventlog 99
```

```
EventEntry 99 owned by ww is VALID.
```

```
LogEntry 99.1 created at 50days 08h:54m:44s uptime.
```

```
Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,  
uprise 16760000 with alarm value 16776314. Alarm sample type is absolute.
```

```
LogEntry 99.2 created at 50days 09h:11m:13s uptime.
```

```
Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,  
less than(or =) 20000000 with alarm value 16951648. Alarm sample type is absolute.
```

```
LogEntry 99.3 created at 50days 09h:18m:43s uptime.
```

```
Description: The alarm formula defined in prialarmEntry 777,  
less than(or =) 15000000 with alarm value 14026493. Alarm sample type is absolute.
```

```
LogEntry 99.4 created at 50days 09h:23m:28s uptime.
```

```
Description: The alarm formula defined in prialarmEntry 777,  
uprise 17000000 with alarm value 17077846. Alarm sample type is absolute.
```

以上举例表明事件 99 产生的告警事件日志, 其中告警表产生的事件日志 2 条, 扩展告警表产生的事件日志 2 条:

- 日志 99.1 由告警表项 77 触发生成, 原因是告警值(16776314)超过了上限阈值(16760000), 采样类型为绝对值采样。
- 日志 99.2 由告警表项 77 触发生成, 原因是告警值(16951648)低于下限阈值(20000000), 采样类型为绝对值采样。
- 日志 99.3 由扩展告警表项 777 触发生成, 原因是告警值(14026493)低于下限阈值(15000000), 采样类型为绝对值采样。
- 日志 99.4 由扩展告警表项 777 触发生成, 原因是告警值(17077846)超过上限阈值(17000000), 采样类型为绝对值采样。

表1-3 display rmon eventlog 命令显示信息描述表

字段	描述
EventEntry entry-number owned by owner is status.	Owner创建的事件日志表项entry-number的当前状态为status - entry-number: 事件日志表项 - owner: 该表项创建者 - status: 与该索引对应的事件日志表项的状态（VALID 表示有效，UNDERCREATION 表示无效。处于无效状态的表项使用 display rmon eventlog 可以查看到，但使用 display current-configuration 和 display this 看不到对应的 rmon eventlog 配置命令）。命令行配置 event 表项时不可配且默认为 VALID
LogEntry entry-number created at created-time uptime.	日志表项entry-number的创建时间为created-time - entry-number: 日志表项索引号，表示方式为 logEventIndex.logIndex，logEventIndex 和 logIndex 为 MIB 节点 - created-time: 日志表项的创建时间
Description	该条日志的描述

【相关命令】

- rmon event

1.1.4 display rmon history

display rmon history 命令用来显示 RMON 历史控制表及历史采样信息。

【命令】

display rmon history [interface-type interface-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-type interface-number: 指定接口类型和接口编号。如果未指定本参数，则显示所有接口下配置的历史控制表及历史采样信息。

【使用指导】

在端口创建历史表项之后，系统会按一定的时间周期统计端口的信息，并将这些信息保存到 etherHistoryEntry 表，使用本命令可以显示该表项存储的记录。

可显示的历史采样信息的数目以及历史采样的间隔可以通过 **rmon history** 命令来设置。

【举例】

显示端口 GigabitEthernet1/0/1 的 RMON 历史控制表及历史采样信息。

```

<Sysname> display rmon history gigabitethernet 1/0/1
HistoryControlEntry 6 owned by user1 is VALID.
  Sampled interface      : GigabitEthernet1/0/1<ifIndex.117>
  Sampling interval      : 8(sec) with 3 buckets max
  Sampling record 1 :
    dropevents           : 0           , octets           : 5869
    packets              : 54          , broadcast packets : 9
    multicast packets    : 23          , CRC alignment errors : 0
    undersize packets    : 0           , oversize packets   : 0
    fragments           : 0           , jabbers            : 0
    collisions           : 0           , utilization         : 0

```

表1-4 display rmon history 命令显示信息描述表

字段	描述
HistoryControlEntry <i>entry-number</i> owned by <i>owner</i> is <i>status</i> .	<i>Owner</i>创建的历史控制表项<i>entry-number</i>的当前状态为<i>status</i> <i>entry-number</i>: 历史控制表项 <i>owner</i>: 该表项的创建者 <i>status</i>: 与该索引对应的历史控制表项的状态（VALID 表示有效，UNDERCREATION 表示无效。处于无效状态的表项使用 display rmon history 命令可以查看到，但使用 display current-configuration 和 display this 看不到对应的 rmon history 配置命令）。命令行配置 HistoryControl 表项时不可配置且默认为 VALID
Sampled Interface	被统计的接口
Sampling interval	统计周期，单位为秒，系统会按周期对端口的信息进行统计
buckets max	系统最多可保存的统计值的条数 - 如果在 rmon history 命令中指定的 buckets 的值超出了设备实际支持的历史表容量，则此处显示的是设备实际支持的历史表容量 - 如果当前保存的统计值条数已经到达了系统支持的最大值，则系统会删除最早的记录来保存新的统计值
Sampling record	历史采样表项索引号
dropevents	统计周期内检测到的丢包事件次数
octets	统计周期内接收到的字节数
packets	统计周期内接收到的包数
broadcast packets	统计周期内接收到的广播包数
multicast packets	统计周期内接收到的组播包数
CRC alignment errors	统计周期内接收到的校验错误的包数
undersize packets	统计周期内接收到的过小的包数 过小包指的是长度小于64字节的包（不包括帧标志位，包括FCS校验码）
oversize packets	统计周期内接收到的超大的包数 超大包指的是长度大于1518字节的包（不包括帧标志位，包括FCS校验码）
fragments	统计周期内接收到的过小且校验错误的包数

字段	描述
jabbers	统计周期内接收到的超大且校验错误的包数
collisions	统计周期内接收到的冲突的包数
utilization	统计周期内的带宽利用率（用百分比表示）

【相关命令】

- **rmon history**

1.1.5 display rmon prialarm

display rmon prialarm 命令用来显示扩展告警表项的相关信息。

【命令】

display rmon prialarm [*entry-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

entry-number: 扩展告警表项的索引，取值范围为 1~65535。如果不指定索引号，则显示所有扩展告警表项的相关信息。

【举例】

显示 RMON 所有的扩展告警表项的相关信息。

```
<Sysname> display rmon prialarm
PrialarmEntry 1 owned by user1 is VALID.
  Sample type           : absolute
  Variable formula       : (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
  Description           : ifUtilization.GigabitEthernet1/0/1
  Sampling interval (in seconds) : 10
  Rising threshold       : 80(associated with event 1)
  Falling threshold      : 5(associated with event 2)
  Alarm sent upon entry startup : risingOrFallingAlarm
  Entry lifetime         : forever
  Latest value           : 85
```

表1-5 display rmon prialarm 命令显示信息描述表

字段	描述
PrialarmEntry entry-number owned by owner is status.	Owner创建的扩展告警表项entry-number的当前状态为status - entry-number: 扩展告警表项 - owner: 该表项创建者 - status: 与该索引对应的扩展告警表项的状态（VALID 表示有效，UNDERCREATION 表示无效。处于无效状态的表项使用 display rmon prialarm 命令可以查看到，但使用 display current-configuration 和 display this 看不到相应的 rmon prialarm 配置命令）。命令行配置 prialarm 表项时不可配且默认为 VALID
Sample type	采样类型，取值为： - absolute: 绝对值采样 - delta: 变化值采样
Variable formula	样本变量的计算公式
Description	扩展告警表项的描述信息
Sampling interval	采样间隔，单位为秒，系统会按一定的时间间隔对采样变量进行绝对值采样或者变化值采样
Rising threshold	告警上限，当采样值大于等于该值时引发上限告警
Falling threshold	告警下限，当采样值小于等于该值时引发下限告警
associated with event	告警对应的事件索引
Alarm sent upon entry startup	初次触发告警类型： - risingAlarm: 表示触发上限告警 - fallingAlarm: 表示触发下限告警 - risingorFallingAlarm: 表示触发上限或下限告警 缺省情况下，触发risingorFallingAlarm类型告警
Entry lifetime	该扩展告警表项的存活时间，可以是永远存在，也可以是在规定的时间内存在
Latest value	最近一次采样值

【相关命令】

- rmon prialarm

1.1.6 display rmon statistics

display rmon statistics 命令用来显示 RMON 统计信息。

【命令】

display rmon statistics [interface-type interface-number]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

interface-type interface-number: 指定接口类型和接口编号。如果未指定本参数，则显示所有接口下配置的统计表及统计信息。

【使用指导】

本命令显示的是从端口创建统计表项到执行显示命令这段时间内端口的统计信息。设备重启时，会清除该统计信息。

【举例】

```
# 显示以太网接口 GigabitEthernet1/0/1 的 RMON 统计信息。
<Sysname> display rmon statistics gigabitethernet 1/0/1
EtherStatsEntry 1 owned by user1 is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets      : 43393306 , etherStatsPkts      : 619825
  etherStatsBroadcastPkts : 503581 , etherStatsMulticastPkts : 44013
  etherStatsUndersizePkts : 0 , etherStatsOversizePkts : 0
  etherStatsFragments    : 0 , etherStatsJabbers    : 0
  etherStatsCRCAlignErrors : 0 , etherStatsCollisions : 0
  etherStatsDropEvents (insufficient resources): 0
  Incoming packets by size:
  64 : 0 , 65-127 : 0 , 128-255 : 0
  256-511: 0 , 512-1023: 0 , 1024-1518: 0
```

表1-6 display rmon statistics 命令显示信息描述表

字段	描述
EtherStatsEntry entry-number owned by owner is status.	Owner创建的统计信息表项entry-number的当前状态为status - entry-number: 统计信息表项 - owner: 该表项创建者 - status: 与该索引对应的统计表项的状态（VALID 表示有效，UNDERCREATION 表示无效。处于无效状态的表项使用 display rmon statistics 命令可以查看到，但使用 display current-configuration 和 display this 看不到对应的 rmon statistics 配置命令）。命令行配置 statistics 表项时不可配且默认为 VALID
Interface	被统计端口
etherStatsOctets	统计时间内，端口收到的所有报文的字节数
etherStatsPkts	统计时间内，端口收到的所有报文的包数
etherStatsBroadcastPkts	统计时间内，端口收到的所有广播包的数量
etherStatsMulticastPkts	统计时间内，端口收到的所有组播包的数量

字段	描述
etherStatsUndersizePkts	统计时间内，端口收到的所有过小包的数量
etherStatsOversizePkts	统计时间内，端口收到的所有超大包的数量
etherStatsFragments	统计时间内，端口收到的所有过小且校验错误包的数量
etherStatsJabbers	统计时间内，端口收到的所有超大且校验错误包的数量
etherStatsCRCAlignErrors	统计时间内，端口收到的所有校验错误包的数量
etherStatsCollisions	统计时间内，端口收到的所有冲突包的数量
etherStatsDropEvents	统计时间内，端口收到的所有丢包事件的数量
Incoming packets by size: 64: 65-127: 128-255: 256-511: 512-1023: 1024-1518:	统计时间内，根据包的长度对接收到的包分区间进行统计。包括： • 长度小于或等于 64 字节的报文的个数 • 长度为 65~127 字节的报文的个数 • 长度为 128~255 字节的报文的个数 • 长度为 256~511 字节的报文的个数 • 长度为 512~1023 字节的报文的个数 • 长度为 1024~1518 字节的报文的个数

【相关命令】

- **rmon statistics**

1.1.7 rmon alarm

rmon alarm 命令用来创建告警表项。

undo rmon alarm 命令用来删除指定的告警表项。

【命令】

```
rmon alarm entry-number alarm-variable sampling-interval { absolute | delta }
[ startup-alarm { falling | rising | rising-falling } ] rising-threshold
threshold-value1 event-entry1 falling-threshold threshold-value2
event-entry2 [ owner text ]
undo rmon alarm entry-number
```

【缺省情况】

告警表中不存在表项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

entry-number: 告警表项的索引号，取值范围为 1~65535。

alarm-variable: 告警变量，为 1~255 个字符的字符串，可以是节点 OID 的点分格式（格式为 *entry.integer.instance* 或者 *叶子节点名.instance*，如 1.3.6.1.2.1.2.1.10.1），也可以是节点名（如 ifInOctets.1）。只有可以解析为 ASN.1 中 INTEGER(INTEGER,INTEGER32,Unsigned32,Counter32,Counter64,Gauge, or TimeTicks) 的数据类型的变量能作为告警变量，比如 etherStatsEntry 表项的叶子节点（etherStatsOctets、etherStatsPkts 和 etherStatsBroadcastPkts 等）的实例，ifEntry 表项的叶子节点（ifInOctets、ifInUcastPkts 和 ifInNUcastPkts 等）的实例。

sampling-interval: 采样间隔时间，取值范围为 5~65535，单位为秒。

absolute: 采样类型为绝对值采样，即采样时间到达时直接提取变量的值。

delta: 采样类型为变化值采样，即采样时间到达时提取的是变量在采样间隔内的变化值。

startup-alarm: 表示初次采样时，如果达到或超出阈值，触发的告警类型。如果未指定本参数，触发 **rising-falling** 类型告警。

rising: 表示只触发上限告警。

falling: 表示只触发下限告警。

rising-falling: 表示触发上限或下限告警。

rising-threshold threshold-value1 event-entry1: 设置上限参数，*threshold-value1* 表示上限阈值，取值范围为-2147483648~2147483647；*event-entry1* 表示上限阈值相应的事件索引号，取值范围为 0~65535（0 表示没有对应的事件，告警被触发后不会采取任何事件动作）。

falling-threshold threshold-value2 event-entry2: 设置下限参数，*threshold-value2* 表示下限阈值，取值范围为-2147483648~2147483647；*event-entry2* 表示下限阈值相应的事件索引号，取值范围为 0~65535（0 表示没有对应的事件，告警被触发后不会采取任何事件动作）。

owner text: 该表项的创建者，为 1~127 个字符的字符串，区分大小写。

【使用指导】

本命令用来设置告警项，以便在出现异常时触发告警事件，再由告警事件来定义具体的处理方式。用户定义了告警表项后，系统会按照定义的时间周期去获取被监视的告警变量的值，并将该值和设定的阈值进行比较，去执行相应的处理过程。当采样值大于等于设定的上限 *threshold-value1*，触发事件表中定义的事件 *event-entry1*；采样值小于等于设定的下限 *threshold-value2*，触发事件表中定义的事件 *event-entry2*。

在添加告警表项之前，需要通过 **rmon event** 命令定义好告警表项中引用的事件。否则，虽然会创建告警表项，但是不能触发告警事件。

如果在新建表项时，指定的告警变量 (*alarm-variable*)、采样间隔 (*sampling-interval*)、采样类型 (**absolute** 或 **delta**)、上限阈值 (*threshold-value1*) 和下限阈值 (*threshold-value2*) 五项参数的值和已经存在的告警表项对应的五项参数值完全相同时，系统将认为这两个表项的配置相同，创建操作失败。

用户最多可以定义 60 个告警表项。

【举例】

在告警表中添加表项 1，对节点 1.3.6.1.2.1.16.1.1.1.4.1 以 10 秒的采样间隔进行绝对值采样，当采样值大于等于 5000 的上限阈值触发事件 1，小于等于下限阈值 5 时触发事件 2，创建者为 user1。

```

<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising-threshold 5000 1
falling-threshold 5 2 owner user1

```

1.3.6.1.2.1.16.1.1.1.4 是叶子节点 `etherStatsOctets` 的 OID，它表示接口收到报文的统计值（以字节为单位）。以上步骤中也可以使用 `etherStatsOctets.1` 来代替 1.3.6.1.2.1.16.1.1.1.4.1 参数，.1 与接口统计表项的编号一致，如果创建的是“rmon statistics 5”，则对应需要使用 `etherStatsOctets.5`。

【相关命令】

- **display rmon alarm**
- **rmon event**

1.1.8 rmon event

rmon event 命令用来创建事件表项。

undo rmon event 命令用来删除指定的事件表项。

【命令】

```

rmon event entry-number [ description string ] { log | log-trap
security-string | none | trap security-string } [ owner text ]
undo rmon event entry-number

```

【缺省情况】

事件表中不存在表项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

entry-number: 事件表项的索引号，取值范围为 1~65535。

description string: 事件的描述信息，为 1~127 个字符的字符串，区分大小写。

log: 日志事件。当该事件被触发时，系统会记录日志。

log-trap: 日志和告警事件。当该事件被触发时，系统会同时记录日志和生成告警信息，生成的告警信息将发送到设备的 SNMP 模块。通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

security-string: 表示 RMON 生成的告警信息中携带的团体名。为 1~127 个字符的字符串，区分大小写。此处支持配置，但配置不生效。告警信息中携带的团体名由 SNMP 模块的配置决定。

none: 不产生动作的事件。当该事件被触发时，系统不做处理。

trap: 告警事件。当该事件被触发时，生成告警信息，生成的告警信息将发送到设备的 **SNMP** 模块。通过设置 **SNMP** 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“**SNMP**”。

owner text: 该表项的创建者，为 1~127 个字符的字符串，区分大小写。

【使用指导】

RMON 的事件管理定义事件索引号及事件的处理方式包括：记录日志、生成告警信息发送给设备的 **SNMP** 模块、记录日志的同时生成告警信息发送给设备的 **SNMP** 模块或者既不记录日志也生成告警信息发送给设备的 **SNMP** 模块。这样系统就可以对告警表中定义的告警事件进行相应的处理。事件组中定义的事件索引号对应告警组中指定事件索引号。

用户最多可以定义 60 个事件表项。

【举例】

在事件表中添加索引号为 10、类型为日志的事件，创建者为 user1。

```
<Sysname> system-view  
[Sysname] rmon event 10 log owner user1
```

【相关命令】

- **display rmon event**
- **rmon alarm**
- **rmon prialarm**

1.1.9 rmon history

rmon history 命令用来创建历史控制表项。

undo rmon history 命令用来删除指定的历史表项。

【命令】

```
rmon history entry-number buckets number interval interval [ owner text ]  
undo rmon history entry-number
```

【缺省情况】

历史控制表中不存在表项。

【视图】

以太网接口视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

entry-number: 历史控制表项的索引号，取值范围为 1~65535。

buckets number: 该历史控制表项对应的历史表容量，即历史表最多可容纳的记录数，取值范围为 1~65535，但实际配置如果超过 50 时，会提示取 50 最大配置值。

interval interval: 统计周期，取值范围为 5~3600，单位为秒。

owner text: 该表项的创建者，为 1~127 个字符的字符串，区分大小写。

【使用指导】

创建历史控制表项后，系统会按周期统计当前端口收发报文的情况，并将统计值作为一个实例保存在 **etherHistoryEntry** 表的叶子节点下。可保存的统计值个数由 **buckets number** 参数决定，当历史表的容量达到最大值时，系统会删除最早的记录来保存新的统计值。统计信息包括端口一个周期内收到的报文总数、广播报文总数和组播报文总数等。

在添加控制历史表项的过程中，如果指定的历史表容量超出了设备实际支持的历史表容量时，新的历史表项会被添加，但该表项对应生效的历史表容量为设备实际支持的历史表容量，可以使用 **display rmon history** 命令来查看配置结果。

如果在创建历史控制表项时，指定的采样间隔（**interval sampling-interval**）参数的值和该接口下已经存在的历史控制表项对应的该项参数值相同时，系统将认为这两个表项的配置相同，创建操作失败。

同一接口下可以创建多个历史控制表项。

【举例】

```
# 创建索引号为 1，表容量为 10，采样时间为 5 秒的历史控制表项，创建者为 user1。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

【相关命令】

- **display rmon history**

1.1.10 rmon prialarm

rmon prialarm 命令用来创建扩展告警表项。

undo rmon prialarm 命令用来删除指定的扩展告警表项。

【命令】

```
rmon prialarm entry-number prialarm-formula prialarm-des sampling-interval  
{ absolute | delta } [ startup-alarm { falling | rising | rising-falling } ]  
rising-threshold threshold-value1 event-entry1 falling-threshold  
threshold-value2 event-entry2 entrytype { forever | cycle cycle-period }  
[ owner text ]  
undo rmon prialarm entry-number
```

【缺省情况】

扩展告警表中不存在表项。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

entry-number: 扩展告警表项的索引号，取值范围为 1~65535。

prialarm-formula: 对告警变量进行计算的告警公式，为 1~255 个字符的字符串。公式中的告警变量必须以 OID 来表示，OID 表达式必须以小数点开始，例如(.1.3.6.1.2.1.2.1.10.1)*8；运算公式由用户定义，可以使用加减乘除四种运算方法对告警变量进行运算，该运算公式的结果取值为长整型数，但不支持负数的输入。用户在编写公式的时候需要注意，公式中每一步的运算结果都不能超过长整型的表达范围，否则可能会得出错误的结果。

prialarm-des: 对该告警的描述，为 1~127 个字符的字符串，区分大小写。

sampling-interval: 采样间隔时间，取值范围为 10~65535，单位为秒。

absolute: 采样类型为绝对值采样，即采样时间到达时直接提取变量的值。

delta: 采样类型为变化值采样，即采样时间到达时提取的是变量在采样间隔内的变化值。

startup-alarm: 表示初次采样时，如果达到或超出阈值，触发的告警类型。如果未指定本参数，触发 rising-falling 类型告警。

rising: 表示只触发上限告警。

falling: 表示只触发下限告警。

rising-falling: 表示触发上限或下限告警。

rising-threshold threshold-value1 event-entry1 : 设置超上限参数，**threshold-value1** 表示上限阈值，取值范围为-2147483648~2147483647；**event-entry1** 表示上限阈值相应的事件索引号，取值范围为 0~65535（0 表示没有对应的事件，告警被触发后不会采取任何事件动作）。

falling-threshold threshold-value2 event-entry2 : 设置下限参数，**threshold-value2** 表示下限阈值，取值范围为-2147483648~2147483647；**event-entry2** 表示下限阈值相应的事件索引号，取值范围为 0~65535（0 表示没有对应的事件，告警被触发后不会采取任何事件动作）。

forever: 本告警实例存活类型为永久。

cycle cycle-period: 本告警实例的存活时间，单位为秒，取值范围 0~4294967。

owner text: 该表项的创建者，为 1~127 个字符的字符串，区分大小写。

【使用指导】

用户定义了扩展告警表项后，系统先对定义的扩展告警公式中的告警变量按照定义的时间间隔进行采样，再将采样值按照定义的运算公式进行计算，最后将计算结果和设定的阈值进行比较，并执行相应的处理过程。

在添加扩展告警表项之前，需要通过 **rmon event** 命令定义好扩展告警表项中引用的事件。

如果在新建表项时，指定的告警变量公式（**prialarm-formula**）、采样间隔（**sampling-interval**）、采样类型（**absolute** 或 **delta**）、上限阈值（**threshold-value1**）和下限阈值（**threshold-value2**）五项参数的值和已经存在的扩展告警表项对应的五项参数值完全相同时，系统将认为这两个表项的配置相同，创建操作失败。

用户最多可以定义 50 个扩展告警表项。

【举例】

使用扩展告警对接口接收到的广播报文比率进行监控。

在扩展告警表中添加索引号为 1 的表项，对相应告警变量以公式 (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)运算，对该公式中涉及的变量以 10 秒的采样间隔进行绝对值采样。上限告警值为 80 对应事件 1（将事件记录在日志表中），下限告警值为 5 对应事件 2（不需要采取措施），表项的存活时间为永远（**forever**），创建者为 *user1*。（广播报文比率的计算公式为：接口接收到的广播报文总数/接口接收到的总报文数，该公式由用户自行定义）

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon prialarm 1 (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
BroadcastPktsRatioOfGE1/0/1 10 absolute rising-threshold 80 1 falling-threshold 5 2
entrytype forever owner user1
```

.1.3.6.1.2.1.16.1.1.1.6.1 是节点 etherStatsBroadcastPkts.1 的 OID，.1.3.6.1.2.1.16.1.1.1.5.1 是节点 etherStatsPkts.1 的 OID。.1 与接口统计表项的编号一致，如果创建的是“rmon statistics 5”，则对应需要使用 .1.3.6.1.2.1.16.1.1.1.6.5 和 .1.3.6.1.2.1.16.1.1.1.5.5。

【相关命令】

- **display rmon prialarm**
- **rmon event**

1.1.11 rmon statistics

rmon statistics 命令用来创建统计表项。

undo rmon statistics 命令用来删除指定的统计表项。

【命令】

```
rmon statistics entry-number [ owner text ]
undo rmon statistics entry-number
```

【缺省情况】

统计表中不存在表项。

【视图】

以太网接口视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

entry-number：统计表项的索引号，取值范围为 1~65535。

owner text：该表项的创建者，为 1~127 个字符的字符串，区分大小写。

【使用指导】

当需要统计某个以太网端口的累加数据时，需要建立统计表。统计信息包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。设备重启时，会清除该统计信息。

用户可以通过 **display rmon statistics** 命令来显示统计表项的信息。

统计表项的 *entry-number* 必须全局唯一，如果已经在其他接口下使用，则创建操作失败。

每个接口下只能定义一个统计表项。

【举例】

在统计表中添加 GigabitEthernet1/0/1 的统计表项，表项的索引号为 20，创建者为 user1。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] rmon statistics 20 owner user1
```

【相关命令】

- **display rmon statistics**

目 录

1 Event MIB	1-1
1.1 Event MIB配置命令	1-1
1.1.1 action	1-1
1.1.2 comparison	1-2
1.1.3 context (Action-set view)	1-3
1.1.4 context (Trigger view)	1-3
1.1.5 delta falling	1-4
1.1.6 delta rising	1-5
1.1.7 description (Event view)	1-6
1.1.8 description (Trigger view)	1-7
1.1.9 display snmp mib event	1-7
1.1.10 display snmp mib event event	1-9
1.1.11 display snmp mib event object list	1-11
1.1.12 display snmp mib event summary	1-12
1.1.13 display snmp mib event trigger	1-13
1.1.14 event (Trigger-boolean view)	1-17
1.1.15 event (Trigger-existence view)	1-17
1.1.16 event enable	1-18
1.1.17 falling	1-19
1.1.18 frequency	1-20
1.1.19 object list (Action-notification view)	1-21
1.1.20 object list (Trigger view)	1-21
1.1.21 object list (Trigger-boolean view)	1-22
1.1.22 object list (Trigger-existence view)	1-23
1.1.23 object list (Trigger-threshold view)	1-24
1.1.24 oid (Action-notification view)	1-25
1.1.25 oid (Action-set view)	1-26
1.1.26 oid (Trigger view)	1-26
1.1.27 rising	1-27
1.1.28 sample	1-28
1.1.29 snmp mib event	1-29
1.1.30 snmp mib event object list	1-30
1.1.31 snmp mib event sample instance maximum	1-31

1.1.32 snmp mib event sample minimum	1-32
1.1.33 snmp mib event trigger	1-33
1.1.34 snmp-agent trap enable event-mib	1-33
1.1.35 startup (Trigger-existence view)	1-34
1.1.36 startup (Trigger-threshold view)	1-35
1.1.37 startup enable	1-36
1.1.38 test	1-37
1.1.39 trigger enable	1-38
1.1.40 type	1-38
1.1.41 value (Action-set view)	1-40
1.1.42 value (Trigger-boolean view)	1-40
1.1.43 wildcard context (Action-set view)	1-41
1.1.44 wildcard context (Trigger view)	1-42
1.1.45 wildcard oid (Action-set view)	1-43
1.1.46 wildcard oid (Trigger view)	1-43

1 Event MIB

1.1 Event MIB配置命令

1.1.1 action

action 命令用来配置事件包含的动作。

undo action 命令用来删除事件的指定动作。

【命令】

```
action { notification | set }  
undo action { notification | set }
```

【缺省情况】

该事件没有包含动作。

【视图】

Event 视图

【缺省用户角色】

network-admin
context-admin

【参数】

notification: 指定事件包含告警动作，当对应的事件被触发时，则向 NMS 发送指定的告警信息。

set: 指定事件包含设置动作，当对应的事件被触发时，可以对指定的 MIB 节点的值进行设置。

【使用指导】

当对应事件被触发后，可以配置的执行动作类型包括 **Set** 和 **Notification**。同一个事件可以配置两种动作。具体如下：

- 如果动作指定为 **Set** 类型，则系统自动生成对应的 **Set** 表，同时进入 **Action-set** 视图，进行 **Set** 表的相关配置。具体配置请参见 **Action-set** 视图下的配置。
- 如果动作指定为 **Notification** 类型，则自动生成相对应 **Notification** 表，同时进入 **Action-notification** 视图，进行 **Notification** 表的相关配置。具体配置请参见 **Action-notification** 视图下的配置。

【举例】

配置用户事件的动作为 **Set** 和 **Notification**，设置节点名 **ipForwarding.0** 的值为 2，告警类型为 **mteEventSetFailure**。

```
<Sysname> system-view  
[Sysname] snmp mib event owner owner1 name EventA  
[Sysname-event-owner1-EventA] action notification  
[Sysname-event-owner1-EventA-notification] oid mteEventSetFailure
```

```
[Sysname-event-owner1-EventA-notification] quit
[Sysname-event-owner1-EventA] action set
[Sysname-event-owner1-EventA-set] oid ipForwarding.0
[Sysname-event-owner1-EventA-set] value 2
```

【相关命令】

- **event enable**
- **snmp mib event**

1.1.2 comparison

comparison 命令用来配置采样值与参考值的比较方式。

undo comparison 命令用来恢复缺省情况。

【命令】

```
comparison { equal | greater | greaterorequal | less | lessorequal | unequal }
undo comparison
```

【缺省情况】

采样值与参考值的比较方式为 **unequal**。

【视图】

Trigger-boolean 视图

【缺省用户角色】

network-admin
context-admin

【参数】

equal: 采样值与参考值的比较方式为 **equal**，即当采样值等于参考值时，满足检测条件。

greater: 采样值与参考值的比较方式为 **greater**，即当采样值大于参考值时，满足检测条件。

greaterorequal: 采样值与参考值的比较方式为 **greaterorequal**，即当采样值大于等于参考值时，满足检测条件。

less: 采样值与参考值的比较方式为 **less**，即当采样值小于参考值时，满足检测条件。

lessorequal: 采样值与参考值的比较方式为 **lessorequal**，即当采样值小于等于参考值时，满足检测条件。

unequal: 采样值与参考值的比较方式为 **unequal**，即当采样值不等于参考值时，满足检测条件。

【使用指导】

被监控的节点为非首次采样，本次采样值满足条件且上次采样值不满足条件则触发指定事件，也就是说如果连续两次采样均满足条件，只在第一次触发指定事件。

被监控节点为首次采样，只有配置了 **startup enable** 命令后才会触发指定事件。

【举例】

配置采样值与参考值的比较方式为 **unequal**。

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
```

```
[Sysname-trigger-owner1-triggerA] test boolean
[Sysname-trigger-owner1-triggerA-boolean] comparison unequal
```

【相关命令】

- **snmp mib event trigger**
- **test**

1.1.3 context (Action-set view)

context 命令用来配置 Set 对象所处的上下文环境。

undo context 命令用来恢复缺省情况。

【命令】

```
context context-name
undo context
```

【缺省情况】

未配置 Set 对象所处的上下文环境。

【视图】

Action-set 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

context-name: 指定 Set 对象所处的上下文环境，为 1~32 个字符的字符串，区分大小写。

【使用指导】

配置上下文环境用于确定唯一的 Set 对象的节点实例。

【举例】

```
# 配置 Set 对象所处的上下文为 contextname1。
<Sysname>system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action set
[Sysname-event-owner1-EventA-set] context contextname1
```

【相关命令】

- **snmp mib event owner**
- **action**
- **wildcard context**

1.1.4 context (Trigger view)

context 命令用来配置监控对象所在的上下文环境。

undo context 命令用来恢复缺省情况。

【命令】

```
context context-name  
undo context
```

【缺省情况】

未配置监控对象所在的上下文环境。

【视图】

Trigger 视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

context-name: 指定监控对象所在的上下文，为 1~32 个字符的字符串，区分大小写。

【使用指导】

配置上下文环境用于确定唯一的监控对象的节点实例。

【举例】

```
# 配置监控对象所在的上下文环境为 contextname1。  
<Sysname> system-view  
[Sysname] snmp mib event trigger owner owner1 name triggerA  
[Sysname-trigger-owner1-triggerA] context contextname1
```

【相关命令】

- **snmp mib event trigger**
- **wildcard context**

1.1.5 delta falling

delta falling 命令用来配置差值采样类型的下限阈值以及采样值小于等于该阈值时对应的触发事件。

undo delta falling 命令用来恢复缺省情况。

【命令】

```
delta falling { event owner event-owner name event-name | value  
integer-value }  
undo delta falling { event | value }
```

【缺省情况】

下限阈值为 0，且未指定对应的触发事件。

【视图】

Trigger-threshold 视图

【缺省用户角色】

network-admin
context-admin

【参数】

event owner event-owner: 配置差值采样类型下限阈值对应事件的所有者，与 Trigger 表中配置的 Trigger 所有者 owner 相同。

name event-name: 配置差值采样类型下限阈值对应的事件名，为 1~32 个字符的字符串，区分大小写。

value integer-value: 差值采样类型的下限阈值，取值范围为-2147483648~2147483647。可以配置任意不大于差值采样类型上限阈值的整数。

【使用指导】

采样类型为差值采样时，采样差值小于或达到差值采样类型下限阈值时，将触发对应的事件。

若采样值连续多次小于或达到下限阈值，只会在第一次触发对应的事件，上限和下限对应事件的触发是交替产生的。

【举例】

配置差值采样类型的下限阈值为 20。

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] delta falling value 20
```

【相关命令】

- snmp mib event trigger
- test
- sample

1.1.6 delta rising

delta rising 命令用来配置差值采样类型的上限阈值以及采样值大于等于该阈值对应的触发事件。

undo delta rising 命令用来恢复缺省情况。

【命令】

```
delta rising { event owner event-owner name event-name | value integer-value }
undo delta rising { event | value }
```

【缺省情况】

上限阈值为 0，且未指定对应的触发事件。

【视图】

trigger-threshold 视图

【缺省用户角色】

network-admin

context-admin

【参数】

event owner event-owner: 配置差值上限阈值事件的所有者，与 Trigger 表中配置的 Trigger 所有者 owner 相同。

name event-name: 配置差值上限阈值的事件，为 1~32 个字符的字符串，区分大小写。

value integer-value: 差值上限阈值，取值范围为-2147483648~2147483647。可以配置任意不小于差值下限阈值的整数。

【使用指导】

采样类型为差值采样时，采样差值达到或超过上限阈值，将触发对应的事件。

若采样值连续多次达到或超过上限阈值，只会在第一次触发对应的事件，上限和下限对应事件的触发是交替产生的。

【举例】

```
# 配置差值采样类型的差值上限阈值为 50，对应的事件所有者为 owner1，事件名为 event1。  
<Sysname> system-view  
[Sysname] snmp mib event trigger owner owner1 name triggerA  
[Sysname-trigger-owner1-triggerA] test threshold  
[Sysname-trigger-owner1-triggerA-threshold] delta rising value 50  
[Sysname-trigger-owner1-triggerA-threshold] delta rising event owner owner1 name event1
```

