1 FCoE 概述	1-1
1.1 FC SAN 简介	1-1
1.2 FC 协议	1-2
1.2.1 基本概念	1-2
1.2.2 通信过程	1-4
1.2.3 VSAN	1-4
1.2.4 FC Zone	1-5
1.3 FCoE 协议	1-5
1.3.1 基本概念	1-6
1.3.2 工作机制	1-7
1.4 FCoE 模式	1-9
1.4.1 FCF 模式	1-9
1.4.2 NPV 模式	1-10
1.4.3 Transit 模式	1-11
1.5 协议规范	1-12
2 FCoE 配置限制和指导	2-1
2.1 配置设备工作在高级模式	2-1
2.2 配置交换机的 FCoE 模式	2-1
2.3 在不同 FCoE 模式下配置 FCoE 功能	2-1
3 VFC 接口	3-1
3.1 配置 VFC 接口	3-1
3.2 VFC 接口显示和维护	
4 FCoE 基础配置	4-1
4.1 FCoE 基础配置任务简介	4-1
4.2 开启 VLAN 的 FCoE 功能,并指定映射 VSAN	4-1
4.3 配置 FCoE 网络的 FC-MAP 值	4-2
4.4 配置 FCoE 网络的 fka-adv-period 值	4-2
4.5 配置 FCoE 网络的 FCF 优先级	4-3
4.6 FCoE 基础配置显示和维护	4-4
4.7 FCoE 基础配置举例	4-4
4.7.1 组网需求	4-4
4.7.2 组网图	4-4

目 录

	4.7.3 配置步骤	4-5
5 VS	SAN	5-1
	5.1 VSAN 简介	5-1
	5.1.1 VSAN 概述	5-1
	5.1.2 VSAN 方式	5-1
	5.2 配置 VSAN	5-2
	5.2.1 创建 VSAN	5-2
	5.2.2 配置 Trunk VSAN	5-3
	5.3 VSAN 显示和维护	5-3
	5.4 VSAN 典型配置举例	5-3
	5.4.1 VSAN 配置举例	5-3
6建	立 Fabric 网络	6-1
	6.1 简介	6-1
	6.1.1 选举主交换机	6-1
	6.1.2 分配域 ID	6-2
	6.1.3 分配 FC 地址······	6-3
	6.2 建立 Fabric 网络配置任务简介	6-3
	6.3 开启/关闭 Fabric 配置功能	6-4
	6.4 配置 Fabric 网络的名称	6-5
	6.5 配置交换机的优先级	6-5
	6.6 配置允许的域 ID 范围	6-6
	6.7 配置域 ID	6-6
	6.8 配置 FC 地址持久化功能	6-7
	6.9 配置 VSAN 下的最大登录节点数	6-7
	6.10 配置 Fabric 定时器	6-8
	6.11 配置 Fabric 重配置	6-9
	6.12 配置接口拒绝收到的 RCF 请求报文	6-10
	6.13 开启 Fabric 告警功能	6-10
	6.14 配置 RSCN 聚合功能	6-10
	6.14.1 RSCN 功能简述	6-10
	6.14.2 RSCN 聚合功能介绍	6-11
	6.14.3 配置 RSCN 聚合功能	6-11
	6.15 配置和探测发现节点设备的 FC4 信息	6-12
	6.15.1 配置 Fabric 自动发现 SCSI-FCP 信息功能	6-12
	6.15.2 配置节点设备的默认 FC4 信息	6-13
	6.16 开启 Smart SAN 功能	6-13

6.16.1 Smart SAN 简介	6-13
6.16.2 开启 Smart SAN 功能	6-13
6.17 Fabric 网络显示和维护	6-14
6.18 建立 Fabric 网络典型配置举例	6-15
6.18.1 静态建立 Fabric 网络配置举例	6-15
6.18.2 动态建立 Fabric 网络配置举例	6-19
7 FC 路由与转发	7-1
7.1 FC 路由与转发简介	7-1
7.1.1 路由表和 FIB 表	7-1
7.1.2 直连路由	7-2
7.1.3 静态路由	7-2
7.1.4 FSPF 路由	7-3
7.2 配置 FC 静态路由	7-4
7.3 配置 FSPF	7-4
7.3.1 FSPF 配置任务简介	7-4
7.3.2 开启 FSPF 功能	7-5
7.3.3 配置最短 SPF 计算间隔	7-5
7.3.4 配置 LSR 最小接收间隔	7-6
7.3.5 配置 LSR 最小刷新间隔	7-6
7.3.6 配置接口的 FSPF 开销	7-6
7.3.7 配置接口的 Hello 时间间隔	7-7
7.3.8 配置接口的 Dead 时间间隔	7-7
7.3.9 配置接口的 LSR 重传间隔	7-7
7.3.10 关闭接口的 FSPF 功能	7-8
7.3.11 配置 FSPF GR	7-8
7.4 FC 路由与转发显示和维护	7-9
7.5 FC 路由与转发典型配置举例	7-9
7.5.1 FC 静态路由配置举例	7-9
7.5.2 FSPF 配置举例	7-14
8 FC Zone	8-1
8.1 FC Zone 简介	8-1
8.1.1 FC Zone 概述	8-1
8.1.2 Zone 模式	8-1
8.1.3 Zone 数据库	8-1
8.1.4 Zone 的 Pairwise 特性	8-4
8.1.5 基本 Zone 的扩散	

8.1.6 增强 Zone 的扩散	8-7
8.1.7 基本 Zone 的合并	8-7
8.1.8 增强 Zone 的合并	8-10
8.1.9 访问控制	8-11
8.2 FC Zone 配置任务简介	8-11
8.3 配置 FC Zone	8-12
8.3.1 配置 Zone 模式	8-12
8.3.2 配置 Zone 的 Pairwise 特性	8-12
8.3.3 配置 Zone 别名	8-13
8.3.4 配置 Zone	8-13
8.3.5 配置 Peer Zone	8-14
8.3.6 配置 Zone set	8-14
8.3.7 配置默认 Zone 策略	8-14
8.3.8 配置 Zone 扩散和合并类型	8-15
8.3.9 配置 Zone 的合并控制模式	8-15
8.3.10 开启硬件 Zone	8-16
8.3.11 激活 Zone set 并发起向全网的扩散过程	8-17
8.3.12 激发完全扩散过程	8-17
8.3.13 重命名 Zone 别名、Zone、Zone set ······	8-18
8.3.14 复制 Zone 别名、Zone、Zone set	8-18
8.3.15 清除 Zone 数据库信息	8-19
8.3.16 开启 Zone 的告警功能	8-19
8.4 FC Zone 显示和维护	8-19
8.5 FC Zone 典型配置举例	8-20
9 NPV	9-1
9.1 NPV 简介	9-1
9.1.1 下行口和下行链路	9-1
9.1.2 上行口和上行链路	9-1
9.1.3 上下行口流量映射	9-2
9.1.4 负载均衡	9-2
9.2 NPV 配置任务简介	9-3
9.3 配置上下行口	9-3
9.3.1 配置上行口	9-3
9.3.2 配置下行口	9-3
9.4 配置上下行口映射关系	9-4
9.5 配置发起手动负载均衡功能	9-4

9.6 配置自动负载均衡功能	9-4
9.7 NPV 显示和维护	9-5
9.8 NPV 典型配置举例	9-5
9.8.1 NPV 配置举例	9-5
10 FIP Snooping	10-1
10.1 FIP Snooping 简介	10-1
10.1.1 FIP Snooping 典型组网	10-1
10.1.2 FIP Snooping 工作机制	10-2
10.2 FIP Snooping 配置任务简介	10-2
10.3 开启 FIP Snooping 功能	10-3
10.4 配置以太网接口的模式	10-3
10.5 配置 FC-MAP 值	
10.6 FIP Snooping 显示和维护	10-4
10.7 FIP Snooping 典型配置举例	10-4
11 FCS	11-1
11.1 FCS 简介	11-1
11.2 配置 FCS	11-2
11.2.1 发起拓扑发现	11-2
11.2.2 取消拓扑发现	11-3
11.3 FCS 显示和维护	11-3
11.4 FCS 典型配置举例	11-3
12 FDMI	12-1
12.1 FDMI 简介	12-1
12.2 FDMI 显示和维护	12-4
13 FC Ping	13-1
13.1 FC Ping 简介	13-1
13.2 配置 FC Ping	13-1
13.3 FC Ping 典型配置举例	13-1
13.3.1 FC Ping 配置举例	13-1
14 FC Tracert-	14-1
14.1 FC Tracert 简介	14-1
14.2 配置 FC Tracert	14-2
14.3 FC Tracert 典型配置举例	14-2
14.3.1 FC Tracert 配置举例	14-2

15 FCoE 综合配置举例
15.1 非 IRF 模式的 FCoE 配置举例15-1
15.1.1 组网需求
15.1.2 组网图15-1
15.1.3 配置思路15-2
15.1.4 配置步骤15-2
15.1.5 验证配置15-10
15.2 IRF 模式的 FCoE 配置举例15-12
15.2.1 组网需求15-12
15.2.2 组网图15-13
15.2.3 配置思路15-13
15.2.4 配置步骤15-14
15.2.5 验证配置15-26
16 附录
16.1 附录 A FC 地址分配16-1
16.2 附录 B Fabric 知名地址16-1

1 FCoE 概述

1.1 FC SAN简介

随着 Internet 应用的不断增长,网络服务器需要存储的数据越来越多,这就导致对服务器存储容量的需求不断增长。当服务器的内部存储容量无法满足信息增长的需求时,就需要将服务器的存储"外部化"。为此,提出了 SAN (Storage Area Networks,存储区域网络)的概念,它为服务器提供了专用的外部存储环境,充分利用新的存储硬件技术和网络技术,满足对大容量、高可靠数据的存储、访问和备份等需求。

根据使用的协议不同,SAN 可以分为 FC SAN 和 IP SAN。FC SAN 使用 FC (Fibre Channel,光 纤通道)协议族, IP SAN 使用 TCP/IP 协议族。本文仅介绍 FC SAN 相关内容。

在 FC SAN 中,通信的双方,通常一端为网络服务器,另一端为磁盘设备。服务器与磁盘设备之间 可以通过光纤或者铜缆直接连接在一起,也可以通过交换机间接连接在一起。

如<u>图 1-1</u>所示。前两种组网方式比较简单,能够连接的设备数量也相对较少,点到点连接只能支持两台设备的互联;仲裁环最多支持 126 台设备。真正能称之为 FC SAN 的连接方式是交换式架构,即通过 FC 交换机将大量的服务器和磁盘设备组织在一个 FC SAN 网络中。在交换式架构中,服务器和磁盘设备都被称之为节点设备(Node),是数据发送和接收的实体;FC 交换机作为中间传输设备提供数据转发和网络控制功能。交换式架构提供了很好的扩展能力,能够支持上万台甚至更多的节点设备互联。



(3) 交换式架构



🕑 说明

- 由 FC 交换机和节点设备组成的网络称为 FC SAN。
- 由 FC 交换机组成的中间传输网络称为 Fabric 网络。

1.2 FC协议

FC 协议作为 FC SAN 中的数据传输协议,提供了高效的数据传输服务。在 FC SAN 中,服务器、FC 交换机和磁盘设备都需要支持 FC 协议。

1.2.1 基本概念

1. WWN

WWN(World Wide Name,全球名字)是一个 64 位的地址,用来标识 Fabric 网络和 FC SAN 中的实体(实体包括 FC 交换机、节点设备以及其上的接口)。FC 的上层协议通过 WWN 进行通信。 FC SAN 中每个实体的 WWN 在设备出厂前就已分配好了。

2. FC 地址

在 FC SAN 中, FC 协议通过 FC 地址访问 FC SAN 中各个通讯实体。FC 地址通常也称为 FC_ID。 FC 地址的结构如图 1-2_所示。FC 地址的长度为 24 比特,分为三个字段: Domain_ID、Area_ID 和 Port_ID,每个字段的长度均为 8 比特。

- Domain_ID: 域 ID, 用来标识一台 FC 交换机, 取值范围是 1~239。一台 FC 交换机以及其 连接的所有 N_Port (关于 N_Port 的介绍请参见 "<u>3.</u>接口模式")构成一个域。
- Area_ID: 一台节点设备上的一个或多个 N_Port 可以被划分为一个 Area, 用 Area_ID 标识。
- Port_ID: 一个 Port_ID 代表一个 N_Port。

图1-2 FC 地址的结构



一个 FC 地址可以唯一标识一台节点设备上的一个 N_Port,同一台节点设备上不同 N_Port 的 FC 地址不同。

一个域 ID 可以唯一标识一台 FC 交换机,同一个 Fabric 网络中不同 FC 交换机的域 ID 不同。在报 文传输时,FC 交换机之间的路由和转发使用的都是域 ID。

FC 协议标准对 FC 地址的使用做了规范限定,请参见"16.1 附录 A FC 地址分配"。

3. 接口模式

在交换式架构中,节点设备和交换机之间通过不同模式的接口进行互联,如图 1-3 所示。



图1-3 接口模式示意图

(1) 节点设备上的接口模式

节点设备上的接口都是 N 模式,称为 N_Port。

N_Port 又分为两种类型:

- N端口:N端口通过直连方式连接到 Fabric。
- NL 端口: NL 端口通过仲裁环连接到 Fabric。

(2) 交换机上的接口模式

交换机上的接口具有下面几种模式:

- E模式:处于本模式的接口称为 E_Port。E_Port 用来连接其它交换机的 E_Port。
- F模式:处于本模式的接口称为 F_Port。F_Port 用来连接节点设备的 N_Port 或者其它交换机 的 NP_Port。
- NP模式:处于本模式的接口称为 NP_Port。NP_Port 用来连接其它交换机的 F_Port。

多台交换机通过 E_Port 互联组成一个 Fabric,通过 F_Port 将节点设备接入到 Fabric 中来。

1.2.2 通信过程

FC 交换机组成的 Fabric 网络的主要功能是提供数据传输服务。服务器通过 FC 交换机能够将命令和数据发送给磁盘设备,或者从磁盘设备读取数据。

图1-4 FC SAN 通信过程



下面以服务器访问磁盘设备为例,简单介绍一下 FC SAN 中的通信过程:

- (1) 服务器和磁盘设备通过 FLOGI(Fabric Login)协议向 FC 交换机进行注册,注册报文中会携带 Port WWN、Node WWN、期望得到的 FC 地址等信息,FC 交换机为与之直连的每个节点 设备分配 FC 地址。
- (2) 服务器和磁盘设备向其直连的 FC 交换机发送名称服务注册请求,注册其名称服务信息。名称服务信息包括节点设备的 FC4 信息等(关于 FC4 信息的详细介绍请参见"<u>6.15 配置和探测</u>发现节点设备的 FC4 信息")。最终,Fabric 网络中的每台 FC 交换机上都保存着所有节点设备的名称服务信息。
- (3) 当服务器要访问磁盘设备时,服务器要向其直连的 FC 交换机发送名称服务查询请求,获取 Fabric 网络中存在的磁盘设备列表,以及这些磁盘设备的 WWN、FC 地址等信息。
- (4) 服务器获取到磁盘设备的 FC 地址后, 就可以将 FC 报文发送给就近的 FC 交换机。FC 报文的 目的 FC 地址就是磁盘设备的 FC 地址。
- (5) FC 交换机收到服务器发送来的 FC 报文后,根据报文中的目的 FC 地址查找转发表(该转发表是 FC 交换机根据 FC 路由协议或配置的静态路由信息计算后生成的),选择数据转发路径,将报文转发到下一跳 FC 交换机。下一跳 FC 交换机同样对 FC 报文进行转发,直到最后一跳 FC 交换机将 FC 报文转发给目的磁盘设备。

1.2.3 VSAN

在实际应用中,若是所有用户的数据都在同一个 FC SAN 网络中进行转发,则不利于数据安全。用 户可以根据实际需要将物理上连通的 FC SAN 网络划分为多个 VSAN (Virtual Storage Area Network, 虚拟存储区域网络), 每个 VSAN 相互隔离, 并独立提供服务, 增强了网络的适应性和安全性, 使其能够为用户提供更有效的服务。

关于 VSAN 的详细介绍,请参见"<u>5 VSAN</u>"。

1.2.4 FC Zone

VSAN 的划分实现了将一个物理连通的 SAN 分割成多个逻辑上的虚拟 SAN,但仅通过 VSAN 却不能对接入 Fabric 网络的服务器及磁盘设备(即 N_Port)进行访问控制。相同 VSAN 内的 N_Port,只要注册了名称服务就可以相互访问,即一台服务器可以访问 VSAN 内的任意磁盘,这样给数据安全带来隐患。

Zone 特性可以有效解决上述问题,其原理是: 在 VSAN 内进一步划分区域 (Zone),在 Zone 内根 据不同的目的添加不同的 N_Port 成员。使不同 Zone 内的 N_Port 成员之间相互隔离,以达到访问 控制的目的。

关于 Zone 的详细介绍,请参见"<u>8 FC Zone</u>"。

1.3 FCoE协议

采用 FC SAN 技术的数据中心一般包括独立的 LAN(Local Area Network,局域网)网络和 SAN 网络。LAN 网络应用于传统的以太网/IP 业务,SAN 网络应用于网络存储。

为了同时为 LAN 网络提供服务并通过 SAN 网络完成存储功能,服务器需要使用独立的以太网卡和 FC 网卡,且以太网交换机和 FC 交换机及其对应网络连接线也是独立的。这就使得网络需要使用较 多的交换机和网卡及线缆,对应的设备投资及维护工作量都比较大,可扩展性比较差。

FCoE 协议可以很好的解决上述问题。FCoE 是将 FC 协议承载在以太网上的一种协议。在 FCoE 解决方案中,服务器只要使用支持 FCoE 协议的以太网卡即可,而支持 FCoE 协议的 FCF (FCoE Forwarder, FCoE 转发器)交换机可以同时替换传统以太网交换机和 FC 交换机,实现 I/O 整合 (I/O Consolidation),使网卡、交换机和连接线缆的数量大为减少,同时减轻网络运行的维护工作量,降低总体成本。





如<u>图 1-5</u>所示,在传统组网中,服务器分别通过以太网接口和 FC 接口接入到 LAN 网络和 SAN 网络。而在 FCoE 组网中,服务器可以通过支持 FCoE 协议的以太网卡连接到支持 FCoE 协议的存储 交换机 FCF switch 上(服务器和 FCF switch 之间的链路可以同时收发以太网报文和 FC 报文),然 后通过 FCF 交换机接入到 LAN 网络和 SAN 网络。

1.3.1 基本概念

FCoE 的典型应用如图 1-6 所示。FCF 交换机和 ENode (ENode 是支持在以太网上传输 FC 协议的 节点设备,包括服务器和磁盘设备)之间的以太网链路可以同时收发以太网报文和 FC 报文。在以 太网链路上收发 FC 报文就是通过 FCoE 协议实现的。



图1-6 FCoE 典型组网图

在介绍 FCoE 的工作机制之前,先介绍几个基本概念。

1. VFC 接口/VN 接口

VFC 接口是 FCF 交换机上手工创建的虚拟逻辑口,它虚拟实现物理 FC 接口的功能。 必须将 VFC 接口和具体的物理以太网接口进行绑定,VFC 接口才能正常工作。 VFC 接口可以和 ENode 相连,也可以和 FCF 交换机相连。 VFC 接口支持三种模式: E 模式、F 模式、NP 模式。默认为 F 模式。 VN 接口是 ENode 上的虚拟逻辑口,它虚拟实现物理 FC 接口的功能。

2. FIP 协议

FIP(FCoE Initialization Protocol, FCoE 初始化协议)是一个建立和维护虚链路的协议。
FCF 交换机和 ENode(或 FCF 交换机)之间通过 FIP 协议在 VFC 接口和 VN 接口(或 VFC 接口)
之间建立一条虚链路,为 FC 报文在以太网上承载提供物理传输的基础。

3. FCoE 报文

FC 报文需要封装在以太网报文中,才能在以太网链路上传输。封装以太网头的 FC 报文就是 FCoE 报文。

FCoE 报文采用 Ethernet II 类型的以太网封装,以太网头中主要字段的内容如下:

• 以太网报文类型: 0x8906。

 目的 MAC 地址/源 MAC 地址:对于交换机,使用的是交换机的 FCoE MAC 地址(可以通过 display fcoe 命令查看)。对于节点设备,使用的是节点设备的 FPMA(Fabric Provided MAC Address, Fabric 提供的 MAC 地址)。FPMA 由 FC-MAP 和 VN 接口的 FC 地址映射得到, 映射方法为 FC-MAP 为高 24 位,FC 地址为低 24 位,如图 1-7 所示。其中,FC-MAP 采用直 连交换机的 FC-MAP 值,该值默认为 0x0efc00,可以在交换机上通过 fcoe fcmap 命令修改。

图1-7 FPMA 地址映射



1.3.2 工作机制

下面将详细介绍 FCoE 协议的工作机制。

图1-8 ENode 和 FCF 交换机的内部框图



🕑 说明

本文仅介绍 FCF 交换机上和 FCoE 协议相关的内容,不介绍 ENode 上和 FCoE 协议相关的内容。

1. 在以太网上收发 FC 报文的过程

FC 报文在以太网上的发送和接收过程如下:

- 在发送 FC 报文之前, FCF 交换机和 ENode(或 FCF 交换机)之间先通过 FIP 协议在 VFC 接口和 VN 接口(或 VFC 接口)之间建立一条虚链路。在虚链路建立起来之后, FCF 交换机 将 FC 报文封装成 FCoE 报文发送出去。
- FCF 交换机在接收到 FCoE 报文之后,剥离 FCoE 报文的以太网头,将还原后的 FC 报文送 给上层进行处理。

2. FIP 协议工作机制

FIP 协议用来建立和维护 VFC 接口和 VN 接口(或 VFC 接口)之间的虚链路。 FIP 协议中用到两类报文:发现请求报文和发现通告报文。其中,发现通告报文又分为两种:

- 请求发现通告报文:用来回应发现请求报文。
- 非请求发现通告报文:周期性发送,用来通告自己的存在或维护建立的虚链路。

下面以 FCF 交换机和 ENode 之间建立虚链路的过程为例,介绍一下 FIP 协议的工作机制。



如图 1-9 所示,虚链路的建立过程为:

- (1) ENode 向外发送发现请求报文,开始建立虚链路。发现请求报文中携带着自己的 FCoE MAC 地址。
- (2) FCF 交换机收到发现请求报文后,根据 VFC 接口是否绑定 FCoE MAC 地址做不同的处理:
- 如果 VFC 接口没有配置绑定 FCoE MAC 地址,则学习 FCoE MAC,即保存该报文中携带的 FCoE MAC 地址,并回应请求发现通告报文。请求发现通告报文的 fcf priority 字段中携带了 VFC 接口的 FCF 优先级。
- 如果 VFC 接口配置了绑定 FCoE MAC 地址,则检查 FCoE MAC,如果该报文中携带的 FCoE MAC 地址与配置的绑定 FCoE MAC 地址一致,则回应请求发现通告报文(请求发现通告报文的 fcf priority 字段中携带了 VFC 接口的 FCF 优先级);否则,丢弃该报文,不继续做其它处理。
- (3) FCF 交换机周期性向外发送非请求发现通告报文(发送周期可以通过 fcoe fka-adv-period 命 令配置,缺省值为 8 秒)。非请求发现通告报文的 fcf priority 字段中携带了系统的 FCF 优先 级。
- (4) ENode 收到发现通告报文后,根据发现通告报文中的 fcf priority 字段选择优先级最高的 FCF, 并向该 FCF 发送 FLOGI 报文,进行注册。

- (5) FCF 交换机接收到 FLOGI 报文后,根据绑定的或者学习到的 FCoE MAC 地址做检查。如果 检查通过则回应 FLOGI LS_ACC,此时虚链路完成建立;如果检查没有通过则丢弃该报文, 不继续做其它处理。
- (6) FCF 交换机周期性发送非请求发现通告报文来维护建立的虚链路。如果 ENode 在 2.5 倍的 fka-adv-period 间隔内没有接收到非请求发现通告报文,则删除该虚链路。

1.4 FCoE模式

交换机支持下面几种 FCoE 模式:

- FCF 模式:工作在本模式的交换机称为 FCF 交换机,其 VFC 接口支持 E 模式和 F 模式,分别称为 E_Port 和 F_Port。
- NPV 模式:工作在本模式的交换机称为 NPV 交换机,其 VFC 接口支持 F 模式和 NP 模式, 分别称为 F_Port 和 NP_Port。
- Transit 模式:工作在本模式的交换机称为 Transit 交换机,其以太网接口可工作在 ENode 模式或 FCF 模式。

具有 FCoE 功能的交换机可工作在以下模式: FCF 模式、NPV 模式、Transit 模式、非 FCoE 模式。

- 当交换机工作在 FCF 模式时,可通过 E_Port 连接其它 FCF 交换机的 E_Port,或使用 F_Port 连接节点设备的 N_Port 或 NPV 交换机的 NP_Port。
- 当交换机工作在 NPV 模式时,可通过 F_Port 连接节点设备的 N_Port,或使用 NP_Port 连接 FCF 交换机的 F_Port。
- 当交换机工作在 Transit 模式时,可通过配置以太网接口为 ENode 模式或 FCF 模式,用于限制以太网接口只能接收来自 ENode 或 FCF 交换机的通信流量。
- 当交换机工作在非 FCoE 模式时,交换机为普通交换机,不具备任何 FCoE 相关的功能。 下面将详细介绍各 FCoE 模式的应用场景。

1.4.1 FCF 模式

支持 FCoE 协议的 FCF 交换机利用以太帧封装 FC 报文的方式,实现了用 FCoE 虚链路替代物理的 FC 链路,从而可在无损以太网中提供标准 Fibre Channel 交换机的能力和特性。



FCF 的应用组网如图 1-10 所示,不同于单纯的 FC 网络,在 FCoE 环境下,ENode 和 FCF 交换机 是通过以太网接口在无损以太网上通信的。ENode 和 FCF 交换机之间的 FCoE 虚链路连接 VN 接 口到 VFC 接口,FCF 交换机和 FCF 交换机之间的 FCoE 虚链路连接 VFC 接口到 VFC 接口。 与 FC 交换机相同,每台 FCF 交换机都会被分配一个域 ID,而每个 FC SAN 最多支持 239 个域 ID, 因此也就限制了一个 FC SAN 中最多只能有 239 台交换机。

1.4.2 NPV 模式

在 FC SAN 中,对于直接连接节点设备的边缘交换机的需求量很大,为了使边缘交换机可以突破一个 FC SAN 中 239 台最大交换机数目的限制,开发了 NPV (N_Port Virtualization, N 端口虚拟化) 模式的交换机,简称 NPV 交换机。



图1-11 NPV 应用组网

NPV 的应用组网如图 1-11 所示。NPV 交换机位于 Fabric 网络边缘,在节点设备与核心交换机之间。 核心交换机是工作在 FCF 模式的交换机。NPV 交换机通过 F_Port 和节点设备的 N_Port 相连,通 过 NP_Port 和核心交换机的 F_Port 相连。最终,节点设备通过 NPV 交换机接入到 Fabric 网络中, NPV 交换机将所有节点设备的流量转发到核心交换机。

对于节点设备来说,NPV 交换机相当于一台 FCF 模式的交换机,接口呈现为 F 模式;对于核心交换机来说,NPV 交换机相当于一台节点设备,接口呈现为 N 模式。

关于 NPV 的详细介绍,请参见"<u>9 NPV</u>"。

1.4.3 Transit 模式

FCoE 协议支持在无损以太网中构建 FC SAN,增加了 FC SAN 的组网灵活性,FCF 交换机与节点 设备之间可以增加 Transit 交换机。如图 1-12 所示, ENode 通过 Transit 交换机接入 FCF 交换机。