【相关命令】

- snmp mib event trigger
- test
- sample

1.1.7 description (Event view)

description 命令用来配置 Event 的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description text

undo description

【缺省情况】

未配置 Event 的描述信息。

【视图】

Event 视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: Event 的描述信息，为 1~255 个字符的字符串，区分大小写。

【举例】

配置拥有者为 owner1 的事件 EventA 的描述信息为 “EventA is an RMON event”。

```
<Sysname> system-view
```

```
[Sysname] snmp mib event owner owner1 name EventA
```

```
[Sysname-event-owner1-EventA] description EventA is an RMON event
```

【相关命令】

- **snmp mib event owner**

1.1.8 description (Trigger view)

description 命令用来配置 Trigger 表项的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description text

undo description

【缺省情况】

未配置 Trigger 表项的描述信息。

【视图】

Trigger 视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: Trigger 表项的描述信息，为 1~255 个字符的字符串，区分大小写。

【举例】

配置所有者为 owner1 名称为 triggerA 的 Trigger 表项的描述信息为 “triggerA is configured for network management events”。

```
<Sysname> system-view
```

```
[Sysname] snmp mib event trigger owner owner1 name triggerA
```

```
[Sysname-trigger-owner1-triggerA] description triggerA is configured for network management events
```

【相关命令】

- **snmp mib event trigger**

1.1.9 display snmp mib event

display snmp mib event 命令用来显示 Event MIB 相关配置及统计信息。

【命令】

display snmp mib event

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

显示所有 Event MIB 相关配置信息及统计信息，包括获取触发事件名称、功能描述、动作类型、使能及实体控制状态。

【举例】

显示 Event MIB 相关配置及统计信息。

```
<Sysname> display snmp mib event
```

```
TriggerFailures           : 0  
EventFailures             : 0  
SampleMinimum             : 1  
SampleInstanceMaximum     : 0  
SampleInstance            : 0  
SampleInstancesHigh       : 0  
SampleInstanceLacks       : 0
```

Trigger entry triggerA owned by owner1:

```
TriggerComment            : triggerA is to monitor the state of the interface  
TriggerTest               : boolean  
TriggerSampleType         : absoluteValue  
TriggerValueID            : 1.3.6.1.2.1.2.2.1.7.3<ifAdminStatus.3>  
TriggerValueIDWildcard    : false  
TriggerTargetTag          : N/A  
TriggerContextName        : context1  
TriggerContextNameWildcard : true  
TriggerFrequency(in seconds): 600  
TriggerEnabled            : true
```

Boolean entry:

```
BoolCmp                   : unequal  
BoolValue                  : 1  
BoolStartUp               : true  
BoolObjOwner              : owner1  
BoolObjName                : Objects1  
BoolEvtOwner               : N/A  
BoolEvtName                : N/A
```

Event entry eventA owned by owner2:

```
EvtComment                : event is to set ifAdminStatus
```

```

EvtAction          : notification | set
EvtEnabled         : true
Notification entry:
  NotifyOID        : 1.3.6.1.2.1.88.2.0.1<mteTriggerFired>
  NotifyObjOwner   : N/A
  NotifyObjName    : N/A
Set entry:
  SetObj           : 1.3.6.1.2.1.2.2.1.7<ifAdminStatus>
  SetObjWildcard   : true
  SetValue        : 2
  SetTargetTag     : N/A
  SetContextName   : context1
  SetContextNameWildcard : false
Object list objectA owned by owner3:
  ObjIndex        : 1
  ObjID           : 1.3.6.1.2.1.2.1.0<ifNumber.0>
  ObjIDWildcard   : false
Object list objectA owned by owner3:
  ObjIndex        : 2
  ObjID           : 1.3.6.1.2.1.2.2.1.2.0<ifDescr.0>
  ObjIDWildcard   : false

```

上述显示信息中相关字段解释详见各表显示信息描述表（[表 1-1](#) 至 [表 1-9](#)）。

【相关命令】

- **snmp mib event trigger**
- **snmp mib event**
- **snmp mib event object list**

1.1.10 display snmp mib event event

display snmp mib event event 命令用来显示设备上已创建的 Event 表信息及其相应的 Action 表。

【命令】

display snmp mib event event [*owner event-owner name event-name*]

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

owner event-owner name event-name: 指定 Event 所有者及 Event 名称。Event 所有者为 SNMPv3 用户；Event 名称为 1~32 个字符的字符串，区分大小写。如不指定本参数，则显示设备上所有已创建的 Event 表及其相应的 Action 表信息。

【举例】

显示已创建的 Event 所有者为 owner2, Event 名称为 eventA 的 Event 表项信息及其相应的 Action 表信息。

```
<Sysname>display snmp mib event event owner owner2 name eventA
Event entry eventA owned by owner2:
  EvtComment          : event is to set ifAdminStatus
  EvtAction           : notification | set
  EvtEnabled          : true
Notification entry:
  NotifyOID           : 1.3.6.1.2.1.88.2.0.1<mteTriggerFired>
  NotifyObjOwner      : N/A
  NotifyObjName       : N/A
Set entry:
  SetObj              : 1.3.6.1.2.1.2.2.1.7<ifAdminStatus>
  SetObjWildcard      : true
  SetValue            : 2
  SetTargetTag        : N/A
  SetContextName      : context1
  SetContextNameWildcard : false
```

表1-1 Event Entry 显示信息描述表

字段	描述
Event entry <i>eventA</i> owned by <i>owner2</i>	<i>owner2</i> : 事件所有者，为SNMPv3用户 <i>eventA</i> : 事件名称
EvtComment	事件信息描述
EvtAction	事件动作，有set和notification两种动作
EvtEnabled	事件使能状态

表1-2 Notification Entry 显示信息描述表

字段	描述
NotifyOID	告警OID，OID类型为Trap节点
NotifyObjOwner	告警绑定对象所有者，为SNMPv3 用户
NotifyObjName	告警绑定对象组名

表1-3 Set Entry 显示信息描述表

字段	描述
SetObj	事件设置对象的OID
SetObjWildcard	设置对象OID的通配标识符，取值为： • false: 精确匹配 • true: 通配
SetValue	设置对象OID的值
SetTargetTag	设置对象远程标识符
SetContextName	事件设置对象上下文环境
SetContextNameWildcard	事件设置对象的上下文通配标识符，取值为： • false: 精确匹配 • true: 通配

【相关命令】

- **snmp mib event**

1.1.11 display snmp mib event object list

display snmp mib event object list 命令用来显示设备上已创建的 Object 表的相关信息。

【命令】

display snmp mib event object list [owner group-owner name group-name]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

owner group-owner name group-name: 指定对象组所有者及对象组名称。对象组所有者为 SNMPv3 用户，对象组名称为 1~32 个字符的字符串，区分大小写。如不指定本参数，则显示设备上所有已创建的 Object 表的信息。

【举例】

显示已创建的对象组所有者为 owner3、对象组名称为 objectA 的 Object 表项信息。

```
<Sysname> display snmp mib event object list owner owner3 name objectA
Object list objectA owned by owner3:
ObjIndex          : 1
ObjID              : 1.3.6.1.2.1.2.1.0<ifNumber.0>
```



```
ObjIDWildcard          : false
Object list objectA owned by owner3:
ObjIndex               : 2
ObjID                  : 1.3.6.1.2.1.2.2.1.2.0<ifDescr.0>
ObjIDWildcard          : false
```

表1-4 display snmp mib event object list 显示信息描述表

字段	描述
Object list <i>objectA</i> owned by <i>owner3</i>	<i>owner3</i> : 绑定对象所有者，为SNMPv3用户，一级索引 <i>objectA</i> : 绑定对象名，二级索引
ObjIndex	绑定对象的索引，三级索引
ObjID	绑定对象的OID
ObjIDWildcard	绑定对象OID的通配标识符，取值为： • false: 精确匹配 • true: 通配

【相关命令】

- **snmp mib event object list**

1.1.12 display snmp mib event summary

display snmp mib event summary 命令用来显示 Event MIB 摘要信息。

【命令】

```
display snmp mib event summary
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【使用指导】

显示全局配置信息包括最小采样时间间隔和最大采样实例数；及显示相关统计值包括当前采样行实例数、采样行数峰值、达到最大采样行数限制而采样失败的行数、Trigger 触发失败次数和执行相应 Event 失败次数。

【举例】

```
# 显示 Event MIB 的摘要信息。
<Sysname> display snmp mib event summary
TriggerFailures      : 0
EventFailures        : 0
```

```

SampleMinimum           : 1
SampleInstanceMaximum   : 0
SampleInstance          : 0
SampleInstancesHigh      : 0
SampleInstanceLacks      : 0

```

表1-5 display snmp mib event summary 显示信息描述表

字段	描述
TriggerFailures	Trigger触发测试失败的次数
EventFailures	Trigger触发Notification或者Set动作失败的次数
SampleMinimum	系统支持的最小采样时间间隔
SampleInstanceMaximum	系统支持的最大采样行数
SampleInstance	当前活动状态的采样节点数
SampleInstancesHigh	采样过程中达到的最大采样行数
SampleInstanceLacks	由于超过系统支持的最大采样行数限制而采样失败的次数

【相关命令】

- **display snmp mib event**

1.1.13 display snmp mib event trigger

display snmp mib event trigger 命令用来显示设备上已创建的 Trigger 的相关信息及相应的 Test 表项信息。

【命令】

display snmp mib event trigger [*owner trigger-owner name trigger-name*]

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

owner trigger-owner name trigger-name: 显示指定所有者及指定名称的 Trigger 的相关信息, *trigger-owner* 表示 Trigger 所有者, 为 SNMPv3 用户; *trigger-name* 表示 Trigger 名称, 为 1~32 个字符的字符串, 区分大小写。如不指定该参数, 则显示设备上已创建的所有 Trigger 及 Test 表的相关信息。

【举例】

显示已创建的所有者为 owner1、名称为 triggerA 的 Trigger 信息及其相应的 Test 表信息。

```

<Sysname> display snmp mib event trigger owner owner1 name triggerA
Trigger entry triggerA owned by owner1:
  TriggerComment          : triggerA is to monitor the state of the interface
  TriggerTest             : existence | boolean | threshold
  TriggerSampleType       : absoluteValue
  TriggerValueID          : 1.3.6.1.2.1.2.2.1.7.3<ifAdminStatus.3>
  TriggerValueIDWildcard  : false
  TriggerTargetTag        : N/A
  TriggerContextName      : context1
  TriggerContextNameWildcard : true
  TriggerFrequency(in seconds): 600
  TriggerObjOwner         : owner1
  TriggerObjName          : obj1
  TriggerEnabled          : true
Existence entry:
  ExiTest                 : present | absent
  ExiStartUp              : present | absent
  ExiObjOwner             : owner1
  ExiObjName              : object1
  ExiEvtOwner             : owner1
  ExiEvtName              : event1
Boolean entry:
  BoolCmp                 : unequal
  BoolValue               : 1
  BoolStartUp             : true
  BoolObjOwner            : owner1
  BoolObjName             : Objects1
  BoolEvtOwner            : N/A
  BoolEvtName             : N/A
Threshold entry:
  ThresStartUp            : falling
  ThresRising             : 40
  ThresFalling            : 20
  ThresDeltaRising        : 40
  ThresDeltaFalling       : 20
  ThresObjOwner           : N/A
  ThresObjName            : N/A
  ThresRisEvtOwner        : owner1
  ThresRisEvtName         : event1
  ThresFalEvtOwner        : owner1
  ThresFalEvtName         : event1
  ThresDeltaRisEvtOwner   : owner1
  ThresDeltaRisEvtName    : event1
  ThresDeltaFalEvtOwner   : owner1
  ThresDeltaFalEvtName    : event1

```

表1-6 Trigger Entry 显示信息描述表

字段	描述
Trigger entry <i>triggerA</i> owned by <i>owner1</i>	<i>owner1</i> : Trigger所有者 <i>triggerA</i> : Trigger名称
TriggerComment	Trigger的功能和使用描述
TriggerTest	Trigger触发条件的检测类型，取值分为existence、boolean和threshold三种类型
TriggerSampleType	Trigger触发采样类型，取值为： - absoluteValue: 绝对值采样 - deltaValue: 差值采样
TriggerValueID	监控对象OID
TriggerValueIDWildcard	监控对象OID通配标识符，取值为： - false: 精确匹配 - true: 通配
TriggerTargetTag	标识监控对象所在的远程系统
TriggerContextName	监控对象OID所处的上下文
TriggerContextNameWildcard	监控对象OID所处的上下文环境的通配标识符，分为精确匹配和通配
TriggerFrequency	Trigger采样间隔
TriggerObjOwner	Trigger绑定对象所有者，为SNMPv3用户
TriggerObjName	Trigger的绑定对象
TriggerEnabled	Trigger是否触发使能： - true: 使能 - false: 未使能

表1-7 Existence Entry 显示信息描述表

字段	描述
ExiTest	Existence触发条件类型，取值为present、absent和changed
ExiStartUp	Existence初始触发条件，取值为present、absent和changed
ExiObjOwner	Existence绑定对象所有者
ExiObjName	Existence的绑定对象
ExiEvtOwner	Existence触发事件所有者
ExiEvtName	Existence触发事件名

表1-8 Boolean Entry 显示信息描述表

字段	描述
BoolCmp	Boolean比较的类型，取值为： 有6种比较类型equal、unequal、less、lessOrEqual、greater、greaterOrEqual，默认情况下是unequal比较对象TriggerValueID与BoolValue
BoolValue	Boolean参考值
BoolStartUp	初始触发条件，取值为true和false
BoolObjOwner	Boolean触发绑定对象所有者，为SNMPv3用户
BoolObjName	Boolean触发的绑定对象
BoolEvtOwner	Boolean触发事件所有者，为SNMPv3用户
BoolEvtName	Boolean触发的事件名

表1-9 Threshold Entry 显示信息描述表

字段	描述
ThresStartUp	初始触发条件，取值为rising(1)、falling(2)和 risingOrFalling(3)
ThresRising	绝对值采样上限阈值
ThresFalling	绝对值采样下限阈值
ThresDeltaRising	差值采样下的上限阈值
ThresDeltaFalling	差值采样下的下限阈值
ThresObjOwner	阈值触发下绑定对象所有者
ThresObjName	阈值触发下的绑定对象
ThresRisEvtOwner	Rising触发事件所有者，为SNMPv3用户
ThresRisEvtName	Rising触发事件名
ThresFalEvtOwner	Falling触发事件所有者，为SNMPv3用户
ThresFalEvtName	Falling触发事件名
ThresDeltaRisEvtOwner	DeltaRising触发事件所有者，为SNMPv3用户
ThresDeltaRisEvtName	DeltaRising触发事件名
ThresDeltaFalEvtOwner	DeltaFalling触发事件所有者，为SNMPv3用户
ThresDeltaFalEvtName	DeltaFalling触发事件名

【相关命令】

- **snmp mib event trigger**

1.1.14 event (Trigger-boolean view)

event 命令用来指定在 Trigger-boolean 视图下满足检测条件时触发的 Event 事件。

undo event 命令用来恢复缺省情况。

【命令】

```
event owner event-owner name event-name
undo event
```

【缺省情况】

未指定 Event 事件。

【视图】

Trigger-boolean 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

owner event-owner: 触发事件的所有者，与 trigger 表中配置的 trigger 所有者 owner 相同。

name event-name: 触发事件名，为 1~32 个字符的字符串，区分大小写。

【使用指导】

当满足触发条件时，就根据指定的触发事件的所有者和名称在配置的 Event 表中查找指定的 Event 事件是否存在；若存在，则执行该 Event 事件指定的动作。

【举例】

配置在满足检测条件时所触发的 Event 事件。

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test boolean
[Sysname-trigger-owner1-triggerA-boolean] event owner owner1 name event1
```

【相关命令】

- **snmp mib event trigger**
- **test**

1.1.15 event (Trigger-existence view)

event 命令用来指定在 Trigger-existence 视图下，满足检测条件时触发的 Event 事件。

undo event 命令用来恢复缺省情况。

【命令】

```
event owner event-owner name event-name
undo event
```

【缺省情况】

未指定 Event 事件。

【视图】

Trigger-existence 视图

【缺省用户角色】

network-admin

context-admin

【参数】

owner *event-owner*: 指定触发事件的所有者，与 Trigger 表中配置的 Trigger 所有者 owner 相同。

name *event-name*: 指定触发事件名，为 1~32 个字符的字符串，区分大小写。

【使用指导】

满足触发条件时，就会查找 Event 表，根据触发事件的所有者和名称查找配置的 Event 事件是否存在。若存在，则执行该 Event 事件指定的动作。

【举例】

配置 Trigger-existence 子视图下，满足检测条件时所触发的 Event 事件。

```
<Sysname> system-view
```

```
[Sysname] snmp mib event trigger owner owner1 name triggerA
```

```
[Sysname-trigger-owner1-triggerA] test existence
```

```
[Sysname-trigger-owner1-triggerA-existence] event owner owner1 name event1
```

【相关命令】

- **snmp mib event trigger**
- **test**

1.1.16 event enable

event enable 命令用来开启事件触发功能。

undo event enable 命令用来关闭事件触发功能。

【命令】

event enable

undo event enable

【缺省情况】

事件触发功能处于关闭状态。

【视图】

Event 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

只有满足 Test 检测条件且开启事件触发功能，才能触发相应的事件。

【举例】

开启事件所有者为 owner1、名称为 EventA 事件的触发功能。

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] event enable
```

【相关命令】

- **snmp mib event**
- **action**

1.1.17 falling

falling 命令用来配置绝对值采样类型的下限阈值，并指定采样值小于等于该阈值时触发的事件。

undo falling 命令用来恢复缺省情况。

【命令】

```
falling { event owner event-owner name event-name | value integer-value }
undo falling { event | value }
```

【缺省情况】

下限阈值为 0，且未配置对应的触发事件。

【视图】

Trigger-threshold 视图

【缺省用户角色】

network-admin
context-admin

【参数】

event owner *event-owner*: 配置下限阈值对应事件的所有者，与 Trigger 表中配置的 Trigger 所有者 owner 相同。

name *event-name*: 配置下限阈值对应的事件名，为 1~32 个字符的字符串，区分大小写。

value *integer-value*: 绝对值采样的下限阈值，取值范围为-2147483648~2147483647。可以配置任意不大于上限阈值的整数。

【使用指导】

采样类型为绝对值采样时，采样值小于或达到下限阈值时，将触发对应的事件。

若采样值连续多次小于或达到下限阈值，只会在第一次触发对应的事件，上限和下限对应事件的触发是交替产生的。

【举例】

配置绝对值采样类型的下限阈值为 20。

```
<Sysname> system-view
```



```
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] falling value 20
```

【相关命令】

- **snmp mib event trigger**
- **test**
- **sample**

1.1.18 frequency

frequency 命令用来配置 Trigger 采样时间间隔。

undo frequency 命令用来恢复缺省情况。

【命令】

```
frequency interval
undo frequency
```

【缺省情况】

采样时间间隔为 600 秒。

【视图】

Trigger 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

interval: 表示 Trigger 采样时间间隔，为任意不小于系统支持的最小采样时间间隔的正整数，取值范围为 1~4294967295，单位为秒。

【使用指导】

系统支持的最小采样时间间隔需使用 **snmp mib event sample minimum** 命令配置。

如果采样节点较多且配置的采样间隔时间过短，可能出现下一次采样时本次采样尚未完成，将导致下一次的采样处理失败，因此请根据实际情况合理配置采样间隔。

【举例】

```
# 配置 Trigger 采样时间间隔为 360 秒。
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] frequency 360
```

【相关命令】

- **snmp mib event trigger**
- **snmp mib event sample minimum**

1.1.19 object list (Action-notification view)

object list 命令用来指定绑定对象组，表示触发 Notification 事件时，需要在此绑定对象组中添加的绑定变量。

undo object list 命令用来恢复缺省情况。

【命令】

object list owner group-owner name group-name

undo object list

【缺省情况】

未指定绑定对象组。

【视图】

Action-notification 视图

【缺省用户角色】

network-admin

context-admin

【参数】

group-owner: 绑定对象的所有者，与对应 Event 配置的 owner 相同。

group-name: 绑定对象组的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

本命令用来配置发送 Notification 时附加的引用 Object 表中的绑定对象组所包含的绑定变量，若不指定或者指定的绑定对象组为空，则不添加绑定变量。关于发送 Notification 的绑定变量描述请参见 Trigger 视图下的 **object list** 的命令。

【举例】

```
# 配置事件所有者为 owner1，事件名为 EventA，绑定对象组名为 listA。
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action notification
[Sysname-event-owner1-EventA-notification] object list owner owner1 name listA
```

【相关命令】

- **snmp mib event owner**
- **action**

1.1.20 object list (Trigger view)

object list 命令用来指定绑定对象组。该 Trigger 触发 Notification 动作发送相应 Trap 时需要添加此绑定对象组中的绑定变量。

undo object list 命令用来恢复缺省情况。

【命令】

object list owner group-owner name group-name

undo object list

【缺省情况】

未指定绑定对象组。

【视图】

Trigger 视图

【缺省用户角色】

network-admin

context-admin

【参数】

owner group-owner: 绑定对象组的所有者，与 Trigger 表中配置的 Trigger 所有者必须相同。

name group-name: 绑定对象组的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

通过指定绑定对象组的所有者和名称来指定一个绑定对象组，每个绑定对象组的成员由 **object list** 命令指定；当 Trigger 触发的事件包含 notification 动作时，发送的 SNMP Trap 报文将携带配置的绑定变量。

发送 Notification 时需要的绑定对象组可以在三处指定：

- Trigger 视图下的 **object list** 命令指定 Trigger 对应的绑定对象组，表示所有由本 Trigger 触发 Notification 事件时需要添加的绑定变量；
- Trigger-test 视图（Trigger-boolean、Trigger-existence、Trigger-threshold）下的 **object list** 命令，统称为 Trigger-test 绑定对象组，表示满足此种检测类型所触发的 Notification 事件时需要添加的绑定变量；
- Action-notification 视图下的 **object list** 命令指定 Notification 绑定对象组，表示引用此事件发送指定 Notification 事件时需要添加的绑定变量。

实际配置时可以只在其中的一处指定，二处指定，或者三处同时指定。当多处指定时，绑定变量添加到 Trap 报文中的顺序，应该为先添加 Trigger 绑定对象组中的变量，再添加 Test 绑定对象组中的变量，最后添加 Notification 绑定对象组中的变量。

【举例】

配置 Trigger 绑定所有者为 owner1，绑定对象组名称为 objectA。

```
<Sysname> system-view
```

```
[Sysname] snmp mib event trigger owner owner1 name triggerA
```

```
[Sysname-trigger-owner1-triggerA] object list owner owner1 name objectA
```

【相关命令】

- **snmp mib event trigger**

1.1.21 object list (Trigger-boolean view)

object list 命令用来指定绑定对象组，表示监控对象值满足 Boolean 检测条件且触发事件为 Notification 时，需要添加此绑定对象组中的绑定变量。

undo object list 命令用来恢复缺省情况。

【命令】

```
object list owner group-owner name group-name  
undo object list
```

【缺省情况】

未指定绑定对象组。

【视图】

Trigger-boolean 视图

【缺省用户角色】

network-admin
context-admin

【参数】

group-owner: 指定 Trigger 绑定对象组的所有者，与 Trigger 表中配置的 Trigger 所有者 **owner** 相同。

group-name: 指定 Trigger 绑定对象组的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

参考 Trigger 视图下的 **object list** 命令。

【举例】

```
# 配置绑定对象组，指定 Trigger 绑定对象组的所有者为 owner1，绑定对象组名称为 objectA。  
<Sysname> system-view  
[Sysname] snmp mib event trigger owner owner1 name triggerA  
[Sysname-trigger-owner1-triggerA] test boolean  
[Sysname-trigger-owner1-triggerA-boolean] object list owner owner1 name objectA
```

【相关命令】

- **snmp mib event trigger**
- **test**

1.1.22 object list (Trigger-existence view)

object list 命令用来指定绑定对象组，表示监控对象值满足 Existence 检测条件且触发事件为 Notification 时，需要添加此绑定对象组中的绑定变量。

undo object list 命令用来恢复缺省情况。

【命令】

```
object list owner group-owner name group-name  
undo object list
```

【缺省情况】

未指定绑定对象组。

【视图】

Trigger-existence 视图

【缺省用户角色】

network-admin
context-admin

【参数】

group-owner: 绑定对象组的所有者，与 Trigger 表中配置的 Trigger 所有者 owner 相同。

group-name: 绑定对象组的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

参考 Trigger 视图下的 **object list** 命令。

【举例】

当监控对象值满足 Trigger-existence 测试条件后，系统执行 Notification 动作并发送 Trap 时需要绑定的对象组。

```
<Sysname> system-view  
[Sysname] snmp mib event trigger owner owner1 name triggerA  
[Sysname-trigger-owner1-triggerA] test existence  
[Sysname-trigger-owner1-triggerA-existence] object list owner owner1 name objectA
```

【相关命令】

- **snmp mib event trigger**
- **test**

1.1.23 object list (Trigger-threshold view)

object list 命令用来指定绑定对象组，表示监控对象值满足 Threshold 检测条件且触发事件为 Notification 时，需要添加此绑定对象组中的绑定变量。

undo object list 命令用来恢复缺省情况。

【命令】

```
object list owner group-owner name group-name  
undo object list
```

【缺省情况】

未指定绑定对象组。

【视图】

Trigger-threshold 视图

【缺省用户角色】

network-admin
context-admin

【参数】

group-owner: 绑定对象组的所有者，与 Trigger 表中配置的 Trigger 所有者 owner 相同。

group-name: 绑定对象组的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

参考 Trigger 视图下的 **object list** 命令。

【举例】

```
# 配置对应的绑定对象组。
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] object list owner owner1 name objectA
```

【相关命令】

- **snmp mib event trigger**
- **test**

1.1.24 oid (Action-notification view)

oid 命令用来配置执行 Notification 事件时需要发送的 Notification 的 OID。

undo oid 命令用来恢复缺省情况。

【命令】

```
oid object-identifier
undo oid
```

【缺省情况】

OID 为 0.0，表示未指定发送 Notification 的 OID。

【视图】

Action-notification 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

object-identifier: 指定发送 Notification 的 OID 值，为 1~255 个字符的字符串，区分大小写。
此 OID 对应的节点必须为告警节点。

【使用指导】

本命令用于配置事件类型为 Notification 时需要发送具体 Notification 的 OID。

【举例】

```
# 设置用户名为 owner1，事件名为 EventA 发送的 notification 的 OID 为 1.3.6.1.2.1.14.16.2.1。
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action notification
[Sysname-event-owner1-EventA-notification] oid 1.3.6.1.2.1.14.16.2.1
```

【相关命令】

- **snmp mib event owner**
- **action**

1.1.25 oid (Action-set view)

oid 命令用来配置事件 Set 操作对象的 OID 值。

undo oid 命令用来恢复缺省情况。

【命令】

oid *object-identifier*

undo oid

【缺省情况】

OID 为 0.0，表示未配置 Set 操作对象。

【视图】

Action-set 视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-identifier: Set 操作对象的 OID，取值为节点 OID 值或者节点名称，为 1~255 个字符的字符串，区分大小写。Set 操作对象可以是表节点、概念行节点、表中列节点、简单叶子节点、叶节点的父节点中的任意一种。

【举例】

设置用户名 owner1，事件名为 EventA 的 set 对象的 OID 为 1.3.6.1.2.1.2.2.1.7.3。

```
<Sysname> system-view
```

```
[Sysname] snmp mib event owner owner1 name EventA
```

```
[Sysname-event-owner1-EventA] action set
```

```
[Sysname-event-owner1-EventA-set] oid 1.3.6.1.2.1.2.2.1.7.3
```

【相关命令】

- **snmp mib event owner**
- **action**
- **wildcard oid** (Action-set view)

1.1.26 oid (Trigger view)

oid 命令用来配置 Trigger 采样的 MIB 节点。

undo oid 命令用来恢复缺省情况。

【命令】

oid *object-identifier*

undo oid

【缺省情况】

OID 为 0.0，表示未配置 Trigger 采样的 MIB 节点，即未指定 Trigger 的监控对象。

【视图】

Trigger 视图

【缺省用户角色】

network-admin

context-admin

【参数】

object-identifier: Trigger 进行采样的 MIB 节点，即 Trigger 的监控对象，可以是表节点、概念行节点、表中列节点、简单叶子节点、叶节点的父节点中的任意一种。取值为节点 OID 或者节点名称，为 1~255 个字符的字符串，区分大小写。

【使用指导】

该命令用来指定 MIB 节点作为监控对象，当配置该命令后，该 Trigger 生效时将按指定的采样间隔周期性地获取该监控对象的值用来判定是否满足事件触发条件。

【举例】

```
# 配置 Trigger 采样的节点值为 1.3.6.1.2.1.2.2.1.1.3。  
<Sysname> system-view  
[Sysname] snmp mib event trigger owner owner1 name triggerA  
[Sysname-trigger-owner1-triggerA] oid 1.3.6.1.2.1.2.2.1.1.3
```

【相关命令】

- **snmp mib event trigger**

1.1.27 rising

rising 命令用来配置绝对值采样类型的上限阈值，并指定采样值大于等于该阈值时触发的事件。

undo rising 命令用来恢复缺省情况。

【命令】

```
rising { event owner event-owner name event-name | value integer-value }  
undo rising { event | value }
```

【缺省情况】

上限阈值为 0，未配置对应的触发事件。

【视图】

Trigger-threshold 视图

【缺省用户角色】

network-admin

context-admin

【参数】

event owner *event-owner*: 配置上限阈值事件的所有者，与 Trigger 配置的 owner 相同。

name *event-name*: 配置上限阈值对应的事件名，为 1~32 个字符的字符串，区分大小写。

value *integer-value*: 绝对值采样的上限阈值，取值范围为-2147483648~2147483647。可以配置任意不小于下限阈值的整数。

【使用指导】

采样类型为绝对值采样时，采样值达到或超过上限阈值时，将触发对应的事件。

若采样值连续多次达到或超过上限阈值，只会在第一次触发对应的事件，上限和下限对应事件的触发是交替产生的。

【举例】

```
# 配置 threshold 测试的上限阈值为 50，对应的事件所有者为 owner1，事件名为 event1。
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] rising value 50
[Sysname-trigger-owner1-triggerA-threshold] rising event owner owner1 name event1
```

【相关命令】

- **snmp mib event trigger**
- **test**
- **sample**

1.1.28 sample

sample 命令用来配置 Trigger 采样的类型。

undo sample 命令用来恢复缺省情况。

【命令】

```
sample { absolute | delta }
undo sample
```

【缺省情况】

Trigger 采样类型为绝对值采样。

【视图】

Trigger 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

absolute: 采样类型为绝对值采样，即采样时间到达时直接获取监控对象的值。

delta: 采样类型为差值采样，即采样时间到达时获取的是监控对象本次与上次采样的差值。

【使用指导】

采样类型为差值采样时，获取本次差值的算法与对应监控对象值类型有关。具体如下：

- 如果监控对象值类型为 **UINT** 类型，则获取本次差值算法：本次采样值与前一次采样值比较，取两者中的较大值减去较小值，保证差值为正值（即也为 **UINT** 类型）；
- 如果监控对象值类型为 **INT** 类型，则获取本次差值算法：当前采样值减去前一次采样值取差值。

【举例】

配置 Trigger 采样的类型为绝对值采样。

```
<Sysname>system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] sample absolute
```

【相关命令】

- **snmp mib event trigger**

1.1.29 snmp mib event

snmp mib event 命令用来创建一个 Event，并进入 Event 视图。如果指定的 Event 已经存在，则直接进入 Event 视图。

undo snmp mib event 命令用来删除指定的 Event。

【命令】

```
snmp mib event owner event-owner name event-name
undo snmp mib event owner event-owner name event-name
```

【缺省情况】

不存在 Event。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

event-owner：事件所有者，应该指定为已存在的 SNMPv3 用户。

event-name：事件的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

事件由所有者和事件名唯一识别。进入 Event 视图后可以配置事件描述、事件动作和事件使能。

【举例】

创建一个事件，其所有者为 owner1，事件名为 EventA，并进入该 Event 视图。

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
```

[Sysname-event-owner1-EventA]

【相关命令】

- **snmp mib event**
- **description**
- **event enable**
- **action**

1.1.30 snmp mib event object list

snmp mib event object list 命令用来配置事件的绑定对象组的信息。

undo snmp mib event object list 命令用来恢复缺省情况。

【命令】

snmp mib event object list owner group-owner name group-name object-index oid object-identifier [wildcard]

undo snmp mib event object list owner group-owner name group-name object-index

【缺省情况】

未指定绑定对象组。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

owner group-owner: 对象组所有者，应该指定为已存在的 SNMPv3 用户。

name group-name: 创建的对象组名，其中组名为 1~32 个字符的字符串，区分大小写。

object-index: 绑定对象表的三级索引，取值范围为 1~4294967295。

oid object-identifier: 绑定的对象，取值为该对象节点 OID 值或者节点名称，为 1~255 个字符的字符串，区分大小写。绑定的节点必须为表节点、概念行节点、表中列节点、简单叶子节点、叶节点的父节点中的任意一种。

wildcard: 表示绑定对象的匹配方式为通配。如未指定该参数，则表示绑定对象的匹配方式为精确匹配。

【使用指导】

绑定的对象由对象组所有者、对象组名和对象表的三级索引唯一确定，用来配置事件的绑定对象组的信息。Event 事件对应动作为 Notification，发送相应的 Trap 时可以从该配置的绑定对象组中获取信息。Notification 绑定的对象组信息是向网管提供其关心的相关数据。

【举例】

配置一个对象列表的信息，其中对象组所有者为 owner1，创建的对象组名为 objectA，绑定对象表的三级索引为 10，绑定对象节点 OID 值为 1.3.6.1.2.1.2.2.1.1.3。

```
<Sysname> system-view
```

```
[Sysname] snmp mib event object list owner owner1 name objectA 10 oid 1.3.6.1.2.1.2.2.1.1.3
```

【相关命令】

- **snmp mib event**
- **snmp mib event trigger**

1.1.31 snmp mib event sample instance maximum

snmp mib event sample instance maximum 命令用来设置系统可同时采样的最大监控对象实例数。

undo snmp mib event sample instance maximum 命令用来恢复缺省情况。

【命令】

```
snmp mib event sample instance maximum max-number
```

```
undo snmp mib event sample instance maximum
```

【缺省情况】

系统可同时采样的最大监控对象实例数为 0，表示采样时对监控对象实例数无限制。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

max-number：系统可同时采样的最大监控对象实例数，取值范围为 0～4294967295。

【使用指导】

当前活动状态的采样实例数：如果此次多个监控对象属性均为通配，即每个监控对象对应多个行实例，则当前活动状态的采样实例数为这些通配对象所有行实例的累加值。**max-number** 值为 0 表示没有上限，无特殊资源限制时应为 0。

最大采样实例数的修改与否存在如下情况：

- 修改此节点不影响已经为活动状态的采样实例，比如修改最大采样行实例数小于活动状态采样实例数，原来处于活动状态的行实例数不会减少，但此时如果出现新的行实例则当前行实例数不会新增；
- 最大采样实例数不变，当前采样实例数小于最大采样实例数，此时如果 **Trigger** 实例有新增，则当前采样实例数会更新，每采样一个实例，当前采样实例数就更新一次，并与配置的最大采样实例数比较，如果更新值刚好达到最大采样实例数，则之后新增的实例就不会再采样。

【举例】

```
# 设置系统可同时采样的最大监控对象实例数为 10。
<Sysname> system-view
[Sysname] snmp mib event sample instance maximum 10
```

【相关命令】

- **snmp mib event sample minimum**

1.1.32 snmp mib event sample minimum

snmp mib event sample minimum 命令用来配置全局允许的最小采样时间间隔。
undo snmp mib event sample minimum 命令用来恢复缺省情况。

【命令】

```
snmp mib event sample minimum min-number
undo snmp mib event sample minimum
```

【缺省情况】

全局允许的最小采样时间间隔为 1 秒。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

min-number：全局允许的最小采样时间间隔，取值范围为 1～2147483647，单位为秒。

【使用指导】

为减少持续采样的系统开销，新配置的 **Trigger** 采样时间间隔必须大于等于该值，否则无法成功采样；

修改本节点不影响正在被采样的 **Trigger**，即使正在被采样的 **Trigger** 的采样间隔小于新配置的最小采样间隔，也可以正常采样。

【举例】

```
# 设置采样的全局最小间隔时间为 50 秒。
<Sysname> system-view
[Sysname] snmp mib event sample minimum 50
```

【相关命令】

- **snmp mib event trigger**
- **frequency**

1.1.33 snmp mib event trigger

snmp mib event trigger 命令用来创建一个 Trigger，并进入 Trigger 视图。如果指定的 Trigger 已经存在，则直接进入 Trigger 视图。

undo snmp mib event trigger 命令用来删除指定的 Trigger。

【命令】

```
snmp mib event trigger owner trigger-owner name trigger-name  
undo snmp mib event trigger owner trigger-owner name trigger-name
```

【缺省情况】

不存在 Trigger。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

trigger-owner: Trigger 所有者，为 1~32 个字符的字符串，区分大小写。该 Trigger 所有者需指定为一个已存在的 SNMPv3 用户，用于判断对监控对象是否有操作权限。

trigger-name: Trigger 名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

Trigger 由所有者和名称唯一确定。进入指定的 Trigger 视图，可以指定监控的 MIB 对象，定时对指定的 MIB 对象进行采样。当获取监控对象所处的状态满足用户配置的事件触发条件时，就会触发相应的事件。

若 Trigger 所有者对该 Trigger 视图下配置的采样节点没有读权限，则采样失败。有关 SNMPv3 用户操作权限的详细介绍，请参见“网络管理与监控”中的“SNMP”。

【举例】

```
# 配置 Trigger 所有者 owner1，Trigger 名称 triggerA，并进入 Trigger 视图。  
<Sysname> system-view  
[Sysname] snmp mib event trigger owner owner1 name triggerA  
[Sysname-trigger-owner1-triggerA]
```

1.1.34 snmp-agent trap enable event-mib

snmp-agent trap enable event-mib 命令用来开启 Event MIB 的告警功能。

undo snmp-agent trap enable event-mib 命令用来关闭 Event MIB 的告警功能。

【命令】

```
snmp-agent trap enable event-mib  
undo snmp-agent trap enable event-mib
```

【缺省情况】

Event MIB 的告警功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

开启 Event MIB 模块的告警功能后，当配置的监控对象采样失败或者满足触发 Trigger 的条件时会产生告警信息，该告警信息包括 Trigger 触发告警、Trigger 触发上限阈值告警、Trigger 触发下限阈值告警、Trigger 触发条件检查失败告警、Trigger 触发事件 Set 动作失败的告警。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。

有关告警信息的详细介绍，请参见“网络管理与监控”中的“SNMP”。

【举例】

```
# 开启 Event MIB 的告警功能。
<Sysname> system-view
[Sysname] snmp-agent trap enable event-mib
```

1.1.35 startup (Trigger-existence view)

startup 命令用来配置首次采样允许触发事件的检测子类型。

undo startup 命令用来关闭指定的检测子类型。

【命令】

```
startup { absent | present }
undo startup { absent | present }
```

【缺省情况】

首次采样允许触发事件的检测子类型为 present 和 absent。

【视图】

Trigger-existence 视图

【缺省用户角色】

network-admin

context-admin

【参数】

absent: 首次采样时，如果指定的监控对象不存在，且使用命令 **type** 配置采样检测类型 Absent，则触发指定的事件。

present: 首次采样时，如果指定的监控对象存在，且使用命令 **type** 配置采样检测类型为 Present，则触发指定的事件。

【使用指导】

本命令作为 **type** 命令的扩展配置，用于首次采样时，若指定的监控对象满足 **type** 指定的检测类型，判断是否触发指定事件。具体如下：

- 当 **type** 和 **startup** 均配置为 **Present**，如果监控对象为精确匹配，首次采样时监控对象存在则触发指定事件；如果监控对象为通配，首次采样时针对每个通配的对象单独触发指定事件。
- 当 **type** 和 **startup** 均配置为 **Absent**，如果监控对象为精确匹配，首次采样时监控对象不存在则触发指定事件；如果监控对象为通配，首次采样不会触发事件。

其他情况下，首次采样都不会触发事件。

【举例】

关闭首次采样允许触发事件的 **Present** 检测子类型。

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test existence
[Sysname-trigger-owner1-triggerA-existence] undo startup present
```

【相关命令】

- **type**

1.1.36 startup (Trigger-threshold view)

startup 命令用来配置绝对值采样时首次采样允许触发的告警类型。

undo startup 命令用来恢复缺省情况。

【命令】

```
startup { falling | rising | rising-or-falling }
undo startup
```

【缺省情况】

绝对值采样时，首次采样允许触发的告警类型为 **rising-or-falling**，即可以触发上限或下限告警。

【视图】

Trigger-threshold 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

falling：表示只触发下限告警。

rising：表示只触发上限告警。

rising-or-falling：表示可以触发上限或下限告警。

【使用指导】

采样类型为绝对值采样时：

- 若首次采样允许触发的告警类型配置为 **rising** 或者 **rising-or-falling**，当首次采样值大于等于配置的上限阈值时，触发上限告警；
- 若首次采样允许触发的告警类型配置为 **falling** 或者 **rising-or-falling**，当首次采样值小于等于配置的下限阈值时，触发下限告警。
- 若前一次采样过程出错或监控对象不存在，那么此次对此监控对象的采样作为第一次采样来处理。

【举例】

配置绝对值采样时首次采样允许触发的告警类型为触发上限告警。

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test threshold
[Sysname-trigger-owner1-triggerA-threshold] startup rising
```

【相关命令】

- **snmp mib event trigger**
- **test**
- **sample**

1.1.37 startup enable

startup enable 命令用来配置首次采样值满足检测条件时触发相应的事件。

undo startup enable 命令用来配置首次采样值满足检测条件时不触发相应的事件。

【命令】

```
startup enable
undo startup enable
```

【缺省情况】

首次采样值满足检测条件时会触发相应的事件。

【视图】

Trigger-boolean 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

当监控节点首次采样值满足 Boolean 测试条件时，并且配置了 **startup enable** 命令才会触发相应的事件，否则将不会触发相应的事件。

若前一次采样过程出错或监控对象不存在，那么此次对该监控对象的采样作为第一次采样来处理。

【举例】

```
# 配置首次采样满足检测条件时触发相应的事件。
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test boolean
[Sysname-trigger-owner1-triggerA-boolean] startup enable
```

【相关命令】

- **comparison**
- **value**

1.1.38 test

test 命令用来配置 Trigger 触发条件的检测类型，并进入相应的 Trigger-test 视图。

undo test 命令用来取消指定的检测类型。

【命令】

```
test { boolean | existence | threshold }
undo test { boolean | existence | threshold }
```

【缺省情况】

未配置 Trigger 触发条件的检测类型。

【视图】

Trigger 视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

boolean: Trigger 触发条件的检测类型为 Boolean 类型，主要用于对监控对象的值与参考值的大小比较等检查条件的设置。

existence: Trigger 触发条件的检测类型为 Existence 类型，主要用于对监控对象存在、消失或者改变等状态的检查条件的设置。

threshold: Trigger 触发条件的检测类型为 Threshold 类型，主要用于对监控对象的值是否超过上限阈值或者低于下限阈值等检查条件的设置。

【使用指导】

用户使用本命令可以配置 Trigger 运行的测试类型（Existence、Boolean、Threshold）。且每种类型都有相应的表（Existence 表、Boolean 表、Threshold 表）与之对应，详细设置请参见对应的 Trigger-boolean 视图、Trigger-existence 视图、Trigger-threshold 视图下的命令。

【举例】

```
# 配置 Trigger 触发条件的检测类型为 Existence。
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
```

```
[Sysname-trigger-owner1-triggerA] test existence
```

【相关命令】

- **snmp mib event trigger**

1.1.39 trigger enable

trigger enable 命令用来开启 Trigger 采样功能。

undo trigger enable 命令用来关闭 Trigger 采样功能。

【命令】

```
trigger enable
undo trigger enable
```

【缺省情况】

Trigger 采样功能处于关闭状态。

【视图】

trigger 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

在开启 Trigger 采样功能前，需要先检查 Trigger 是否满足可以开启的条件：

- 必须指定监控对象；
- 采样时间间隔必须大于等于系统支持的最小采样时间间隔。

【举例】

#当前最小采样时间间隔为 100，开启 Trigger 的采样功能。

```
<Sysname>system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] oid 1.3.6.1.2.1.2.2.1.1.3
[Sysname-trigger-owner1-triggerA] frequency 360
[Sysname-trigger-owner1-triggerA] trigger enable
```

【相关命令】

- **snmp mib event trigger**

1.1.40 type

type 命令用来指定 Trigger-existence 视图下的检测类型。

undo type 命令用于取消检测类型配置。

【命令】

```
type { absent | changed | present }
undo type { absent | changed | present }
```

【缺省情况】

检测类型为 Present 和 Absent。

【视图】

Trigger-existence 视图

【缺省用户角色】

network-admin

context-admin

【参数】

absent: 此次 Trigger 监控对象不存在，上一次 Trigger 监控对象存在，将触发指定的事件。首次采样时，若监控对象属性为精确匹配且监控对象不存在，必须同时满足设置命令 **startup absent**，才会触发相应事件。

changed: 当 Trigger 监控对象的值发生改变时，触发指定事件。如果上一次采样值获取不到则不触发。

present: 此次 Trigger 监控对象存在，上一次 Trigger 监控对象不存在，将触发指定的事件。首次采样时，若监控对象存在，必须同时满足设置命令 **startup present**，才会触发相应事件。

【使用指导】

对于第一次采样，参考 **startup** 命令使用指导。

如果不是第一次采样：

- 当执行 **type present** 命令时，对于精确匹配，如果此次监控对象存在，前一次监控对象不存在，则触发指定事件；对于通配，获取当前监控对象的集合，将其中的每一个监控对象都与前一次通配到的所有监控对象比较，如果前一次无相同的监控对象，则触发指定事件。
- 当执行 **type absent** 命令时，对于精确匹配，如果此次监控对象不存在，前一次监控对象存在，则触发指定事件；对于通配，获取当前监控对象的集合，将前一次的每一个监控对象都与此次通配到的所有监控对象比较，如果此次无相同的监控对象，则触发指定事件。
- 当执行 **type changed** 命令时，对于精确匹配，如果此次与前一次都有相同的监控对象，那么会将两次监控对象的值进行比较，若其值不同，则触发指定事件；对于通配，获取当前监控对象的集合，将其中的每一个监控对象都与前一次通配到的所有监控对象比较，如果两次都有相同的监控对象，那么比较两次监控对象的值，若其值不同，则触发指定事件。

【举例】

配置 Trigger-existence 子视图下检测类型为 Present。

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test existence
[Sysname-trigger-owner1-triggerA-existence] type present
```

【相关命令】

- **snmp mib event trigger**
- **test**
- **startup**

1.1.41 value (Action-set view)

value 命令用来配置 Set 操作对象的值。

undo value 命令用来恢复缺省情况。

【命令】

value *integer-value*

undo value

【缺省情况】

Set 操作对象的值为 0。

【视图】

Action-set 视图

【缺省用户角色】

network-admin

context-admin

【参数】

integer-value: Set 操作对象的值，取值范围为-2147483648～2147483647。

【举例】

将 Set 操作对象 1.3.6.1.2.1.2.2.1.7.3 的值设置为 2。

```
<Sysname> system-view
```

```
[Sysname] snmp mib event owner owner1 name EventA
```

```
[Sysname-event-owner1-EventA] action set
```

```
[Sysname-event-owner1-EventA-set] oid 1.3.6.1.2.1.2.2.1.7.3
```

```
[Sysname-event-owner1-EventA-set] value 2
```

【相关命令】

- **snmp mib event owner**
- **action**
- **oid**

1.1.42 value (Trigger-boolean view)

value 命令用来配置与采样值进行比较的参考值。

undo value 命令用来恢复缺省情况。

【命令】

value *integer-value*

undo value

【缺省情况】

与采样值进行比较的参考值为 0。

【视图】

Trigger-boolean 视图

【缺省用户角色】

network-admin

context-admin

【参数】

integer-value: 用于跟采样值进行比较的参考值，取值范围为-2147483648～2147483647。

【使用指导】

根据 **comparison** 命令配置的比较方式，将获取的采样值与 **value** 命令配置的参考值进行比较并确定是否满足检测条件。

【举例】

配置与采样值进行比较使用的参考值为 5。

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] test boolean
[Sysname-trigger-owner1-triggerA-boolean] value 5
```

【相关命令】

- **comparison**

1.1.43 wildcard context (Action-set view)

wildcard context 命令用来配置 Set 对象所在上下文的匹配方式为通配。

undo wildcard context 用来恢复缺省情况。

【命令】

wildcard context

undo wildcard context

【缺省情况】

Set 对象所处上下文的匹配方式为精确匹配。

【视图】

Action-set 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

本命令和 **context** 命令配合使用，共同决定 Set 对象所在的 SNMP 上下文。精确匹配表示配置为特定的 SNMP 上下文环境名，而通配由两部分组成，一部分为 **mteEventSetContextName** 指定的 contextname，另一部分为 Trigger 表中 contextName 的通配部分。

【举例】

配置 Set 对象所处的上下文环境名为 **contextname1** 的匹配方式为通配。

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action set
[Sysname-event-owner1-EventA-set] context contextname1
[Sysname-event-owner1-EventA-set] wildcard context
```

【相关命令】

- **snmp mib event owner**
- **action set**
- **context**

1.1.44 wildcard context (Trigger view)

wildcard context 命令用来配置监控对象所在上下文的匹配方式为通配。

undo wildcard context 命令用来恢复缺省情况。

【命令】

```
wildcard context
undo wildcard context
```

【缺省情况】

监控对象所在上下文的匹配方式为精确匹配。

【视图】

Trigger 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

本命令和 **context** 命令配合使用，共同决定监控对象所在的上下文环境：

- 精确匹配表示配置为特定的上下文环境名；
- 通配表示只指定上下文的前缀，即配置系统中存在的相同前缀的所有上下文环境名。

【举例】

配置监控对象所在的上下文环境名为 **contextname** 的匹配方式为通配。

```
<Sysname> system-view
[Sysname] snmp mib event trigger owner owner1 name triggerA
[Sysname-trigger-owner1-triggerA] context contextname
[Sysname-trigger-owner1-triggerA] wildcard context
```

【相关命令】

- **snmp mib event trigger**
- **context**

1.1.45 wildcard oid (Action-set view)

wildcard oid 命令用来配置 Set 操作对象的匹配方式为通配。

undo wildcard oid 命令用来恢复缺省情况。

【命令】

```
wildcard oid
undo wildcard oid
```

【缺省情况】

Set 操作对象的匹配方式为精确匹配。

【视图】

Action-set 视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

Set 对象的 OID 属性为通配，表示 Set 对象的 OID 由两部分组成：一部分为 mteEventSetObject 指定的 OID，另一部分为 Trigger 表中监控对象 OID 的通配部分；

Set 对象的 OID 属性为精确匹配：表示 oid 命令指定的 MIB 节点 OID 即为 Set 对象的 OID。

【举例】

配置用户名 name1, 事件名为 EventA 的 Set 对象 OID 为 1.3.6.1.2.1.2.2.1.7 的匹配方式为通配。

```
<Sysname> system-view
[Sysname] snmp mib event owner owner1 name EventA
[Sysname-event-owner1-EventA] action set
[Sysname-event-owner1-EventA-set] oid 1.3.6.1.2.1.2.2.1.7
[Sysname-event-owner1-EventA-set] wildcard oid
```

【相关命令】

- **snmp mib event owner**
- **action set**
- **oid**

1.1.46 wildcard oid (Trigger view)

wildcard oid 命令用来配置 Trigger 采样的 MIB 节点的匹配方式为通配。

undo wildcard oid 命令用来恢复缺省情况。

【命令】

```
wildcard oid
undo wildcard oid
```

【缺省情况】

Trigger 采样的 MIB 节点匹配方式为精确匹配。

【视图】

Trigger 视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

本命令与 **oid** 命令配合使用，共同决定监控的对象：

- 当匹配类型为精确匹配时，表示 **oid** 命令指定的监控对象为一个具体的实例，比如需要监控接口索引为 2 的接口描述节点，则配置 **oid ifDescr.2**，匹配类型配置为精确匹配。
- 当匹配类型为通配时，表示 **oid** 命令只指定了监控对象的 OID 前缀，系统中存在的所有 MIB 对象只要前缀与此相同均作为监控对象，比如需要监控所有接口对应的接口描述节点，则配置 **oid ifDescr**，并将匹配类型配置为通配。

【举例】

配置 trigger 采样的节点值为 1.3.6.1.2.1.1.6，采样节点匹配方式为通配。

```
<Sysname>system-view
```

```
[Sysname] snmp mib event trigger owner owner1 name triggerA
```

```
[Sysname-trigger-owner1-triggerA] oid 1.3.6.1.2.1.1.6
```

```
[Sysname-trigger-owner1-triggerA] wildcard oid
```

【相关命令】

- **snmp mib event trigger**
- **oid**

目 录

1 NETCONF	1-1
1.1 NETCONF配置命令	1-1
1.1.1 display netconf service	1-1
1.1.2 display netconf session	1-2
1.1.3 netconf capability specific-namespace	1-4
1.1.4 netconf idle-timeout	1-4
1.1.5 netconf log	1-5
1.1.6 netconf soap acl	1-7
1.1.7 netconf soap domain	1-8
1.1.8 netconf soap enable	1-9
1.1.9 netconf soap http port	1-10
1.1.10 netconf ssh acl	1-10
1.1.11 netconf ssh server enable	1-11
1.1.12 netconf ssh server port	1-12
1.1.13 reset netconf service statistics	1-13
1.1.14 reset netconf session statistics	1-13
1.1.15 xml	1-14

1 NETCONF

1.1 NETCONF配置命令

1.1.1 display netconf service

display netconf service 命令用来显示当前 NETCONF 服务的状态及全局统计信息。

【命令】

display netconf service

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示当前 NETCONF 服务的状态及全局统计信息。

```
<Sysname> display netconf service
NETCONF over SOAP over HTTP: Enabled (port 80)
NETCONF over SOAP over HTTPS: Enabled (port 443)
NETCONF over SSH: Enabled (port 830)
NETCONF over Telnet: Enabled
NETCONF over Console: Enabled
SOAP timeout: 10 minutes    Agent timeout: 10 minutes
Active sessions: 1
Service statistics:
NETCONF start time: 2015-10-10T08:08:08
Output notifications: 50
Output RPC errors: 20
Dropped sessions: 0
Sessions: 100
Received bad hellos: 0
Received RPCs: 1000
Received bad RPCs: 20
```

表1-1 display netconf service 命令显示信息描述表

字段	描述
NETCONF over SOAP over HTTP	基于HTTP的SOAP的NETCONF服务状态、以及监听端口号： - Enabled 表示该服务处于开启状态 - Disabled 表示该服务处于关闭状态
NETCONF over SOAP over HTTPS	基于HTTPS的SOAP的NETCONF服务状态、以及监听端口号： - Enabled 表示该服务处于开启状态 - Disabled 表示该服务处于关闭状态
NETCONF over SSH	基于SSH的NETCONF服务状态、以及监听端口号： - Enabled 表示该服务处于开启状态 - Disabled 表示该服务处于关闭状态
NETCONF over Telnet	基于Telnet的NETCONF服务状态： - Enabled 表示该服务处于开启状态 - Disabled 表示该服务处于关闭状态
NETCONF over Console	基于Console和AUX的NETCONF服务状态： - Enabled 表示该服务处于开启状态 - Disabled 表示该服务处于关闭状态
SOAP timeout	基于NETCONF over SOAP over HTTP/HTTPS的会话超时时间，单位为分钟
Agent timeout	基于NETCONF over SSH/Telnet/Console的会话超时时间，单位为分钟
Active sessions	当前活跃的NETCONF会话数量
Service statistics	NETCONF服务运行过程中的统计信息： - NETCONF start time 表示 NETCONF 服务的开启时间 - Output notifications 表示设备输出的订阅日志数量 - Output RPC errors 表示设备输出的错误 RPC 请求数量 - Dropped sessions 表示因超时和异常断开而丢弃的会话的数量 - Sessions 表示设备建立的 NETCONF 会话数量 - Received bad hellos 表示设备接收的错误 Hello 信息数量 - Received RPCs 表示设备接收的 RPC 总数 - Received bad RPCs 表示设备接收的错误 RPC 总数

1.1.2 display netconf session

display netconf session 命令用来显示 NETCONF 会话信息。

【命令】

display netconf session

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 显示当前 NETCONF 会话信息。
<Sysname> display netconf session
Session ID: 1 Session type: Agent
Username: test
Login time: 2015-10-10T08:08:08
Client IP address: 192.168.1.1
Session statistics:
Received RPCs      : 10          Received bad RPCs    : 0
  Output RPC errors: 10          Output notifications: 0
Session ID: 2 Session type: SOAP
Username: test
Login time: 2015-10-10T08:08:08
Client IP address: 192.168.1.1
Session statistics:
  Received RPCs      : 10          Received bad RPCs    : 0
  Output RPC errors: 10          Output notifications: 0
```

表1-2 display netconf session 命令显示信息描述表

字段	描述
Session ID	当前NETCONF会话的ID
Session type	当前NETCONF会话类型： • soap 表示基于 NETCONF over SOAP over HTTP/HTTPS 的会话 • agent 表示基于 NETCONF over SSH/Telnet/Console 的会话
Username	与设备建立NETCONF会话时使用的用户名称 对于SOAP类型的NETCONF会话，此处显示为用户名；对于Agent类型的NETCONF会话： • 配置为认证登录时，此处显示为用户名 • 配置为无认证登录时，此处显示为“-”
Login time	与设备建立NETCONF会话的时间
Client IP address	与设备建立NETCONF会话的客户端IP地址 如果使用Console或AUX与设备建立NETCONF会话，此处显示为“-”

字段	描述
Session statistics	当前NETCONF会话的统计信息: - Received RPCs 表示包括设备接收到的 NETCONF 请求报文数量 - Received bad RPCs 表示设备接收到的无法处理的请求报文数量 - Output RPC errors 表示设备输出的 RPC 错误报文数量 - Output notifications 表示设备输出的 NETCONF 通知数量

1.1.3 netconf capability specific-namespace

netconf capability specific-namespace 命令用来配置设备使用专用命名空间。

undo netconf capability specific-namespace 命令用来恢复缺省情况。

【命令】

```
netconf capability specific-namespace
undo netconf capability specific-namespace
```

【缺省情况】

NETCONF 使用共用命名空间。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

设备支持共用命名空间和专用命名空间，两种类型的命名空间互不兼容。客户端与设备必须使用相同的命名空间才能建立会话。缺省情况下，设备使用共用命名空间。如果客户端不支持共用命名空间，则需要配置本命令，让设备和客户端建立会话时使用专用命名空间。

配置该命令后，用户需要重新建立 NETCONF 会话，以使客户端和设备使用相同的命名空间。

【举例】

```
# 配置设备使用专用命名空间。
<Sysname> system-view
[Sysname] netconf capability specific-namespace
```

1.1.4 netconf idle-timeout

netconf idle-timeout 命令用来配置 NETCONF 会话超时时间。

undo netconf idle-timeout 命令用来恢复缺省情况。

【命令】

```
netconf { soap | agent } idle-timeout minute
undo netconf { soap | agent } idle-timeout
```

【缺省情况】

基于 NETCONF over SOAP over HTTP 和 NETCONF over SOAP over HTTPS 的会话超时时间为 10 分钟。

基于 NETCONF over SSH、NETCONF over Telnet 和 NETCONF over Console 的会话超时时间为 0，即不超时。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

soap: 用来配置基于 NETCONF over SOAP over HTTP 和 NETCONF over SOAP over HTTPS 的会话超时时间。

agent: 用来配置基于 NETCONF over SSH、NETCONF over Telnet 和 NETCONF over Console 的会话超时时间。

minute: 表示空闲超时时间，单位为分钟，取值范围为：

- 对于基于 NETCONF over SOAP over HTTP 和 NETCONF over SOAP over HTTPS 的会话，取值范围为 1~999。
- 对于基于 NETCONF over SSH、NETCONF over Telnet 和 NETCONF over Console 的会话，取值范围为 0~999，0 表示不超时。

【使用指导】

用户通过 Telnet、SSH、Console、或配置工具与设备建立 NETCONF 连接，如果在超时时间内，用户与设备无任何 NETCONF 报文交互，达到超时时间后，设备将断开与用户配置端的 NETCONF 连接。

【举例】

配置基于 NETCONF over SOAP over HTTP 和 NETCONF over SOAP over HTTPS 的会话超时时间为 20 分钟。

```
<Sysname> system-view
```

```
[Sysname] netconf soap idle-timeout 20
```

1.1.5 netconf log

netconf log 命令用来配置 NETCONF 日志功能。

undo netconf log 命令用来取消指定类型的 NETCONF 日志配置。

【命令】

```
netconf log source { all | { agent | soap | web } * } { protocol-operation  
{ all | { action | config | get | session | set | syntax | others } * } |  
row-operation | verbose }
```

```
undo netconf log source { all | { agent | soap | web } * } { protocol-operation  
{ all | { action | config | get | session | set | syntax | others } * } |  
row-operation | verbose }
```

【缺省情况】

未配置 NETCONF 日志功能。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

source: 表示需要输出日志的 NETCONF 操作来源:

- **all:** 表示输出所有来源的 NETCONF 日志。
- **agent:** 表示输出源自 Telnet/SSH/NETCONF over SSH/Console 类型的 NETCONF 日志。
- **soap:** 表示输出源自 SOAP over HTTP 和 SOAP over HTTPS 类型的 NETCONF 日志。
- **web:** 表示输出源自本设备 Web 类型的 NETCONF 日志。

protocol-operation: 表示按 NETCONF 操作类型输出日志:

- **all:** 表示所有 NETCONF 操作类型。
- **action:** 表示 action 操作。
- **config:** 表示配置类的 NETCONF 操作, 包括 CLI、save、load、rollback、save-point、lock、unlock。
- **get:** 表示获取数据的 NETCONF 操作, 包括 get、get-bulk、get-config、get-bulk-config、get-sessions。
- **session:** 表示与会话相关的 NETCONF 操作, 包括 kill-session、close-session、hello。
- **set:** 表示所有 edit-config 操作。
- **syntax:** 表示包含 xml 和 schema 的格式错误的请求。
- **others:** 表示除 action、config、get、set、session、set、syntax 外, 其他类型的 NETCONF 操作。

row-operation: 表示按 NETCONF 行操作输出日志。该参数仅支持 action 和 set 操作。

verbose: 表示输出 NETCONF 操作的详细日志信息。

- 对于请求类型的日志: 当请求报文格式正确时, 设备在简要日志后输出源报文的内容。
- 对于处理结果类型的日志: 仅支持输出 **set** 的详细日志信息。即, 当 edit-config 操作执行错误时输出详细错误信息。

【使用指导】

NETCONF 日志功能支持按 NETCONF 操作类型 (**protocol-operation**) 输出日志和按 NETCONF 行操作 (**row-operation**) 输出日志:

- 配置按 NETCONF 操作类型输出日志时，用户每下发一次 NETCONF 操作，设备输出该 NETCONF 操作、以及操作结果的日志。例如用户下发 NETCONF 操作，创建 ID 为 3~5 的 VLAN 时，设备输出的日志如下：

```
%Mar 21 17:11:34:479 2017 Sysname XMLSOAP/6/XML_REQUEST: test from 192.168.100.198, session id 2,message-id 100, receive edit-config request.
```

```
%Mar 21 17:11:34:483 2017 Sysname XMLSOAP/6/EDIT-CONFIG: test from 192.168.100.198, session id 2,message-id 100, execute success.
```

- 配置按 NETCONF 行操作输出日志时，用户下发一次 NETCONF 操作后，设备输出该操作中每个请求行操作的日志，日志中包含 NETCONF 行操作名称和处理结果。例如用户下发 NETCONF 操作，创建 ID 为 3~5 的 VLAN 时，设备输出的日志如下：

```
%Mar 31 17:50:02:608 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20, session ID 1), message ID=100, operation=create VLAN/VLANS (ID=3), result=Succeeded. No attributes.
```

```
%Mar 31 17:50:02:609 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20, session ID 1), message ID=100, operation=create VLAN/VLANS (ID=4), result=Succeeded. No attributes.
```

```
%Mar 31 17:50:02:611 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20, session ID 1), message ID=100, operation=create VLAN/VLANS (ID=5), result=Succeeded. No attributes.
```

设备先将 NETCONF 日志发送到信息中心，根据信息中心的输出规则将日志信息输出到不同方向。信息中心的相关配置请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

配置设备输出源自 agent 的 edit-config 类型的操作日志。

```
<Sysname> system-view
```

```
[sysname] netconf log source agent protocol-operation set
```

1.1.6 netconf soap acl

netconf soap acl 命令用来配置 NETCONF over SOAP 关联 ACL。

undo netconf soap acl 命令用来恢复缺省情况。

【命令】

```
netconf soap { http | https } [ ipv6 ] acl { acl-number | name acl-name }
```

```
undo netconf soap { http | https } [ ipv6 ] acl
```

【缺省情况】

未配置 NETCONF over SOAP 关联 ACL。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

http: 开启基于 HTTP 的 NETCONF over SOAP 关联 ACL。

https: 开启基于 HTTPS 的 NETCONF over SOAP 关联 ACL。

ipv6: 指定关联的 ACL 类型为 IPv6 ACL。如果未指定本参数，则表示关联 IPv4 ACL。仅当指定 **http** 参数时，支持关联 IPv6 ACL。

acl-number: 基本 ACL 的编号，取值范围为 2000~2999。

name acl-name: 指定 ACL 的名称。**acl-name** 表示 ACL 的名称，为 1~63 个字符的字符串，不区分大小写，必须以英文字母 **a~z** 或 **A~Z** 开头。为避免混淆，ACL 的名称不允许使用英文单词 **all**。仅当指定名称的 ACL 存在且为基本 ACL 时生效。

【使用指导】

配置 SOAP 服务与 ACL 关联后，只有 ACL 允许通过的 NETCONF 客户端能够通过 SOAP 方式登录设备。不匹配 ACL 或 ACL 拒绝通过的 NETCONF 客户端将不能通过 SOAP 方式登录设备。

当未引用 ACL、引用的 ACL 不存在、或者引用的 ACL 下没有配置规则时，允许所有 NETCONF 客户端访问设备。

多次执行 **netconf soap http acl** 命令，最后一次执行的命令生效。**netconf soap https acl** 命令亦然。

【举例】

配置基于 HTTP 的 NETCONF over SOAP 功能与 IPv4 ACL 2001 关联，只允许 10.10.0.0/16 网段的客户端访问设备。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf soap http acl 2001
```

配置基于 HTTP 的 NETCONF over SOAP 功能与 IPv6 ACL 2002 关联，不允许 6::2/64 网段的客户端访问设备。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2002
[Sysname-acl-ipv6-basic-2002] rule deny source 6::2 64
[Sysname-acl-ipv6-basic-2002] quit
[Sysname] netconf soap http ipv6 acl 2002
```

1.1.7 netconf soap domain

netconf soap domain 命令用来配置 NETCONF 用户的强制认证域。

undo netconf soap domain 命令用来恢复缺省情况。

【命令】

```
netconf soap domain domain-name
undo netconf soap domain
```

【缺省情况】

未配置 NETCONF 用户的强制认证域。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

domain-name: ISP 域名，为 1~255 个字符的字符串，不区分大小写。关于 ISP 域的详细介绍请参见“安全配置指导”中的“AAA”。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

NETCONF 支持使用如下方式指定认证域：

- 通过 **netconf soap domain** 命令配置强制认证域。配置该命令后，所有用户都会使用强制认证域进行认证。
- 在 SOAP 请求的<UserName>中携带认证域信息。SOAP 请求中携带的认证域仅对当前请求生效。通过 **netconf soap domain** 命令配置强制认证域后，SOAP 请求中携带的认证域不生效。

【举例】

配置 NETCONF 用户的强制认证域为 my-domain。

```
<Sysname> system-view  
[Sysname] netconf soap domain my-domain
```

1.1.8 netconf soap enable

netconf soap enable 命令用来开启 NETCONF over SOAP 功能。

undo netconf soap enable 命令用来关闭 NETCONF over SOAP 功能。

【命令】

```
netconf soap { http | https } enable  
undo netconf soap { http | https } enable
```

【缺省情况】

NETCONF over SOAP 处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

http: 开启基于 HTTP 的 NETCONF over SOAP 功能。

https: 开启基于 HTTPS 的 NETCONF over SOAP 功能。

【使用指导】

配置该命令后，表示设备能够解析这样的 HTTP/HTTPS 报文，报文中的数据为 SOAP 封装过的 NETCONF 指令。

【举例】

```
# 开启基于 HTTP 的 SOAP 功能。  
<Sysname> system-view  
[Sysname] netconf soap http enable
```