图1-12 Transit 应用组网



Transit 交换机上的以太网接口有两种模式: FCF 模式和 ENode 模式。与 ENode 相连的以太网接口需要配置为 ENode 模式; 与 FCF 交换机相连的以太网接口需要配置为 FCF 模式。

Transit 交换机级联时需保证以太网接口模式的正确性。如图 1-13 上的模式配置, ENode 2 仅能通过 FCF 交换机 2 进行注册,不能通过 FCF 交换机 1 进行注册。如果 ENode 2 有向 FCF 交换机 1 进行注册的需求,则需要修改 Transit 交换机间的模式配置。

图1-13 Transit 交换机级联组网



图 1-14 所示为NPV 交换机和 Transit 交换机的正确组网, NPV 交换机的位置在 FCF 交换机和 Transit 交换机之间, Transit 交换机下游接入 ENode。

图1-14 NPV、Transit 交换机组网



相较于 FCF 以及 NPV 模式的交换机,工作于 Transit 模式的交换机对 FCoE 协议报文的处理更为简单,其主要功能是过滤和转发。但不同于普通以太网交换机的是,工作在 Transit 模式的交换机 具有识别 FCoE 协议报文、控制网络中 FCoE 协议相关报文流量以及保障网络安全的能力。

1.5 协议规范

与 FC 和 FCoE 相关的协议规范有:

- FC-FS-3: Fibre Channel Framing and Signaling 3
- FC-SW-5: Fibre Channel Switch Fabric 5
- FC-LS-2: Fibre Channel Link Services 2
- FC-GS-6: Fibre Channel Generic Services 6
- FC-BB-5: Fibre Channel Back Bone 5

2 FCoE 配置限制和指导

目前仅以下接口板支持 FCoE 功能:

- SE 系列接口板
- SF 系列接口板
- **SG** 系列接口板

2.1 配置设备工作在高级模式

设备只有工作在高级模式下,才支持 FCoE 功能。关于设备工作模式的详细介绍和相关配置请参见 "基础配置指导"中的"设备管理"。

2.2 配置交换机的FCoE模式

具有 FCoE 功能的交换机可工作在以下模式: FCF 模式、NPV 模式、Transit 模式、非 FCoE 模式。 交换机只能从非 FCoE 模式切换至三种 FCoE 模式,或从三种 FCoE 模式切换为非 FCoE 模式,三 种 FCoE 模式之间不能直接切换。当需要修改 FCoE 模式时,必须首先切换至非 FCoE 模式。当交 换机从 FCoE 模式切换至非 FCoE 模式后,原 FCoE 模式下的所有 FCoE 相关配置将被清空,仅保 留己创建的 VFC 接口。

表2-1 配置交换机的 FCoE 模式

操作	命令	说明
进入系统视图	system-view	-
配置交换机的FCoE模式	fcoe-mode { fcf fcf-npv npv transit }	缺省情况下,交换机工作在非FCoE模式,即 不具备任何FCoE相关的功能 需要注意的是,设备不支持配置fcf-npv参数
显示交换机的FCoE模式	display fcoe-mode	display命令可以在任意视图执行

2.3 在不同FCoE模式下配置FCoE功能

交换机支持三种 FCoE 模式: FCF 模式、NPV 模式、Transit 模式。在不同 FCoE 模式下,交换机 所支持的 FCoE 功能不同,具体情况如表 2-2 所示。用户可以根据交换机的 FCoE 模式来选择配置 不同的 FCoE 功能。

表2-2 交换机工作在不同 FCoE 模式下所支持的 FCoE 功能

FCoE 模式 FCoE 功能	FCF 模式	NPV 模式	Transit 模式
<u>VFC接口</u>	支持	支持	不支持
FCoE基础配置	支持	支持	不支持

FCoE 模式 FCoE 功能	FCF 模式	NPV 模式	Transit 模式
<u>VSAN</u>	支持	支持	不支持
<u>建立Fabric网络</u>	支持	支持 <u>配置Fabric定时器</u> ,其余功能均不 支持	不支持
<u>FC路由与转发</u>	支持	 支持如下功能: 显示 FC 路由表信息 显示 FC FIB 表项信息 显示 FC Exchange 表项信息 其余功能均不支持 	不支持
FC Zone	支持	不支持	不支持
<u>NPV</u>	不支持	支持	不支持
FIP Snooping	不支持	不支持	支持
<u>FCS</u>	支持	不支持	不支持
<u>FDMI</u>	支持	不支持	不支持
FC Ping	支持	不支持	不支持
FC Tracert	支持	不支持	不支持

3 vfc 接口

VFC 接口可以和 ENode 相连,也可以和 FCF、NPV、Transit 三种交换机相连。

VFC 接口支持三种模式: E 模式、F 模式、NP 模式。默认为 F 模式。

VFC 接口是手工创建的虚拟逻辑口,它虚拟实现物理 FC 接口的功能,必须将 VFC 接口和以太网 接口进行绑定,VFC 接口才能正常工作。VFC 接口绑定以太网接口后,交换机将 VFC 接口上的 FC 报文封装成 FCoE 报文在以太网链路上传输。

如果 VFC 接口绑定的以太网接口的链路类型为 Hybrid 或 Trunk,请务必保证该以太网接口允许缺 省 VLAN 的报文通过,否则,将导致以太网接口参数协商失败,VFC 接口无法达到 UP 状态。如果 接口的缺省 VLAN 是 VLAN 1,则接口下不能配置 undo port hybrid vlan 1 或 undo port trunk permit vlan 1;如果接口的缺省 VLAN 是其他 VLAN,则接口下需要配置 port hybrid vlan *pvid* untagged 或 port trunk permit *vlan* pvid。

为了保证 FCoE 报文在以太网上可以实现无损传输,在 VFC 接口绑定的以太网接口上必须进行如下配置:

- 交换机和服务器连接的以太网接口上需要配置 DCBX、自动协商模式的 PFC 和 ETS 功能。
- 交换机和磁盘设备连接的以太网接口上需要配置 DCBX、自动协商模式的 PFC 功能。
- 交换机与交换机连接的以太网接口上要强制开启 PFC 功能。

关于 DCBX (Data Center Bridging Exchange Protocol,数据中心桥能力交换协议)、PFC (Priority-based Flow Control,基于优先级的流量控制)和 ETS(Enhanced Transmission Selection, 增强传输选择)功能的详细介绍和相关配置请参考"二层技术-以太网交换配置指导"中的"LLDP"。

3.1 配置VFC接口

表3-1 配置 VFC 接口

操作	命令	说明
进入系统视图	system-view	-
创建VFC接口,并进入VFC接口视 图	interface vfc interface-number	-
配置VFC接口的模式		缺省情况下,VFC接口的模式为F模式
	fc mode { e f np }	• 当交换机工作在 FCF 模式时, VFC 接口支持 E、F 模式
		• 当交换机工作在 NPV 模式时, VFC 接口支持 F、NP 模式
b 将VFC接口绑定到以太网接口 加		缺省情况下,VFC接口没有与以太网接 口绑定
	bind interface interface-type interface-number [mac mac-address]	VFC接口通过所绑定的以太网接口发 送和接收报文
		VFC接口通过Transit交换机连接多个 ENode时,将该VFC接口绑定到以太网 接口时必须指定MAC地址

操作	命令	说明
将VFC接口以Trunk方式加入	缺省情况下,接口不以 Trunk 方式加入 任何 VSAN	
VSAN,即允许指定的VSAN通过当 前接口	날 port trunk vsan <i>vsan-id-list</i>	可以先将VFC接口以Trunk方式加入一 个还不存在的VSAN中,然后再创建该 VSAN
(可选)配置VFC接口的描述信息	description text	缺省情况下,接口的描述信息为" <i>该接</i> <i>口的接口名</i> Interface",例如: Vfc1 Interface
(可选)配置VFC接口的期望带宽	bandwidth bandwidth-value	缺省情况下,VFC接口的期望带宽=接口的波特率÷1000(kbit/s)
(可选)恢复VFC接口的缺省配置	default	-
打开VFC接口	undo shutdown	缺省情况下,VFC接口处于开启状态

3.2 VFC接口显示和维护

在完成上述配置后,在任意视图下执行 display 命令可以显示配置后 VFC 接口的运行情况,通过查看显示信息验证配置的效果。

在用户视图下执行 reset 命令可以清除 VFC 接口的统计信息。

表3-2 VFC 接口显示和维护

操作	命令
显示VFC接口的相关信息	display interface [vfc [interface-number]] [brief [description down]]
清除VFC接口的统计信息	reset counters interface [vfc [interface-number]]

4 FCoE 基础配置

开启 FCoE 功能后,FCoE 相关特性才能正常运行。

4.1 FCoE基础配置任务简介

表4-1 FCoE 基础配置任务简介

配置任务	说明	详细配置
开启VLAN的FCoE功能,并指定映射VSAN	必选	<u>4.2</u>
配置FCoE网络的FC-MAP值	可选	<u>4.3</u>
配置FCoE网络的fka-adv-period值	可选	<u>4.4</u>
配置FCoE网络的FCF优先级	可选	<u>4.5</u>

4.2 开启VLAN的FCoE功能,并指定映射VSAN

在通过 VFC 接口发送报文时,其绑定的以太网接口可能同时允许多个 VLAN 的报文通过,因此需 要开启某个 VLAN 的 FCoE 功能,并将该 VLAN 与某 VSAN 进行映射,这样映射 VSAN 内的报文 会被打上该 VLAN 的 Tag,在该 VLAN 内进行发送。

配置本功能时需要注意:

- 不能在 VLAN 1 内开启 FCoE 功能。
- VLAN 与 VSAN 是一一对应的,一个 VLAN 只能映射一个 VSAN,一个 VSAN 也只能被一个 VLAN 映射。
- 通信两端的设备必须在相同 VLAN 内开启 FCoE 功能,并将该 VLAN 映射到同一个 VSAN。
- 用户需保证 VFC 接口绑定的以太网接口允许开启 FCoE 功能的 VLAN 通过。

开启某 VLAN 的 FCoE 功能后,该 VLAN 会有如下变化:

- 该 VLAN 内仅转发 FCoE 流量,不转发其它业务流量,例如 IP 流量。
- 该 VLAN 内的成员端口之间被设置为二层隔离,不会形成广播环路,因此,FCoE VLAN 内不 需要运行 STP 协议或其它环路检测协议,否则可能会导致 FCoE 转发链路被阻塞。
- 该 VLAN 内可以运行二层协议,但由于成员端口之间被设置为二层隔离,二层协议运行状态 会按照端口隔离拓扑运行。

表4-2 开启 VLAN 的 FCoE 功能,并指定映射 VSAN

操作	命令	说明
进入系统视图	system-view	-
进入VLAN视图	vlan vlan-id	-
开启VLAN的FCoE功能,并指定映射 VSAN的ID	fcoe enable [vsan vsan-id]	缺省情况下,VLAN的FCoE功能处于关闭状态

4.3 配置FCoE网络的FC-MAP值

FC-MAP 值用来标识一个 FCoE 网络,同一个 FCoE 网络中的所有的交换机必须具有相同的 FC-MAP 值。

🖞 提示

配置 FC-MAP 值后, VFC 接口会重新进行协商。两端都配置相同的 FC-MAP 值才能够协商成功。

表4-3 配置 FC-MAP 值

操作	命令	说明
进入系统视图	system-view	-
配置FC-MAP值	fcoe fcmap fc-map	缺省情况下,FC-MAP值为0x0EFC00

4.4 配置FCoE网络的fka-adv-period值

1. 功能简介

fka-adv-period 值的作用如下:

- 虚链路建立以后,在E模式VFC接口上,交换机以fka-adv-period为间隔周期性向外发送非 请求发现通告报文来维护建立的虚链路,非请求发现通告报文中携带fka-adv-period值。对端 交换机收到非请求发现通告报文后,维持虚链路的状态,并记录fka-adv-period值。如果交换 机在2.5倍的fka-adv-period间隔(收到的非请求发现通告报文中携带的值,非本机配置的值) 内没有收到非请求发现通告报文,则删除该虚链路。
- 虚链路建立以后,在F模式VFC接口上,交换机以fka-adv-period为间隔周期性向外发送非请求发现通告报文来维护建立的虚链路,非请求发现通告报文中携带fka-adv-period值。对端ENode收到非请求发现通告报文后,维持虚链路的状态,并记录fka-adv-period值。如果ENode在2.5倍的fka-adv-period间隔内没有收到非请求发现通告报文,则删除该虚链路。同时ENode使用记录的fka-adv-period间隔周期性发送保活报文,交换机收到保活报文后,维持虚链路的状态。如果交换机在2.5倍的fka-adv-period间隔内没有收到保活报文,则删除该虚链路。
- NP 模式的 VFC 接口与 ENode 的行为相同,不受本交换机配置的 fka-adv-period 值的影响, 使用从对端交换机学习到的 fka-adv-period 值。

2. 配置限制和指导

配置 fka-adv-period 值时,需要注意:

- FC-BB-5标准中规定,fka-adv-period取值上限为90秒,交换机的fka-adv-period配置上限为600秒,超出了协议规定的取值范围。因此,当交换机与服务器、存储设备或其他厂商交换机互通时,配置的fka-adv-period值不能超出90秒。
- 通常情况下,使用 fka-adv-period 的缺省值(8秒)即可。在交换机进行主备倒换或者有备用 主控板的 ISSU 软重启升级时,为了保证业务不中断,如果 FCoE 配置较多,则需要适当调大

fka-adv-period 值,建议配置为 60~90 秒之间。关于 ISSU 的详细介绍,请参见"基础配置指导"中的"ISSU"。

- 超出 90 秒的配置,建议用户在无备用主控板的 ISSU 软重启升级时使用。当交换机进行无备用主控板 ISSU 软重启升级时,由于没有备用主控板的存在,会有较长一段时间无法发送非请求发现通告报文或保活报文,为了使对端设备不会在此期间因超时而删除虚链路,从而保证业务不中断,建议调整 fka-adv-period 值到 300~600 秒之间,使得 ISSU 软重启升级能够完成。
- NPV 交换机进行主备倒换或者 ISSU 软重启升级时,为了保证业务不中断,除了要调整本交换机的 fka-adv-period 值,还要调整上游 FCF 交换机的 fka-adv-period 值。这是因为,NPV 交换机上的 fka-adv-period 值,仅影响本机 F 模式 VFC 接口和其连接的下游 ENode 的行为。
 NP 模式 VFC 接口使用的是从上游 FCF 交换机学习到的 fka-adv-period 值。因此,NPV 交换机进行主备倒换或者 ISSU 软重启升级时,需要同时调整本交换机和上游 FCF 交换机的 fka-adv-period 值。