1.1.9 netconf soap http port

netconf soap http port 命令用来配置基于 HTTP 的 NETCONF over SOAP 功能使用的端口号。

undo netconf soap http port 命令用来恢复缺省情况。

【命令】

```
netconf soap http port port-number  
undo netconf soap http port
```

【缺省情况】

基于 HTTP 的 NETCONF over SOAP 功能使用的端口号为 80。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

port-number：基于 HTTP 的 NETCONF over SOAP 功能使用的端口号，取值范围为 1~65535。

【使用指导】

配置该命令后，原 NETCONF over SOAP 会话将失效，请通过配置工具重新建立 NETCONF over SOAP 会话。

【举例】

```
# 配置基于 HTTP 的 NETCONF over SOAP 功能使用的端口号为 1000。  
<Sysname> system-view  
[Sysname] netconf soap http port 1000
```

1.1.10 netconf ssh acl

netconf ssh acl 命令用来配置 NETCONF over SSH 关联的 IPv4 ACL。

undo netconf ssh acl 命令用来恢复缺省情况。

【命令】

```
netconf ssh acl { ipv4-acl-number | name ipv4-acl-name }
```

undo netconf ssh acl

【缺省情况】

未配置 NETCONF over SSH 关联的 IPv4 ACL。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv4-acl-number: IPv4 ACL 的编号，取值范围为 2000～2999。

name ipv4-acl-name: 指定 IPv4 ACL 的名称。*ipv4-acl-name* 表示 IPv4 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，IPv4 ACL 的名称不允许使用英文单词 **all**。

【使用指导】

使用 IPv4 ACL 参数可以限制通过 SSH 访问设备的 NETCONF 客户端：

- 当未引用 IPv4 ACL 时，允许所有 NETCONF 客户端访问设备。
- 当引用的 IPv4 ACL 不存在、或者引用的 IPv4 ACL 下没有配置规则时，不允许 NETCONF 客户端访问设备。
- 当引用的 IPv4 ACL 下配置了规则时，则只有规则中 **permit** 的 NETCONF 客户端才能访问设备，其他 NETCONF 客户端不允许访问设备。
- 指定 IPv4 ACL 的名称时，仅当对应的 IPv4 ACL 存在且为基本 IPv4 ACL 时生效。

关于 ACL 的详细描述和介绍请参见“ACL 配置指导”中的“ACL”。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 NETCONF over SSH 与 ACL 2001 关联，只允许 IPv4 地址为 10.10.0.0/16 网段的客户端访问设备。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] netconf ssh acl 2001
```

【相关命令】

- **netconf soap acl**

1.1.11 netconf ssh server enable

netconf ssh server enable 命令用来开启 NETCONF over SSH 的接入方式。

undo netconf ssh server enable 命令用来关闭 NETCONF over SSH 的接入方式。

【命令】

```
netconf ssh server enable
undo netconf ssh server enable
```

【缺省情况】

NETCONF over SSH 的接入方式处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

用户配置该命令后，可以利用 SSH 客户端通过 SSH 子系统的方式接入设备的 NETCONF 系统，然后直接进入 NETCONF 配置模式，而不用手工输入 XML 命令。

配置该命令前必须在设备上把 SSH 连接终端的认证方式设置为 `scheme`，支持 NETCONF over SSH 的客户端才能连接到 NETCONF 系统，目前只支持用 `urn:ietf:params:netconf:base:1.0`（设备与终端共同支持的能力集）连接系统。

【举例】

```
# 开启 NETCONF over SSH 的接入方式。
<Sysname> system-view
[Sysname] netconf ssh server enable
```

1.1.12 netconf ssh server port

netconf ssh server port 命令用来设置 NETCONF over SSH 接入方式的监听端口号。
undo netconf ssh server port 命令用来恢复缺省情况。

【命令】

```
netconf ssh server port port-number
undo netconf ssh server port
```

【缺省情况】

NETCONF over SSH 接入方式的监听端口为 830。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

port-number：基于 NETCONF over SSH 的接入方式的监听端口，取值范围为 1～65535。

【使用指导】

用户可以在必要时使用此命令来重新配置一个端口作为 NETCONF 子系统的监听端口,但由于 SSH 服务使用共享端口的方式来分配监听端口,为了保证正常使用,必须保证分配的端口不和其他使用的端口冲突。

【举例】

```
# 配置 NETCONF over SSH 接入方式的监听端口为 800。  
<sysname> system-view  
[sysname] netconf ssh server port 800
```

1.1.13 reset netconf service statistics

reset netconf service statistics 命令用来清除当前 NETCONF 服务的全局统计信息。

【命令】

reset netconf service statistics

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 清除当前 NETCONF 服务的全局统计信息。  
<Sysname> reset netconf service statistics
```

【相关命令】

- **display netconf service**

1.1.14 reset netconf session statistics

reset netconf session statistics 命令用来清除当前 NETCONF 会话的统计信息。

【命令】

reset netconf session statistics

【视图】

用户视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 清除当前 NETCONF 的会话统计信息。  
<Sysname> reset netconf session statistics
```

【相关命令】

- **display netconf session**

1.1.15 xml

xml 命令用来进入 XML 视图。

【命令】

xml

【视图】

用户视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【使用指导】

进入 XML 视图后可以输入 NETCONF 指令来配置或者获取系统数据。用户登录时使用的角色不同，可执行的 NETCONF 操作也不同：

- network-admin 和 context-admin 可执行全部操作。
- network-operator 和 context-operator 可执行 get、get-bulk、get-config、get-bulk-config、get-sessions、close-session 操作。

进入 XML 视图后，用户需要严格按照 NETCONF 报文格式将报文拷贝、粘贴到 XML 视图中。在 NETCONF 配置过程中，请勿进行其他任何操作（例如手工输入 NETCONF 报文），否则可能导致 NETCONF 配置失败。

在 XML 视图下进行 NETCONF 配置时，NETCONF 报文最后需要添加“**]]>]]>**”，否则设备无法识别。

进入 XML 视图后，设备将自动向客户端发送自身支持的 NETCONF 能力集，此时，客户端需要向设备发送自身支持的 NETCONF 能力集，完成能力交换后，用户即可使用客户端对设备进行配置。用户输入的 NETCONF 指令必须符合 XML 语言格式要求和《NETCONF XML API 手册》中的语法、语义要求。建议使用第三方软件来协助生成 NETCONF 指令，命令行手工输入方式通常用于研发和测试环境。

退出 XML 视图时需要使用相关的 NETCONF 指令，不能使用 **quit**。

在 XML 模式下终止任务的快捷键有重置缓存的功能，快捷键之前的内容都会被清除掉。如果在用户线/用户线类视图下使用 **escape-key** 命令配置了终止任务的快捷键（缺省为 Ctrl+C），可能会影响 XML 视图下相关配置。例如：在用户线视图下配置了 **escape-key a**，当 NETCONF 指令中含有字符 ‘a’ 时，其实只有 NETCONF 指令最后一个 ‘a’ 之后的内容能够得到处理；当 NETCONF 指令中不含有字符 ‘a’ 时，则对 XML 视图下的配置没有影响。

【举例】

进入 XML 视图。


```

<Sysname> xml
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities><capability>urn:ietf:params:netconf:base:1.1</capability><capability>urn:ietf:params:netconf:writable-running</capability><capability>urn:ietf:params:netconf:capability:notification:1.0</capability><capability>urn:ietf:params:netconf:capability:validate:1.1</capability><capability>urn:ietf:params:netconf:capability:interleave:1.0</capability><capability>urn:unis:params:netconf:capability:unis-netconf-ext:1.0</capability></capabilities><session-id>1</session-id></hello>]]>]]>
# 进行能力交换。
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
      urn:ietf:params:netconf:base:1.0
    </capability>
  </capabilities>
</hello>]]>]]>
# 退出 XML 视图。
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <close-session/>
</rpc>]]>]]>
<Sysname>

```

目 录

1 进程监控和维护	1-1
1.1 进程监控和维护命令	1-1
1.1.1 display exception context	1-1
1.1.2 display exception filepath	1-6
1.1.3 display kernel deadlock	1-6
1.1.4 display kernel deadlock configuration	1-9
1.1.5 display kernel exception	1-10
1.1.6 display kernel reboot	1-13
1.1.7 display kernel starvation	1-16
1.1.8 display kernel starvation configuration	1-19
1.1.9 display process	1-20
1.1.10 display process cpu	1-23
1.1.11 display process log	1-24
1.1.12 display process memory	1-25
1.1.13 display process memory heap	1-27
1.1.14 display process memory heap address	1-28
1.1.15 display process memory heap size	1-29
1.1.16 exception filepath	1-31
1.1.17 monitor kernel deadlock action threshold	1-31
1.1.18 monitor kernel deadlock enable	1-32
1.1.19 monitor kernel deadlock exclude-thread	1-33
1.1.20 monitor kernel deadlock time	1-34
1.1.21 monitor kernel starvation enable	1-35
1.1.22 monitor kernel starvation exclude-thread	1-36
1.1.23 monitor kernel starvation time	1-37
1.1.24 monitor process	1-38
1.1.25 monitor thread	1-43
1.1.26 process core	1-47
1.1.27 reset exception context	1-48
1.1.28 reset kernel deadlock	1-48
1.1.29 reset kernel exception	1-49
1.1.30 reset kernel reboot	1-50
1.1.31 reset kernel starvation	1-50

1 进程监控和维护



说明

设备支持的存储介质与设备型号相关，本手册使用 flash 类型的存储介质举例，实际使用过程中，请以设备实际情况为准。

1.1 进程监控和维护命令

display memory、**display process**、**display process cpu**、**monitor process** 和 **monitor thread** 命令既可显示用户态进程的相关信息，又可显示内核线程的相关信息，为简便起见，在这些命令中，统一使用“进程”一词来指代。

1.1.1 display exception context

display exception context 命令用来显示用户态进程异常时的上下文信息。

【命令】

```
display exception context [ count value ] [ slot slot-number [ cpu cpu-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

context-admin

【参数】

count value: 表示上下文信息的显示个数，取值范围为 1~20，缺省值为 1。

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

当用户态进程发生一次异常，系统会生成一个 core 文件，还会生成一条上下文信息，用于记录异常用户态进程的 ID、生成 core 文件的时间、core 文件存放的位置、栈信息和寄存器信息。一个 core 文件对应一条上下文信息，最多可记录的上下文信息数和可记录的 core 文件数目相同。

【举例】

显示在 x86 体系 32 位登录设备上的异常上下文信息。

```
<Sysname> display exception context  
Index 1 of 1  
-----
```

```
Crashed PID: 120 (routed)
Crash signal: SIGBUS
Crash time: Tue Apr 9 17:14:30 2013
Core file path:
flash:/core/node0_routed_120_7_20130409-171430_1365527670.core
#0  0xb7caba4a
#1  0x0804cb79
#2  0xb7cd77c4
#3  0x08049f45
Backtrace stopped.
```

```
Registers' content
eax:0xffffffffc ebx:0x00000003 ecx:0xbfe244ec edx:0x0000000a
esp:0xbfe244b8 ebp:0xbfe244c8 esi:0xfffffffff edi:0xbfe24674
eip:0xb7caba4a eflag:0x00000292 cs:0x00000073 ss:0x0000007b
ds:0x0000007b es:0x0000007b fs:0x00000000 gs:0x00000033
```

显示在 x86 体系 64 位登录设备上的异常上下文信息。

```
<Sysname> display exception context
Index 1 of 1
```

```
-----
Crashed PID: 121 (routed)
Crash signal: SIGBUS
Crash time: Sun Mar 31 11:12:21 2013
Core file path:
flash:/core/node0_routed_121_7_20130331-111221_1364728341.core
#0  0x00007fae7dbad20c
#1  0x00000000004059fa
#2  0x00007fae7dbd96c0
#3  0x0000000000402b29
Backtrace stopped.
```

```
Registers' content
rax:0xfffffffffffffffc rbx:0x00007fff88a5dd10
rcx:0xfffffffffffffffc rdx:0x000000000000000a
rsi:0x00007fff88a5dd10 rdi:0x0000000000000003
rbp:0x00007fff88a5dcf0 rsp:0x00007fff88a5dcf0
r8:0x00007fae7ea587e0 r9:0x0000000000000079
r10:0xfffffffffffffffc r11:0x0000000000000246
r12:0x0000000000405b18 r13:0x00007fff88a5ff7a
r14:0x00007fff88a5de30 r15:0x0000000000000000
rip:0x00007fae7dbad20c flag:0x0000000000000246
cs:0x0000000000000033 ss:0x000000000000002b
ds:0x0000000000000000 es:0x0000000000000000
fs:0x0000000000000000 gs:0x0000000000000000
fs_base:0x00007fae80a5d6a0 gs_base:0x0000000000000000
orig_ax:0x00000000000000e8
```

显示在 powerpc 体系 32 位登录设备上的异常上下文信息。

```
<Sysname> display exception context
Index 1 of 1
```

```
-----
```

Crashed PID: 133 (routed)
Crash signal: SIGBUS
Crash time: Wed Apr 10 15:47:49 2013
Core file path:
flash:/core/node0_routed_133_7_20130410-154749_1365608869.core
#0 0x184720bc
#1 0x10006b4c
Backtrace stopped.

Registers' content

grp00: 0x000000ee 0x7ffd6ad0 0x1800f440 0x00000004
grp04: 0x7ffd6af8 0x0000000a 0xffffffff 0x184720bc
grp08: 0x0002d200 0x00000003 0x00000001 0x1847209c
grp12: 0x10006b4c 0x10020534 0xd6744100 0x00000000
grp16: 0x00000000 0xa0203ff0 0xa028b12c 0xa028b13c
grp20: 0xa028b148 0xa028b168 0xa028b178 0xa028b190
grp24: 0xa028b1a8 0xa028b1b8 0x00000000 0x7ffd6c08
grp28: 0x10006cac 0x7ffd6f92 0x184c1b84 0x7ffd6ae0

nip:0x184720bc lr:0x10006b4c cr:0x38000022 ctr:0x1847209c
msr:0x0002db00 xer:0x00000000 ret:0xffffffff dsisr:0x08000000
gr3:0x00000003 mq:0x00000000 trap:0x00000c00 dar:0x1833114c

显示在 powerpc 体系 64 位登录设备上的异常上下文信息。

<Sysname> display exception context
Index 1 of 1

Crashed PID: 172 (routed)
Crash signal: SIGBUS
Crash time: Sat Sep 15 16:53:16 2007
Core file path:
flash:/core/node1_routed_172_7_20070915-165316_1189875196.core
#0 0x00000fff803c66b4
#1 0x0000000010009b94
#2 0x00000fff80401814
Backtrace stopped.

Registers' content

grp00: 0x00000000000000ee 0x00000fffffd04840
grp02: 0x00000fff80425c28 0x0000000000000004
grp04: 0x00000fffffd048c0 0x000000000000000a
grp06: 0xffffffffffffffff 0x00000fff803c66b4
grp08: 0x000000008002d000 0x0000000000000000
grp10: 0x0000000000000000 0x0000000000000000
grp12: 0x0000000000000000 0x00000fff80a096b0
grp14: 0x000000007b964c00 0x000000007b7d0000
grp16: 0x0000000000000001 0x000000000000000b
grp18: 0x0000000000000031 0x000000000a205b8
grp20: 0x000000000a20677 0x0000000000000000
grp22: 0x000000007bb91014 0x0000000000000000
grp24: 0xc000000005ae1c8 0x0000000000000000

```

grp26: 0xc0000001f00bfff20 0xc0000001f00b0000
grp28: 0x000000fffffd04a30 0x000000001001aed8
grp30: 0x000000fffffd04fae 0x000000fffffd04840

nir:0x000000fff803c66b4      lr:0x0000000010009b94
cr:0x0000000058000482      ctr:0x000000fff803c66ac
msr:0x000000008002d000      xer:0x0000000000000000
ret:0xfffffffffffffffffc    dsisr:0x0000000000000000
gr3:0x0000000000000003      softe:0x0000000000000001
trap:0x00000000000000c00    dar:0x000000fff8059d14c

```

显示在 mips 体系 32 位登录设备上的异常上下文信息。

<Sysname> display exception context

Index 1 of 1

Crashed PID: 182 (routed)

Crash signal: SIGBUS

Crash time: Sun Jan 2 08:11:38 2013

Core file path:

flash:/core/node4_routed_182_10_20130102-081138_1293955898.core

#0 0x2af2faf4

#1 0x00406d8c

Backtrace stopped.

Registers' content

```

zero:0x00000000 at:0x1000dc00 v0:0x00000004 v1:0x00000003
a0:0x00000003 a1:0x7fd267e8 a2:0x0000000a a3:0x00000001
t0:0x00000000 t1:0xcf08fa14 t2:0x80230510 t3:0xffffffff
t4:0x69766520 t5:0x00000000 t6:0x63cc6000 t7:0x44617461
s0:0x7fd26f81 s1:0x00401948 s2:0x7fd268f8 s3:0x803e1db0
s4:0x803e1da0 s5:0x803e1d88 s6:0x803e1d70 s7:0x803e1d60
t8:0x00000008 t9:0x2af2fae0 k0:0x00000000 k1:0x00000000
gp:0x2af9a3a0 sp:0x7fd267c0 s8:0x7fd267c0 ra:0x00406d8c
sr:0x0000dc13 lo:0xef9db265 hi:0x0000003f bad:0x2add2010
cause:0x00800020 pc:0x2af2faf4

```

显示在 mips 体系 64 位登录设备上的异常上下文信息。

<Sysname> display exception context

Index 1 of 1

Crashed PID: 270 (routed)

Crash signal: SIGBUS

Crash time: Wed Mar 27 12:39:12 2013

Core file path:

flash:/core/node16_routed_270_10_20130327-123912_1364387952.core

#0 0x0000005555a3bcb4

#1 0x0000000120006c1c

Backtrace stopped.

Registers' content

```

zero:0x0000000000000000 at:0x0000000000000014
v0:0x0000000000000004 v1:0x0000000000000003

```

```

a0:0x0000000000000003      a1:0x000000ffff899d90
a2:0x000000000000000a      a3:0x0000000000000001
a4:0x0000000555a9b4e0      a5:0x0000000000000000
a6:0xffffffff8021349c      a7:0x20696e206368616e
t0:0x0000000000000000      t1:0xffffffff80105068
t2:0xffffffff80213890      t3:0x0000000000000008
s0:0x0000000555a99c40      s1:0x000000ffff89af5f
s2:0x0000000120007320      s3:0x0000000555a5f470
s4:0x000000ffff899f80      s5:0xffffffff803cc6c0
s6:0xffffffff803cc6a8      s7:0xffffffff803cc690
t8:0x0000000000000002      t9:0x0000000555a3bc98
k0:0x0000000000000000      k1:0x0000000000000000
gp:0x0000000120020460      sp:0x000000ffff899d70
s8:0x000000ffff899d80      ra:0x0000000120006c1c
sr:0x000000000400fff3      lo:0xdf3b645a1cac08c9
hi:0x000000000000007f      bad:0x000000055589ba84
cause:0x0000000000800020    pc:0x0000000555a3bcb4

```

表1-1 display exception context 命令输出信息描述表

字段	描述
Crashed PID	发生异常的用户态进程ID
Crash signal	导致异常的信号： • SIGABRT: 异常终止 (abort) • SIGBUS: 总线错误 • SIGFPE: 浮点异常 • SIGILL: 程序执行了非法指令，导致异常 • SIGQUIT: 终端退出符 • SIGSEGV: 无效存储访问 • SIGSYS: 无效系统调用 • SIGTRAP: 跟踪断点时发生了异常 • SIGXCPU: 超过 CPU 限制 (setrlimit) • SIGXFSZ: 超过文件长度限制 (setrlimit) • SIGUNKNOW: 未知原因
Crash time	异常发生的时间
Core file path	core文件存放的位置
Backtrace stopped	表示栈信息已经显示完毕
Registers' content	寄存器的内容

【相关命令】

- **reset exception context**

1.1.2 display exception filepath

display exception filepath 命令用来显示 core 文件的保存路径。

【命令】

display exception filepath [*slot slot-number* [*cpu cpu-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【举例】

显示指定 slot 上 core 文件的保存路径。

```
<Sysname> display exception filepath slot 1  
The exception filepath on slot 1 is flash:.
```

1.1.3 display kernel deadlock

display kernel deadlock 命令用来显示内核线程死循环信息。

【命令】

display kernel deadlock *show-number* [*offset*] [**verbose**] [*slot slot-number* [*cpu cpu-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

show-number: 需要显示的死循环信息的数目，取值范围为 1~20。

offset: 需要显示的起始条目距最近条目的偏移，取值范围为 0~19，缺省值为 0。

verbose: 表示显示详细信息。不指定该参数时，显示概要信息。

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

【举例】

显示最近一条内核线程死循环的概要信息。

<Sysname> display kernel deadlock 1

----- Deadloop record 1 -----

Description : BUG: soft lockup - CPU#0 stuck for 61! [comsh: 16306]
Recorded at : 2013-05-01 11:16:00.823018
Occurred at : 2013-05-01 11:16:00.823018
Instruction address : 0x4004158c
Thread : comsh (TID: 16306)
Context : thread context
Slot : 1
Cpu : 0
VCPU ID : 0
Kernel module info : module name (mrpnc) module address (0xe332a000)

显示最近一条内核线程死循环的详细信息。

<Sysname> display kernel deadlock 1 verbose

----- Deadloop record 1 -----

Description : BUG: soft lockup - CPU#0 stuck for 61! [comsh: 16306]
Recorded at : 2013-05-01 11:16:00.823018
Occurred at : 2013-05-01 11:16:00.823018
Instruction address : 0x4004158c
Thread : comsh (TID: 16306)
Context : thread context
Slot : 1
Cpu : 0
VCPU ID : 0
Kernel module info : module name (mrpnc) module address (0xe332a000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->

swapper (11:16:00.833018)-->

kthreadd (11:16:00.833518)-->

swapper (11:16:00.833550)-->

disk (11:16:00.833560)

Register content:

Reg: r0, Val = 0x00000000 ;	Reg: r1, Val = 0xe2be5ea0 ;
Reg: r2, Val = 0x00000000 ;	Reg: r3, Val = 0x77777777 ;
Reg: r4, Val = 0x00000000 ;	Reg: r5, Val = 0x00001492 ;
Reg: r6, Val = 0x00000000 ;	Reg: r7, Val = 0x0000ffff ;
Reg: r8, Val = 0x77777777 ;	Reg: r9, Val = 0x00000000 ;
Reg: r10, Val = 0x00000001 ;	Reg: r11, Val = 0x0000002c ;
Reg: r12, Val = 0x057d9484 ;	Reg: r13, Val = 0x00000000 ;
Reg: r14, Val = 0x00000000 ;	Reg: r15, Val = 0x02000000 ;
Reg: r16, Val = 0xe2be5f00 ;	Reg: r17, Val = 0x00000000 ;
Reg: r18, Val = 0x00000000 ;	Reg: r19, Val = 0x00000000 ;
Reg: r20, Val = 0x024c10f8 ;	Reg: r21, Val = 0x057d9244 ;
Reg: r22, Val = 0x00002000 ;	Reg: r23, Val = 0x0000002c ;
Reg: r24, Val = 0x00000002 ;	Reg: r25, Val = 0x24000024 ;
Reg: r26, Val = 0x00000000 ;	Reg: r27, Val = 0x057d9484 ;
Reg: r28, Val = 0x0000002c ;	Reg: r29, Val = 0x00000000 ;

```

Reg:      r30, Val = 0x0000002c ; Reg:      r31, Val = 0x00000000 ;
Reg:      cr, Val = 0x84000028 ; Reg:      nip, Val = 0x057d9550 ;
Reg:      xer, Val = 0x00000000 ; Reg:      lr, Val = 0x0186eff0 ;
Reg:      ctr, Val = 0x682f7344 ; Reg:      msr, Val = 0x00784b5c ;
Reg:      trap, Val = 0x0000b030 ; Reg:      dar, Val = 0x77777777 ;
Reg:      dsisr, Val = 0x40000000 ; Reg:      result, Val = 0x00020300 ;

```

Dump stack (total 1024 bytes, 16 bytes/line):

```

0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

```

Call trace:

```

Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00

```

Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0

Instruction dump:

41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bffffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c

表1-2 display kernel deadlock 命令显示信息描述表

字段	描述
Description	发生死循环的内核线程的描述信息，包括死循环内核线程所在的CPU的编号、内核线程连续运行的时间、内核线程的名称和编号
Recorded at	内核线程死循环被记录的时间点，精确到微秒
Occurred at	内核线程发生死循环的时间，精确到微秒
Instruction address	内核线程被检测到发生死循环时对应的指令信息
Thread	发生死循环的内核线程的名称和编号
Context	内核线程被检测到发生死循环时所在的上下文环境
Cpu	运行该内核线程的CPU的编号
VCPU ID	运行该内核线程的CPU核的编号
Kernel module info	内核线程被检测到发生死循环时，系统中已加载的内核模块信息。包括： - module name 表示内核模块名称 - module address 内核模块加载的内存地址
Last 5 thread switches	内核线程被检测到发生死循环时，记录死循环发生的CPU上、最近五次的内核线程切换轨迹。包括内核线程的名称和内核线程切换时间点，时间精确到微秒
Register content	内核线程被检测到发生死循环时现场的寄存器信息。Reg表示寄存器名称，Val表示寄存器中保存的值
Dump stack	内核线程被检测到发生死循环时现场的堆栈信息
Call trace	内核线程被检测到发生死循环时现场的函数调用栈信息，即每级调用函数的指令地址
Instruction dump	内核线程被检测到发生死循环时对应的指令码。非法指令用ffffff表示
No information to display	表示系统中没有内核线程死循环记录

【相关命令】

- **reset kernel deadlock**

1.1.1.4 display kernel deadlock configuration

display kernel deadlock configuration 命令用来显示内核线程死循环监控参数配置。

【命令】

display kernel deadlock configuration [slot slot-number [cpu cpu-number]]

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。
cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

【举例】

```
# 显示内核线程死循环监控参数配置。
<Sysname> display kernel deadloop configuration
Thread dead loop detection: Enabled
Dead loop timer (in seconds): 20
Cores with dead loop detection enabled: 0-1
Dead loop action threshold: 2 consecutive dead loops
Threads excluded from monitoring: 1
  TID:      15   Name: co0
```

表1-3 display kernel deadloop configuration 命令显示信息描述表

字段	描述
Thread dead loop detection: Enabled	内核线程死循环检测功能处于开启状态
Thread dead loop detection: Disabled	内核线程死循环检测功能处于关闭状态
Dead loop timer (in seconds): <i>n</i>	内核线程死循环判定周期（单位为秒），即内核线程连续运行时间大于 <i>n</i> 秒时，则判定为死循环
Cores with dead loop detection enabled	开启了内核线程死循环功能的CPU核的编号
Dead loop action threshold: 2 consecutive dead loops	配置内核线程死循环后触发纠错动作的阈值：系统连续检测到内核线程死循环的次数
Threads excluded from monitoring	不进行死循环检测的内核线程列表，配置 monitor kernel deadloop exclude-thread 命令后才会显示该信息
Name	不进行死循环检测的内核线程的名称
TID	不进行死循环检测的内核线程的编号
No thread is excluded from monitoring	对所有内核线程都进行死循环检查

1.1.5 display kernel exception

display kernel exception 命令用来显示内核线程的异常信息。

【命令】

display kernel exception show-number [*offset*] [**verbose**] [**slot slot-number**] [**cpu cpu-number**]]

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

show-number: 需要显示的异常信息的数目，取值范围为 1~20。

offset: 开始显示的条目距最近条目的偏移，取值范围为 0~19，缺省值为 0。

verbose: 显示详细信息。不指定该参数时，显示概要信息。

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

当内核线程在运行过程中发生异常时，系统会自动记录异常信息，以便设备维护人员定位问题。

【举例】

显示最近一条内核线程异常的概要信息。

```
<Sysname> display kernel exception 1
----- Exception record 1 -----
Description           : Oops[#0]
Recorded at           : 2017-05-01 11:16:00.823018
Occurred at           : 2017-05-01 11:16:00.823018
Instruction address    : 0x4004158c
Thread                : comsh (TID: 16306)
Context               : thread context
Slot                  : 1
Cpu                   : 0
VCPU ID               : 0
Kernel module info    : module name (mrpnc) module address (0xe332a000)
                       : module name (disk) module address (0xe00bd000)
```

显示最近一条内核线程异常的详细信息。

```
<Sysname> display kernel exception 1 verbose
----- Exception record 1 -----
Description           : Oops[#0]
Recorded at           : 2017-05-01 11:16:00.823018
Occurred at           : 2017-05-01 11:16:00.823018
Instruction address    : 0x4004158c
Thread                : comsh (TID: 16306)
Context               : thread context
Slot                  : 1
Cpu                   : 0
```

VCPU ID : 0
Kernel module info : module name (mrpnc) module address (0xe332a000)
module name (12500) module address (0xe00bd000)

Last 5 thread switches : migration/0 (11:16:00.823018)-->
swapper (11:16:00.833018)-->
kthreadd (11:16:00.833518)-->
swapper (11:16:00.833550)-->
disk (11:16:00.833560)

Register content:

Reg: r0, Val = 0x00000000 ;	Reg: r1, Val = 0xe2be5ea0 ;
Reg: r2, Val = 0x00000000 ;	Reg: r3, Val = 0x77777777 ;
Reg: r4, Val = 0x00000000 ;	Reg: r5, Val = 0x00001492 ;
Reg: r6, Val = 0x00000000 ;	Reg: r7, Val = 0x0000ffff ;
Reg: r8, Val = 0x77777777 ;	Reg: r9, Val = 0x00000000 ;
Reg: r10, Val = 0x00000001 ;	Reg: r11, Val = 0x0000002c ;
Reg: r12, Val = 0x057d9484 ;	Reg: r13, Val = 0x00000000 ;
Reg: r14, Val = 0x00000000 ;	Reg: r15, Val = 0x02000000 ;
Reg: r16, Val = 0xe2be5f00 ;	Reg: r17, Val = 0x00000000 ;
Reg: r18, Val = 0x00000000 ;	Reg: r19, Val = 0x00000000 ;
Reg: r20, Val = 0x024c10f8 ;	Reg: r21, Val = 0x057d9244 ;
Reg: r22, Val = 0x00002000 ;	Reg: r23, Val = 0x0000002c ;
Reg: r24, Val = 0x00000002 ;	Reg: r25, Val = 0x24000024 ;
Reg: r26, Val = 0x00000000 ;	Reg: r27, Val = 0x057d9484 ;
Reg: r28, Val = 0x0000002c ;	Reg: r29, Val = 0x00000000 ;
Reg: r30, Val = 0x0000002c ;	Reg: r31, Val = 0x00000000 ;
Reg: cr, Val = 0x84000028 ;	Reg: nip, Val = 0x057d9550 ;
Reg: xer, Val = 0x00000000 ;	Reg: lr, Val = 0x0186eff0 ;
Reg: ctr, Val = 0x682f7344 ;	Reg: msr, Val = 0x00784b5c ;
Reg: trap, Val = 0x0000b030 ;	Reg: dar, Val = 0x77777777 ;
Reg: dsisr, Val = 0x40000000 ;	Reg: result, Val = 0x00020300 ;

Dump stack (total 1024 bytes, 16 bytes/line):

```
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
```

```

0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44

```

Call trace:

```

Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0

```

Instruction dump:

```

41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bffffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c

```

本命令显示信息的详细描述请参见 [表 1-2](#)。

【相关命令】

- **reset kernel exception**

1.1.6 display kernel reboot

display kernel reboot 命令用来显示成员设备的重启信息。

【命令】

```

display kernel reboot show-number [ offset ] [ verbose ] [ slot slot-number
[ cpu cpu-number ] ]

```

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

show-number: 需要显示的重启信息的数目，取值范围为 1~20。

offset: 需要显示的起始条目距最近条目的偏移，取值范围为 0~19，缺省值为 0。

verbose: 表示显示详细信息。不指定该参数时，显示概要信息。

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。成员设备的信息会记录在 IRF 当前主设备的内存中，主设备掉电后会删除该信息。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

【举例】

显示最近一条重启概要信息。

```
<Sysname> display kernel reboot 1
----- Reboot record 1 -----
Recorded at      : 2013-05-01 11:16:00.823018
Occurred at      : 2013-05-01 11:16:00.823018
Reason           : 0x31
Thread           : comsh (TID: 16306)
Context          : thread context
Slot             : 1
Target Slot      : 1
Cpu              : 0
Target CPU       : 7
VCPU ID          : 0
Kernel module info : module name (mrpnc) module address (0xe332a000)
                   : module name (12500) module address (0xe00bd000)
```

显示最近一条重启详细信息。

```
<Sysname> display kernel reboot 1 verbose
----- Reboot record 1 -----
Recorded at      : 2013-05-01 11:16:00.823018
Occurred at      : 2013-05-01 11:16:00.823018
Reason           : 0x31
Thread           : comsh (TID: 16306)
Context          : thread context
Slot             : 1
Target Slot      : 1
Cpu              : 0
Target CPU       : 7
VCPU ID          : 0
Kernel module info : module name (mrpnc) module address (0xe332a000)
                   : module name (12500) module address (0xe00bd000)
```

Last 5 thread switches : migration/0 (11:16:00.823018)-->

```
swapper (11:16:00.833018)-->
kthreadd (11:16:00.833518)-->
swapper (11:16:00.833550)-->
disk (11:16:00.833560)
```

Dump stack (total 1024 bytes, 16 bytes/line):

```
0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44
```

Call trace:

```
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
```

Function Address = 0x801223a0

表1-4 display kernel reboot 命令显示信息描述表

字段	描述
Recorded at	重启被记录的时间点，精确到微秒
Occurred at	重启的时间，精确到微秒
Reason	重启的原因
Thread	重启时运行的内核线程的名称和编号
Context	重启时所在的上下文环境
Slot	触发重启事件的Slot的编号
Target Slot	实际发生重启的Slot的编号
Cpu	触发重启事件的CPU的编号
Target CPU	实际发生重启的CPU的编号
VCPU ID	触发重启事件的CPU核的编号
Kernel module info	重启发生时，系统中已加载的内核模块信息。包括内核模块名和内核模块加载的内存地址
Last 5 thread switches	重启时，记录重启的CPU上、最近五次的内核线程切换轨迹。包括内核线程的名称和内核线程切换时间点，时间精确到微秒
Dump stack	重启时，运行线程的堆栈信息
Call trace	重启时，运行线程的函数调用栈信息
No information to display	表示系统中没有重启记录

【相关命令】

- reset kernel reboot

1.1.7 display kernel starvation

display kernel starvation 命令用来显示内核线程饿死信息。

【命令】

display kernel starvation show-number [offset] [verbose] [slot slot-number [cpu cpu-number]]

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

show-number：需要显示的饿死信息的数目，取值范围为 1~20。

offset: 需要显示的起始条目距最近条目的偏移，取值范围为 0~19，缺省值为 0。

verbose: 表示显示详细信息。不指定该参数时，显示概要信息。

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

【举例】

显示最近一条内核线程饿死的概要信息。

```
<Sysname> display kernel starvation 1
----- Starvation record 1 -----
Description      : INFO: task comsh: 16306 blocked for more than 10 seconds.
Recorded at      : 2013-05-01 11:16:00.823018
Occurred at      : 2013-05-01 11:16:00.823018
Instruction address : 0x4004158c
Thread           : comsh (TID: 16306)
Context          : thread context
Slot             : 1
Cpu              : 0
VCPU ID          : 0
Kernel module info : module name (mrpnc) module address (0xe332a000)
                   : module name (12500) module address (0xe00bd000)
```

显示最近一条内核线程饿死的详细信息。

```
<Sysname> display kernel starvation 1 verbose
----- Starvation record 1 -----
Description      : INFO: task comsh: 16306 blocked for more than 10 seconds.
Recorded at      : 2013-05-01 11:16:00.823018
Occurred at      : 2013-05-01 11:16:00.823018
Instruction address : 0x4004158c
Thread           : comsh (TID: 16306)
Context          : thread context
Slot             : 1
Cpu              : 0
VCPU ID          : 0
Kernel module info : module name (mrpnc) module address (0xe332a000)
                   : module name (12500) module address (0xe00bd000)
```

```
Last 5 thread switches : migration/0 (11:16:00.823018)-->
                        swapper (11:16:00.833018)-->
                        kthreadd (11:16:00.833518)-->
                        swapper (11:16:00.833550)-->
                        disk (11:16:00.833560)
```

Register content:

```
Reg:      r0, Val = 0x00000000 ; Reg:      r1, Val = 0xe2be5ea0 ;
Reg:      r2, Val = 0x00000000 ; Reg:      r3, Val = 0x77777777 ;
```

```

Reg:      r4, Val = 0x00000000 ; Reg:      r5, Val = 0x00001492 ;
Reg:      r6, Val = 0x00000000 ; Reg:      r7, Val = 0x0000ffff ;
Reg:      r8, Val = 0x77777777 ; Reg:      r9, Val = 0x00000000 ;
Reg:      r10, Val = 0x00000001 ; Reg:     r11, Val = 0x0000002c ;
Reg:      r12, Val = 0x057d9484 ; Reg:     r13, Val = 0x00000000 ;
Reg:      r14, Val = 0x00000000 ; Reg:     r15, Val = 0x02000000 ;
Reg:      r16, Val = 0xe2be5f00 ; Reg:     r17, Val = 0x00000000 ;
Reg:      r18, Val = 0x00000000 ; Reg:     r19, Val = 0x00000000 ;
Reg:      r20, Val = 0x024c10f8 ; Reg:     r21, Val = 0x057d9244 ;
Reg:      r22, Val = 0x00002000 ; Reg:     r23, Val = 0x0000002c ;
Reg:      r24, Val = 0x00000002 ; Reg:     r25, Val = 0x24000024 ;
Reg:      r26, Val = 0x00000000 ; Reg:     r27, Val = 0x057d9484 ;
Reg:      r28, Val = 0x0000002c ; Reg:     r29, Val = 0x00000000 ;
Reg:      r30, Val = 0x0000002c ; Reg:     r31, Val = 0x00000000 ;
Reg:      cr, Val = 0x84000028 ; Reg:     nip, Val = 0x057d9550 ;
Reg:      xer, Val = 0x00000000 ; Reg:     lr, Val = 0x0186eff0 ;
Reg:      ctr, Val = 0x682f7344 ; Reg:     msr, Val = 0x00784b5c ;
Reg:      trap, Val = 0x0000b030 ; Reg:     dar, Val = 0x77777777 ;
Reg:      dsisr, Val = 0x40000000 ; Reg:     result, Val = 0x00020300 ;

```

Dump stack (total 1024 bytes, 16 bytes/line):

```

0xe2be5ea0: 02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0xe2be5eb0: 00 00 00 04 00 00 00 00 00 00 00 00 28 05 8d 34 c4
0xe2be5ec0: 02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0xe2be5ed0: 02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ee0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5ef0: 95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f00: a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f10: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 e9 00 00
0xe2be5f20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be5f30: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be5f40: 02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0xe2be5f50: 02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0xe2be5f60: 02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0xe2be5f70: 05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0xe2be5f80: 02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0xe2be5f90: 00 03 00 00 00 00 00 00 02 be 5f e0 00 00 00 30
0xe2be5fa0: 02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0xe2be5fb0: 02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0xe2be5fc0: 02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0xe2be5fd0: 02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0xe2be5fe0: 00 00 00 00 00 00 00 00 00 00 00 00 02 be 60 18
0xe2be5ff0: 02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0xe2be6000: 02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6010: 02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0xe2be6020: 02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0xe2be6030: 02 27 00 00 00 00 00 00 00 00 00 02 be 60 68
0xe2be6040: 02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98

```

```
0xe2be6050: 00 00 00 04 02 21 00 00 00 00 00 00 01 e9 00 00
0xe2be6060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0xe2be6070: 00 00 00 00 00 00 00 00 02 be 66 c0 02 be 66 d0
0xe2be6080: 02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0xe2be6090: 00 00 00 00 02 21 00 00 05 8d 34 c4 05 7d 92 44
```

Call trace:

```
Function Address = 0x8012a4b4
Function Address = 0x8017989c
Function Address = 0x80179b30
Function Address = 0x80127438
Function Address = 0x8012d734
Function Address = 0x80100a00
Function Address = 0xe0071004
Function Address = 0x8016ce0c
Function Address = 0x801223a0
```

Instruction dump:

```
41a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4bffffe6c 80780290 7f64db78 4804ea35 <807f002c> 38800000 38a00080 3863000c
```

本命令显示信息的详细描述请参见 [表 1-2](#)。

【相关命令】

- **reset kernel starvation**

1.1.8 display kernel starvation configuration

display kernel starvation configuration 命令用来显示内核线程的饿死监控参数的配置。

【命令】

```
display kernel starvation configuration [ slot slot-number [ cpu
cpu-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

【举例】

显示内核线程饿死监控参数配置。

```
<Sysname> display kernel starvation configuration
Thread starvation detection: Disabled
Starvation timer (in seconds): 10
Threads excluded from monitoring: 1
  TID:    123    Name: co0
```

表1-5 display kernel starvation configuration 命令显示信息描述表

字段	描述
Thread starvation detection: Enabled	内核线程饿死检测功能处于开启状态
Thread starvation detection: Disabled	内核线程饿死检测功能处于关闭状态
Starvation timer (in seconds): <i>n</i>	内核线程饿死判定周期（单位为秒）。即如果内核线程在 <i>n</i> 秒内一直不能运行，则判定为饿死
Threads excluded from monitoring	不进行饿死检测的内核线程列表
Name	不进行饿死检测的内核线程的名称
TID	不进行饿死检测的内核线程的编号

【相关命令】

- **monitor kernel starvation enable**
- **monitor kernel starvation exclude-thread**
- **monitor kernel starvation time**

1.1.9 display process

display process 命令用来显示进程的状态信息。

【命令】

```
display process [ all | job job-id | name process-name ] [ slot slot-number
[ cpu cpu-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

all: 显示所有进程的状态信息。指定 **all** 参数和不指定任何可选参数时，命令行的执行效果相同。
job job-id: 任务编号，用于唯一标识一个进程，该编号不会随着进程的重启而改变，取值范围为 1~2147483647。

name process-name: 进程名称，为 1~15 个字符的字符串，不区分大小写，不能包含问号和空格。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【举例】

显示进程 scmd 的状态信息。

```
<Sysname> display process name scmd
      Job ID: 1
      PID: 1
      Parent JID: 0
      Parent PID: 0
      Executable path: /sbin/scmd
      Instance: 0
      Respawn: OFF
      Respawn count: 1
      Max. spawns per minute: 0
      Last started: Wed Jun  1 14:45:46 2013
      Process state: sleeping
      Max. core: 0
      ARGS: -
      TID  LAST_CPU  Stack    PRI    State  HH:MM:SS:MSEC  Name
      1      0      0K      120    S      0:0:5:220      scmd
```

表1-6 display process name 命令显示信息描述表

字段	描述
Job ID	任务编号，用于唯一标识一个进程，该编号不会随着进程的重启而改变
PID	进程编号，用于标识一个进程，但该编号可能会随着进程的重启而改变
Parent JID	父进程的任务编号
Parent PID	父进程的进程编号
Executable path	进程执行路径（内核线程执行路径显示为“-”）
Instance	进程的实例号（一个进程根据需要在软件实现时决定了它是否会运行多个实例）
Respawn	运行出错时，该进程是否会自动重启： - ON 表示自动重启 - OFF 表示不自动重启
Respawn count	进程重启的次数（初始值为1）
Max. spawns per minute	进程一分钟内允许异常重启的最大次数（如果进程在一分钟内异常重启次数超过该值，则系统会自动关闭该进程）
Last started	进程最近一次启动的日期和时间

字段	描述
Process state	进程状态，可能的取值为： • running: 运行状态或正在队列中等待调度 • sleeping: 可中断睡眠状态 • traced or stopped: 暂停状态 • uninterruptible sleep: 不可中断睡眠状态 • zombie: 僵死状态（僵死状态指的是进程已经退出，但是仍然占用部分资源的状态）
Max. core	进程最多可以生成的core文件的数量，如果为0表示不生成core文件（进程异常重启一次，会产生一个core文件。如果生成的core文件的数目达到最大值，则不再生成core文件。软件开发和维护人员能够根据core文件的内容来定位异常的原因和异常的位置）
ARGS	进程启动时携带的参数。如果进程不带参数，显示为“-”
TID	线程编号
LAST_CPU	进程最近一次被调度时，所在的CPU
Stack	堆栈大小
PRI	线程优先级
State	线程状态，可能的取值为： • R: running, 运行状态或正在队列中等待调度 • S: sleeping, 可中断睡眠状态 • T: traced or stopped, 暂停状态 • D: uninterruptible sleep, 不可中断睡眠状态 • Z: zombie, 僵死状态
HH:MM:SS:MSEC	进程最近一次启动后的运行时间
Name	进程名称

显示所有进程的状态信息。

<Sysname> display process all

JID	PID	%CPU	%MEM	STAT	PRI	TTY	HH:MM:SS	COMMAND
1	1	0.0	0.0	S	120	-	00:00:04	scmd
2	2	0.0	0.0	S	115	-	00:00:00	[kthreadd]
3	3	0.0	0.0	S	99	-	00:00:00	[migration/0]
4	4	0.0	0.0	S	115	-	00:00:05	[ksoftirqd/0]
5	5	0.0	0.0	S	99	-	00:00:00	[watchdog/0]
6	6	0.0	0.0	S	115	-	00:00:00	[events/0]
7	7	0.0	0.0	S	115	-	00:00:00	[khelper]
8	8	0.0	0.0	S	115	-	00:00:00	[kblockd/0]
9	9	0.0	0.0	S	115	-	00:00:00	[ata/0]
10	10	0.0	0.0	S	115	-	00:00:00	[ata_aux]
11	11	0.0	0.0	S	115	-	00:00:00	[kseriod]
12	12	0.0	0.0	S	120	-	00:00:00	[vzmond]
13	13	0.0	0.0	S	120	-	00:00:00	[pdflush]

```

14      14  0.0  0.0  S  120      -  00:00:00 [pdflush]
15      15  0.0  0.0  S  115      -  00:00:00 [kswapd0]
16      16  0.0  0.0  S  115      -  00:00:00 [aio/0]
17      17  0.0  0.0  S  115      -  00:00:00 [scsi_eh_0]
18      18  0.0  0.0  S  115      -  00:00:00 [scsi_eh_1]
19      19  0.0  0.0  S  115      -  00:00:00 [scsi_eh_2]
35      35  0.0  0.0  D  100      -  00:00:00 [lipc_topology]
---- More ----

```

表1-7 display process all 命令显示信息描述

字段	描述
JID	任务编号，用于唯一标识一个进程，该编号不会随着进程的重启而改变
PID	进程编号
%CPU	CPU使用率（用百分比表示）
%MEM	内存使用率（用百分比表示）
STAT	进程状态，可能的取值为： • R: running，运行状态或处于运行队列 • S: sleeping，可中断睡眠状态 • T: traced or stopped，暂停状态 • D: uninterruptible sleep，不可中断睡眠状态 • Z: zombie，僵死状态
PRI	进程优先级（优先级在进程调度时发挥作用，优先级高的会优先得到调度）
TTY	进程使用的终端（在非缺省Context内该项总显示为“-”）
HH:MM:SS	进程最近一次启动后的运行时间。当进程的持续运行时间大于或等于100小时时，该列仅显示小时数，不再显示分和秒
COMMAND	进程名称以及进程运行的参数（如果进程名称带有“[]”标记，则表示内核线程）

1.1.10 display process cpu

display process cpu 命令用来显示所有进程的 CPU 使用率信息。

【命令】

display process cpu [slot slot-number [cpu cpu-number]]

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator
context-admin
context-operator

```

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【举例】

显示所有进程 CPU 使用率信息。

```
<Sysname> display process cpu
```

CPU utilization in 5 secs: 16.8%; 1 min: 4.7%; 5 mins: 4.7%

JID	5Sec	1Min	5Min	Name
1	0.0%	0.0%	0.0%	scmd
2	0.0%	0.0%	0.0%	[kthreadd]
3	0.1%	0.0%	0.0%	[ksoftirqd/0]

其它显示信息略……。

表1-8 display process cpu 命令显示信息描述表

字段	描述
CPU utilization in 5 secs: 16.8%; 1 min: 4.7%; 5 mins: 4.7%	系统最近5秒CPU使用率；最近1分钟CPU使用率；最近5分钟CPU使用率
JID	任务编号（用于唯一标识一个进程，该编号不会随着进程的重启而改变）
5Sec	最近5秒钟内进程的CPU使用率
1Min	最近1分钟内进程的CPU使用率
5Min	最近5分钟内进程的CPU使用率
Name	进程名称（如果进程名称带有“[]”标记，则表示该进程为内核线程）

1.1.11 display process log

display process log 命令用来显示所有用户态进程的日志信息。

【命令】

```
display process log [ slot slot-number [ cpu cpu-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【举例】

显示所有用户态进程的日志信息。

```
<Sysname> display process log
Process      JobID  PID   Abort Core Exit Kill StartTime      EndTime
knotify      92     92    N     N    0    36   12-17 07:10:27 12-17 07:10:27
knotify      93     93    N     N    0    --   12-17 07:10:27 12-17 07:10:27
automount    94     94    N     N    0    --   12-17 07:10:27 12-17 07:10:28
knotify      111    111    N     N    0    --   12-17 07:10:28 12-17 07:10:28
comsh        121    121    N     N    0    --   12-17 07:10:30 12-17 07:10:30
knotify      152    152    N     N    0    --   12-17 07:10:31 12-17 07:10:31
autocfgd     155    155    N     N    0    --   12-17 07:10:31 12-17 07:10:31
pkg_update   122    122    N     N    0    --   12-17 07:10:30 12-17 07:10:31
```

表1-9 display process log 命令显示信息描述表

字段	描述
Process	用户态进程名
JobID	用户态进程任务编号
PID	用户态进程编号
Abort	是否异常退出： - Y 表示异常退出 - N 表示正常退出
Core	是否产生core文件 - Y 表示产生 - N 表示未产生
Exit	进程退出码，取值为： - 数字表示进程退出码 --表示无退出码，进程被信号关闭
Kill	关闭进程的信号，取值为： - 数字表示关闭进程的信号的数值 --表示没有关闭信号，进程主动退出，并非被信号关闭
StartTime	用户态进程创建时间
EndTime	用户态进程结束时间

1.1.12 display process memory

display process memory 命令用来显示所有用户态进程的代码段、数据段以及堆栈等的内存使用信息。

【命令】

```
display process memory [ slot slot-number [ cpu cpu-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。
cpu cpu-number: 表示 CPU 的编号。

【使用指导】

用户态进程启动时，会向系统申请 Text、Data、Stack 和 Dynamic 类型的内存：

- Text 类型的内存用来存放用户态进程的代码。
- Data 类型的内存用来存放用户态进程的数据。
- Stack 内存指的是栈内存，一般存放临时数据。
- Dynamic 类型的内存指的是堆内存（heap），由系统根据用户态进程运行需要进行动态分配（malloc）和释放（free），可使用 **display process memory heap** 命令显示 Dynamic 类型内存的详细信息。

【举例】

```
# 显示所有用户态进程的内存使用信息。
<Sysname> display process memory
  JID      Text      Data      Stack      Dynamic      Name
  ---      -
   1       384       1800        16         36       scmd
   2         0         0         0          0      [kthreadd]
   3         0         0         0          0      [ksoftirqd/0]
   4         0         0         0          0      [watchdog/0]
   5         0         0         0          0      [events/0]
   6         0         0         0          0      [khelper]
  29         0         0         0          0      [kblockd/0]
  49         0         0         0          0      [vzmond]
  52         0         0         0          0      [pdflush]
---- More ----
```

表1-10 display process memory 命令显示信息描述表

字段	描述
JID	任务编号。用于唯一标识一个用户态进程，该编号不会随着用户态进程的重启而改变
Text	用户态进程占用的代码段大小，单位为KB（内核线程该项大小为0）
Data	用户态进程占用的数据段大小，单位为KB（内核线程该项大小为0）
Stack	用户态进程占用的堆栈大小，单位为KB（内核线程该项大小为0）
Dynamic	用户态进程动态申请内存大小，单位为KB（内核线程该项大小为0）

字段	描述
Name	用户态进程名称（如果用户态进程名称带有“[]”标记，则表示该进程为内核线程）

【相关命令】

- **display process memory heap**
- **display process memory heap address**
- **display process memory heap size**

1.1.13 display process memory heap

display process memory heap 命令用来显示指定用户态进程的堆内存统计信息。

【命令】

```
display process memory heap job job-id [ verbose ] [ slot slot-number [ cpu  
cpu-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

job job-id: 任务编号，用于唯一标识一个用户态进程，该编号不会随着用户态进程的重启而改变。取值范围为 1~2147483647。

verbose: 显示内存详细统计信息。不指定该参数时，显示内存概要统计信息。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

系统的堆内存由固定大小（比如 **size=16** 字节、**size=64** 字节等）的内存块构成，用于存放用户态进程运行过程中需要用到数据或者中间变量。当用户态进程启动时，系统会根据用户态进程运行需要，给用户态进程动态分配堆内存。用户态进程的堆内存信息可使用 **display process memory heap** 命令显示。

每个内存块都有地址，该地址用十六进制数表示，可通过 **display process memory heap size** 命令显示。用户使用内存块的地址可以访问内存块，获取内存块的内容，内存块的内容可通过 **display process memory heap address** 命令显示。

【举例】

显示 job 1 的堆内存概要统计信息。

```
<Sysname> display process memory heap job 1
```

```
Total virtual memory heap space(in bytes) : 2228224
Total physical memory heap space(in bytes) : 262144
Total allocated memory(in bytes)          : 161576
# 显示 job 1 的堆内存详细统计信息。
```

```
<Sysname> display process memory heap job 1 verbose
```

```
Heap usage:
Size      Free      Used      Total      Free Ratio
16         8        52        60         13%
64         3       1262      1265        0.2%
128        2        207       209         1%
512        3         55        58         5.1%
4096       3        297       300         1%
8192       1         19        20          5%
81920     0          1          1          0%
```

```
Summary:
Total virtual memory heap space (in bytes) : 2293760
Total physical memory heap space (in bytes) : 58368
Total allocated memory (in bytes)          : 42368
```

以上显示信息表明：job 1 分得 size 大小 16 字节的内存块 60 个（已用 52 个，还有 8 个未使用），size 大小为 64 字节的内存块 1265 个（已用 1262 个，还有 3 个未使用），以此类推。

表1-11 display process memory heap 命令显示信息描述表

命令字	功能描述
Total virtual memory heap space(in bytes)	虚拟堆内存总大小，单位为字节
Total physical memory heap space(in bytes)	物理堆内存总大小，单位为字节
Total allocated memory(in bytes)	任务已使用的堆内存大小，单位为字节
Size	内存块大小，单位为字节
Free	空闲的内存块个数
Used	已使用的内存块个数
Total	指定大小内存块总个数，为Free和Used之和
Free Ratio	Free与Total的比率，可以反映这种大小内存块的碎片情况

【相关命令】

- display process memory
- display process memory heap address
- display process memory heap size

1.1.14 display process memory heap address

display process memory heap address 命令用来显示从指定地址开始的内存空间的内容。

【命令】

display process memory heap job *job-id* address *starting-address* length *memory-length* [slot *slot-number* [cpu *cpu-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

job *job-id*: 任务编号，用于唯一标识一个用户态进程，该编号不会随着用户态进程的重启而改变，取值范围为 1~2147483647。

address *starting-address*: 内存块的起始地址。

length *memory-length*: 内存的长度，取值范围为 1~1024，单位为字节。

slot *slot-number*: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu *cpu-number*: 表示 CPU 的编号。

【使用指导】

当用户态进程运行异常时，使用该命令可以帮助设备维护人员诊断和定位问题。

【举例】

显示 job 1 从地址 0xb7e30580 开始，长度为 128 字节的内存空间的内容。

```
<Sysname> display process memory heap job 1 address b7e30580 length 128
B7E30580:  14 00 EF FF 00 00 00 00 E4 39 E2 B7 7C 05 E3 B7  .....9..|...
B7E30590:  14 00 EF FF 2F 73 62 69 6E 2F 73 6C 62 67 64 00  ....sbin/slbgd.
B7E305A0:  14 00 EF FF 00 00 00 00 44 3B E2 B7 8C 05 E3 B7  .....D;.....
B7E305B0:  14 00 EF FF 2F 73 62 69 6E 2F 6F 73 70 66 64 00  ....sbin/ospfd.
B7E305C0:  14 00 EF FF 00 00 00 00 A4 3C E2 B7 AC 05 E3 B7  .....<.....
B7E305D0:  14 00 EF FF 2F 73 62 69 6E 2F 6D 73 74 70 64 00  ....sbin/mstpd.
B7E305E0:  14 00 EF FF 00 00 00 00 04 3E E2 B7 CC 05 E3 B7  .....>.....
B7E305F0:  14 00 EF FF 2F 73 62 69 6E 2F 6E 74 70 64 00 00  ....sbin/ntpd..
```

【相关命令】

- **display process memory heap**
- **display process memory heap size**

1.1.15 display process memory heap size

display process memory heap size 命令用来显示指定大小已使用内存块的地址。

【命令】

display process memory heap job *job-id* size *memory-size* [offset *offset-size*] [slot *slot-number* [cpu *cpu-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

job job-id: 任务编号，用于唯一标识一个用户态进程，该编号不会随着用户态进程的重启而改变，取值范围为 1~2147483647。

size memory-size: 内存块大小，取值范围为 1~4294967295。

offset offset-size: 要查询的内存块的偏移，取值范围为 0~4294967295，缺省值为 128。比如，系统给 job 1 分配了 size 为 16 字节的内存块 100 个，用户态进程当前已用了 66 个，如果执行命令 **display process memory heap job 1 size 16 offset 50**，则会显示该用户态进程第 51 到第 66 个 size 为 16 字节的内存块的地址。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

该命令显示的地址为十六进制格式，使用该地址，通过 **display process memory heap address** 命令可以显示该地址内存的具体内容。

【举例】

显示 job 1 已使用的 size 大小为 16 字节的内存块的地址。

```
<Sysname> display process memory heap job 1 size 16
0xb7e300c0 0xb7e300d0 0xb7e300e0 0xb7e300f0
0xb7e30100 0xb7e30110 0xb7e30120 0xb7e30130
0xb7e30140 0xb7e30150 0xb7e30160 0xb7e30170
0xb7e30180 0xb7e30190 0xb7e301a0 0xb7e301b0
0xb7e301c0 0xb7e301d0 0xb7e301e0 0xb7e301f0
0xb7e30200 0xb7e30210 0xb7e30220 0xb7e30230
```

显示 job 1 已使用的 size 大小为 16 字节的内存块的地址，从第 5 个已使用内存块开始显示。

```
<Sysname> display process memory heap job 1 size 16 offset 4
0xb7e30100 0xb7e30110 0xb7e30120 0xb7e30130
0xb7e30140 0xb7e30150 0xb7e30160 0xb7e30170
0xb7e30180 0xb7e30190 0xb7e301a0 0xb7e301b0
0xb7e301c0 0xb7e301d0 0xb7e301e0 0xb7e301f0
0xb7e30200 0xb7e30210 0xb7e30220 0xb7e30230
```

【相关命令】

- **display process memory heap**
- **display process memory heap address**

1.1.16 exception filepath

exception filepath 命令用来配置 core 文件的保存路径。

undo exception filepath 命令用来将 core 文件的保存路径配置为空。

【命令】

exception filepath *directory*

undo exception filepath *directory*

【缺省情况】

Core 文件的保存路径为设备缺省文件系统的根目录。关于缺省文件的详细介绍请参见“基础配置指导”中的“文件系统管理”。

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

directory: 表示 core 文件的保存路径，只能为存储介质的根目录。

【使用指导】

仅缺省 Context 支持本命令。

本命令配置成功后，设备会将生成的 core 文件存放到当前主设备上指定存储介质根目录下的 core 文件夹下。如果存储介质根目录下没有 core 文件夹，则会先创建 core 文件夹，再保存 core 文件。

当设备上有不同类型存储介质的时候，可使用该命令修改 core 文件的保存路径。

需要注意的是，当 core 文件的保存路径为空或无法正常访问时，系统将无法保存 core 文件。

【举例】

配置 core 文件的保存路径。

```
<Sysname> exception filepath flash:/*
```

【相关命令】

- **display exception filepath**
- **process core**

1.1.17 monitor kernel deadlock action threshold

monitor kernel deadlock action threshold 命令用来配置内核线程死循环后触发纠错动作的阈值。

undo monitor kernel deadlock action threshold 命令用来恢复缺省情况。

【命令】

monitor kernel deadlock action threshold *threshold* [*slot slot-number* [*cpu cpu-number*]]

```
undo monitor kernel deadlock action threshold [ slot slot-number [ cpu
cpu-number ] ]
```

【缺省情况】

当系统检测到 1 次内核线程发生死循环时，就触发纠错动作。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

threshold: 内核线程连续发生死循环的次数，取值范围为 1~20。

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

配置本命令后，当内核线程连续发生死循环的次数达到指定值时，设备会采取指定的动作来消除死循环。

【举例】

内核线程死循环后触发纠错动作的阈值为内核线程连续发生 5 次死循环。

```
<Sysname> system-view
```

```
[Sysname] monitor kernel deadlock action threshold 5
```

【相关命令】

- **display kernel deadlock configuration**
- **monitor kernel deadlock enable**

1.1.18 monitor kernel deadlock enable

monitor kernel deadlock enable 命令用来开启内核线程死循环检测功能。

undo monitor kernel deadlock enable 命令用来关闭内核线程死循环检测功能。

【命令】

```
monitor kernel deadlock enable [ slot slot-number [ cpu cpu-number [ core
core-number<<1-64> ] ] ]
```

```
undo monitor kernel deadlock enable [ slot slot-number [ cpu cpu-number ] ]
```

【缺省情况】

内核线程死循环检测功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

core core-number<1-64>: 表示 CPU 核的编号。不指定该参数时，表示当前 CPU 上的所有核。<1-64>表示前面的参数最多可以输入 64 次。

【使用指导】

仅缺省 Context 支持本命令。

在内核态空间中，所有资源都是共享的，多个内核线程之间通过任务调度协调工作。如果某个内核线程长时间一直占用 CPU，就会导致其它内核线程获取不到运行机会，整个系统挂死，这种现象称为死循环。

开启内核线程死循环检测功能后，如果系统发现某内核线程在指定时间内一直占用 CPU，则判定该内核线程为死循环。系统会记录一条死循环信息供管理员查询，并自动重启整个系统来解除死循环。通常情况下，使用缺省配置即可。如果确实需要修改配置，请在工程师的指导下进行，以免引起系统异常。

【举例】

开启内核线程死循环检测功能。

```
<Sysname> system-view
```

```
[Sysname] monitor kernel deadlock enable
```

【相关命令】

- **display kernel deadlock**
- **display kernel deadlock configuration**
- **monitor kernel deadlock exclude-thread**
- **monitor kernel deadlock time**

1.1.19 monitor kernel deadlock exclude-thread

monitor kernel deadlock exclude-thread 命令用来配置不检测指定内核线程是否发生了死循环。

undo monitor kernel deadlock exclude-thread 命令用来恢复对指定内核线程是否发生了死循环进行检测。

【命令】

```
monitor kernel deadlock exclude-thread tid [ slot slot-number [ cpu  
cpu-number ] ]
```

```
undo monitor kernel deadlock exclude-thread [ tid ] [ slot slot-number [ cpu  
cpu-number ] ]
```

【缺省情况】

开启内核线程死循环检测功能后，系统会监控所有内核线程是否发生了死循环。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

tid: 表示内核线程编号，用于唯一标识一个内核线程，取值范围为 1~2147483647。不指定该参数时，表示恢复到缺省情况。

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

多次执行该命令，可以配置对多个内核线程不进行检测，最多可以配置 128 个。

通常情况下，使用缺省配置即可。如果确实需要修改配置，请在工程师的指导下进行，以免引起系统异常。

【举例】

```
# 对编号为 15 的内核线程不进行死循环检测。
<Sysname> system-view
[Sysname]monitor kernel deadlock exclude-thread 15
```

【相关命令】

- **display kernel deadlock configuration**
- **display kernel deadlock**
- **monitor kernel deadlock enable**

1.1.20 monitor kernel deadlock time

monitor kernel deadlock time 命令用来配置判定内核线程是否死循环的时长。

undo monitor kernel deadlock time 命令用来恢复缺省情况。

【命令】

```
monitor kernel deadlock time time [ slot slot-number [ cpu cpu-number ] ]
undo monitor kernel deadlock time [ slot slot-number [ cpu cpu-number ] ]
```

【缺省情况】

当某内核线程连续运行超过 20 秒钟，则判定为死循环。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time time: 表示内核线程死循环判定时长，取值范围为 1~65535，单位为秒。

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

开启内核线程检测功能后，如果某内核线程持续运行指定时间，则认为该内核线程已经死循环。

通常情况下，使用缺省配置即可。如果确实需要修改配置，请在工程师的指导下进行，以免引起系统异常。

【举例】

配置当某内核线程连续运行超过 8 秒钟，则判定为死循环。

```
<Sysname> system-view
```

```
[Sysname] monitor kernel deadloop time 8
```

【相关命令】

- **display kernel deadloop configuration**
- **display kernel deadloop**
- **monitor kernel deadloop enable**

1.1.21 monitor kernel starvation enable

monitor kernel starvation enable 命令用来开启内核线程饿死检测功能。

undo monitor kernel starvation enable 命令用来关闭内核线程饿死检测功能。

【命令】

```
monitor kernel starvation enable [ slot slot-number [ cpu cpu-number ] ]
```

```
undo monitor kernel starvation enable [ slot slot-number [ cpu cpu-number ] ]
```

【缺省情况】

内核线程饿死检测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

如果内核线程本身的触发条件没有达到，会导致该内核线程在一段时间内一直得不到调度，这种现象称为饿死。

开启内核线程饿死检测功能后，当系统检测到某内核线程饿死时，会记录一条饿死信息供管理员查询。

内核线程饿死并不会影响整个系统的运行，当触发条件达到，处于饿死状态的内核线程会自动执行。通常情况下，使用缺省配置即可。如果确实需要修改配置，请在工程师的指导下进行，以免引起系统异常。

【举例】

开启内核线程饿死检测功能。

```
<Sysname> system-view
```

```
[Sysname] monitor kernel starvation enable
```

【相关命令】

- **display kernel starvation configuration**
- **display kernel starvation**
- **monitor kernel starvation time**
- **monitor kernel starvation exclude-thread**

1.1.22 monitor kernel starvation exclude-thread

monitor kernel starvation exclude-thread 命令用来配置不检测指定内核线程是否发生了饿死。

undo monitor kernel starvation exclude-thread 命令用来恢复对指定内核线程是否发生了饿死进行检测。

【命令】

```
monitor kernel starvation exclude-thread tid [ slot slot-number [ cpu  
cpu-number ] ]
```

```
undo monitor kernel starvation exclude-thread [ tid ] [ slot slot-number  
[ cpu cpu-number ] ]
```

【缺省情况】

开启内核线程饿死检测功能后，会监控所有内核线程是否发生了饿死。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

tid: 表示内核线程编号，用于唯一标识一个内核线程，取值范围为 1~2147483647。不指定该参数时，表示恢复到缺省情况。

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

多次执行该命令，可以配置对多个内核线程不进行检测，最多可以配置 128 个。

通常情况下，使用缺省配置即可。如果确实需要修改配置，请在工程师的指导下进行，以免引起系统异常。

【举例】

对编号为 15 的内核线程不进行饿死检测。

```
<Sysname> system-view
```

```
[Sysname] monitor kernel starvation exclude-thread 15
```

【相关命令】

- **display kernel starvation**
- **display kernel starvation configuration**
- **monitor kernel starvation enable**

1.1.23 monitor kernel starvation time

monitor kernel starvation time 命令用来配置判定内核线程是否饿死的时长。

undo monitor kernel starvation time 命令用来恢复缺省情况。

【命令】

```
monitor kernel starvation time time [ slot slot-number [ cpu cpu-number ] ]
```

```
undo monitor kernel starvation time [ slot slot-number [ cpu cpu-number ] ]
```

【缺省情况】

当某内核线程在 120 秒内一直没有运行，则认为该内核线程被饿死。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time *time*: 表示内核线程饿死判定时长，取值范围为 1~65535，单位为秒。

slot *slot-number*: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu *cpu-number*: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

通常情况下，使用缺省配置即可。如果确实需要修改配置，请在工程师的指导下进行，以免引起系统异常。

【举例】

配置当内核线程在 120 秒内一直没有运行，则认为该内核线程被饿死。

```
<Sysname> system-view
```


[Sysname] monitor kernel starvation time 120

【相关命令】

- **display kernel starvation**
- **display kernel starvation configuration**
- **monitor kernel starvation enable**

1.1.24 monitor process

monitor process 命令用来显示进程的统计信息。

【命令】

monitor process [**dumbtty**] [**iteration number**] [**slot slot-number** [**cpu cpu-number**]]

【视图】

任意视图

【缺省用户角色】

network-admin
context-admin

【参数】

dumbtty: 以哑终端方式显示进程统计信息（即屏幕不支持定时刷新统计信息）。指定该参数时，全部进程的统计信息以 CPU 使用率降序排列输出到屏幕上；不指定该参数时，统计信息以交互模式显示，缺省情况下按 CPU 占用率降序显示前 10 个进程的统计信息，且每隔 5 秒刷新一次。

iteration number: 表示进程统计信息的显示次数，取值范围为 1~4294967295。指定 **dumbtty** 参数时，**number** 的缺省值为 1；不指定 **dumbtty** 且不配置 **number** 参数时，表示显示次数没有限制，统计信息会每隔 5 秒刷新一次，一直显示。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

不指定 **dumbtty** 参数的情况下，统计信息将以交互模式显示。在交互模式下，系统可以根据用户输入的交互命令字来调整显示方式或直接终止进程。在用户输入交互命令字之前，系统会自动计算可显示的进程个数，超出屏幕范围的进程不会显示。

在交互模式下可以使用的交互命令字及对应的功能请参见 [表 1-12](#)。

表1-12 monitor process 命令支持的交互命令字描述表

命令字	功能描述
?或h	帮助信息，显示可用的交互式命令字

命令字	功能描述
1	各物理CPU状态的显示开关。比如： 1. 输入 1，分别显示各物理 CPU 的参数值 2. 再次输入 1，显示所有 CPU 的参数平均值 3. 第三次输入 1，又分别显示各物理 CPU 的参数值 4. 如此循环 缺省情况下，显示所有CPU的参数平均值
c	按CPU占用率降序排列，缺省情况下采用降序排列
d	配置统计信息的更新时间间隔，取值范围为1~2147483647秒，缺省值为5
f	按进程打开的文件句柄数降序排列
k	终止一个任务，此命令会影响系统运行，请谨慎使用
l	刷新屏幕
m	按进程使用内存大小降序排列
n	改变显示的进程个数，取值范围为0~2147483647（缺省值为10，0表示不作限制）；超过屏幕范围时，仍只显示一屏内可容纳的进程个数
q	退出交互模式
t	按进程最近一次启动后的运行时间降序排列
<	排序项向左移动一列
>	排序项向右移动一列

【举例】

以哑终端方式显示进程统计信息。（使用该方式显示时，系统会一次显示所有进程的统计信息，并且不支持定时刷新，显示完毕后，会退回到命令视图）

```
<Sysname> monitor process dumbtty
428 processes; 561 threads; 2336 fds
Thread states: 18 running, 543 sleeping, 0 stopped, 0 zombie
CPU0: 89.53% idle, 0.00% user, 7.14% kernel, 3.33% interrupt, 0.00% steal
CPU1: 94.81% idle, 0.47% user, 2.36% kernel, 2.36% interrupt, 0.00% steal
Memory: 31775M total, 26159M available, page size 4K
```

JID	PID	PRI	State	Fds	MEM	HH:MM:SS	CPU	Name
404	404	120	S	16	16432K	03:22:57	0.68%	diagd
1	1	120	S	18	11136K	00:08:21	0.27%	scmd
348	348	115	R	0	0K	05:54:40	0.15%	[kdrvfd20]
349	349	115	R	0	0K	05:57:55	0.14%	[kdrvfd21]
350	350	115	R	0	0K	05:52:45	0.14%	[kdrvfd22]
352	352	115	R	0	0K	05:47:38	0.14%	[kdrvfd24]
354	354	115	R	0	0K	05:38:52	0.14%	[kdrvfd26]
344	344	115	R	0	0K	05:41:15	0.13%	[kdrvfd16]
345	345	115	R	0	0K	05:34:40	0.13%	[kdrvfd17]
346	346	115	R	0	0K	05:33:35	0.13%	[kdrvfd18]
347	347	115	R	0	0K	05:22:29	0.13%	[kdrvfd19]

351	351	115	R	0	OK	05:39:24	0.13%	[kdrvfw23]
353	353	115	R	0	OK	05:29:42	0.13%	[kdrvfw25]
355	355	115	R	0	OK	05:26:17	0.13%	[kdrvfw27]
356	356	115	R	0	OK	05:28:52	0.13%	[kdrvfw28]
357	357	115	R	0	OK	05:26:31	0.13%	[kdrvfw29]

.....其他显示信息略.....