由于上述配置限制,当无备用主控板的接入 FCF 交换机或 NPV 交换机进行 ISSU 软重启升级时, FCoE 流量会中断。这是因为接入 FCF 交换机或 NPV 交换机连接服务器、存储设备或者其他厂商 NPV 设备,由于互通限制,fka-adv-period 值不能超过 90 秒。由于没有备用主控板存在,ISSU 软 重启升级需要的时间较长,超过了 2.5 * 90 秒的超时间隔,ISSU 软重启升级期间虚链路会超时删 除,所以,FCoE 流量会中断。

3. 配置步骤

表4-4 配置 fka-adv-period 值

操作	命令	说明
进入系统视图	system-view	-
配置fka-adv-period值	fcoe fka-adv-period fka-adv-period	缺省情况下,fka-adv-period值为8秒

4.5 配置FCoE网络的FCF优先级

FCF 优先级分为两种:系统的 FCF 优先级、VFC 接口的 FCF 优先级。应用场合如下:

- 发送非请求发现通告报文时,报文中的 fcf priority 字段将填写系统的 FCF 优先级的值。
- 发送请求发现通告报文时,报文中的 fcf priority 字段将填写 VFC 接口的 FCF 优先级的值。

ENode 在收到多个 FCF 发送的发现通告报文的情况下,将从这些发现通告报文中选择 fcf priority 优先级最高的 FCF,并向其发送 FLOGI 报文,进行注册。

FCF 优先级仅在 VFC 接口为 F 模式时生效,即仅在与 ENode 相连的 VFC 接口上才有效。

表4-5 配置系统的 FCF 优先级

操作	命令	说明
进入系统视图	system-view	
配置系统的FCF优先级	fcoe global fcf-priority priority	缺省情况下,系统的FCF优先级为128 本配置对所有F模式的VFC接口生效

表4-6 配置 VFC 接口的 FCF 优先级

操作	命令	说明
进入系统视图	system-view	-
进入VFC接口视图	interface vfc interface-number	-
配置VFC接口的FCF优先级	fcoe fcf-priority priority	缺省情况下,VFC接口的FCF优先级为128 本配置仅在VFC接口为F模式时生效,在E模 式下可以配置,但不生效

4.6 FCoE基础配置显示和维护

在完成上述配置后,在任意视图下执行 display 命令可以显示配置后 FCoE 基础配置的运行情况,通过查看显示信息验证配置的效果。

表4-7 FCoE 基础配置显示和维护

操作	命令
显示FCoE全局配置相关信息	display fcoe

4.7 FCoE基础配置举例

4.7.1 组网需求

在构建一个包含 LAN 网络和 SAN 网络的数据中心时,为了节省设备、网卡和线缆的数量,采用 FCoE 解决方案。

4.7.2 组网图

图4-1 配置 FCoE 功能组网图



4.7.3 配置步骤

1. 配置 Switch A

(1) 开启高级模式

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view

[SwitchA] system-working-mode advance

Do you want to change the system working mode? $[{\tt Y}/{\tt N}]{\rm :}{\tt y}$

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchA] save

[SwitchA] quit

<SwitchA> reboot

(2) VLAN 和接口部署

创建 VLAN 10、20, 分别用来传输以太网数据流量和存储数据流量。

<SwitchA> system-view

[SwitchA] vlan 10

[SwitchA-vlan10] quit

[SwitchA] vlan 20

[SwitchA-vlan20] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 为 Hybrid 接口,允许 VLAN 10 的以太网数据报文不带 Tag 标签通过,允许 VLAN 20 的存储数据报文带 Tag 标签通过,设置接口的 PVID 为 VLAN 10。

[SwitchA] interface ten-gigabitethernet 1/0/1

[SwitchA-Ten-GigabitEthernet1/0/1] port link-type hybrid

[SwitchA-Ten-GigabitEthernet1/0/1] port hybrid vlan 10 untagged

[SwitchA-Ten-GigabitEthernet1/0/1] port hybrid vlan 20 tagged

[SwitchA-Ten-GigabitEthernet1/0/1] port hybrid pvid vlan 10

[SwitchA-Ten-GigabitEthernet1/0/1] quit

配置以太网接口 Ten-GigabitEthernet1/0/2 为 Trunk 接口,允许 VLAN 20 的存储数据报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/2

[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 20

[SwitchA-Ten-GigabitEthernet1/0/2] quit

配置以太网接口 Ten-GigabitEthernet1/0/3 为 Trunk 接口, 允许 VLAN 10 的以太网数据报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/3

[SwitchA-Ten-GigabitEthernet1/0/3] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10

[SwitchA-Ten-GigabitEthernet1/0/3] quit

(3) DCBX 部署

全局开启 LLDP 功能。

[SwitchA] lldp global enable

创建编号为 4000 的二层 ACL,并为其创建规则来匹配 FCoE 报文(协议号为 0x8906)和 FIP 报

文(协议号为0x8914)。

[SwitchA] acl mac 4000

[SwitchA-acl-mac-4000] rule 0 permit type 8906 ffff

[SwitchA-acl-mac-4000] rule 5 permit type 8914 ffff

[SwitchA-acl-mac-4000] quit

定义名为 DCBX 的类,其下各规则间的关系为逻辑或,并定义其匹配 ACL 4000。

[SwitchA] traffic classifier DCBX operator or

[SwitchA-classifier-DCBX] if-match acl 4000

[SwitchA-classifier-DCBX] quit

定义名为 DCBX 的流行为,并配置标记报文的 802.1p 优先级为 3。

[SwitchA] traffic behavior DCBX

[SwitchA-behavior-DCBX] remark dot1p 3

[SwitchA-behavior-DCBX] quit

定义名为 DCBX 的 QoS 策略,为类 DCBX 指定采用的流行为是 DCBX,并指定该策略为 DCBX 模式。

[SwitchA] qos policy DCBX

[SwitchA-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx

[SwitchA-qospolicy-DCBX] quit

在以太网接口 Ten-GigabitEthernet1/0/1 上开启 LLDP 功能,并允许该接口发送 LLDP 报文时携带 DCBX TLV 字段。

[SwitchA] interface ten-gigabitethernet 1/0/1

[SwitchA-Ten-GigabitEthernet1/0/1] lldp enable

[SwitchA-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx

在以太网接口 Ten-GigabitEthernet1/0/1 的出方向上应用 QoS 策略 DCBX。

[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound

(4) PFC 部署

在以太网接口 Ten-GigabitEthernet1/0/1 上配置与服务器自动协商是否开启 PFC 功能,且设置对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control auto

[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3

[SwitchA-Ten-GigabitEthernet1/0/1] qos trust dot1p

[SwitchA-Ten-GigabitEthernet1/0/1] quit

在以太网接口 Ten-GigabitEthernet1/0/2 上配置强制开启 PFC 功能,且设置对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

[SwitchA] interface ten-gigabitethernet 1/0/2

[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control enable

[SwitchA-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dot1p 3

[SwitchA-Ten-GigabitEthernet1/0/2] qos trust dot1p

```
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

(5) ETS 部署

配置 802.1p 优先级到本地优先级的映射,将 802.1p 优先级 3 映射到本地优先级 1,配置其它的 802.1p 优先级映射到本地优先级 0。

[SwitchA] qos map-table dot1p-1p

[SwitchA-maptbl-dot1p-lp] import 3 export 1

[SwitchA-maptbl-dotlp-lp] import 0 1 2 4 5 6 7 export 0

[SwitchA-maptbl-dot1p-lp] quit

在以太网接口 Ten-GigabitEthernet1/0/1 上配置 WRR 队列,使 FCoE 流量和普通 LAN 流量各占 50%带宽。

[SwitchA] interface ten-gigabitethernet 1/0/1 [SwitchA-Ten-GigabitEthernet1/0/1] gos wrr byte-count [SwitchA-Ten-GigabitEthernet1/0/1] gos wrr 1 group 1 byte-count 1 [SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 0 group 1 byte-count 1 # 在以太网接口 Ten-GigabitEthernet1/0/1 上配置其它的队列为 SP 调度方式。 [SwitchA-Ten-GigabitEthernet1/0/1] gos wrr 2 group sp [SwitchA-Ten-GigabitEthernet1/0/1] gos wrr 3 group sp [SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 4 group sp [SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 5 group sp [SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 6 group sp [SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 7 group sp [SwitchA-Ten-GigabitEthernet1/0/1] quit (6) FCoE 部署 # 配置 FCoE 模式为 FCF 模式并创建 VSAN 10。 [SwitchA] fcoe-mode fcf [SwitchA] vsan 10 [SwitchA-vsan10] guit # 创建 VFC 接口 VFC1, 配置 VFC1 接口工作在 F 模式, 将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 10, 即允许 VSAN 10 的报 文通过 VFC1 接口。 [SwitchA] interface vfc 1 [SwitchA-Vfc1] fc mode f [SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1 [SwitchA-Vfc1] port trunk vsan 10 [SwitchA-Vfc1] quit # 创建 VFC 接口 VFC2 接口, 配置 VFC2 接口工作在 E 模式, 将 VFC2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2 上,并将 VFC2 接口以 Trunk 方式加入 VSAN 10, 即允许 VSAN 10 的报 文通过 VFC2 接口。 [SwitchA] interface vfc 2 [SwitchA-Vfc2] fc mode e [SwitchA-Vfc2] bind interface ten-gigabitethernet1/0/2 [SwitchA-Vfc2] port trunk vsan 10 [SwitchA-Vfc2] quit

开启 VLAN 20 的 FCoE 功能,并将其与 VSAN 10 进行映射。

[SwitchA] vlan 20

[SwitchA-vlan20] fcoe enable vsan 10

[SwitchA-vlan20] quit

#缺省情况下,服务器和磁盘设备属于默认 Zone,为了实现两者互通,需要配置允许默认 Zone 内的成员互相访问。关于 Zone 的介绍,请参见"<u>8 FC Zone"</u>。

[SwitchA] vsan 10

[SwitchA-vsan10] zone default-zone permit

[SwitchA-vsan10] quit

2. 配置 Switch B

(1) 开启高级模式

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchB> system-view

[SwitchB] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the system to make it effective.

[SwitchB] save

[SwitchB] quit

<SwitchB> reboot

(2) VLAN 和接口部署

创建 VLAN 20, 用来传输存储数据流量。

<SwitchB> system-view

[SwitchB] vlan 20

[SwitchB-vlan20] quit

配置以太网接口 Ten-GigabitEthernet1/0/2 为 Trunk 接口,允许 VLAN 20 的存储数据报文通过。

[SwitchB] interface ten-gigabitethernet 1/0/2

[SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk

[SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 20

[SwitchB-Ten-GigabitEthernet1/0/2] quit

(3) PFC 部署

在以太网接口 Ten-GigabitEthernet1/0/2 上配置强制开启 PFC 功能,且设置对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

[SwitchB] interface ten-gigabitethernet 1/0/2

[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control enable

[SwitchB-Ten-GigabitEthernet1/0/2] priority-flow-control no-drop dotlp 3

[SwitchB-Ten-GigabitEthernet1/0/2] qos trust dot1p

[SwitchB-Ten-GigabitEthernet1/0/2] quit

(4) FCoE 部署

配置 FCoE 模式为 FCF 模式并创建 VSAN 10。

<SwitchB> system-view

[SwitchB] fcoe-mode fcf

[SwitchB] vsan 10

[SwitchB-vsan10] quit

创建 VF2 接口, 配置 VFC2 接口工作在 E 模式,将 VFC2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2上,并将 VFC2 接口以 Trunk 方式加入 VSAN 10, 即允许 VSAN 10 的报 文通过 VFC2 接口。

[SwitchB] interface vfc 2

[SwitchB-Vfc2] fc mode e

[SwitchB-Vfc2] bind interface ten-gigabitethernet1/0/2 $\,$

[SwitchB-Vfc2] port trunk vsan 10

[SwitchB-Vfc2] quit

开启 VLAN 20 的 FCoE 功能,并将其与 VSAN 10 进行映射。

[SwitchB] vlan 20

[SwitchB-vlan20] fcoe enable vsan 10

[SwitchB-vlan20] quit

缺省情况下,服务器和磁盘设备属于默认 Zone,为了实现两者互通,需要配置允许默认 Zone内的成员互相访问。关于 Zone 的介绍,请参见"<u>8 FC Zone"</u>。 [SwitchB] vsan 10 [SwitchB-vsan10] zone default-zone permit

[SwitchB-vsan10] quit

5 VSAN

5.1 VSAN简介

5.1.1 VSAN 概述

VSAN 的目的是将一个物理上连通的 SAN 网络分割成多个逻辑上的虚拟 SAN 网络。每个 VSAN 相互隔离,并独立提供服务,增强了网络的适应性和安全性,使其能够为用户提供更有效的服务。 对每一个 VSAN 来说,其本身就相当于一个 SAN 网络,VSAN 内的设备无法获得该 VSAN 以外的 其它 VSAN 和设备的信息。每个 VSAN 内都独立运行主交换机选举,基于每个 VSAN 配置域 ID, 独立运行路由协议,独立维护路由转发表,独立提供所需的服务等。

VSAN 的优点如下:

- 提高网络安全性:每个 VSAN 可以做到相互隔离。
- 提高网络适应性:每个 VSAN 可以独立运行,独立提供各种服务,不同 VSAN 可以使用重复的地址空间,增强了组网能力。
- 组网灵活:通过配置可以方便地将接口加入到不同的 VSAN,而不需要改变 SAN 网络的物理 连接。

5.1.2 VSAN 方式

VFC 接口只支持 Trunk 方式。

Trunk 方式:接口可以同时属于多个 VSAN。

1. FC 网络中 Trunk 方式工作原理

Trunk 方式可以真正实现不同 VSAN 之间的逻辑隔离。其实现原理是:在 FC 报文中增加 Virtual Fabric Tagging Header 报文头(VFT_Header,一种 FC 报文的扩展报文头,也称为 VSAN Tag), VFT_Header 中包括的 VF_ID(也称 VSAN ID)字段,表明了报文所属的 VSAN。带有不同 VF_ID 的报文限制在各自的 VSAN 内,不同 VSAN 不能互通。这样就达到了网络在物理上连通,但逻辑上隔离的目的。

Trunk 方式的典型组网如图 5-1 所示,两种不同颜色区域的 F_Port 的 Access VSAN_ID 分别配置为 VSAN 1、VSAN 2, E_Port 配置 Trunk VSAN 1~VSAN 2。当服务器读写磁盘时,不同服务器的 N_Port 发送不带 VFT_Header 的报文到 FC 交换机 A 的各自相连的 F_Port 上,分别在各自 F_Port Access 加入的 VSAN 内查找转发表,出接口为相同的 E_Port。报文从 E_Port 转发出去时,分别 添加 VSAN 1 和 VSAN 2 的 VFT_Header,中间可能会经过多台支持 VSAN 的交换机,转发到 FC 交换机 B 的 E_Port 上,并根据 VFT_Header 中的 VF_ID 字段,在相应 VSAN 中查找转发表,将报 文转发到相应的 F_Port 上,F_Port 去掉报文的 VFT_Header 后,将报文发送到不同磁盘设备的 N_Port 上。同样,从每个磁盘设备返回给服务器的数据报文也经过上述处理,最终到达不同的服务器。

图5-1 Trunk 方式应用组网图



从上面描述可以看出,报文在传输过程中会发生添加和去除 VFT_Header 的过程。同一台交换机上 要支持多个 VSAN,可以使用相同的物理接口,减少了网络的物理连接。真正做到了在物理连通的 SAN 网络之上的逻辑隔离。

2. FCoE 网络中 Trunk 方式工作原理

FCoE 网络是在以太网上承载 FC 协议,需要将 FC 协议中的 VSAN 资源映射到以太网中的 VLAN 资源,根据用户配置的 VSAN 到 VLAN 的映射关系,将 VSAN 内的转发表项存储到映射的 VLAN 内。FCoE 报文中使用 VLAN_Header 替代 FC 报文中的 VFT_Header,报文转发时根据 FCoE 报文中的 VLAN_Header 内的 VLAN ID 在相应的 VLAN 内查找转发表实现转发。

VFC 接口仅支持 Trunk 方式, VFC 接口绑定的以太网接口也要求工作在 Trunk 模式下, 且以太网接口 Trunk 的 VLAN 列表要与 VFC 接口 Trunk 的 VSAN 列表相匹配, 即存在 VSAN 到 VLAN 的映射关系。这样,从 VFC 接口传输的 FCoE 报文就可以使用 VLAN_Header 中的 VLAN ID 标识报文所属的 VLAN。

5.2 配置VSAN

5.2.1 创建 VSAN

初始情况下,只存在缺省 VSAN(VSAN 1)。用户不能创建或删除缺省 VSAN。用户可以创建的 VSAN 范围是 2~3839。

表5-1 创建 VSAN

操作	命令	说明
进入系统视图	system-view	-
创建VSAN,并进入VSAN视图	vsan vsan-id	缺省情况下,系统只有一个缺省VSAN (VSAN 1),且VSAN 1的名称为 VSAN0001

5.2.2 配置 Trunk VSAN

VFC 接口可以以 Trunk 方式加入多个 VSAN。

多次配置接口 Trunk VSAN,最终形成的接口 Trunk VSAN List 为配置的 Trunk VSAN 的集合。

表5-2 将接口以 Trunk 方式加入 VSAN

操作	命令	说明
进入系统视图	system-view	-
进入VFC接口视图	interface vfc interface-number	-
配置接口以Trunk方式加入VSAN,即允 许指定的VSAN通过当前接口	port trunk vsan vsan-id-list	缺省情况下,接口不以Trunk方式 加入任何VSAN 将接口以Trunk方式加入指定 VSAN时,此VSAN无需已经存在

5.3 VSAN显示和维护

在完成上述配置后,在任意视图下执行 display 命令可以显示配置后 VSAN 的运行情况,通过查看显示信息验证配置的效果。

表5-3 VSAN 显示和维护

操作	命令
显示VSAN配置的接口成员	display vsan [vsan-id] port-member

5.4 VSAN典型配置举例

5.4.1 VSAN 配置举例

1. 组网需求

SAN 网络如图 5-2 所示,要求:

- 服务器 Server A 能读写磁盘设备 Disk A 和 Disk B 中的数据;
- 服务器 Server B 只能读写磁盘设备 Disk C 中的数据。

2. 组网图

图5-2 配置 VSAN 组网图



3. 配置思路

- 为了实现上述需求,可将 SAN 网络划分为 2 个 VSAN,分别为 VSAN 10、VSAN 20,每个 VSAN 包含一组可以进行数据交互的服务器和磁盘设备。
- FCF 交换机 Switch A 上与服务器连接的 2 个接口需要配置为 F 模式,并将 Trunk VSAN 分别 配置为 VSAN 10、VSAN 20。
- FCF 交换机 Switch B 上与磁盘设备连接的 3 个接口需要配置为 F 模式,并将 Trunk VSAN 配置为 VSAN 10 或 VSAN 20。
- 两台 FCF 交换机之间的链路需要同时收发 2 个 VSAN 的报文,因此,需将链路两端的接口配置为 E 模式, Trunk VSAN list 中包括 VSAN 10、VSAN 20。

4. 配置步骤



本例中只列出 VSAN 相关配置,其它配置步骤略。

(1) 配置 Switch A

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