以哑终端方式显示进程统计信息，并且执行一次命令显示两次统计结果。

```
<Sysname> monitor process dumbtty iteration 2
```

```
428 processes; 561 threads; 2336 fds
```

```
Thread states: 18 running, 543 sleeping, 0 stopped, 0 zombie
```

```
CPU0: 89.53% idle, 0.00% user, 7.14% kernel, 3.33% interrupt, 0.00% steal
```

```
CPU1: 94.81% idle, 0.47% user, 2.36% kernel, 2.36% interrupt, 0.00% steal
```

```
Memory: 31775M total, 26159M available, page size 4K
```

JID	PID	PRI	State	FDs	MEM	HH:MM:SS	CPU	Name
404	404	120	S	16	16432K	03:22:57	0.68%	diagd
1	1	120	S	18	11136K	00:08:21	0.27%	scmd
348	348	115	R	0	OK	05:54:40	0.15%	[kdrvfw20]
349	349	115	R	0	OK	05:57:55	0.14%	[kdrvfw21]
350	350	115	R	0	OK	05:52:45	0.14%	[kdrvfw22]
352	352	115	R	0	OK	05:47:38	0.14%	[kdrvfw24]
354	354	115	R	0	OK	05:38:52	0.14%	[kdrvfw26]
344	344	115	R	0	OK	05:41:15	0.13%	[kdrvfw16]
345	345	115	R	0	OK	05:34:40	0.13%	[kdrvfw17]
346	346	115	R	0	OK	05:33:35	0.13%	[kdrvfw18]
347	347	115	R	0	OK	05:22:29	0.13%	[kdrvfw19]
351	351	115	R	0	OK	05:39:24	0.13%	[kdrvfw23]
353	353	115	R	0	OK	05:29:42	0.13%	[kdrvfw25]
355	355	115	R	0	OK	05:26:17	0.13%	[kdrvfw27]
356	356	115	R	0	OK	05:28:52	0.13%	[kdrvfw28]
357	357	115	R	0	OK	05:26:31	0.13%	[kdrvfw29]

.....其他进程的显示信息略.....

// 5 秒钟后，系统会自动统计一次，并显示统计信息如下。（相当于执行了两次 **monitor process dumbtty**，两次执行的时间间隔为 5 秒）

```
428 processes; 561 threads; 2338 fds
```

```
Thread states: 19 running, 542 sleeping, 0 stopped, 0 zombie
```

```
CPU0: 86.26% idle, 1.05% user, 8.99% kernel, 3.70% interrupt, 0.00% steal
```

```
CPU1: 90.44% idle, 1.06% user, 4.78% kernel, 3.72% interrupt, 0.00% steal
```

```
Memory: 31775M total, 26158M available, page size 4K
```

JID	PID	PRI	State	FDs	MEM	HH:MM:SS	CPU	Name
404	404	120	R	18	16460K	03:23:03	0.50%	diagd
1	1	120	S	18	11136K	00:08:21	0.24%	scmd
344	344	115	R	0	OK	05:41:25	0.13%	[kdrvfw16]
348	348	115	R	0	OK	05:54:51	0.13%	[kdrvfw20]
349	349	115	R	0	OK	05:58:06	0.13%	[kdrvfw21]
350	350	115	R	0	OK	05:52:56	0.13%	[kdrvfw22]
352	352	115	R	0	OK	05:47:49	0.13%	[kdrvfw24]
345	345	115	R	0	OK	05:34:51	0.12%	[kdrvfw17]

346	346	115	R	0	0K	05:33:45	0.12%	[kdrvfw18]
347	347	115	R	0	0K	05:22:39	0.12%	[kdrvfw19]
351	351	115	R	0	0K	05:39:34	0.12%	[kdrvfw23]
353	353	115	R	0	0K	05:29:52	0.12%	[kdrvfw25]
354	354	115	R	0	0K	05:39:02	0.12%	[kdrvfw26]
356	356	115	R	0	0K	05:29:02	0.12%	[kdrvfw28]
357	357	115	R	0	0K	05:26:41	0.12%	[kdrvfw29]

.....其他进程的显示信息略.....

以交互方式显示进程统计信息。

<Sysname> monitor process

428 processes; 561 threads; 2336 fds

Thread states: 20 running, 541 sleeping, 0 stopped, 0 zombie

CPU: 98.21% idle, 0.17% user, 1.57% kernel, 0.05% interrupt, 0.00% steal

Memory: 31775M total, 26158M available, page size 4K

JID	PID	PRI	State	FDs	MEM	HH:MM:SS	CPU	Name
348	348	115	R	0	0K	05:55:08	0.09%	[kdrvfw20]
349	349	115	R	0	0K	05:58:22	0.09%	[kdrvfw21]
350	350	115	R	0	0K	05:53:12	0.09%	[kdrvfw22]
352	352	115	R	0	0K	05:48:05	0.09%	[kdrvfw24]
344	344	115	R	0	0K	05:41:41	0.09%	[kdrvfw16]
351	351	115	R	0	0K	05:39:50	0.09%	[kdrvfw23]
404	404	120	S	16	16468K	03:23:12	0.09%	diagd
353	353	115	R	0	0K	05:30:07	0.09%	[kdrvfw25]
354	354	115	R	0	0K	05:39:18	0.09%	[kdrvfw26]
345	345	115	R	0	0K	05:35:07	0.08%	[kdrvfw17]

以上信息会每隔 5 秒刷新一次。

- 输入“h”或“?”，将显示如下帮助信息。

Help for interactive commands:

```

?,h   Show the available interactive commands
1     Toggle SMP view: '1' single/separate states
c     Sort by the CPU field(default)
d     Set the delay interval between screen updates
f     Sort by number of open files
k     Kill a job
l     Refresh the screen
m     Sort by memory used
n     Set the maximum number of processes to display
q     Quit the interactive display
t     Sort by run time of processes since last restart
<     Move sort field to the next left column
>     Move sort field to the next right column

```

Press any key to continue

- 输入“d”后，根据出现的提示如果输入“3”，则统计信息将会每隔 3 秒更新一次。

Enter the delay interval between updates(1~2147483647): 3

- 输入“n”后，根据出现的提示如果输入“5”，则显示的进程数目将会变为 5 个。

Enter the max number of processes to display(0 means unlimited): 5

428 processes; 561 threads; 2336 fds

Thread states: 18 running, 543 sleeping, 0 stopped, 0 zombie

CPU: 97.24% idle, 0.28% user, 2.41% kernel, 0.07% interrupt, 0.00% steal

Memory: 31775M total, 26158M available, page size 4K

JID	PID	PRI	State	FDs	MEM	HH:MM:SS	CPU	Name
349	349	115	R	0	0K	05:59:31	0.14%	[kdrvfw21]
348	348	115	R	0	0K	05:56:16	0.14%	[kdrvfw20]
350	350	115	R	0	0K	05:54:20	0.14%	[kdrvfw22]
352	352	115	R	0	0K	05:49:12	0.14%	[kdrvfw24]
404	404	120	S	16	16480K	03:24:25	0.14%	diagd

- 输入“f”，统计信息将以打开的文件句柄数降序输出（c、m、t命令字类似）。

366 processes; 467 threads; 3408 fds

Thread states: 1 running, 466 sleeping, 0 stopped, 0 zombie

CPU: 98.41% idle, 0.41% user, 1.16% kernel, 0.02% interrupt, 0.00% steal

Memory: 3933M total, 2087M available, page size 4K

JID	PID	PRI	State	FDs	MEM	HH:MM:SS	CPU	Name
570	570	120	S	402	121288K	00:02:47	0.00%	ntopd
205	205	100	S	221	44496K	00:00:07	0.00%	dbmd
549	549	120	S	111	288520K	00:52:52	0.03%	dpid
502	502	125	S	80	25468K	00:00:24	0.00%	ipstackd
208	208	105	S	66	2208K	00:00:00	0.00%	had
70414	70414	125	S	65	16736K	00:00:21	0.00%	ip6stackd
249	249	120	S	57	41100K	00:00:16	0.00%	aclmgrd
521	521	120	S	56	51844K	00:38:49	0.03%	ospfd
236	236	120	S	48	10364K	00:00:37	0.00%	aaad
510	510	120	S	48	23092K	00:00:00	0.00%	l3vpnd

- 输入“k”后，根据出现的提示如果输入 208，将会终止此 JID 对应的任务“had”。

Enter the JID to kill: 208

365 processes; 466 threads; 3341 fds

Thread states: 1 running, 465 sleeping, 0 stopped, 0 zombie

CPU: 98.33% idle, 0.45% user, 1.20% kernel, 0.02% interrupt, 0.00% steal

Memory: 3933M total, 2087M available, page size 4K

JID	PID	PRI	State	FDs	MEM	HH:MM:SS	CPU	Name
570	570	120	S	402	121288K	00:02:47	0.00%	ntopd
205	205	100	S	220	44496K	00:00:07	0.00%	dbmd
549	549	120	S	111	288520K	00:52:53	0.05%	dpid
502	502	125	S	80	25468K	00:00:24	0.01%	ipstackd
70414	70414	125	S	65	16736K	00:00:21	0.00%	ip6stackd
249	249	120	S	57	41100K	00:00:16	0.00%	aclmgrd
521	521	120	S	56	51844K	00:38:50	0.03%	ospfd
236	236	120	S	48	10364K	00:00:37	0.01%	aaad
510	510	120	S	48	23092K	00:00:00	0.00%	l3vpnd
136620	136620	120	S	48	49232K	00:06:08	0.03%	ospfv3d

- 输入“q”，将退出交互模式。

表1-13 monitor process 命令输出信息描述表

字段	描述
84 processes; 107 threads; 683 fds	系统的进程总数，线程总数，文件句柄总数
Thread states: 1 running, 102 sleeping, 0 stopped, 0 zombie	线程状态：处于running状态的线程数，处于sleeping（包括interruptible sleep和uninterruptible sleep）状态的线程数，处于stopped状态的线程数，处于zombie状态的线程数
CPU: 97.39% idle, 0.19% user, 2.04% kernel, 0.38% interrupt, 0.00% steal	CPU状态：空闲率，用户态占用率，内核态占用率，中断占用率，虚拟CPU等待物理CPU响应的时间占总CPU时间的百分比
Memory	内存状态：总量，可用内存数，page大小，单位为KB
JID	任务编号（用于唯一标识一个进程，该编号不会随着进程的重启而改变）
PID	进程编号
PRI	进程优先级
State	进程状态，可能的取值为： • R: running，运行状态或处于运行队列 • S: sleeping，可中断睡眠状态 • T: traced or stopped，暂停状态 • D: uninterruptible sleep，不可中断睡眠状态 • Z: zombie，僵死状态
FDs	file descriptions，进程打开的文件句柄数
MEM	进程所使用的内存大小（内核线程该项显示为0）
HH:MM:SS	进程自最近一次启动以来的运行时间
CPU	进程CPU使用率
Name	进程名称（如果进程名称带有“[]”标记，则表示该进程为内核线程）

1.1.25 monitor thread

monitor thread 命令用来显示线程的统计信息。

【命令】

```
monitor thread [ dumbtty ] [ iteration number ] [ slot slot-number [ cpu
cpu-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
context-admin

【参数】

dumbtty: 以哑终端方式显示线程统计信息（即屏幕不支持定时刷新统计信息）。指定该参数时，全部线程的统计信息以 CPU 使用率降序排列输出到屏幕上。不指定该参数时，统计信息以交互模式显示，缺省情况下按 CPU 占用率降序显示前 10 个线程的统计信息，且每隔 5 秒更新一次。

iteration number: 进程统计信息的显示次数，取值范围为 1~4294967295。指定 **dumbtty** 参数时 **number** 的缺省值为 1；不指定 **dumbtty** 且不配置 **number** 参数时，表示显示次数没有限制，统计信息会一直显示。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

不指定 **dumbtty** 参数的情况下，统计信息将以交互模式显示。在交互模式下，系统可以根据用户输入的交互命令字来调整显示方式或直接终止进程。在用户输入交互命令字之前，系统会自动计算可显示的线程个数，超出屏幕范围的线程不会显示。

在交互模式下可以使用的交互命令字及对应的功能请参见 [表 1-14](#)。

表1-14 monitor thread 命令支持的交互命令字描述表

命令字	功能描述
?或h	帮助信息，显示可用的交互式命令字
1	各物理CPU状态的显示开关。比如： 1. 输入 1，分别显示各物理 CPU 的参数值 2. 再次输入 1，显示所有 CPU 的参数的平均值 3. 第三次输入 1，又分别显示各物理 CPU 的参数值 4. 如此循环 缺省情况下，显示所有CPU的参数的平均值
c	按CPU占用率降序排列，缺省情况下采用降序排列
d	配置统计信息的更新时间间隔，单位为秒，缺省值为5
k	终止一个任务（进程），此命令会影响系统运行，请谨慎使用
l	刷新屏幕
n	改变显示的线程个数，取值为0~2147483647（缺省值为10，0表示不作限制）；超过屏幕范围时，仍只显示一屏内可容纳的线程个数
q	退出交互模式
t	按进程最近一次启动后的运行时间降序排列
<	排序项向左移动一列
>	排序项向右移动一列

【举例】

以哑终端方式显示线程统计信息。

<Sysname> monitor thread dumbtty

84 processes; 107 threads

Thread states: 1 running, 106 sleeping, 0 stopped, 0 zombie

CPU states: 83.19% idle, 1.68% user, 10.08% kernel, 5.04% interrupt

Memory: 755M total, 417M available, page size 4K

JID	TID	LAST_CPU	PRI	State	HH:MM:SS	MAX	CPU	Name
1175	1175	0	120	R	00:00:00	1	10.75%	top
1	1	0	120	S	00:00:06	1	2.68%	scmd
881	881	0	120	S	00:00:09	1	2.01%	diagd
776	776	0	120	S	00:00:01	0	0.67%	[DEVD]
866	866	0	120	S	00:00:11	1	0.67%	devd
2	2	0	115	S	00:00:00	0	0.00%	[kthreadd]
3	3	0	115	S	00:00:01	0	0.00%	[ksoftirqd/0]
4	4	0	99	S	00:00:00	1	0.00%	[watchdog/0]
5	5	0	115	S	00:00:00	0	0.00%	[events/0]
6	6	0	115	S	00:00:00	0	0.00%	[khelper]
796	796	0	115	S	00:00:00	0	0.00%	[kip6fs/1]

<Sysname>

以交互模式显示线程统计信息。

<Sysname> monitor thread

84 processes; 107 threads

Thread states: 1 running, 106 sleeping, 0 stopped, 0 zombie

CPU states: 94.43% idle, 0.76% user, 3.64% kernel, 1.15% interrupt

Memory: 755M total, 417M available, page size 4K

JID	TID	LAST_CPU	PRI	State	HH:MM:SS	MAX	CPU	Name
1176	1176	0	120	R	00:00:01	1	3.42%	top
866	866	0	120	S	00:00:12	1	0.85%	devd
881	881	0	120	S	00:00:09	1	0.64%	diagd
1	1	0	120	S	00:00:06	1	0.42%	scmd
1160	1160	0	120	S	00:00:01	1	0.21%	sshd
2	2	0	115	S	00:00:00	0	0.00%	[kthreadd]
3	3	0	115	S	00:00:01	0	0.00%	[ksoftirqd/0]
4	4	0	99	S	00:00:00	1	0.00%	[watchdog/0]
5	5	0	115	S	00:00:00	0	0.00%	[events/0]
6	6	0	115	S	00:00:00	0	0.00%	[khelper]

- 输入“h”或“?”，帮助信息显示如下：

Help for interactive commands:

?,h	Show the available interactive commands
1	Toggle SMP view: '1' single/separate states
c	Sort by the CPU field(default)
d	Set the delay interval between screen updates
k	Kill a job
l	Refresh the screen
n	Set the maximum number of threads to display
q	Quit the interactive display
t	Sort by run time of threads since last restart
<	Move sort field to the next left column
>	Move sort field to the next right column

Press any key to continue

- 输入“d”后，根据出现的提示如果输入“3”，统计信息将会每隔3秒更新一次。
Enter the delay interval between screen updates (1~2147483647): 3
- 输入“n”后，根据出现的提示如果输入“5”，显示的线程数目将会变为5个。
Enter the max number of threads to display(0 means unlimited): 5
84 processes; 107 threads
Thread states: 1 running, 106 sleeping, 0 stopped, 0 zombie
CPU states: 93.26% idle, 0.99% user, 4.23% kernel, 1.49% interrupt
Memory: 755M total, 417M available, page size 4K

JID	TID	LAST_CPU	PRI	State	HH:MM:SS	MAX	CPU	Name
1176	1176	0	120	R	00:00:02	1	3.71%	top
1	1	0	120	S	00:00:06	1	0.92%	scmd
866	866	0	120	S	00:00:13	1	0.69%	devd
881	881	0	120	S	00:00:10	1	0.69%	diagd
720	720	0	115	D	00:00:01	0	0.23%	[TMTH]

- 输入“k”后，根据出现的提示输入881，将会终止此JID对应的任务diagd。
Enter the JID to kill: 881
83 processes; 106 threads
Thread states: 1 running, 105 sleeping, 0 stopped, 0 zombie
CPU states: 96.26% idle, 0.54% user, 2.63% kernel, 0.54% interrupt
Memory: 755M total, 418M available, page size 4K

JID	TID	LAST_CPU	PRI	State	HH:MM:SS	MAX	CPU	Name
1176	1176	0	120	R	00:00:04	1	1.86%	top
866	866	0	120	S	00:00:14	1	0.87%	devd
1	1	0	120	S	00:00:07	1	0.49%	scmd
730	730	0	0	S	00:00:04	1	0.12%	[DIBC]
762	762	0	120	S	00:00:22	1	0.12%	[MNET]

- 输入“q”，将退出交互模式。

表1-15 monitor thread 命令显示信息描述表

显示项	内容描述
84 processes; 107 threads	系统的进程总数，线程总数
Thread states	线程状态：处于running状态的线程数，处于sleeping（包括interruptible sleep和uninterruptible sleep）状态的线程数，处于stopped状态的线程数，处于zombie状态的线程数
CPU states	CPU状态：空闲率，用户态占用率，内核态占用率，中断占用率
Memory	内存状态：总量，可用内存数，page大小
JID	任务编号，用于唯一标识一个进程，该编号不会随着进程的重启而改变
TID	线程编号
LAST_CPU	线程最近一次被调度所在的CPU的编号
PRI	线程优先级

显示项	内容描述
State	进程状态，可能的取值为： • R: running, 运行状态或处于运行队列 • S: sleeping, 可中断睡眠状态 • T: traced or stopped, 暂停状态 • D: uninterruptible sleep, 不可中断睡眠状态 • Z: zombie, 僵死状态
HH:MM:SS	线程自最近一次启动以来的运行时间
MAX	线程单次调度占用CPU的最长时间，以毫秒为单位
CPU	线程CPU使用率
Name	线程名称（如果线程名称带有“[]”标记，则表示该线程为内核线程）

1.1.26 process core

process core 命令用来开启/关闭用户态进程异常时生成 core 文件的功能，并配置可生成 core 文件的最大个数。

【命令】

```
process core { maxcore value | off } { job job-id | name process-name } [ slot slot-number [ cpu cpu-number ] ]
```

【视图】

用户视图

【缺省情况】

同一用户态进程在首次异常时会生成 core 文件，后续异常不再生成 core 文件。即 **maxcore** 的最大数值为 1。

【缺省用户角色】

network-admin
context-admin

【参数】

off: 表示关闭用户态进程异常时生成 core 文件的功能。

maxcore value: 表示开启用户态进程的 core 文件生成功能，并配置能生成的 core 文件的最大个数。*value* 表示用户态进程能生成的 core 文件的最大个数，取值范围为 1~10，缺省值为 1。

name process-name: 用户态进程的名称，为 1~15 个字符的字符串，不区分大小写。**process core** 命令的配置对用户态进程下的所有实例有效。

job job-id: 任务 ID，用于唯一标识一个进程，该 ID 不会随着进程的重启而改变，取值范围为 1~2147483647。

slot slot-number: 表示设备在 IRF 中的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

开启用户态进程的 **core** 文件生成功能，并配置能生成的 **core** 文件的最大个数后，用户态进程异常重启一次，就会产生一个 **core** 文件并记录用户态进程的异常信息。如果生成的 **core** 文件的数目达到最大值，则不再生成新的 **core** 文件。软件开发和维护人员能够根据 **core** 文件的内容来定位异常的原因和异常的位置。

因为生成的 **core** 文件会占用系统存储资源，如果用户对某些用户态进程的异常退出不关心，可以关闭这些用户态进程的 **core** 文件记录功能。

【举例】

关闭用户态进程 **routed** 的 **core** 文件生成功能。

```
<Sysname> process core off name routed
```

开启用户态进程 **routed** 的 **core** 文件生成功能，并且最多可生成 5 个 **core** 文件。

```
<Sysname> process core maxcore 5 name routed
```

【相关命令】

- **display exception context**
- **exception filepath**

1.1.27 reset exception context

reset exception context 命令用来清除用户态进程异常时记录的上下文信息。

【命令】

```
reset exception context [ slot slot-number [ cpu cpu-number ] ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【举例】

清除用户态进程异常记录。

```
<Sysname> reset exception context
```

【相关命令】

- **display exception context**

1.1.28 reset kernel deadlock

reset kernel deadlock 命令用来清除内核线程死循环信息。

【命令】

reset kernel deadloop [**slot** *slot-number* [**cpu** *cpu-number*]]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number*: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu *cpu-number*: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

【举例】

清除内核线程死循环信息。

<Sysname> reset kernel deadloop

【相关命令】

- **display kernel deadloop**

1.1.29 reset kernel exception

reset kernel exception 命令用来清除内核线程的异常信息。

【命令】

reset kernel exception [**slot** *slot-number* [**cpu** *cpu-number*]]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number*: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu *cpu-number*: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

【举例】

清除内核线程的异常信息。

<Sysname> reset kernel exception

【相关命令】

- **display kernel exception**

1.1.30 reset kernel reboot

reset kernel reboot 命令用来清除内核线程重启信息。

【命令】

reset kernel reboot [slot slot-number [cpu cpu-number]]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

【举例】

清除内核线程重启信息。

<Sysname> reset kernel reboot

【相关命令】

- **display kernel reboot**

1.1.31 reset kernel starvation

reset kernel starvation 命令用来清除内核线程饿死信息。

【命令】

reset kernel starvation [slot slot-number [cpu cpu-number]]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 表示 IRF 中设备的成员编号。不指定该参数时，表示主设备。

cpu cpu-number: 表示 CPU 的编号。

【使用指导】

仅缺省 Context 支持本命令。

【举例】

清除内核线程饿死信息。

<Sysname> reset kernel starvation

【相关命令】

- `display kernel starvation`

目 录

1 快速日志输出.....	1-1
1.1 快速日志输出命令.....	1-1
1.1.1 customlog character-encoding utf-8	1-1
1.1.2 customlog format	1-2
1.1.3 customlog host.....	1-3
1.1.4 customlog host source	1-4
1.1.5 customlog timestamp.....	1-5

1 快速日志输出

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	说明
T5000-G20	不支持
T5000-G30	支持
T1000-G20/T1000-G50/T1000-G60/T1000-G80	不支持
T1000-CN60/T1000-CN80	支持

1.1 快速日志输出命令

1.1.1 customlog character-encoding utf-8

customlog character-encoding utf-8 命令用来配置快速日志输出使用 UTF-8 编码方式输出日志。

undo customlog character-encoding 命令用来恢复缺省情况。

【命令】

```
customlog character-encoding utf-8
undo customlog character-encoding
```

【缺省情况】

快速日志输出使用 GB18030 编码方式输出日志。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

如果日志接收服务器和设备使用的中文字符集编码不同，日志服务器上可能会出现中文字符乱码的情况。使用本命令可以将快速日志输出模块发送日志信息时使用的字符集编码配置为 UTF-8 或者 GB18030。

【举例】

```
# 配置快速日志输出使用 UTF-8 编码方式输出日志。
<Sysname> system-view
[Sysname] customlog character-encoding utf-8
```


1.1.2 customlog format

customlog format 命令用来开启快速日志输出功能。

undo customlog format 命令用来关闭快速日志输出功能。

【命令】

```
customlog format { attack-defense | dpi [ anti-virus | audit | ip-reputation  
| ips [ sgcc ] | url-filter [ unicom ] | waf ] | keepalive sgcc | packet-filter  
[ sgcc ] | scd | security-policy sgcc | session }  
undo customlog format { attack-defense | dpi [ anti-virus | audit |  
ip-reputation | ips | url-filter [ unicom ] | waf ] * | keepalive |  
packet-filter | scd | security-policy | session } *
```

【缺省情况】

快速日志输出功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

attack-defense: 将攻击检测与防范模块的日志快速输出到日志主机。

dpi: 将 DPI（Deep Packet Inspection，深度报文检测）相关模块的日志快速输出到日志主机。不指定任何参数时，则表示将所有 DPI 相关模块的日志快速输出到日志主机。

anti-virus: 将防病毒模块的日志快速输出到日志主机。

audit: 将应用审计与管理模块的日志快速输出到日志主机。

ip-reputation: 将 IP 信誉模块的日志快速输出到日志主机。

ips: 将入侵防御模块的日志快速输出到日志主机。

sgcc: 配置入侵防御快速输出日志时使用国家电网格式。若不指定此参数，则使标准格式输出命中入侵防御策略的日志。

url-filter: 将 URL 过滤模块的日志快速输出到日志主机。

unicom: 配置 URL 过滤模块快速输出日志时使用中国联通格式。若不配置此参数，则使用标准格式输出日志。

waf: 将 WAF 模块的日志快速输出到日志主机。

keepalive: 将心跳日志输出到日志主机。配置本参数后，日志服务器将会接收此心跳日志，如果定期接收不到就认为设备 down 掉了。

packet-filter: 将报文过滤模块的日志快速输出到日志主机。

scd: 将服务器外联防护模块的日志快速输出到日志主机。

security-policy: 将安全策略的日志快速输出到日志主机。

session: 将会话管理模块的日志快速输出到日志主机。

sgcc: 配置快速输出日志时使用国家电网格式。若不指定此参数，则使用标准格式输出。

【使用指导】

快速日志输出功能用于快速地将用户关心的日志发往日志主机。配置该功能后，业务模块生成的日志通过快速输出通道直接发送给日志主机，不经过信息中心模块处理。相比通过信息中心输出，该方式可以节省系统资源，更快捷。

【举例】

```
# 开启会话管理模块快速日志输出功能。  
<Sysname> system  
[Sysname] customlog format session
```

1.1.3 customlog host

customlog host 命令用来配置快速日志输出参数。

undo customlog host 命令用来取消快速日志输出参数配置。

【命令】

```
customlog host [ vpn-instance vpn-instance-name ] { hostname | ipv4-address |  
ipv6 ipv6-address } [ port port-number ] export { attack-defense | dpi |  
anti-virus | audit | ip-reputation | ips | url-filter | waf } * | keepalive |  
packet-filter | scd | security-policy | session } *  
undo customlog host [ vpn-instance vpn-instance-name ] { hostname |  
ipv4-address | ipv6 ipv6-address } [ port port-number ]
```

【缺省情况】

未配置快速日志输出参数。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

vpn-instance *vpn-instance-name*: 指定日志主机所属的VPN实例。*vpn-instance-name*表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示日志主机位于公网中。

hostname: 指定日志的主机名，为 1~253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”和“.”。

ipv4-address: 指定日志主机的 IPv4 地址。

ipv6 *ipv6-address*: 指定日志主机的 IPv6 地址。

port *port-number*: 指定日志主机接收日志信息的端口号，取值范围为 1~65535，缺省值为 514。该参数的值需要和日志主机侧的配置一致，否则日志主机接收不到日志信息。

export: 指定可以发送日志的模块。

attack-defense: 允许设备向指定的日志主机发送攻击检测与防范模块的日志。

dpi: 允许设备向指定的日志主机发送 DPI 相关模块的日志。不指定任何参数时，则表示允许设备向指定的日志主机发送所有 DPI 相关模块的日志。

anti-virus: 允许设备向指定的日志主机发送防病毒模块的日志。

audit: 允许设备向指定的日志主机发送应用审计与管理模块的日志。

ip-reputation: 允许设备向指定的日志主机发送 IP 信誉模块的日志。

ips: 允许设备向指定的日志主机发送入侵防御模块的日志。

url-filter: 允许设备向指定的日志主机发送 URL 过滤模块的日志。

waf: 允许设备向指定的日志主机发送 WAF 模块的日志。

keepalive: 允许设备向指定的日志主机发送心跳日志。

packet-filter: 允许设备向指定的日志主机发送报文过滤模块的日志。

scd: 允许设备向指定的日志主机发送服务器外联防护模块的日志。

security-policy: 允许设备向指定的日志主机发送安全策略模块的日志。

session: 允许设备向指定的日志主机发送会话模块的日志。

【使用指导】

只有配置 **customlog format** 命令后，**customlog host** 命令才会生效。

【举例】

配置系统向 IP 地址为 1.1.1.1 的日志主机发送会话管理模块日志。

```
<Sysname> system-view
```

```
[Sysname] customlog host 1.1.1.1 port 1000 export session
```

1.1.4 customlog host source

customlog host source 命令用来配置快速日志输出时使用的源 IP 地址。

undo customlog host source 命令用来恢复缺省情况。

【命令】

customlog host source *interface-type interface-number*

undo customlog host source

【缺省情况】

快速日志输出时使用的源 IP 地址为出接口的主 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type interface-number: 指定快速输出日志的源 IP 地址对应的出接口的类型和编号。

【使用指导】

配置本命令后，不管实际使用哪个物理接口发送日志信息，日志信息的源 IP 地址均为指定接口的主 IP 地址。当日志主机需要根据日志的源 IP 对日志进行过滤显示时，请配置该命令。

只有配置 **customlog format** 和 **customlog host** 命令后，**customlog host source** 命令才会生效。

【举例】

配置快速日志输出时使用的源 IP 地址为 Loopback0 的 IP 地址。

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] ip address 2.2.2.2 32
[Sysname-LoopBack0] quit
[Sysname] customlog host source loopback 0
```

1.1.5 customlog timestamp

customlog timestamp localtime 命令用来配置快速输出日志的时间戳为系统时间。

undo customlog timestamp localtime 命令用来恢复缺省情况。

【命令】

```
customlog timestamp localtime
undo customlog timestamp localtime
```

【缺省情况】

快速输出日志的时间戳为格林威治时间。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【举例】

配置快速输出日志的时间戳为系统时间。