```
<SwitchA> system-view
```

[SwitchA] system-working-mode advance

Do you want to change the system working mode? $[{\tt Y}/{\tt N}]:{\tt y}$

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchA] save

[SwitchA] quit

<SwitchA> reboot

配置 FCoE 模式为 FCF 模式,创建 VSAN 10、20。

<SwitchA> system-view [SwitchA] fcoe-mode fcf [SwitchA] vsan 10 [SwitchA-vsan10] quit [SwitchA] vsan 20 [SwitchA-vsan20] quit

创建 VFC 接口 VFC1, 配置 VFC1 接口工作在 F 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 10, 即允许 VSAN 10 的报 文通讨 VFC1 接口。

[SwitchA] interface vfc 1

[SwitchA-Vfc1] fc mode f

[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchA-Vfc1] port trunk vsan 10

[SwitchA-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/1

[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[SwitchA-Ten-GigabitEthernet1/0/1] quit

创建 VFC 接口 VFC2, 配置 VFC2 接口工作在 F 模式,将 VFC2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2 上,并将 VFC2 接口以 Trunk 方式加入 VSAN 20, 即允许 VSAN 20 的报 文通过 VFC2 接口。

[SwitchA] interface vfc 2

[SwitchA-Vfc2] fc mode f

[SwitchA-Vfc2] bind interface ten-gigabitethernet 1/0/2

[SwitchA-Vfc2] port trunk vsan 20

[SwitchA-Vfc2] quit

配置以太网接口 Ten-GigabitEthernet1/0/2 允许 VLAN 20 的报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/2

[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 20

[SwitchA-Ten-GigabitEthernet1/0/1] quit

创建 VFC 接口 VFC4, 配置 VFC4 接口工作在 E 模式,将 VFC4 接口绑定到以太网接口 Ten-GigabitEthernet1/0/4上,并将 VFC4 接口以 Trunk 方式加入 VSAN 10、VSAN 20,即允许 VSAN 10、VSAN 20 的报文通过 VFC4 接口。

[SwitchA] interface vfc 4

[SwitchA-Vfc4] fc mode e

[SwitchA-Vfc4] bind interface ten-gigabitethernet 1/0/4

[SwitchA-Vfc4] port trunk vsan 10 20

[SwitchA-Vfc4] quit

配置以太网接口 Ten-GigabitEthernet1/0/4 允许 VLAN 10、VLAN 20 的报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/4

[SwitchA-Ten-GigabitEthernet1/0/4] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/4] port trunk permit vlan 10 20

[SwitchA-Ten-GigabitEthernet1/0/4] quit

开启 VLAN 10 的 FCoE 功能,并将其与 VSAN 10 进行映射。
```
[SwitchA] vlan 10
[SwitchA-vlan10] fcoe enable vsan 10
[SwitchA-vlan10] quit
# 开启 VLAN 20 的 FCoE 功能,并将其与 VSAN 20 进行映射。
[SwitchA] vlan 20
[SwitchA-vlan20] fcoe enable vsan 20
[SwitchA-vlan20] quit
# 缺省情况下,服务器和磁盘设备属于默认Zone,为了实现两者互通,需要配置允许默认Zone 内的成员互相访问。关于 Zone 的介绍,请参见 "<u>8 FC Zone</u>"。
[SwitchA] vsan 10
[SwitchA-vsan10] zone default-zone permit
[SwitchA-vsan10] quit
[SwitchA] vsan 20
```

[SwitchA-vsan20] zone default-zone permit

```
[SwitchA-vsan20] quit
```

(2) 配置 Switch B

Switch B上的配置与 Switch A 类似, 配置步骤略。

5. 验证配置

```
(1) 在 Switch A 上进行验证
#显示所有 VSAN 配置的接口成员。
[SwitchA] display vsan port-member
VSAN 1:
 Access Ports:
 Trunk Ports:
VSAN 10:
 Access Ports:
 Trunk Ports:
   Vfc1
   Vfc4
VSAN 20:
 Access Ports:
 Trunk Ports:
   Vfc2
   Vfc4
(2) 在 Switch B 上进行验证
验证结果与 Switch A 类似,显示内容略。
```

6 建立 Fabric 网络

6.1 简介

Fabric 网络为服务器和磁盘设备提供数据传输服务。通过 Fabric 网络传输数据之前,必须为 Fabric 网络中的每台 FCF 交换机分配域 ID、为 Fabric 网络连接的每个节点设备分配 FC 地址。

如图 6-1 所示, Fabric 网络可以通过静态和动态两种方式建立:

- 静态方式:手工为网络中的所有交换机指定域 ID,然后每台交换机为与之相连的 N_Port 分配
 FC 地址。此方式适用于组网结构简单、规模较小的网络。静态方式可以有效避免不必要的网络震荡。
- 动态方式:自动进行主交换机选举,由选举出来的主交换机为网络中的所有交换机分配域 ID, 最后每台交换机为与之相连的 N_Port 分配 FC 地址。此方式适用于规模较大的网络,可以对 整个网络进行集中管理。

图6-1 Fabric 网络建立过程



下面将详细描述 Fabric 网络建立的每个过程。

6.1.1 选举主交换机

在 Fabric 网络的动态建立过程中,主交换机用来为网络中的所有交换机分配域 ID。 在主交换机选举过程中,优先级(以小为优)最高的交换机将被选举为主交换机。如果多台交换机 优先级相同,则选择交换机 WWN 最小的那台交换机作为主交换机。 主交换机的选举过程如下:

- (1) 在开始主交换机选举时,所有交换机都认为自己是主交换机,记录本机信息为主交换机信息,同时启动超时时间为 10 秒的 PSST(Principal Switch Selection Timer,主交换机选举定时器)定时器。
- (2) 在 PSST 定时器超时前,交换机间通过交换携带有各自记录的主交换机信息的报文来选举主 交换机。收到报文后,将本机记录的主交换机的优先级和 WWN 与报文中携带的主交换机的 优先级和 WWN 进行比较,如果报文中携带的优先级更高,或者优先级相同但是 WWN 更小,

则将本机的主交换机信息更新为报文中携带的主交换机信息,并通知其它交换机。最后,网络中所有交换机记录的主交换机信息将达成一致。

- (3) 在 PSST 定时器超时后,如果记录的主交换机信息和本机信息一样,则该交换机成为主交换机。
- 主交换机选举出来后,主交换机的 WWN 作为 Fabric 网络的名称。

🕑 说明

在主交换机选举过程中,交换机若收到导致更新本机记录的主交换机信息的报文,则记录收到该报 文的 E_Port,此 E_Port对应的链路称为上游主链路。

6.1.2 分配域 ID

前面已经说过,一台交换机以及其直连的 N_Port 形成一个域,每个域需要分配一个域 ID。 FCF 交换机可以自动分配域 ID,也可通过配置静态指定域 ID。

- 如果通过静态配置指定域 ID,则需要为 Fabric 网络中的每台交换机都指定域 ID,且每台交换 机的域 ID 必须是唯一的。
- 如果动态分配域 ID,则 Fabric 网络中的交换机会自动完成主交换机选举和域 ID 分配的过程。
 当主交换机被选举出来之后,由主交换机负责为网络中的每台交换机分配域 ID。每一台交换机都会有一个唯一的域 ID。

动态分配域 ID 的过程如下:

- (1) 主交换机首先为自己分配域 ID。如果主交换机上预先配置了自己想要获取的域 ID,则主交换机将给自己分配该域 ID;否则,主交换机将给自己随机分配一个域 ID。主交换机给自己分配域 ID 后通知其下游交换机开始向其申请域 ID。
- (2) 下游交换机收到通知后,开始向主交换机申请域 ID。如果下游交换机上配置了自己想要获取 的域 ID,则下游交换机将向主交换机申请该域 ID。
- (3) 主交换机在收到下游交换机的域 ID 申请后,给下游交换机分配域 ID,并通知下游交换机。在分配域 ID 时:
- 如果下游交换机申请指定的域 ID 而且该域 ID 没有被主交换机分配出去,则主交换机将为之分 配该域 ID。
- 如果下游交换机没有申请指定的域 ID 或者主交换机无法为之分配指定的域 ID,则主交换机将 为之随机分配一个域 ID。
- 如果所有可以分配的域 ID 都已经分配出去,则主交换机将通知下游交换机无法完成分配。
- (4) 下游交换机在收到主交换机分配的域 ID 通知后:
- 如果下游交换机上配置了 static 模式的域 ID(关于域 ID 模式的详细介绍请参见"<u>6.7 配置域</u> <u>ID</u>"),并且该域 ID 与主交换机为之分配的域 ID 不一样,或者主交换机通知无法完成分配,则 下游交换机将隔离上游主链路(上游主链路对应的接口的状态变为 down)。
- 否则,下游交换机接受主交换机分配的域 ID,并通知其相邻的下游交换机开始向主交换机申 请域 ID。
- (5) 重复步骤(2)~(4),直到所有的下游交换机都获得域 ID。



- 在动态分配域 ID 过程中,交换机若收到申请域 ID 的请求报文,则记录收到该报文的 E_Port, 此 E Port 对应的链路称为下游主链路。
- 分配到的域 ID 将被记录到隐藏文件中。下次申请域 ID 时若无用户配置,则优先使用该文件中记录的域 ID 向主交换机申请。为防止频繁写该文件,域 ID 变化后会启动一个五秒钟的延迟定时器,超时后再将新的域 ID 写入该文件。若更新域 ID 后需要重启设备,请等待五秒,以保证最新的域 ID 已写入该文件。

6.1.3 分配 FC 地址

当交换机获取到域 ID 之后,便可以为与其直连的 N_Port 分配 FC 地址。

FC 地址中 Domain_ID 字段的值就是与 N_Port 相连的交换机的域 ID,不需要分配; Area_ID 和 Port_ID 字段的值由交换机统一分配。

FC 地址分配原则如下:

- 如果为 N_Port 绑定了 FC 地址的绑定关系,既配置 FC 地址持久化表项,则交换机为其分配 绑定的 FC 地址。
- 如果 N_Port 有指定要分配的 FC 地址,则交换机应该尽量分配指定的 FC 地址;
- 如果 N_Port 没有绑定或指定要分配的 FC 地址,或交换机无法分配其指定要分配的地址,则 交换机为其分配最小可以分配的 Area_ID 和 Port_ID。

6.2 建立Fabric网络配置任务简介

在规模较大的网络中,为了便于对网络进行集中管理,通常采用动态方式建立 Fabric 网络;而在组网结构简单、规模较小的网络中,为了有效避免不必要的网络震荡,通常采用静态方式建立 Fabric 网络。

表6-1 静态建立 Fabric 网络配置任务简介

配置任务	说明	详细配置
关闭Fabric配置功能	必选 静态建立Fabric网络时,必须关闭Fabric配置功能	<u>6.3</u>
配置Fabric网络的名称	必选 静态建立Fabric网络时,必须手工配置Fabric网络的 名称,并保证网络中所有交换机上配置的Fabric网络 的名称相同	<u>6.4</u>
配置允许的域ID范围	可选	<u>6.6</u>
配置域ID	必选 静态建立Fabric网络时,必须为每台交换机手工配置 域ID	<u>6.7</u>
配置FC地址持久化功能	可选	<u>6.8</u>
配置VSAN下的最大登录节点数	可选	<u>6.9</u>

配置任务	说明	详细配置
配置Fabric定时器	可选	<u>6.10</u>
配置RSCN聚合功能	可选	<u>6.14</u>
配置和探测发现节点设备的FC4信息	可选	<u>6.15</u>
开启Smart SAN功能	可选	<u>6.16</u>

表6-2 动态建立 Fabric 网络配置任务简介

配置任务	说明	详细配置
开启Fabric配置功能	必选 动态建立Fabric网络时,必须开启Fabric配置功能	<u>6.3</u>
配置交换机的优先级	可选 优先级的值将影响主交换机选举	<u>6.5</u>
配置允许的域ID范围	可选	<u>6.6</u>
配置域ID	可选 动态建立Fabric网络时,可以配置交换机想要获取的域 ID	<u>6.7</u>
配置FC地址持久化功能	可选	<u>6.8</u>
配置VSAN下的最大登录节点数	可选	<u>6.9</u>
配置Fabric定时器	可选	<u>6.10</u>
配置Fabric重配置	可选	<u>6.11</u>
配置接口拒绝收到的RCF请求报文	可选	<u>6.12</u>
开启Fabric告警功能	可选	<u>6.13</u>
配置RSCN聚合功能	可选	<u>6.14</u>
配置和探测发现节点设备的FC4信息	可选	<u>6.15</u>
开启Smart SAN功能	可选	<u>6.16</u>

6.3 开启/关闭Fabric配置功能

FCF 交换机在开启 Fabric 配置功能后,就会通过消息交互选举主交换机,之后由选举出来的主交换机为网络中的所有交换机动态分配域 ID。因此,在动态建立 Fabric 网络时,必须开启 Fabric 配置功能;在静态建立 Fabric 网络时,必须关闭 Fabric 配置功能,手工配置各交换机的域 ID。

表6-3	开启/关闭	Fabric	配置功能
------	-------	--------	------

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-

操作	命令	说明
开启Fabric配置功能	domain configure enable	在动态建立Fabric网络时,必须开启VSAN内所有交
关闭Fabric配置功能	undo domain configure enable	换机的Fabric配直切能; 在静态建立Fabric网络时, 必须关闭VSAN内所有交换机的Fabric配置功能 缺省情况下, Fabric配置功能处于开启状态

6.4 配置Fabric网络的名称

FCF 交换机支持为每个 VSAN 分配一个 Fabric 网络名称,其格式与 WWN 格式相同,是一个 64 位 的地址。当 VSAN 创建后,如果用户未配置 Fabric 网络的名称,则使用本交换机的 WWN 作为 Fabric 网络的名称。

需要注意的是,仅在静态建立 Fabric 网络时才需要配置 Fabric 网络的名称,并且同一 VSAN 内所 有交换机的 Fabric 网络名称必须一样。动态建立 Fabric 网络时并不需要配置 Fabric 网络的名称,系统将使用主交换机的 WWN 作为 Fabric 网络的名称。

表6-4 配置 Fabric 网络的名称

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置Fabric网络的名称	fabric-name name	缺省情况下,使用该VSAN内本交换机的WWN作为 Fabric网络的名称

6.5 配置交换机的优先级

FCF 交换机的优先级取值范围为 1~254, 取值越小,优先级越高。优先级高的 FCF 交换机优先被 选为主交换机。

优先级是按每个 VSAN 进行配置的,同一台 FCF 交换机在不同 VSAN 中的优先级可以不同。

交换机优先级的配置不能立即生效,需通过命令 domain restart disruptive 进行一次中断重配置 后才能生效。

交换机的运行优先级和配置的优先级可能不同:如果 Fabric 网络已处于稳定状态,此时去配置交换 机的优先级并不会立即生效,使用本命令查看时就有可能出现运行优先级和配置优先级不一致的情况。如果配置了优先级之后立即通过命令 domain restart disruptive 进行一次中断重配置,新配 置的优先级就会生效。待 Fabric 网络稳定后:

- 对于主交换机,如果配置的优先级<=2,则运行和配置优先级一致,如果配置的优先级数值大于2,则会将运行优先级修改为2,运行和配置优先级不一致。
- 对于非主交换机,如果配置的优先级<=2,会将运行优先级修改为3,运行和配置优先级不一 致;如果配置的优先级数值大于2,则运行和配置优先级一致。

表6-5 配置交换机的优先级

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置交换机的优先级	priority value	缺省情况下,交换机的优先级为128

6.6 配置允许的域ID范围

配置允许的域 ID 范围对交换机的影响如下:

- 主交换机:只能从允许的域 ID 范围内分配域 ID。如果配置的允许域 ID 范围不包含已分配的 域 ID 和本地配置的域 ID, 配置均会失败。
- 非主交换机:手工配置的域 ID 必须在允许的域 ID 范围内,否则会配置失败。
- 主交换机为本交换机分配的域 ID 必须在允许的域 ID 范围内,否则不接受所分配的域 ID,并 隔离连接主交换机的接口。如果交换机当前运行时域 ID(动态分配或者手工指定域 ID 后,交 换机实际使用的域 ID)不在新配置的允许的域 ID 范围内时,将导致配置失败。

建议一个 VSAN 内所有交换机配置相同的允许域 ID 范围。

表6-6 配置允许的域 ID 范围

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置交换机允许的域ID范围	allowed-domain-id domain-id-list	缺省情况下,允许的域ID范围为1~239

6.7 配置域ID

在不同情况下,配置的域 ID 含义不同:

- 在静态建立 Fabric 网络的情况下,配置的域 ID 就是交换机的域 ID。
- 在动态建立 Fabric 网络的情况下,配置的域 ID 表示交换机想要获取的域 ID。

静态建立 Fabric 网络时,必须为每台交换机手工配置域 ID。

动态建立 Fabric 网络时,可以配置交换机想要获取的域 ID,但最后实际分配到的域 ID 可能和配置的域 ID 不同。

配置的域 ID 分为 static 和 preferred 两种模式:

- 在静态建立 Fabric 网络时,两种模式没有区别。
- 在动态建立 Fabric 网络时,如果非主交换机向主交换机请求分配自己想要获取的域 ID 失败, preferred 模式下,非主交换机可以使用主交换机分配的其它域 ID; static 模式下,非主交换 机将隔离上游主链路,不使用主交换机分配的其它域 ID。

建议一个 VSAN 内所有交换机配置相同模式的域 ID。

表6-7 配置域 ID

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置交换机的域ID	domain-id domain-id { preferred static }	缺省情况下,交换机的域ID为0,采用 preferred模式

6.8 配置FC地址持久化功能

FC 地址持久化功能是指通过手工配置或自动生成的方式,将 N_Port/NP_Port 的 WWN 与 FC 地址 形成绑定关系,这样当 N_Port/NP_Port 上线后,便会获得绑定后的 FC 地址。我们将这种绑定关 系称为 FC 地址持久化表项,该表项又分为以下两种:

- 静态 FC 地址持久化表项:只能通过手工配置生成。
- 动态 FC 地址持久化表项:既可通过手工配置生成,也可自动生成。自动生成是指,当节点上 线并获得 FC 地址后,系统会自动将该节点的 WWN 与该 FC 地址形成绑定关系并写入设备, 只要用户保存了配置,设备重启后该节点上线时便能获得该 FC 地址。

🕑 说明

- 每个 N_Port/NP_Port 只能绑定一个 FC 地址,一个 FC 地址也只能与一个 N_Port/NP_Port 绑定。
- 要绑定的 N_Port/NP_Port 如果已 Login 并分配了其它 FC 地址,或者要绑定的 FC 地址已被分 配给其它 N_Port/NP_Port,则不允许将二者绑定。
- 只有开启了 FC 地址持久化功能后,手工配置的 FC 地址持久化表项才能生效。

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
开启FC地址持久化功能	fcid persistent enable	缺省情况下,FC地址持久化功能处于开启状态
(可选)配置 FC 地址持久 化表项	wwn wwn-value fcid fcid-value [dynamic]	缺省情况下,不存在手工配置的FC地址持久化表项

表6-8 配置 FC 地址持久化功能

6.9 配置VSAN下的最大登录节点数

用户可以配置 VSAN 下的最大登录节点数,以防止某 VSAN 下的登录节点过多,占用大量的 ACL 资源。这里的登录节点数=交换机直连的 NPV 交换机的数+登录到本交换机上的服务器和磁盘数。

如果已登录节点数大于配置的最大登录节点数,不会将已登录节点强制下线,但后续任何新节点均 无法登录。用户可以通过手工关闭接口等方式将不需要的节点下线。

需要注意的是,登录节点数即受本配置、也受硬件 ACL 资源的限制,当硬件 ACL 资源耗尽时,新 节点也无法登录。

表6-9 配置 VSAN 下的最大登录节点数

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置VSAN下的最大登录节点数	fc login-limit max-number	缺省情况下,不限制VSAN下的最大登录节 点数

6.10 配置Fabric定时器

用户可以配置如下 Fabric 定时器的取值:分布式服务超时时间、错误检测超时时间、资源分配超时时间。关于这些 Fabric 定时器的详细介绍请参见 FC 相关的协议规范。

对 Fabric 定时器的配置有两种方式:

- 在系统视图下配置:对所有 VSAN 生效。
- 在 VSAN 视图下配置: 对单个 VSAN 生效。

如果在系统视图和 VSAN 视图下均进行配置,则采用 VSAN 视图下的配置值。

表6-10 在系统视图下配置 Fabric 定时器

操作	命令	说明
进入系统视图	system-view	-
配置全局分布式服务超时时间	fc timer distributed-services value	缺省情况下,分布式服务超时时间为 5000毫秒
配置全局错误检测超时时间	fc timer error-detect value	缺省情况下,错误检测超时时间为 2000毫秒
配置全局资源分配超时时间	fc timer resource-allocation value	缺省情况下,资源分配超时时间为 10000毫秒

表6-11 在 VSAN 视图下配置 Fabric 定时器

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置指定VSAN内的分布式服务 超时时间	timer distributed-services value	缺省情况下,分布式服务超时时间为 5000毫秒
配置指定VSAN内的错误检测超 时时间	timer error-detect value	缺省情况下,错误检测超时时间为 2000毫秒

操作	命令	说明
配置指定VSAN内的资源分配超 时时间	timer resource-allocation value	缺省情况下,资源分配超时时间为 10000毫秒

6.11 配置Fabric重配置



只有开启 Fabric 配置功能, Fabric 重配置功能才生效。

Fabric 重配置一般在网络改造(比如两个 Fabric 网络合并等)或外部干预(比如管理员通过命令行 发起重配置)时发生。Fabric 重配置将触发整个网络重新开始主交换机选举、域 ID 分配和 FC 地址 分配。

Fabric 重配置分为两种:中断重配置、非中断重配置。

- 中断重配置:在整个 Fabric 中洪泛 RCF (Reconfigure Fabric)报文,通知所有交换机进行 中断重配置。重配置过程中,会清除所有运行数据重新进行协商,因此整个 Fabric 网络的数 据传输都会中断。
- 非中断重配置:在整个 Fabric 中洪泛 BF (Build Fabric)报文,通知所有交换机进行非中断 重配置。重配置过程中,会尽量保留上一次的运行数据,以保证交换机的域 ID 尽量不发生变 化,从而不影响 Fabric 网络的数据传输。

根据触发条件不同,可将 Fabric 重配置分为两种:自动重配置、手工发起重配置。触发场景如下:

- 自动中断重配置:两个 Fabric 网络合并时,如果域 ID 列表重叠,交换机会自动进行中断重配置。
- 自动非中断重配置:两个 Fabric 网络合并时,如果两个 Fabric 网络的主交换机信息不同,而 且域 ID 列表非空且不重叠,系统会自动进行非中断重配置。主交换机宕机时,系统会自动进 行非中断重配置。
- 手工中断重配置:当两个 Fabric 网络合并时接口被隔离或者修改了交换机的优先级等情况下, 管理员可以手工发起中断重配置,触发整个 Fabric 网络重新进行配置。

表6-12 配置自动 Fabric 重配置功能

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
开启自动Fabric重配置功能	domain auto-reconfigure enable	缺省情况下,自动Fabric重配置功能 处于关闭状态

表6-13 手工发起 Fabric 重配置

操作	命令	说明
进入系统视图	system-view	-

操作	命令	说明
进入VSAN视图	vsan vsan-id	-
发起Fabric重配置	domain restart [disruptive]	-

6.12 配置接口拒绝收到的RCF请求报文

在一个稳定的网络中,可以配置接口拒绝收到的特定 VSAN 内的 RCF 请求报文,以防止交换机进行不必要的中断重配置。配置该功能后,如果接口收到该 VSAN 内的 RCF 请求报文,交换机会回应拒绝报文,并将该接口隔离。

表6-14 配置接口拒绝收到的 RCF 请求报文

操作	命令	说明
进入系统视图	system-view	-
进入VFC接口视图	interface vfc interface-number	-
配置当前接口拒绝收到的RCF 请求报文	fc domain rcf-reject vsan vsan-id	缺省情况下,接口不拒绝收到的RCF 请求报文

6.13 开启Fabric告警功能

开启 Fabric 模块或名称服务相关的告警功能后,该模块会生成告警信息,用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块,通过设置 SNMP 中告警信息的发送参数,来决定告警信息输出的相关属性。有关告警信息的详细介绍,请参见"网络管理和监控配置指导"中的"SNMP"。

表6-15 开启 Fabric 告警功能

操作	命令	说明
进入系统视图	system-view	-
开启Fabric模块的告警功能	snmp-agent trap enable fc-fabric [domain-id-change fabric-change] *	缺省情况下,Fabric模块的所有 告警功能均处于关闭状态
开启名称服务相关的告警 功能	snmp-agent trap enable fc-name-service [login logout] *	缺省情况下,名称服务相关的所 有告警功能均处于关闭状态