```
<Sysname> system-view
[Sysname] customlog timestamp localtime
```

目 录

1 信息中心.....	1-1
1.1 信息中心配置命令.....	1-1
1.1.1 diagnostic-logfile save	1-1
1.1.2 display character-set	1-1
1.1.3 display diagnostic-logfile summary	1-3
1.1.4 display info-center.....	1-3
1.1.5 display info-center filter	1-5
1.1.6 display info-center source.....	1-6
1.1.7 display logbuffer	1-7
1.1.8 display logbuffer summary	1-9
1.1.9 display logfile summary.....	1-10
1.1.10 display security-logfile summary	1-11
1.1.11 enable log updown	1-12
1.1.12 info-center diagnostic-logfile directory.....	1-12
1.1.13 info-center diagnostic-logfile enable	1-13
1.1.14 info-center diagnostic-logfile frequency	1-14
1.1.15 info-center diagnostic-logfile quota.....	1-14
1.1.16 info-center enable	1-15
1.1.17 info-center filter.....	1-15
1.1.18 info-center format.....	1-17
1.1.19 info-center logbuffer.....	1-17
1.1.20 info-center logbuffer size	1-18
1.1.21 info-center logfile directory	1-19
1.1.22 info-center logfile enable.....	1-20
1.1.23 info-center logfile frequency	1-20
1.1.24 info-center logfile module alarm-threshold	1-21
1.1.25 info-center logfile size-quota.....	1-22
1.1.26 info-center logging suppress duplicates	1-23
1.1.27 info-center loghost.....	1-23
1.1.28 info-center loghost source.....	1-24
1.1.29 info-center security-logfile alarm-threshold.....	1-25
1.1.30 info-center security-logfile directory	1-26
1.1.31 info-center security-logfile enable	1-26

1.1.32 info-center security-logfile frequency	1-27
1.1.33 info-center security-logfile size-quota.....	1-28
1.1.34 info-center source	1-28
1.1.35 info-center synchronous	1-30
1.1.36 info-center syslog min-age	1-31
1.1.37 info-center syslog trap buffersize	1-32
1.1.38 info-center syslog utf-8 enable	1-32
1.1.39 info-center timestamp	1-33
1.1.40 info-center timestamp loghost	1-34
1.1.41 info-center trace-logfile quota.....	1-35
1.1.42 logfile save	1-35
1.1.43 reset logbuffer	1-36
1.1.44 security-logfile save	1-36
1.1.45 snmp-agent trap enable syslog	1-37
1.1.46 terminal debugging.....	1-38
1.1.47 terminal logging level	1-39
1.1.48 terminal monitor.....	1-39

1 信息中心



说明

设备支持的存储介质与设备型号相关，本手册使用 flash 类型的存储介质举例，实际使用过程中，请以设备实际情况为准。

1.1 信息中心配置命令

1.1.1 diagnostic-logfile save

diagnostic-logfile save 命令用来手动将诊断日志文件缓冲区中的内容全部保存到诊断日志文件。

【命令】

diagnostic-logfile save

【视图】

任意视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

诊断日志文件的保存路径可以通过 **info-center diagnostic-logfile directory** 命令配置。

诊断日志文件保存成功后，诊断日志文件缓冲区中的内容会被清空。

如果执行本命令时，诊断日志文件缓冲区中没有日志，本命令会执行成功，但不会创建或更新已有诊断日志文件。

【举例】

手动将诊断日志文件缓冲区中的内容保存到诊断日志文件。

```
<Sysname> diagnostic-logfile save
```

```
The contents in the diagnostic log file buffer have been saved to the file  
flash:/diagfile/diagfile.log.
```

【相关命令】

- **info-center diagnostic-logfile enable**
- **info-center diagnostic-logfile directory**

1.1.2 display character-set

display character-set 命令用来显示设备或登录软件当前使用的字符集编码。

【命令】

display character-set [terminal]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

terminal: 显示登录软件当前使用的中文字符集编码。不指定该参数时，显示设备当前使用的字符集编码（设备当前使用的字符集编码为 GB18030，不支持通过命令行修改）。

【使用指导】

当用户使用登录软件登录设备，且设备往登录软件发送的信息中包含中文字符时，如果登录软件和设备使用的中文字符集编码不同，可能会出现中文字符在登录软件上显示为乱码的情况。

执行 **display character-set terminal** 命令，设备会向用户使用的登录软件分别发送 UTF-8 和 GB18030 格式的字符串进行测试：

- 如果 UTF-8 行的 Test characters 字段显示为“中文”，则表示该登录软件使用的中文字符集编码为 UTF-8；
- 如果 GB18030 行的 Test characters 字段显示为“中文”，则表示该登录软件使用的中文字符集编码为 GB18030。

【举例】

```
# 显示设备当前使用的字符集编码。
<Sysname> system-view
[Sysname] display character-set
Current character set encoding: GB18030
# 显示用户的登录软件当前使用的字符集编码。
<Sysname> system-view
[Sysname] display character-set terminal
Character set          Test characters
UTF-8                  涓  杓
GB18030                中文
```

表1-1 display character-set 命令显示信息描述表

字段	描述
Current character set encoding	设备当前使用的字符集编码
Character set	设备向登录软件发送测试字符时使用的字符集编码，取值为UTF-8和GB18030
Test characters	显示测试字符串的解析结果。Test Characters取值为“中文”的行的“Character set”取值即为登录软件当前使用的字符集编码

【相关命令】

- info-center syslog utf-8 enable

1.1.3 display diagnostic-logfile summary

display diagnostic-logfile summary 命令用来显示诊断日志文件的配置。

【命令】

display diagnostic-logfile summary

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【举例】

```
# 显示诊断日志文件配置。
<Sysname> display diagnostic-logfile summary
Diagnostic log file: Enabled.
Diagnostic log file size quota: 10 MB
Diagnostic log file directory: flash:/diagfile
Writing frequency: 24 hour 0 min 0 sec
```

表1-2 display logfile summary 命令显示信息描述表

字段	描述
Diagnostic log file	诊断日志文件当前的状态： • Enabled: 表示已开启 • Disabled: 表示未开启
Diagnostic log file size quota	单个诊断日志文件最大能占用的存储空间的大小，单位为MB
Diagnostic log file directory	诊断日志文件存储的路径
Writing frequency	系统自动保存诊断日志文件的频率

1.1.4 display info-center

display info-center 命令用来显示各个输出方向的信息。

【命令】

display info-center

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

```
# 显示各个输出方向的信息。  
<Sysname> display info-center  
Information Center: Enabled  
Console: Enabled  
Monitor: Enabled  
Log host: Enabled  
    192.168.0.1, log output filter: loghost1  
    port number: 5000, host facility: local7  
Log buffer: Enabled  
    Max buffer size 1024, current buffer size 512,  
    Current messages 0, dropped messages 0, overwritten messages 0  
Log file: Enabled  
Security log file: Enabled  
Information timestamp format:  
    Log host: Date  
    Other output destination: Date
```

表1-3 display info-center 命令显示信息描述表

字段	描述
Information Center	信息中心当前的状态： - Enabled: 表示允许输出日志 - Disabled: 表示禁止输出日志
Console	控制台方向当前的状态： - Enabled: 表示允许向控制台输出日志 - Disabled: 表示禁止向控制台输出日志
Monitor	监视终端方向当前的状态： - Enabled: 表示允许向监视终端输出日志 - Disabled: 表示禁止向监视终端输出日志

字段	描述
Log host: Enabled 192.168.0.1, log output filter: loghost1 port number: 5000, host facility: local7	日志主机方向的信息： • Enabled: 表示允许向日志主机输出日志 • Disabled: 表示禁止向日志主机输出日志 只有开启后，才有下面具体的显示内容，包括： • 日志主机的 IP 地址 • 关联的日志输出规则名称 • 日志主机接收日志信息的端口 • 日志主机的记录工具
Log buffer: Enabled Max buffer size 1024, current buffer size 512, Current messages 0, dropped messages 0, overwritten messages 0	日志缓冲区方向的信息，包括开启状态、最大容量、当前容量、当前信息数、已丢弃的信息数、被覆盖的信息数
Log file	日志文件方向当前的状态： • Enabled: 表示允许向日志文件输出日志 • Disabled: 表示禁止向日志文件输出日志
Security log file	安全日志文件方向当前的状态： • Enabled: 表示允许向安全日志文件输出日志 • Disabled: 表示禁止向安全日志文件输出日志
Information timestamp format: Log host: Date Other output destination: Date	信息时间戳配置，包括日志主机输出方向和非日志主机输出方向日志信息的时间戳类型，分为boot、date、iso、none和no-year-date五种

1.1.5 display info-center filter

display info-center filter 命令用来显示用户创建的日志输出规则的相关信息。

【命令】

display info-center filter [*filtername*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

filter-name: 显示指定日志输出规则的相关信息。**filter-name** 表示日志信息输出规则的名称，必须为设备上已创建的日志输出规则。不指定该参数时，显示所有日志输出规则的相关信息。

【举例】

```
# 显示日志输出规则 loghost1 的相关信息。
<Sysname> display info-center filter loghost1
Log output filter: loghost1
Module                Rule
ARP                   Debugging
CFGLOG                Deny
Default               Informational
```

表1-4 日志主机关联日志输出规则描述表

字段	描述
Log output filter:	日志输出规则名
Module	输出规则中的模块
Rule	模块对应的输出规则

【相关命令】

- **info-center filter**

1.1.6 display info-center source

display info-center source 命令用来显示日志信息的输出规则。

【命令】

```
display info-center source [ module module-name ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

module module-name: 显示指定模块日志信息的输出规则。*module-name* 表示模块的名称，配置时需要完整输入，不区分大小写，执行 **display info-center source module ?**命令，通过帮助信息可获得该参数的取值。不指定该参数时，表示显示所有模块日志信息的输出规则。

【使用指导】

日志在各输出方向都有缺省输出规则，缺省输出规则请参见 [表 1-11](#)，用户也可以通过**info-center source**命令用来配置日志信息的输出规则，**display info-center source**命令显示的是日志信息当前的实际输出规则。

【举例】

显示所有模块日志信息的输出规则。

```
<Sysname> display info-center source
Module   Console      Monitor      Loghost      Logbuffer     Logfile
ACL       DEBUG         DEBUG        INFO         INFO          INFO
ADJ4      DEBUG         DEBUG        INFO         INFO          INFO
ADJ6      DEBUG         DEBUG        INFO         INFO          INFO
```

……其他显示信息略……

显示 EDEV 模块日志信息的输出规则。

```
<Sysname> display info-center source module EDEV
Module   Console      Monitor      Loghost      Logbuffer     Logfile
EDEV      DEBUG         DEBUG        INFO         INFO          INFO
```

表1-5 display info-center source 命令显示信息描述表

字段	描述
Module	模块名称
Console	在控制台的输出规则，若取值为deny则代表日志不允许在该方向输出
Monitor	在监控终端的输出规则，若取值为deny则代表日志不允许在该方向输出
Loghost	在日志主机的输出规则，若取值为deny则代表日志不允许在该方向输出
Logbuffer	在日志缓冲区的输出规则，若取值为deny则代表日志不允许在该方向输出
Logfile	在日志文件的输出规则，若取值为deny则代表日志不允许在该方向输出

【相关命令】

- info-center source

1.1.7 display logbuffer

display logbuffer 命令用来显示日志缓冲区的状态和日志缓冲区记录的日志信息。

【命令】

```
display logbuffer [ module module-name [ submodule submodule-name ] ]
[ reverse ] [ level severity | size buffersize | slot slot-number ] *
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

module module-name: 显示指定模块日志缓冲区的状态和日志缓冲区记录的日志信息。*module-name* 表示模块的名称,配置时需要完整输入,不区分大小写,执行 **display logbuffer module ?**命令,通过帮助信息可获得该参数的取值。不指定该参数时,表示该配置对通用日志缓冲区生效。

submodule submodule-name: 显示当前模块下指定子模块日志缓冲区的状态和日志缓冲区记录的日志信息。*submodule-name* 表示子模块名称,配置时需要完整输入,不区分大小写。当前模块是否支持子模块以及子模块的取值,请通过执行 **display logbuffer module module-name submodule ?**命令获取。不指定该参数时,表示该配置对当前模块下所有子模块生效。

reverse: 指定日志的显示顺序为从新到旧。如果不指定该参数,将先显示旧日志,最后显示最新的日志。

level severity: 显示日志缓存中指定级别日志的信息, *severity* 表示信息级别,取值范围为0~7。不带该参数时将显示系统日志缓冲区内所有级别的日志信息。

表1-6 信息级别列表

数值	信息级别	描述
0	emergency	表示设备不可用的信息,如系统授权已到期
1	alert	表示设备出现重大故障,需要立刻做出反应的信息,如流量超出接口上限
2	critical	表示严重信息,如设备温度已经超过预警值,设备电源、风扇出现故障等
3	error	表示错误信息,如接口链路状态变化等
4	warning	表示警告信息,如接口连接断开,内存耗尽告警等
5	notification	表示正常出现但是重要的信息,如通过终端登录设备,设备重启等
6	informational	表示需要记录的通知信息,如通过命令行输入命令的记录信息,执行ping命令的日志信息等
7	debugging	表示调试过程产生的信息

size buffersize: 显示日志缓冲区中指定条数的最新日志。*buffersize* 表示要显示的日志缓冲区中最新的日志信息的条数,取值范围为1~1024。不带该参数时将显示系统日志缓冲区内所有的日志信息。

slot slot-number: 显示指定成员设备的日志缓冲区状态及日志缓冲区中记录的日志信息。*slot-number* 表示设备在IRF中的成员编号。如不指定该参数,将显示所有成员设备的日志缓冲区状态及日志缓冲区中记录的日志信息。

【举例】

显示系统日志缓冲区的状态和缓冲区记录的日志信息。

```
<Sysname> display logbuffer
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 718
```

Current messages: 512

Some messages might not be displayed due to permission issues.

%Jun 17 15:57:09:578 2017 Sysname SYSLOG/7/SYS_RESTART:System restarted --

其它显示信息略……。

表1-7 display logbuffer 命令显示信息描述表

字段	描述
Log buffer	是否允许输出到日志缓冲区方向： • Enabled: 表示允许 • Disabled: 表示不允许
Max buffer size	允许的日志缓冲区可存储的最大信息条数
Actual buffer size	当前配置的日志缓冲区可存储的最大信息条数
Dropped messages	被丢弃的信息数（内存分配失败或分配日志缓冲区过小时丢失的信息数）
Overwritten messages	被覆盖的信息数（如果缓冲区存储空间不足，最早收到的信息数会被新的信息覆盖掉）
Current messages	当前记录的信息数
Some messages might not be displayed due to permission issues.	由于当前登录用户的角色不同，可以查看的日志内容不同。关于用户角色的详细介绍，请参见“基础配置指导”中的“RBAC”

【相关命令】

- info-center logbuffer
- reset logbuffer

1.1.8 display logbuffer summary

display logbuffer summary 命令用来显示系统日志缓冲区的概要信息。

【命令】

display logbuffer summary [level severity | slot slot-number] *

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【参数】

level severity: 显示日志缓存中指定级别日志的概要信息，**severity**表示信息级别，取值范围为 0~7，具体内容请参见 [表 1-6](#)。不带该参数时，将显示系统日志缓冲区内所有级别的日志概要信息。

slot slot-number: 显示指定成员设备的日志缓冲区的概要信息。*slot-number* 表示设备在 IRF 中的成员编号。如不指定该参数，将显示所有成员设备上的日志缓冲区概要信息。

【举例】

```
# 显示系统日志缓冲区的概要信息。
<Sysname> display logbuffer summary
  Slot EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
    1    0    0    0    7    0    34    38    0
```

表1-8 display logbuffer summary 命令显示信息描述表

字段	描述
EMERG	emergency级别的信息数，请参见 表1-6
ALERT	alert级别的信息数，请参见 表1-6
CRIT	critical级别的信息数，请参见 表1-6
ERROR	error级别的信息数，请参见 表1-6
WARN	warning级别的信息数，请参见 表1-6
NOTIF	notification级别的信息数，请参见 表1-6
INFO	informational级别的信息数，请参见 表1-6
DEBUG	debugging级别的信息数，请参见 表1-6

1.1.9 display logfile summary

display logfile summary 命令用来显示日志文件的配置。

【命令】

```
display logfile summary
```

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator
- context-admin
- context-operator

【举例】

```
# 显示日志文件配置。
<Sysname> display logfile summary
  Log file: Enabled.
  Log file size quota: 10 MB
  Log file directory: flash:/logfile
  Writing frequency: 24 hour 0 min 10 sec
```


表1-9 display logfile summary 命令显示信息描述表

字段	描述
Log file	是否允许输出到日志文件方向： - Enabled: 表示已开启 - Disabled: 表示未开启
Log file size quota	单个日志文件最大能占用的存储空间的大小，单位为MB
Log file directory	日志文件存储的路径
Writing frequency	系统自动保存日志文件的频率

1.1.10 display security-logfile summary

display security-logfile summary 命令用来显示安全日志文件的概要信息。

【命令】

display security-logfile summary

【视图】

任意视图

【缺省用户角色】

security-audit

【使用指导】

只有具有安全日志管理员角色的本地用户才能使用本命令。安全日志管理员的配置请参见“安全命令参考”中的“AAA”。

【举例】

显示安全日志文件概要信息。

```
<Sysname> display security-logfile summary
Security log file: Enabled
Security log file size quota: 10 MB
Security log file directory: flash:/seclog
Alarm threshold: 80%
Current usage: 30%
Writing frequency: 24 hour 0 min 0 sec
```

表1-10 display security-logfile summary 命令显示信息描述表

字段	描述
Security log file	安全日志文件当前的状态： - Enabled: 表示已开启 - Disabled: 表示未开启
Security log file size quota	单个安全日志文件最大能占用的存储空间的大小
Security log file directory	安全日志文件存储的路径

字段	描述
Alarm-threshold	安全日志文件使用率告警门限
Current usage	当前的安全日志文件使用率
Writing frequency	系统自动保存安全日志文件的频率

【相关命令】

- **authorization-attribute**（安全命令参考/AAA）

1.1.11 enable log updown

enable log updown 命令用来允许端口在状态发生改变时生成 Link up 和 Link down 的日志信息。

undo enable log updown 命令用来禁止端口在状态发生改变时生成 Link up 和 Link down 的日志信息。

【命令】

enable log updown
undo enable log updown

【缺省情况】

允许所有端口在状态发生改变时生成端口 Link up 和 Link down 的日志信息。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【举例】

```
# 禁止端口 GigabitEthernet1/0/1 在状态发生改变时生成 Link up 和 Link down 的日志信息。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo enable log updown
```

1.1.12 info-center diagnostic-logfile directory

info-center diagnostic-logfile directory 命令用来修改存储诊断日志文件的路径。

【命令】

info-center diagnostic-logfile directory *dir-name*

【缺省情况】

存储诊断日志文件路径为设备缺省文件系统根目录下的 diagfile 文件夹。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

dir-name: 诊断日志文件存储的路径，为 1~64 个字符的字符串。

【使用指导】

在执行该配置前，存储诊断日志文件的文件夹必须为当前已创建的目录。
配置会在 IRF 重启或主从设备倒换后失效。

【举例】

```
# 配置存放诊断日志文件的目录为 flash:/test。  
<Sysname> mkdir test  
Creating directory flash:/test... Done.  
<Sysname> system-view  
[Sysname] info-center diagnostic-logfile directory flash:/test
```

1.1.13 info-center diagnostic-logfile enable

info-center diagnostic-logfile enable 命令用来开启诊断日志同步保存功能。
undo info-center diagose-logfile enable 命令用来关闭诊断日志同步保存功能。

【命令】

```
info-center diagnostic-logfile enable  
undo info-center diagnostic-logfile enable
```

【缺省情况】

诊断日志同步保存功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

开启诊断日志同步保存功能后，系统将诊断日志进行集中处理：当生成的诊断日志时，系统会将诊断日志信息同步保存到诊断日志文件。这样既实现了诊断日志的集中管理，又有利于用户随时快捷地查看诊断日志，了解设备状态。

【举例】

```
# 开启诊断日志同步保存功能。  
<Sysname> system-view  
[Sysname] info-center diagnostic-logfile enable
```

1.1.14 info-center diagnostic-logfile frequency

info-center diagnostic-logfile frequency 命令用来配置设备自动保存诊断日志文件的频率。

undo info-center diagnostic-logfile frequency 命令用来恢复缺省情况。

【命令】

info-center diagnostic-logfile frequency *freq-sec*

undo info-center diagnostic-logfile frequency

【缺省情况】

设备自动保存诊断日志文件的频率为 86400 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

freq-sec: 系统自动保存诊断日志文件的频率，取值范围为 10~86400，单位为秒。

【使用指导】

配置设备自动保存诊断日志文件的频率后，诊断日志会先被输出到诊断日志文件缓冲区（**diagnostic-logfile buffer**），系统会按照配置中指定的频率将诊断日志文件缓冲区的内容写入诊断日志文件。

【举例】

配置诊断日志自动保存到文件的频率为 600 秒。

```
<Sysname> system-view
```

```
[Sysname] info-center diagnostic-logfile frequency 600
```

【相关命令】

- **info-center diagnostic-logfile enable**

1.1.15 info-center diagnostic-logfile quota

info-center diagnostic-logfile quota 命令用来配置单个诊断日志文件最大可占用的存储空间的大小。

undo info-center diagnostic-logfile quota 命令用来恢复缺省情况。

【命令】

info-center diagnostic-logfile quota *size*

undo info-center diagnostic-logfile quota

【缺省情况】

单个诊断日志文件最大能占用的存储空间为 10MB。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

size: 单个诊断日志文件可使用的存储空间的最大值，取值范围为 1~10，单位为 MB。

【举例】

配置单个诊断日志文件最大能占用的存储空间的大小为 6MB。

```
<Sysname> system-view
```

```
[Sysname] info-center diagnostic-logfile quota 6
```

1.1.16 info-center enable

info-center enable 命令用来开启信息中心功能。

undo info-center enable 命令用来关闭信息中心功能。

【命令】

info-center enable

undo info-center enable

【缺省情况】

信息中心处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【举例】

开启信息中心功能。

```
<Sysname> system-view
```

```
[Sysname] info-center enable
```

```
Information center is enabled.
```

1.1.17 info-center filter

info-center filter 命令用来创建日志输出规则。

undo info-center filter 命令用来删除日志输出规则。

【命令】

```
info-center filter filter-name { module-name | default } { deny | level  
severity }
```

undo info-center filter *filter-name* [*module-name* | **default**]

【缺省情况】

未创建日志输出规则。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

filter-name: 日志信息输出规则的名称，为 1~8 个字符的字符串，不区分大小写。

module-name: 为指定模块配置日志输出规则，该参数的取值可通过在系统视图下输入 **info-center filter filter-name ?** 来获得。

default: 配置所有应用模块日志信息的缺省输出规则。

deny: 禁止输出日志信息。

level severity: 指定允许输出的日志信息的最低级别，取值为 **alert**、**critical**、**debugging**、**emergency**、**error**、**informational**、**notification**、**warning**，各参数的含义请参见 [表 1-6](#)。例如，本参数配置为 **warning**，则表示配置对 **emergency**、**alert**、**critical**、**error** 和 **warning** 级别的日志均生效。

【使用指导】

多次执行本命令可以创建多个输出规则，将输出规则和日志主机绑定，可以为不同的日志主机指定不同的输出规则。**info-center source** 命令也可以配置日志输出规则。本命令配置的输出规则目前只支持应用到日志主机输出方向，**info-center source** 命令配置的日志输出规则适用于所有输出方向。对于日志主机输出方向，本命令配置的输出规则优先于 **info-center source** 命令配置的输出规则。

用户可以使用 **module-name** 参数为应用模块单独配置输出规则，也可以使用 **default** 参数为所有应用模块配置缺省输出规则，这两种配置可以同时存在。多次使用 **module-name** 参数为同一应用模块配置输出规则时，最后一次执行的命令生效；多次使用 **default** 参数配置缺省输出规则时，最后一次执行的命令生效。

对于应用模块：

- 优先使用带 **module-name** 参数的配置。
- 如果没有使用 **module-name** 参数为应用模块单独配置输出规则，则该模块使用 **default** 参数配置的输出规则。

如果配置了带 **module-name** 参数的命令，未配置带 **default** 参数的命令行，则未单独配置输出规则的应用模块允许 **alert**~**informational** 级别的日志输出。

给应用模块单独配置输出规则后，必须使用 **module-name** 参数来修改或删除该规则，使用 **default** 参数进行的配置对该模块不生效。

【举例】

配置名称为 loghost1 的输出规则，用来允许 ARP 模块 alert~notification 级别的日志信息输出，SNMP 模块 alert~warning 级别的日志信息输出，其他模块的日志信息禁止输出。

```
<Sysname> system-view
[Sysname] info-center filter loghost1 arp level notification
[Sysname] info-center filter loghost1 snmp level warning
[Sysname] info-center filter loghost1 default deny
```

【相关命令】

- **display info-center filter**
- **info-center loghost**
- **info-center source**

1.1.18 info-center format

info-center format 命令用来配置发往日志主机的日志信息的输出格式。

undo info-center format 命令用来恢复缺省情况。

【命令】

```
info-center format { cmcc | unicom }
undo info-center format
```

【缺省情况】

发往日志主机的日志信息的格式为非定制格式。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

cmcc：配置发往日志主机的日志信息的输出格式为中国移动格式。

unicom：配置发往日志主机的日志信息的输出格式为中国联通格式。

【使用指导】

发往日志主机的日志信息有以下格式：非定制格式、中国联通格式和中国移动格式。有关日志信息格式的详细介绍请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

配置发往日志主机的日志信息的格式为中国联通格式。

```
<Sysname> system-view
[Sysname] info-center format unicom
```

1.1.19 info-center logbuffer

info-center logbuffer 命令用来允许日志信息输出到日志缓冲区。

undo info-center logbuffer 命令用来禁止日志信息输出日志缓冲区。

【命令】

```
info-center logbuffer
undo info-center logbuffer
```

【缺省情况】

允许日志信息输出到日志缓冲区。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

配置 **info-center logbuffer** 命令后,设备会将业务模块生成的日志保存到日志缓冲区。其中,设备会为一些业务模块(例如会话等)、子模块分别创建独立的日志缓冲区,模块的日志缓冲区用来存储该模块的日志,子模块的日志缓冲区用来存储该子模块的日志,其它业务模块的日志会统一存储到通用日志缓冲区中。用户可使用 **display logbuffer** 命令查看这些日志缓冲区的内容或者使用 **info-center logbuffer size** 命令配置这些日志缓冲区的大小。

【举例】

```
# 配置允许日志信息输出到日志缓冲区。
<Sysname> system-view
[Sysname] info-center logbuffer
```

【相关命令】

- **display logbuffer**
- **info-center enable**

1.1.20 info-center logbuffer size

info-center logbuffer size 命令用来配置日志缓冲区可存储的信息条数。

undo info-center logbuffer size 命令用来恢复缺省情况。

【命令】

```
info-center logbuffer [ module module-name ] size buffersize
undo info-center logbuffer [ module module-name ] size
```

【缺省情况】

日志缓冲区可存储 512 条信息。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

module *module-name*: 配置指定模块的日志缓冲区可存储的信息条数。*module-name* 表示模块的名称，配置时需要完整输入，不区分大小写，执行 **info-center logbuffer module ?** 命令，通过帮助信息可获得该参数的取值。不指定该参数时，表示该配置对通用日志缓冲区生效。
buffersize: 日志缓冲区可存储的信息条数，取值范围为 0~1024，缺省值为 512。

【举例】

```
# 配置日志缓冲区可存储的信息条数为 50。
<Sysname> system-view
[Sysname] info-center logbuffer size 50
# 恢复日志缓冲区可存储的信息条数为 512。
<Sysname> system-view
[Sysname] undo info-center logbuffer size
```

【相关命令】

- **display logbuffer**
- **info-center enable**

1.1.21 info-center logfile directory

info-center logfile directory 命令用来配置存放日志文件的目录。

【命令】

info-center logfile directory *dir-name*

【缺省情况】

存放日志文件的目录为设备缺省文件系统根目录下的 **logfile** 文件夹。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

dir-name: 存放日志文件的路径，为 1~64 个字符的字符串。

【使用指导】

在执行该配置前，存放日志文件的目录必须为当前已创建的目录。

生成的日志文件的后缀名为 **.log**。

配置会在 IRF 重启或主从设备倒换后失效。

【举例】

```
# 配置存放日志文件的目录为 flash:/test。  
<Sysname> mkdir test  
Creating directory flash:/test... Done.  
<Sysname> system-view  
[Sysname] info-center logfile directory flash:/test
```

【相关命令】

- **info-center logfile enable**

1.1.22 info-center logfile enable

info-center logfile enable 命令用来允许日志信息输出到日志文件。

undo info-center logfile enable 命令用来禁止日志信息输出到日志文件。

【命令】

```
info-center logfile enable  
undo info-center logfile enable
```

【缺省情况】

允许日志信息输出到日志文件。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

配置本命令后，设备会将业务模块生成的日志保存到日志文件。其中，设备会为一些业务模块（例如会话、攻击防御等）、子模块分别分配独立的日志文件，模块的日志文件用来存储该模块的日志，子模块的日志文件用来存储该子模块的日志，其它业务模块的日志会统一存储到通用日志文件中。模块日志文件以模块名和“.log”后缀为文件名，形如：session.log 等。

设备在出厂时已经确定了可以单独存储日志的业务模块的名称，用户不能修改。

【举例】

```
# 配置允许日志信息输出到日志文件。  
<Sysname> system-view  
[Sysname] info-center logfile enable
```

1.1.23 info-center logfile frequency

info-center logfile frequency 命令用来配置系统自动保存日志文件的频率。

undo info-center logfile frequency 命令用来恢复缺省情况。

【命令】

```
info-center logfile frequency freq-sec
```

undo info-center logfile frequency

【缺省情况】

设备自动保存日志文件的频率为 86400 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

freq-sec: 系统自动保存日志文件的频率，取值范围为 1~86400，单位为秒。

【使用指导】

配置系统自动保存日志文件的频率后，系统会按照指定的频率将日志文件缓冲区的内容写入日志文件。

【举例】

```
# 配置设备自动保存日志文件的频率为 60000 秒。  
<Sysname> system-view  
[Sysname] info-center logfile frequency 60000
```

【相关命令】

- **info-center logfile enable**

1.1.24 info-center logfile module alarm-threshold

info-center logfile module alarm-threshold 命令用来配置模块日志文件使用率的告警门限。

undo info-center logfile module alarm-threshold 命令用来恢复缺省情况。

【命令】

```
info-center logfile module module-name alarm-threshold usage  
undo info-center logfile module module-name alarm-threshold
```

【缺省情况】

模块日志文件使用率的告警门限是 80。即当模块日志文件使用率达到 80%时，系统会提醒用户。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

module-name: 表示模块的名称，配置时需要完整输入，不区分大小写，执行 **info-center logfile module ?**命令，通过帮助信息可获得该参数的取值。

usage: 表示日志文件使用率的告警门限，取值范围为 0~100。取值为 0 时，表示关闭该模块日志文件的使用率告警功能。

【使用指导】

使用本命令可以配置模块日志文件使用率的告警门限。当使用率超过告警门限时，系统会生成日志提醒用户，此时，用户可以将日志文件进行备份，以防历史数据丢失。

【举例】

当 SESSION 模块的日志文件使用率达到 90%时进行告警。

```
<Sysname> system-view
```

```
[Sysname] info-center logfile module SESSION alarm-threshold 90
```

1.1.25 info-center logfile size-quota

info-center logfile size-quota 命令用来配置单个日志文件最大能占用的存储空间的大小。

undo info-center logfile size-quota 命令用来恢复缺省情况。

【命令】

info-center logfile [module module-name] size-quota size

undo info-center logfile [module module-name] size-quota

【缺省情况】

单个通用日志文件可使用的存储空间的最大值为 10MB，指定模块的单个日志文件可使用的存储空间的最大值为 1MB。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

module module-name: 配置指定模块的单个日志文件最大能占用的存储空间的大小。

module-name 表示模块的名称，配置时需要完整输入，不区分大小写，执行 **info-center logfile module ?**命令，通过帮助信息可获得该参数的取值。不指定该参数时，表示该配置对通用日志文件生效。

size: 单个日志文件可使用的存储空间的最大值，取值范围为 1~10，单位为 MB。

【举例】

配置单个日志文件最大能占用的存储空间的大小为 2MB。

```
<Sysname> system-view
```

```
[Sysname] info-center logfile size-quota 2
```

【相关命令】

- **info-center logfile enable**

1.1.26 info-center logging suppress duplicates

info-center logging suppress duplicates 命令用来开启抑制重复日志输出功能。

undo info-center logging suppress duplicates 命令用来关闭抑制重复日志输出功能。

【命令】

info-center logging suppress duplicates

undo info-center logging suppress duplicates

【缺省情况】

抑制重复日志输出功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

当设备持续生成相同的日志，大量重复的信息会浪费设备资源和网络资源，并导致有用的信息被淹没，不利于设备的维护。为了避免此问题，可开启重复日志抑制功能。

【举例】

开启抑制重复日志输出功能。

```
<Sysname> system-view
```

```
[Sysname] info-center logging suppress duplicates
```

1.1.27 info-center loghost

info-center loghost 命令用来配置日志主机及相关参数。

undo info-center loghost 命令用来取消日志主机及相关参数的配置。

【命令】

info-center loghost [vpn-instance vpn-instance-name] { hostname | ipv4-address | ipv6 ipv6-address } [port port-number] [facility local-number] [filter filter-name]

undo info-center loghost [vpn-instance vpn-instance-name] { hostname | ipv4-address | ipv6 ipv6-address }

【缺省情况】

未配置日志主机及相关参数。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

vpn-instance *vpn-instance-name*: 指定日志主机所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则表示日志主机位于公网中。

hostname: 指定日志的主机名, 为 1~253 个字符的字符串, 不区分大小写, 字符串中可以包含字母、数字、“-”、“_”和“.”。

ipv4-address: 指定日志主机的 IPv4 地址。

ipv6 *ipv6-address*: 指定日志主机的 IPv6 地址。

port *port-number*: 指定日志主机接收日志信息的端口号, 取值范围为 1~65535, 缺省值为 514。该参数的值需要和日志主机侧的配置一致, 否则日志主机接收不到日志信息。

facility *local-number*: 配置日志主机的记录工具。取值范围为 local0~local7, 缺省值为 local7。主要用于在日志主机端标志不同的日志来源, 查找、过滤对应日志源的日志。

filter *filter-name*: 指定日志主机关联的日志输出规则的名称, 只有符合规则的日志才能输出到对应的日志主机。*filter-name* 表示日志信息输出规则的名称, 为 1~8 个字符的字符串, 不区分大小写。不指定该参数时, 则采用 **info-center source** 命令日志主机方向的配置作为日志输出规则。

【使用指导】

用户只有使用 **info-center enable** 命令开启了信息中心功能, 配置 **info-center loghost** 命令才会生效。

【举例】

配置系统向 IP 地址为 1.1.1.1 的日志主机发送日志信息。

```
<Sysname> system-view  
[Sysname] info-center loghost 1.1.1.1
```

【相关命令】

- **info-center filter**
- **info-center source**

1.1.28 info-center loghost source

info-center loghost source 命令用来配置发送的日志信息的源 IP 地址。

undo info-center loghost source 命令用来恢复缺省情况。

【命令】

```
info-center loghost source interface-type interface-number  
undo info-center loghost source
```

【缺省情况】

使用出接口的主 IP 地址作为发送的日志信息的源 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

interface-type interface-number: 指定发送日志信息的源 IP 地址对应的出接口的类型和编号。

【使用指导】

配置日志信息的源 IP 地址后，不管实际使用哪个物理接口发送日志信息，日志信息的源 IP 地址均为指定接口的主 IP 地址。

用户只有使用 **info-center enable** 命令开启了信息中心功能，配置 **info-center loghost source** 命令才会生效。

【举例】

配置使用 Loopback0 的 IP 地址作为发送的日志信息的源 IP 地址。

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] ip address 2.2.2.2 32
[Sysname-LoopBack0] quit
[Sysname] info-center loghost source loopback 0
```

1.1.29 info-center security-logfile alarm-threshold

info-center security-logfile alarm-threshold 命令用来配置安全日志文件使用率的告警门限。

undo info-center security-logfile alarm-threshold 命令用来恢复缺省情况。

【命令】

info-center security-logfile alarm-threshold *usage*

undo info-center security-logfile alarm-threshold

【缺省情况】

安全日志文件使用率的告警门限是 80（即当安全日志文件使用率达到 80%时，系统会提醒用户）。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

usage: 安全日志文件使用率的告警门限，取值范围为 1~100 的整数。

【使用指导】

当安全日志文件大小达到上限时，新的安全日志会覆盖旧的安全日志，从而导致安全日志丢失。为防止这种情况发生，用户可以使用本命令配置安全日志文件使用率的告警门限。当使用率超过此门限值时，系统会发出日志提醒用户，此时，用户可以将安全日志文件进行备份，以防重要历史数据丢失。

【举例】

配置当安全日志文件使用率达到 90%时进行告警。

```
<Sysname> system-view
```

```
[Sysname] info-center security-logfile alarm-threshold 90
```

【相关命令】

- **info-center security-logfile size-quota**

1.1.30 info-center security-logfile directory

info-center security-logfile directory 命令用来修改存储安全日志文件的路径。

【命令】

info-center security-logfile directory *dir-name*

【缺省情况】

存储安全日志文件路径为设备缺省文件系统根目录下的 **seclog** 文件夹。

【视图】

系统视图

【缺省用户角色】

security-audit

【参数】

dir-name：安全日志文件存储的路径，为 1~64 个字符的字符串。

【使用指导】

在执行该配置前，存储安全日志文件的文件夹必须为当前已创建的目录。

只有配置了安全日志管理员权限的本地用户才能使用本命令。

配置会在 IRF 重启或主从设备倒换后失效。

【举例】

配置存放安全日志文件的目录为 flash:/test。

```
<Sysname> mkdir test
```

```
Creating directory flash:/test... Done.
```

```
<Sysname> system-view
```

```
[Sysname] info-center security-logfile directory flash:/test
```

1.1.31 info-center security-logfile enable

info-center security-logfile enable 命令用来开启安全日志同步保存功能。

undo info-center security-logfile enable 命令用来关闭安全日志同步保存功能。

【命令】

```
info-center security-logfile enable
undo info-center security-logfile enable
```

【缺省情况】

安全日志同步保存功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【使用指导】

开启安全日志同步保存功能后，系统将安全日志进行集中处理：当生成的日志信息中有安全日志，在不影响日志信息现有输出规则的前提下，系统会将安全日志信息同步保存到专用的安全日志文件。这样既实现了安全日志的集中管理，又有利于用户随时快捷地查看安全日志，了解设备状态。

【举例】

```
# 开启安全日志同步保存功能。
<Sysname> system-view
[Sysname] info-center security-logfile enable
```

1.1.32 info-center security-logfile frequency

info-center security-logfile frequency 命令用来配置设备自动保存安全日志文件的频率。

undo info-center security-logfile frequency 命令用来恢复缺省情况。

【命令】

```
info-center security-logfile frequency freq-sec
undo info-center security-logfile frequency
```

【缺省情况】

设备自动保存安全日志文件的频率为 86400 秒。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

freq-sec：系统自动保存安全日志文件的频率，取值范围为 10～86400，单位为秒。

【使用指导】

配置设备自动保存安全日志文件的频率后，安全日志会先被输出到安全日志文件缓冲区（`security-logfile buffer`），系统会按照配置中指定的频率将安全日志文件缓冲区的内容写入安全日志文件。

【举例】

```
# 配置安全日志自动保存到文件的频率为 600 秒。
<Sysname> system-view
[Sysname] info-center security-logfile frequency 600
```

【相关命令】

- **info-center security-logfile enable**

1.1.33 info-center security-logfile size-quota

info-center security-logfile size-quota 命令用来配置单个安全日志文件最大能占用的存储空间的大小。

undo info-center security-logfile size-quota 命令用来恢复缺省情况。

【命令】

```
info-center security-logfile size-quota size
undo info-center security-logfile size-quota
```

【缺省情况】

单个安全日志文件最大能占用的存储空间的大小为 10MB。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

size：单个安全日志文件可使用的存储空间的最大值，取值范围为 1~10，单位为 MB。

【举例】

```
# 配置单个安全日志文件最大能占用的存储空间的大小为 6MB。
<Sysname> system-view
[Sysname] info-center security-logfile size-quota 6
```

【相关命令】

- **info-center security-logfile alarm-threshold**

1.1.34 info-center source

info-center source 命令用来配置日志信息的输出规则。

undo info-center source 命令用来恢复缺省情况。

【命令】

```
info-center source { module-name | default } { console | logbuffer | logfile |  
loghost | monitor } { deny | level severity }  
undo info-center source { module-name | default } { console | logbuffer |  
logfile | loghost | monitor }
```

【缺省情况】

日志信息的输出规则请参见 [表 1-11](#)：

表1-11 日志信息的缺省输出规则

输出方向	日志信息来源	开关	等级
控制台	所有支持的模块	开	debugging
监视终端	所有支持的模块	关	debugging
日志主机	所有支持的模块	开	informational
日志缓冲区	所有支持的模块	开	informational
日志文件	所有支持的模块	开	informational

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

module-name：配置指定应用模块日志信息的输出规则。系统支持的来源模块可以通过在系统视图下输入 **info-center source ?** 进行查看。

default：配置所有应用模块日志信息的缺省输出规则。

console：输出到控制台。

logbuffer：输出到日志缓冲区。

logfile：输出到日志文件。

loghost：输出到日志主机。

monitor：输出到监视终端。

deny：禁止输出信息。

level severity：指定信息级别，取值范围为 0~7，具体内容请参见 [表 1-6](#)。通过该参数可以控制允许/禁止输出的日志信息的最低级别。

【使用指导】

如果没有使用 **module-name** 参数为应用模块单独配置输出规则，则该模块使用 **default** 参数配置的输出规则。如果未使用 **default** 参数配置输出规则，则使用缺省输出规则。

给应用模块单独配置输出规则后，必须使用 *module-name* 参数来修改或删除该规则，使用 **default** 参数进行的新配置对该模块不生效。

多次使用 *module-name* 参数为同一应用模块配置输出规则，最后一次执行的命令生效；多次使用 **default** 参数配置缺省输出规则，最后一次执行的命令生效。

【举例】

只允许 VLAN 模块的信息输出控制台，且输出信息的级别为 **emergency** 的日志信息。

```
<Sysname> system-view
```

```
[Sysname] info-center source default console deny
```

```
[Sysname] info-center source vlan console level emergency
```

在前面例子基础上撤销控制台方向上 VLAN 模块的输出（即全部信息不在控制台显示）。

```
<Sysname> system-view
```

```
[Sysname] undo info-center source vlan console
```

1.1.35 info-center synchronous

info-center synchronous 命令用来开启命令行输入回显功能。

undo info-center synchronous 命令用来关闭命令行输入回显功能。

【命令】

info-center synchronous

undo info-center synchronous

【缺省情况】

命令行输入回显功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

当用户进行命令行、参数或者 Y/N 确认信息输入时，如果被大量的日志信息打断，用户可能记不清已经输入了哪些字符串，还需要输入哪些字符串。使用命令行输入回显功能，能够协助用户配置。系统会在日志信息输出完毕后回显用户已有的输入或者 Y/N 确认信息，以便用户继续执行配置。

【举例】

开启设备命令行输入回显功能，输入 **display current-configuration** 命令查看设备当前配置。

```
<Sysname> system-view
```

```
[Sysname] info-center synchronous
```

```
Info-center synchronous output is on
```

```
[Sysname] display current-
```

此时，收到日志报文，则系统在所有的日志报文显示完以后，附加显示用户的输入（此例为“display current-”）。

```
%May 21 14:33:19:425 2007 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.44
[Sysname] display current-
此时，用户可以继续输入 configuration（完成命令 display current-configuration 的完整输入），回车，即可执行该命令。
# 开启设备命令行输入回显功能，保存当前配置（输入交互信息）。
<Sysname> system-view
[Sysname] info-center synchronous
Info-center synchronous output is on
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:
此时，收到日志信息，则系统会在所有的日志报文显示完以后，附加显示[Y/N]:。
%May 21 14:33:19:425 2007 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 192.168.1.44
[Y/N]:
此时，用户可以输入 Y 或者 N，继续日志信息输出前的操作。
```

1.1.36 info-center syslog min-age

info-center syslog min-age 命令用来配置日志信息的最短保存时间。

undo info-center syslog min-age 命令用来恢复缺省情况。

【命令】

```
info-center syslog [ module module-name ] min-age min-age
undo info-center syslog [ module module-name ] min-age
```

【缺省情况】

未配置日志信息的最短保存时间。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

module *module-name*: 配置指定模块的日志信息的最短保存时间。*module-name* 表示模块的名称，不区分大小写，执行 **info-center syslog module ?**命令，通过帮助信息可获得该参数的取值。不指定该参数时，表示该配置对通用日志生效。

min-age: 表示日志信息的最短保存时间，取值范围为 1~8760，单位为小时。

【举例】

将日志信息的最短保存时间配置为 168 小时。

```
<Sysname> system-view
[Sysname] info-center syslog min-age 168
```

1.1.37 info-center syslog trap buffersize

info-center syslog trap 命令用来配置日志告警缓冲区的大小。

undo info-center syslog trap 命令用来恢复缺省情况。

【命令】

info-center syslog trap buffersize *buffersize*

undo info-center syslog trap buffersize

【缺省情况】

日志告警缓冲区的大小为 1024 条。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

buffersize：表示日志告警缓冲区的大小，取值范围为 0～65535，单位为条。当取值为 0 时，表示不缓存日志告警。

【使用指导】

配置 **snmp-agent trap enable syslog** 命令后，设备会将日志封装成告警信息，存储在日志告警缓冲区。用户通过访问“日志告警缓冲区对应的 MIB 节点”，就可以直接读取日志告警。

通常情况下，日志告警缓冲区的大小采用缺省值即可。当日志告警缓冲区内存储的信息达到上限，且还需要存储信息时，新信息会覆盖旧信息。

【举例】

配置日志告警缓冲区的大小为 2048 条。

```
<Sysname> system-view
```

```
[Sysname] info-center syslog trap buffersize 2048
```

【相关命令】

- **snmp-agent trap enable syslog**

1.1.38 info-center syslog utf-8 enable

info-center syslog utf-8 enable 命令用来配置信息中心使用 UTF-8 编码方式输出日志。

undo info-center syslog utf-8 enable 命令用来恢复缺省情况。

【命令】

info-center syslog utf-8 enable

undo info-center syslog utf-8 enable

【缺省情况】

信息中心使用 GB18030 编码方式输出日志。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

当用户使用登录软件登录设备，且设备往登录软件发送的信息中包含中文字符时，如果登录软件和设备使用的中文字符集编码不同，可能会出现中文字符在登录软件上显示为乱码的情况。

使用本命令可以将信息中心发送日志信息时使用的字符集编码配置为 UTF-8 或者 GB18030。

【举例】

配置信息中心使用 UTF-8 编码方式输出日志。

```
<Sysname> system-view
```

```
[Sysname] info-center syslog utf-8 enable
```

【相关命令】

- **display character-set**

1.1.39 info-center timestamp

info-center timestamp 命令用来配置发往控制台、监视终端、日志缓冲区和日志文件方向的日志信息的时间戳输出格式。

undo info-center timestamp 命令用来恢复缺省情况。

【命令】

```
info-center timestamp { boot | date | none }
```

```
undo info-center timestamp
```

【缺省情况】

时间戳输出格式为 **date** 格式。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

boot: 系统启动后经历的时间，格式为：xxx.yyy，其中 xxx 是系统自启动后经历时间的毫秒数高 32 位，yyy 是低 32 位，形如 0.21990989（等效于 Jun 25 14:09:26:881 2007）。

date: 系统当前的日期和时间，格式为“MMM DD hh:mm:ss:xxx YYYY”，形如 Dec 8 10:12:21:708 2007。

- “MMM” 为英语月份的缩写，具体取值如下：Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec。

- “DD”表示日期，如果日期的值小于10，则格式为“空格+日期”，如“7”。
 - “hh:mm:ss:xxx”表示本地时间，hh的取值范围为00~23，mm和ss的取值范围均为00~59，xxx的取值范围为0~999。
 - “YYYY”表示年份。
- none:** 不带时间信息。

【举例】

```
# 配置日志信息时间戳输出格式为 boot 格式。
<Sysname> system-view
[Sysname] info-center timestamp boot
```

【相关命令】

- **info-center timestamp loghost**

1.1.40 info-center timestamp loghost

info-center timestamp loghost 命令用来配置发往日志主机的日志信息的时间戳输出格式。

undo info-center timestamp loghost 命令用来恢复缺省情况。

【命令】

```
info-center timestamp loghost { date | iso | no-year-date | none }
undo info-center timestamp loghost
```

【缺省情况】

发往日志主机的日志信息的时间戳输出格式为 **date** 格式。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

date: 系统当前日期和时间，格式为：mmm dd hh:mm:ss yyyy，形如 Dec 8 10:12:21 2007，但最终显示格式由日志主机决定。

iso: 配置时间戳采用 ISO 8601 标准格式，形如：2009-09-21T15:32:55。

no-year-date: 系统当前日期和时间，但不包含年份信息。

none: 不带时间信息。

【举例】

```
# 配置发往日志主机的日志信息的时间戳为 no-year-date 格式。
<Sysname> system-view
[Sysname] info-center timestamp loghost no-year-date
```

【相关命令】

- **info-center timestamp**

1.1.41 info-center trace-logfile quota

info-center trace-logfile quota 命令用来配置调试跟踪日志文件最大能占用的存储空间的大小。

undo info-center trace-logfile quota 命令用来恢复缺省情况。

【命令】

info-center trace-logfile quota size

undo info-center trace-logfile quota

【缺省情况】

调试跟踪日志文件最大能占用的存储空间的大小为 1MB。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

size: 调试跟踪日志文件最大能占用的存储空间的大小，取值范围为 1~10，单位为 MB。

【举例】

配置调试跟踪日志文件最大能占用的存储空间的大小为 6MB。

<Sysname> system-view

[Sysname] info-center trace-logfile quota 6

1.1.42 logfile save

logfile save 命令用来手动将日志文件缓冲区中的内容全部保存到日志文件。

【命令】

logfile save

【视图】

任意视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

日志文件的保存路径可以通过 **info-center logfile directory** 命令配置。

日志文件保存成功后，日志文件缓冲区中的内容会被清空。

如果执行本命令时，日志文件缓冲区中没有日志，本命令会执行成功，但不会创建或更新已有日志文件。

【举例】

手动将日志文件缓冲区中的内容保存到日志文件。

```
<Sysname> logfile save
```

The contents in the log file buffer have been saved to the file flash:/logfile/logfile.log.

【相关命令】

- **info-center logfile enable**
- **info-center logfile directory**

1.1.43 reset logbuffer

reset logbuffer 命令用来清除日志缓冲区中的信息。

【命令】

```
reset logbuffer [ module module-name [ submodule submodule-name ] ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

context-admin

【参数】

module *module-name*: 清除指定模块日志缓冲区中的信息。*module-name* 表示模块的名称，不区分大小写，执行 **reset logbuffer ?** 命令，通过帮助信息可获得该参数的取值。不指定该参数时，表示该配置对通用日志生效。

submodule *submodule-name*: 清除当前模块下指定子模块日志缓冲区的状态和日志缓冲区记录的日志信息。*submodule-name* 表示子模块名称，配置时需要完整输入，不区分大小写。当前模块是否支持子模块以及子模块的取值，请通过执行 **display logbuffer module *module-name* submodule ?** 命令获取。不指定该参数时，表示该配置对当前模块下所有子模块生效。

【举例】

清除日志缓冲区中的信息。

```
<Sysname> reset logbuffer
```

【相关命令】

- **display logbuffer**

1.1.44 security-logfile save

security-logfile save 命令用来手动将安全日志文件缓冲区中的内容全部保存到安全日志文件。

【命令】

```
security-logfile save
```

【视图】

任意视图

【缺省用户角色】

security-audit

【使用指导】

安全日志文件保存成功后，安全日志文件缓冲区中的内容会被立即清空。

需要注意的是，只有具有安全日志管理员角色的本地用户才能使用本命令。

如果执行本命令时，安全日志文件缓冲区中没有日志，本命令会执行成功，但不会创建或更新已有安全日志文件。

【举例】

手动将安全日志缓冲区中的内容保存到安全日志文件。

```
<Sysname> security-logfile save
```

```
The contents in the security log file buffer have been saved to the file  
flash:/seclog/seclog.log.
```

【相关命令】

- **info-center security-logfile directory**
- **authorization-attribute**（安全命令参考/AAA）

1.1.45 snmp-agent trap enable syslog

snmp-agent trap enable syslog 命令用来将系统日志封装成告警信息发送。

undo snmp-agent trap enable syslog 命令用来恢复缺省情况。

【命令】

snmp-agent trap enable syslog

undo snmp-agent trap enable syslog

【缺省情况】

系统日志不会封装成告警信息发送。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

配置该命令后，设备除了根据输出规则将日志输出到各方向外，还会将日志信息封装成告警信息，发送到 SNMP 模块和日志告警缓冲区。

- 发送到 SNMP 模块后，是否输出到目的主机，以 Trap 还是 Inform 形式发送，由 SNMP 模块的配置决定，关于告警信息以及 SNMP 配置的详细介绍请参见“网络管理和监控配置指导”中的“SNMP”。

- 发送到日志告警缓冲区后，用户可通过“日志告警缓冲区对应的 MIB 节点”来直接读取日志信息封装成的告警信息。用户还可通过 **info-center syslog trap buffersize** 命令来配置日志告警缓冲区的大小。

【举例】

```
# 将系统日志封装成告警信息发送。  
<Sysname> system-view  
[Sysname] snmp-agent trap enable syslog
```

【相关命令】

- **info-center syslog trap buffersize**

1.1.46 terminal debugging

terminal debugging 命令用来开启当前终端对调试信息的显示功能。

undo terminal debugging 命令用来关闭当前终端对调试信息的显示功能。

【命令】

```
terminal debugging  
undo terminal debugging
```

【缺省情况】

当前终端对调试信息的显示功能处于关闭状态。

【视图】

用户视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

如果需要在控制台显示调试信息，请先配置 **terminal debugging** 命令，再使能信息中心功能（信息中心功能缺省处于使能状态），最后使用 **debugging** 命令打开功能模块的调试信息开关。

如果需要在监视终端上显示调试信息，请先配置 **terminal monitor** 和 **terminal debugging** 命令，再使能信息中心功能（信息中心功能缺省处于使能状态），最后使用 **debugging** 命令打开功能模块的调试信息开关。

需要注意的是，本命令只对当前连接有效。当终端与设备重新建立连接后，本命令会恢复到缺省情况。

执行 **terminal logging level 7** 命令或 **terminal debugging** 命令，都可以开启当前终端对调试信息的显示功能，但两条命令有如下区别：

- 执行 **terminal logging level 7** 命令，当前终端允许输出级别为 0~7 的所有日志。
- 执行 **terminal debugging** 命令，当前终端仅输出 **terminal logging level** 命令配置的日志信息和级别为 7 的调试信息。

【举例】

```
# 允许 debugging 日志信息输出到当前终端。  
<Sysname> terminal debugging  
The current terminal is enabled to display debugging logs.
```

【相关命令】

- **terminal logging level**
- **terminal monitor**

1.1.47 terminal logging level

terminal logging level 命令用来配置当前终端允许输出的日志信息的最低级别。

undo terminal logging level 命令用来恢复缺省情况。

【命令】

```
terminal logging level severity  
undo terminal logging level
```

【缺省情况】

当前终端允许输出的日志信息的最低级别均为 6（Informational）。

【视图】

用户视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

severity: 当前终端允许输出的日志信息的最低级别，取值为 0~7 的整数或者 alert、critical、debugging、emergency、error、informational、notification、warning。

【使用指导】

在配置了当前终端允许输出的日志信息的最低级别后，当系统输出信息时，所有信息等级高于或等于配置等级的信息都会被输出。例如，当配置的允许输出的日志信息的最低级别 6（informational）时，等级 0~6 的信息均会被输出。

本命令配置的显示属性只对当前连接有效，当终端与设备的连接超时、重新建立连接后，显示属性将恢复到缺省情况。

【举例】

```
# 配置当前终端监控的最低日志级别为 debugging。  
<Sysname> terminal logging level 7
```

1.1.48 terminal monitor

terminal monitor 命令用来允许日志信息输出到当前终端。

undo terminal monitor 命令用来禁止日志信息输出到当前终端。

【命令】

```
terminal monitor  
undo terminal monitor
```

【缺省情况】

允许日志信息输出到控制台，不允许日志信息输出到监视终端。

【视图】

用户视图

【缺省用户角色】

```
network-admin  
context-admin
```

【使用指导】

本命令只对当前连接有效。当终端与设备重新建立连接后，本命令会恢复到缺省情况。

【举例】

```
# 允许日志信息输出到当前终端。  
<Sysname> terminal monitor  
The current terminal is enabled to display logs.
```

目 录

1 报文捕获	1-1
1.1 报文捕获命令	1-1
1.1.1 display packet-capture status	1-1
1.1.2 packet-capture max-bytes	1-2
1.1.3 packet-capture max-file-packets	1-2
1.1.4 packet-capture start	1-3
1.1.5 packet-capture stop	1-4
1.1.6 packet-capture storage	1-4

1 报文捕获

1.1 报文捕获命令

1.1.1 display packet-capture status

display packet-capture status 命令用来显示报文捕获功能的配置和状态信息。

【命令】

display packet-capture status

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示当前报文捕获功能的配置和状态信息。

```
<Sysname> display packet-capture status
  Capture status: Started
  Filter: ACL 3000
          Interface GigabitEthernet1/0/1
```

表1-1 display packet-capture status 命令显示信息描述表

字段	描述
Capture status	表示报文捕获功能的状态，包括如下取值： - Started: 报文捕获进行中 - Stopped: 报文捕获已停止 - Saving: 正在保存缓存中的报文
Filter	表示报文捕获的过滤条件，包括如下取值： - ACL: 根据 IPv4 高级 ACL 进行过滤 - ACL IPv6: 根据 IPv6 高级 ACL 进行过滤 - Interface: 根据接口进行过滤 若报文捕获已停止，则不显示该字段

【相关命令】

- packet-capture start
- packet-capture stop

1.1.2 packet-capture max-bytes

packet-capture max-bytes 命令用来配置捕获报文的最大长度。

undo packet-capture max-bytes 命令用来恢复缺省情况。

【命令】

packet-capture max-bytes *bytes*

undo packet-capture max-bytes

【缺省情况】

捕获报文的最大长度为 1600 字节。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

bytes: 表示可捕获报文的最大长度，取值范围为 512~4096，单位为字节。

【使用指导】

对于一个报文，报文捕获功能仅能捕获最大长度以内的部分，并生成一条捕获信息，对于超出的部分不再进行捕获。因此，为能够捕获到完整报文，建议配置捕获报文的最大长度不低于接口的 MTU 值。

报文捕获开始后，不允许调整捕获报文的最大长度。

【举例】

配置捕获报文的最大长度为 1500 字节。

```
<Sysname> system-view
```

```
[Sysname] packet-capture max-bytes 1500
```

1.1.3 packet-capture max-file-packets

packet-capture max-file-packets 命令用来配置捕获文件存储捕获条目的最大数。

undo packet-capture max-file-packets 命令用来恢复缺省情况。

【命令】

packet-capture max-file-packets *number*

undo packet-capture max-file-packets

【缺省情况】

捕获文件存储捕获条目的最大数为 100。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

number: 表示捕获文件存储捕获条目的最大数，取值范围为 100~1000，单位为条。

【使用指导】

当捕获文件存储的捕获条目达到最大存储个数后，系统会将内存中的捕获文件上传到指定的存储路径上，并将内存中的捕获文件删除。

捕获文件存储的捕获条目越多占用的内存也就越大，因此在系统内存剩余较少的情况下，请将捕获文件存储捕获条目的最大数调小。

报文捕获开始后，不允许调整捕获文件存储捕获条目的最大数。

【举例】

配置捕获文件存储捕获条目的最大数为 500。

```
<Sysname> system-view
```

```
[Sysname] packet-capture max-file-packets 500
```

1.1.4 packet-capture start

packet-capture start 命令用来启动报文捕获功能。

【命令】

```
packet-capture start [ acl { acl-number | ipv6 acl-number } | interface interface-type interface-number ] *
```

【缺省情况】

报文捕获功能处于停止状态。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

acl: 表示捕获匹配高级 ACL 中 **permit** 规则的报文。

acl-number: 表示 IPv4 高级 ACL，取值范围为 3000~3999。

ipv6 acl-number: 表示 IPv6 高级 ACL，取值范围为 3000~3999。

interface interface-type interface-number: 表示捕获指定接口上接收和发送的所有报文。

【使用指导】

启动报文捕获功能会对设备的性能产生影响，因此建议只在需要捕获报文的情况下开启该功能。

在捕获报文存储在本地的情况下，报文捕获开始后系统会删除捕获文件存储路径下所有 **.cap** 后缀的文件，因此请及时导出所需的捕获文件。

启动报文捕获时，如果没有指定任何参数，则表示捕获设备接收和发送的所有报文。

在非缺省 Context 中不支持在共享接口上开启此功能。

【举例】

启动报文捕获功能，捕获匹配高级 ACL 3000 中 **permit** 规则的报文。

```
<Sysname> system-view
[Sysname] packet-capture start acl 3000
The operation will delete .cap files in storage path,continue?[y/n]
```

1.1.5 packet-capture stop

packet-capture stop 命令用来停止报文捕获功能。

【命令】

packet-capture stop [immediately]

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

immediately: 表示立刻停止报文捕获功能，且缓存中的报文不再保存到捕获文件。若不指定此参数，则表示将缓存中的报文全部保存到捕获文件后，才停止报文捕获功能。

【使用指导】

停止报文捕获功能后，当缓存中的报文比较多时，将这些缓存的报文全部保存到捕获文件会需要较长的时间，这时如果不再需要继续保存缓存中的报文，则可以使用立刻停止报文捕获功能。

【举例】

```
# 停止报文捕获功能。
<Sysname> system-view
[Sysname] packet-capture stop
# 立刻停止报文捕获功能。
<Sysname> system-view
[Sysname] packet-capture stop immediately
```

1.1.6 packet-capture storage

packet-capture storage 命令用来配置捕获文件的存储路径。

undo packet-capture storage 命令用来恢复缺省情况。

【命令】

```
packet-capture storage { local [ limit limit-space ] | remote serverpath  
[ vpn-instance vpn-instance-name ] [ user username [ password { cipher |  
simple } string ] ] }  
undo packet-capture storage
```

【缺省情况】

捕获文件存储在当前主用设备缺省文件系统的 pcap 文件夹下。

【视图】

系统视图

【缺省用户角色】

network-admin
context-admin

【参数】

local: 表示将捕获文件存储在设备本地。

limit limit-space: 表示捕获文件占用的最大存储空间，当捕获文件总大小超过最大存储空间限制时，自动停止抓包。**limit-space** 是存储空间，取值范围为 1024~10240，缺省值为 4096，单位为 KB。

remote: 表示将捕获文件存储到外部的服务器。

serverpath: 表示外部 FTP/TFTP 服务器的存储路径，为 1~253 个字符的字符串，区分大小写，仅包含字母、数字、“-”、“_”、“:”、“/”和“.”。

vpn-instance vpn-instance-name: 指定 FTP/TFTP 服务器所属的 VPN 实例。**vpn-instance-name** 表示 MPLS L3VPN 的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则表示 FTP/TFTP 服务器位于公网。

user username: 表示登录远程 FTP 服务器使用的用户名，为 1~255 个字符的字符串，区分大小写，不能包括“\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和“@”。

password: 表示登录远程 FTP 服务器使用的密码。

cipher: 表示以密文方式设置密码。

simple: 表示以明文方式设置密码，该密码将以密文形式存储。

string: 密钥字符串，区分大小写。明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。

【使用指导】

由于设备存储空间有限，建议将捕获文件存储到外部的服务器。

捕获开始后，不允许更改捕获文件的存储路径。

【举例】

```
# 配置捕获文件存储路在 FTP 服务器上，服务器地址为 1.1.1.2，用户名为 zhangsan，密码为 123。  
<Sysname> system-view  
[Sysname] packet-capture storage remote ftp://1.1.1.2 user zhangsan password simple 123
```



UNIS 入侵检测系统

VPN 实例命令参考

Copyright © 2019 北京紫光恒越网络科技有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

UNIS 为北京紫光恒越网络科技有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。紫光恒越保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，紫光恒越尽全力在本手册中提供准确的信息，但是紫光恒越并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考介绍了各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省级别、用途描述和举例等。《VPN 实例命令参考》主要 VPN 实例相关的命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [技术支持](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用 “[]” 括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项中选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由 “#” 号开始的行表示为注释行。

2. 图形界面格式约定

格 式	意 义
< >	带尖括号 “< >” 表示按钮名，如 “单击<确定>按钮”。
[]	带方括号 “[]” 表示窗口名、菜单名和数据表，如 “弹出[新建用户]窗口”。
/	多级菜单用 “/” 隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下

格 式	意 义
	的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：<http://www.unishy.com>

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

目 录

1 VPN实例.....	1-1
1.1 VPN实例配置命令	1-1
1.1.1 description (VPN instance view).....	1-1
1.1.2 display ip vpn-instance.....	1-1
1.1.3 ip binding vpn-instance	1-2
1.1.4 ip vpn-instance (System view)	1-3

1 VPN实例

1.1 VPN实例配置命令

1.1.1 description (VPN instance view)

description 命令用来配置当前 VPN 实例的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

未配置 VPN 实例的描述信息。

【视图】

VPN 实例视图

【缺省用户角色】

network-admin

context-admin

【参数】

text: VPN 实例的描述信息，为 1~79 个字符的字符串，区分大小写。

【使用指导】

多次执行本命令，最后一次执行的命令生效。

【举例】

配置名为 vpn1 的 VPN 实例的描述信息为 “This is vpn1”。

```
<Sysname> system-view
```

```
[Sysname] ip vpn-instance vpn1
```

```
[Sysname-vpn-instance-vpn1] description This is vpn1
```

1.1.2 display ip vpn-instance

display ip vpn-instance 命令用来显示 VPN 实例的信息。

【命令】

display ip vpn-instance [*instance-name* *vpn-instance-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator
context-admin
context -operator

【参数】

instance-name vpn-instance-name: 显示指定 VPN 实例的详细信息。*vpn-instance-name* 表示 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，则显示创建的所有 VPN 实例的简要信息。

【举例】

显示所有 VPN 实例的简要信息。

```
<Sysname> display ip vpn-instance
Total VPN-Instances configured : 1
VPN-Instance Name      RD              Create time
management             1000000000:1    2017/12/15 09:48:30
```

表1-1 display ip vpn-instance 命令显示信息描述表

字段	描述
VPN-Instance Name	VPN实例名称
RD	VPN实例的路由标识符
Create time	VPN实例创建的时间

1.1.3 ip binding vpn-instance

ip binding vpn-instance 命令用来配置接口与指定 VPN 实例关联。
undo ip binding vpn-instance 命令用来恢复缺省情况。

【命令】

ip binding vpn-instance vpn-instance-name
undo ip binding vpn-instance

【缺省情况】

接口未关联 VPN 实例，接口属于公网。

【视图】

接口视图

【缺省用户角色】

network-admin
context-admin

【参数】

vpn-instance-name: 接口关联的 VPN 实例名称，为 1~31 个字符的字符串，区分大小写。

【使用指导】

配置或取消接口与 VPN 实例关联后，该接口上的 IP 地址、路由协议等配置将被删除。建议在接口视图下通过 **display this** 命令查看接口的当前配置，并根据需要重新配置 IP 地址、路由协议等。

接口关联的 VPN 实例，必须已经通过系统视图下的 **ip vpn-instance** 命令创建。

不能通过重复执行本命令修改接口关联的 VPN 实例。如需修改接口关联的 VPN 实例，请先通过 **undo ip binding vpn-instance** 命令取消关联的 VPN 实例后，再执行 **ip binding vpn-instance** 命令关联新的 VPN 实例。

【举例】

将接口 GigabitEthernet1/2/5/1 与名为 vpn1 的 VPN 实例关联。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/2/5/1
[Sysname-GigabitEthernet1/2/5/1] ip binding vpn-instance vpn1
```

【相关命令】

- **ip vpn-instance** (System view)

1.1.4 ip vpn-instance (System view)

ip vpn-instance 命令用来创建 VPN 实例，并进入 VPN 实例视图。如果指定的 VPN 实例已经存在，则直接进入 VPN 实例视图。

undo ip vpn-instance 命令用来删除指定的 VPN 实例。

【命令】

```
ip vpn-instance vpn-instance-name
undo ip vpn-instance vpn-instance-name
```

【缺省情况】

不存在 VPN 实例。

【视图】

系统视图

【缺省用户角色】

```
network-admin
context-admin
```

【参数】

vpn-instance-name: VPN 实例的名称，为 1~31 个字符的字符串，区分大小写。

【举例】

创建一个名为 vpn1 的 VPN 实例，并进入 VPN 实例视图。

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1]
```