6.14 配置RSCN聚合功能

6.14.1 RSCN 功能简述

Fabric 网络中,交换机上保存了整个 Fabric 网络的名称服务数据信息,既包括本地注册的节点设备 信息,也包括远端交换机上的节点设备信息。当节点设备发生注册、注销或改变注册数据等变化事 件时,交换机使用 RSCN(Registered State Change Notification,注册状态变化通知)报文,向 交换机或节点设备来进行变化通知。交换机或节点设备收到 RSCN 报文后,会主动发送名称服务查 询报文,进行表项更新。

RSCN 报文分为交换机之间通知变化的 SW_RSCN 报文,以及交换机通知本机直连节点设备的 ELS_RSCN 报文。RSCN 报文仅携带当前发生变化的节点设备的 FC 地址,进行变化通告,而并不 实际同步数据。

当变化事件发生时,交换机感应该变化,使用 ELS_RSCN 报文通知其它本地直连且关心该变化的 节点设备,触发节点设备向交换机查询数据进行更新;同时,交换机发送 SW_RSCN 报文通知其 它路由可达的交换机,其它交换机在收到 SW_RSCN 报文后,响应变化,主动查询、更新数据, 并使用 ELS_RSCN 报文通知各自本地直连且关心该变化的节点设备,最终完成变化数据的全网通 知和数据更新。



交换机是否支持 SW_RSCN 通知取决于路由计算完成后,交换机之间进行的 ESS(Exchange Switch Support,交换机能力协商)协商;而节点设备是否响应 ELS_RSCN 报文,取决于在节点 设备注册成功后,是否发送 SCR(State Change Registration,状态变化注册)报文向交换机注册 关心响应。

6.14.2 RSCN 聚合功能介绍

随着节点设备的规模增大,网络中存在大量节点设备的情况下,当远端或本机有多个节点设备同时 发生注册、注销或改变注册数据等变化事件时,对于每一个发生变化的节点设备,都需要通知一次 其它关心该变化的节点设备,对应发送携带一个变化 FC 地址(发生变化的节点设备的 FC 地址) 的 RSCN 报文。因此有可能短时间内向关心该变化的节点设备发送大量 RSCN 报文,导致网络拥 塞,设备的传输和处理性能急剧降低。

对于交换机发送给节点设备的 ELS_RSCN 报文,可以开启 RSCN 聚合功能来优化网络性能:如果 在 RSCN 聚合等待时间内,有多个节点设备产生变化事件,则使用携带了多个变化 FC 地址的一个 ELS_RSCN 报文,来代替以前只携带一个变化 FC 地址的多个 ELS_RSCN 报文,以此减少向关心 该变化的节点设备发送 ELS_RSCN 报文的数量,减少变化通知次数。

6.14.3 配置 RSCN 聚合功能

开启 RSCN 聚合功能后,用户可以根据设备性能调整 RSCN 聚合的等待时间,以此控制设备响应 RSCN 变化的频率。

需要注意的是,只有开启 RSCN 聚合功能后,RSCN 聚合等待时间才会生效。建议一个 VSAN 内的所有交换机同时开启 RSCN 聚合功能,并配置相同的 RSCN 聚合等待时间,以避免可能产生的设备互通问题。

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-

表6-16 配置 RSCN 聚合功能

操作	命令	说明
开启RSCN聚合功能	rscn aggregation enable	缺省情况下,RSCN聚合功能处于关闭状态
配置RSCN聚合等待时间	rscn aggregation timer value	缺省情况下,RSCN聚合等待时间为2000毫秒

6.15 配置和探测发现节点设备的FC4信息

大部分节点设备连入 Fabric 网络时,会先携带一些基础信息(例如 Port WWN、Node WWN、期 望得到的 FC 地址等)登录到交换机,待交换机为之分配 FC 地址后,节点设备会继续发送名称服 务的节点属性注册报文,注册节点设备的其它一系列扩展信息,其中就包括 FC4 信息。

FC4 信息描述了节点设备支持的上层协议类型,以及协议对应的属性。FC4 信息包括如下内容:

- FC4-Type: FC4 层协议类型, 描述了节点设备支持的上层协议, 包括 SCSI-FCP、IP、SNMP、 NPV 等。
- Feature: FC4 层协议的属性。每种 FC4-Type 拥有四种属性,每种属性的具体含义由各 FC4-Type 分别定义。

关于各种 FC4-Type 及其 Feature 的详细介绍请查看相关的协议文档。用户可以在交换机上通过 display fc name-service database 命令查看名称服务数据库中记录的节点设备的 FC4 信息。

节点设备在 Fabric 网络中进行互通时,会首先向交换机获取所有支持 SCSI-FCP 协议的节点信息,然后根据这些节点支持 SCSI-FCP 协议的 Feature 值,来决定具体的互通行为。

一般情况下,服务器连入Fabric 网络时,会注册支持 SCSI-FCP 协议,同时注册 Feature 为 Initiator, 而磁盘设备连入 Fabric 网络时也会注册支持 SCSI-FCP 协议,同时注册 Feature 为 Target,这样服 务器就能向交换机获取支持 SCSI-FCP 协议的节点信息,并根据 SCSI-FCP 的 Feature 值决定哪些 节点属于磁盘设备,能够发送访问请求,进行设备互通。

6.15.1 配置 Fabric 自动发现 SCSI-FCP 信息功能

某些节点设备有时不会主动注册支持 SCSI-FCP 协议(比如节点设备离线又重新上线后,不再主动 注册 FC4-Type 或 Feature),也因此没有 SCSI-FCP 协议对应的 Feature 值,对节点设备间的互通 可能产生影响。

Fabric 自动发现 SCSI-FCP 信息功能可以主动获取节点设备的 SCSI-FCP 协议及其对应的 Feature 值,开启该功能后,FCF 交换机在节点设备登录后,会主动向节点设备发送 PRLI 报文,询问节点 设备是否支持 SCSI-FCP 协议,同时获取节点设备支持 SCSI-FCP 协议对应的 Feature 信息,并将 此信息保存在名称服务数据库中。

需要注意的是,开启 Fabric 自动发现 SCSI-FCP 信息功能后,某些较老型号的网卡可能不会再向交换机自动注册节点设备信息。请用户根据实际情况选择是否开启本功能。

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
开启Fabric自动发现SCSI-FCP信	fc name-service auto-discovery	

表6-17 配置 Fabric 自动发现 SCSI-FCP 信息功能

操作	命令	说明
息功能		SCSI-FCP信息功能处于开启状态

6.15.2 配置节点设备的默认 FC4 信息

为了不影响节点设备之间的互通,用户可以手工配置节点设备的默认 FC4 信息 (FC4-Type 和 Feature)。当节点设备不注册 FC4 信息并且交换机主动探测 SCSI-FCP 信息也不成功时,名称服 务数据库中记录的将是该默认 FC4 信息。此后,如果节点设备又主动注册了 FC4 信息或交换机又 探测到了 SCSI-FCP 信息,则名称服务数据库中将保存节点设备注册或交换机探测到的 FC4 信息。 配置本命令时,每条配置命令只能表示某个 N_Port 支持的一种 FC4-Type 及其 Feature,如果该 N_Port 还支持其它 FC4-Type 及其 Feature,则需要再配置一条命令。

表6-18 配置节点设备的默认 FC4 信息

操作	命令	说明
进入系统视图	system-view	-
配置节点设备的默认 FC4信息	<pre>fc wwn wwn-value default-fc4-type { type-value feature feature-map scsi-fcp feature { feature-map both initiator target } }</pre>	缺省情况下,未配置节点设 备的默认FC4信息

6.16 开启Smart SAN功能

6.16.1 Smart SAN 简介

随着 SAN 网络的广泛应用, SAN 网络的管理、诊断和部署的需求越来越多, 面对的一些问题也逐渐暴露出来。SAN 网络急需进行协议架构的完善和革新, 使用新的技术方案推动其发展, 满足用户 在智能化、简单化、可维护、可诊断、自我修复等方面越来越迫切的需求。

Smart SAN 是由 UNIS 提出的 SAN 网络配置与管理解决方案。Smart SAN 一方面将增强 SAN 网络的可管理性,另一方面又会大大简化用户的操作,为 SAN 网络的广泛部署奠定基础。它采用分布式的框架结构,部署于包括存储设备、服务器和交换机在内的所有 SAN 网络对象上。其中,交换机主要完成如下工作:

- 搜集服务器与存储设备的信息,为服务器与存储设备之间的发现提供依据;
- 控制服务器与存储设备之间的访问,实现 Zone 的自动化配置,包括 Peer Zone 的创建和删除, 为 Peer Zone 添加成员,将 Peer Zone 加入 Zone set 并激活 Zone set;
- 搜集服务器与存储设备的诊断信息,为监控网络环境、诊断网络问题提供参考;
- 控制服务器与存储设备的自动化登录。

6.16.2 开启 Smart SAN 功能

Smart SAN 功能包含两种应用类型:FC/FCoE 类型和 iSCSI 类型。iSCSI 类型暂不支持。

如果交换机需要支持基于 FC/FCoE 协议标准的 Smart SAN 功能,则需要在该交换机上开启 Smart SAN 功能并指定其应用类型为 FC/FCoE 类型。完成此配置后,该交换机会通知 FDMI(Fabric Device Management Interface, Fabric 设备管理接口)和 FC Zone 模块进行相应的处理:

- FDMI 模块会启动一个定时器,定期向登录交换机的节点设备发送 RDP (Read Diagnostic Parameters,诊断参数读取请求)请求报文获取节点设备的诊断信息,更新本地接口的诊断信息,并向其它交换机发送同步 RDP 数据库信息的 ADP (Add Diagnostic Parameter,增加 诊断信息)同步报文。
- FC Zone 模块自动配置每个 VSAN 工作在增强 Zone 模式。

表6-19 开启 Smart SAN 功能

操作	命令	说明
进入系统视图	system-view	-
开启Smart SAN功能并指 定其应用类型	smartsan enable [fcoe iscsi]	缺省情况下, Smart SAN功能处 于关闭状态
配置RDP请求报文的发送 时间间隔	rdp request-polling-interval interval	缺省情况下,发送RDP请求报 文的时间间隔是30分钟 只有开启Smart SAN功能并指 定其应用类型为FC/FCoE类型 后,交换机才支持配置RDP请

6.17 Fabric网络显示和维护

在完成上述配置后,在任意视图下执行 **display** 命令可以显示配置后 **Fabric** 网络的运行情况,通过 查看显示信息验证配置的效果。

表6-20 Fabric 网络显示和维护

操作	命令
显示VSAN内的域信息	display fc domain [vsan vsan-id]
显示VSAN内动态分配的域列表	display fc domain-list [vsan vsan-id]
显示Fabric定时器信息	display fc timer [distributed-services error-detect resource-allocation] [vsan vsan-id]
显示本交换机的WWN	display fc switch-wwn
显示节点注册的相关信息	display fc login [vsan vsan-id] [count]
显示N端口注册的SCR列表	display fc scr-table [vsan vsan-id] [count]
显示名称服务数据库信息	display fc name-service database [vsan <i>vsan-id</i> [fcid fcid]] [verbose] display fc name-service database [vsan <i>vsan-id</i>] count
显示ESS协商结果	display fc ess [vsan vsan-id]
显示FC地址的分配情况	display fcid allocation [vsan vsan-id]
显示FC地址持久化表项	display fcid persistent [unused] [vsan vsan-id]

操作	命令
显示RDP数据库信息	display rdp database [port-name port-name]
显示RDP请求报文的发送时间间 隔	display rdp request-polling-interval
显示Smart SAN的状态信息	display smartsan status
清除FC地址持久化表项	reset fcid persistent [static] [vsan vsan-id]

6.18 建立Fabric网络典型配置举例

6.18.1 静态建立 Fabric 网络配置举例

1. 组网需求

网络由两台交换机 Switch A、Switch B,和磁盘设备 Disk、服务器 Server 组成。 网络结构比较简单,采用静态方式建立 Fabric 网络。

2. 组网图

图6-2 静态建立 Fabric 网络组网图



3. 配置步骤



本例中只列出建立 Fabric 网络的相关配置,其它配置步骤略。

(1) 配置 Switch A

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view

[SwitchA] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchA] save

[SwitchA] quit

<SwitchA> reboot

#关闭 Fabric 配置功能并把交换机模式配置为 FCF 模式。

<SwitchA> system-view

[SwitchA] fcoe-mode fcf

[SwitchA] vsan 1

[SwitchA-vsan1] undo domain configure enable

配置 Fabric 网络的名称。

[SwitchA-vsan1] fabric-name 11:11:11:11:11:11:11:11

配置域 ID 为 1。

[SwitchA-vsan1] domain-id 1 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[\rm Y/N]:y$

[SwitchA-vsan1] quit

创建 VFC 1 接口, 配置 VFC 1 接口工作在 F 模式,将 VFC 1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC 1 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1的报 文通过 VFC 1 接口。

[SwitchA] interface vfc 1

[SwitchA-Vfc1] fc mode f

[SwitchA-Vfc1] bind interface ten-gigabitethernet1/0/1

[SwitchA-Vfc1] port trunk vsan 1

[SwitchA-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 20 的报文通过。

[SwitchA] vlan 20

[SwitchA-Vlan20] quit

[SwitchA] interface ten-gigabitethernet1/0/1

[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 20

[SwitchA-Ten-GigabitEthernet1/0/1] quit

创建 VFC 2 接口, 配置 VFC 2 接口工作在 E 模式,将 VFC 2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2 上,并将 VFC 2 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报 文通过 VFC 2 接口。

[SwitchA] interface vfc 2

[SwitchA-Vfc2] fc mode e

[SwitchA-Vfc2] bind interface ten-gigabitethernet1/0/2

[SwitchA-Vfc2] port trunk vsan 1

[SwitchA-Vfc2] quit

配置以太网接口 Ten-GigabitEthernet1/0/2 允许 VLAN 20 的报文通过。

[SwitchA] vlan 20

[SwitchA-Vlan20] quit

[SwitchA] interface ten-gigabitethernet1/0/2

[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 20

[SwitchA-Ten-GigabitEthernet1/0/2] quit

开启 VLAN 20 的 FCoE 功能,并将其与 VSAN 1 进行映射。

[SwitchA] vlan 20

[SwitchA-vlan20] fcoe enable vsan 1

[SwitchA-vlan20] quit

#缺省情况下,服务器和磁盘设备属于默认 Zone,为了实现两者互通,需要配置允许默认 Zone内的成员互相访问。关于 Zone 的介绍,请参见"<u>8 FC Zone"</u>。

[SwitchA] vsan 1

[SwitchA-vsan1] zone default-zone permit

[SwitchA-vsan1] quit

(2) 配置 Switch B

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchB> system-view

[SwitchB] system-working-mode advance

Do you want to change the system working mode? $[\ensuremath{\mathtt{Y}}/\ensuremath{\mathtt{N}}]\ensuremath{:}\ensuremath{\mathtt{y}}$

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchB] save

[SwitchB] quit

<SwitchB> reboot

#关闭 Fabric 配置功能并把交换机模式配置为 FCF 模式。

<SwitchB> system-view

[SwitchB] fcoe-mode fcf

[SwitchB] vsan 1

[SwitchB-vsan1] undo domain configure enable

配置 Fabric 网络的名称。

[SwitchA-vsan1] fabric-name 11:11:11:11:11:11:11:11

配置域 ID 为 2。

[SwitchB-vsan1] domain-id 2 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[\rm Y/N]:y$

[SwitchB-vsan1] quit

创建 VFC 1 接口, 配置 VFC 1 接口工作在 F 模式,将 VFC 1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC 1 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1的报 文通过 VFC 1 接口。

[SwitchB] interface vfc 1 [SwitchB-Vfc1] fc mode f [SwitchB-Vfc1] bind interface ten-gigabitethernet1/0/1 [SwitchB-Vfc1] port trunk vsan 1 [SwitchB-Vfc1] guit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 20 的报文通过。

[SwitchB] vlan 20

[SwitchB-Vlan20] quit

[SwitchB] interface ten-gigabitethernet1/0/1

[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 20

[SwitchB-Ten-GigabitEthernet1/0/1] quit

创建 VFC 2 接口, 配置 VFC 2 接口工作在 E 模式,将 VFC 2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2 上,并将 VFC 2 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报 文通过 VFC 2 接口。

[SwitchB] interface vfc 2 [SwitchB-Vfc2] fc mode e [SwitchB-Vfc2] bind interface ten-gigabitethernet1/0/2 [SwitchB-Vfc2] port trunk vsan 1 [SwitchB-Vfc2] quit # 配置以太网接口 Ten-GigabitEthernet1/0/2 允许 VLAN 20 的报文通过。

[SwitchB] vlan 20

[SwitchB-Vlan20] quit

[SwitchB] interface ten-gigabitethernet1/0/2

[SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk

[SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 20

[SwitchB-Ten-GigabitEthernet1/0/2] quit

开启 VLAN 20 的 FCoE 功能,并将其与 VSAN 1 进行映射。

[SwitchB] vlan 20

[SwitchB-vlan20] fcoe enable vsan 1

[SwitchB-vlan20] quit

#缺省情况下,服务器和磁盘设备属于默认 Zone,为了实现两者互通,需要配置允许默认 Zone内的成员互相访问。关于 Zone 的介绍,请参见 "8 FC Zone"。

[SwitchB] vsan 1

[SwitchB-vsan1] zone default-zone permit

[SwitchB-vsan1] quit

4. 验证配置

(1) 验证 Switch A

[SwitchA-vsan1] display fc domain vsan 1 Domain Information of VSAN 1:

Running time information:

```
State: Stable
Switch WWN: 48:33:43:2d:46:43:1A:1A
Fabric name: 11:11:11:11:11:11:11:11
Priority: 128
Domain ID: 1
Configuration information:
Domain configure: Disabled
Domain auto-reconfigure: Disabled
Fabric name: 11:11:11:11:11:11:11:11
Priority: 128
Domain ID: 1 (static)
Principal switch running time information:
Priority: 128
```

No interfaces available. 上述信息表明,域配置已经结束,SwitchA的运行域ID是1。

(2) 验证 Switch B

[SwitchB-vsan1] display fc domain vsan 1 Domain Information of VSAN 1:

Running time information: State: Stable Switch WWN: 48:33:43:2d:46:43:1B:1B

```
Fabric name: 11:11:11:11:11:11:11:11
```

```
Priority: 128
Domain ID: 2
Configuration information:
Domain configure: Disabled
Domain auto-reconfigure: Disabled
Fabric name: 11:11:11:11:11:11:11:11
Priority: 128
Domain ID: 2 (static)
Principal switch running time information:
Priority: 128
```

No interfaces available. 上述信息表明,域配置已经结束, Switch B 的运行域 ID 是 2。

6.18.2 动态建立 Fabric 网络配置举例

1. 组网需求

网络由交换机 Switch A、Switch B、Switch C、Switch D, 和磁盘设备 Disk、服务器 Server 组成。 网络结构比较复杂,采用动态方式建立 Fabric 网络。

2. 组网图

图6-3 动态建立 Fabric 网络组网图



3. 配置步骤



本例中只列出建立 Fabric 网络的相关配置,其它配置步骤略。

(1) 配置 Switch A

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view

[SwitchA] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the system to make it effective.

[SwitchA] save [SwitchA] quit <SwitchA> reboot #开启 Fabric 配置功能(本步骤可选, Fabric 配置功能缺省开启),并把交换机模式配置为 FCF 模 式。 <SwitchA> system-view [SwitchA] fcoe-mode fcf [SwitchA] vsan 1 [SwitchA-vsan1] domain configure enable # 配置域 ID 为 11。 [SwitchA-vsan1] domain-id 11 preferred Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? [Y/N]:y [SwitchA-vsan1] quit #开启 VLAN 10 的 FCoE 功能、并将其与 VSAN 1 进行映射。 [SwitchA] vlan 10 [SwitchA-vlan10] fcoe enable vsan 1 [SwitchA-vlan10] quit # 创建 VFC 2 接口并将其与物理端口 Ten-GigabitEthernet1/0/2 绑定:将 VFC 2 接口配置为 E 模式、 并以 Trunk 方式加入 VSAN 1。 [SwitchA] interface Vfc 2 [SwitchA-Vfc2] bind interface ten-gigabitethernet1/0/2 [SwitchA-Vfc2] fc mode e [SwitchA-Vfc2] port trunk vsan 1 [SwitchA-Vfc2] quit # 创建 VFC 1 接口并将其与物理端口 Ten-GigabitEthernet1/0/1 绑定;将 VFC 1 接口配置为 E 模式、 并以 Trunk 方式加入 VSAN 1。 [SwitchA] interface Vfc 1 [SwitchA-Vfc1] bind interface ten-gigabitethernet1/0/1 [SwitchA-Vfc1] fc mode e [SwitchA-Vfc1] port trunk vsan 1 [SwitchA-Vfc1] guit #缺省情况下,服务器和磁盘设备属于默认 Zone,为了实现两者互通,需要配置允许默认 Zone 内 的成员互相访问。关于 Zone 的介绍,请参见"<u>8 FC Zone"</u>。 [SwitchA] vsan 1 [SwitchA-vsan1] zone default-zone permit [SwitchA-vsan1] quit (2) 配置 Switch B # 配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。 <SwitchB> system-view [SwitchB] system-working-mode advance Do you want to change the system working mode? [Y/N]:y The system working mode is changed, please save the configuration and reboot the system to make it effective. [SwitchB] save [SwitchB] quit

<SwitchB> reboot

#开启 Fabric 配置功能(本步骤可选, Fabric 配置功能缺省开启),并把交换机模式配置为 FCF 模式。

<SwitchB> system-view

[SwitchB] fcoe-mode fcf

[SwitchB] vsan 1

[SwitchB-vsan1] domain configure enable

配置交换机的优先级为 1,使 Switch B 成为主交换机。

[SwitchB-vsan1] priority 1

[SwitchB-vsan1] quit

#开启 VLAN 10 的 FCoE 功能、并将其与 VSAN 1 进行映射。

[SwitchB] vlan 10

[SwitchB-vlan10] fcoe enable vsan 1

[SwitchB-vlan10] quit

创建 VFC 1 接口并将其与物理端口 Ten-GigabitEthernet1/0/1 绑定;将 VFC 1 接口配置为 E 模式、

并以 Trunk 方式加入 VSAN 1。

[SwitchB] interface Vfc 1

[SwitchB-Vfc1] bind interface ten-gigabitethernet1/0/1

[SwitchB-Vfc1] fc mode e

[SwitchB-Vfc1] port trunk vsan 1

[SwitchB-Vfc1] quit

#创建VFC2接口并将其与物理端口Ten-GigabitEthernet1/0/2绑定;将VFC2接口配置为E模式、

并以 Trunk 方式加入 VSAN 1。

[SwitchB] interface Vfc 2

[SwitchB-Vfc2] bind interface ten-gigabitethernet1/0/2

[SwitchB-Vfc2] fc mode e

[SwitchB-Vfc2] port trunk vsan 1

[SwitchB-Vfc2] quit

#创建VFC3接口并将其与物理端口Ten-GigabitEthernet1/0/3绑定;将VFC3接口配置为E模式、

并以 Trunk 方式加入 VSAN 1。

[SwitchB] interface Vfc 3

[SwitchB-Vfc3] bind interface ten-gigabitethernet1/0/3

[SwitchB-Vfc3] fc mode e

[SwitchB-Vfc3] port trunk vsan 1

[SwitchB-Vfc3] quit

#缺省情况下,服务器和磁盘设备属于默认 Zone,为了实现两者互通,需要配置允许默认 Zone 内的成员互相访问。关于 Zone 的介绍,请参见"<u>8 FC Zone"</u>。

[SwitchB] vsan 1

[SwitchB-vsan1] zone default-zone permit

[SwitchB-vsan1] quit

(3) 配置 Switch C

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。 <SwitchC> system-view

Switcene, Sybtem view

[SwitchC] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the system to make it effective. [SwitchC] save [SwitchC] quit <SwitchC> reboot #开启 Fabric 配置功能(本步骤可选, Fabric 配置功能缺省开启),并把交换机模式配置为 FCF 模 式。 <SwitchC> system-view [SwitchC] fcoe-mode fcf [SwitchC] vsan 1 [SwitchC-vsan1] domain configure enable # 配置域 ID 为 13。 [SwitchC-vsan1] domain-id 13 preferred Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? [Y/N]:y #开启 VLAN 10 的 FCoE 功能、并将其与 VSAN 1 进行映射。 [SwitchC] vlan 10 [SwitchC-vlan10] fcoe enable vsan 1 [SwitchC-vlan10] quit # 创建 VFC 1 接口并将其与物理端口 Ten-GigabitEthernet1/0/1 绑定:将 VFC 1 接口配置为 F 模式、 并以 Trunk 方式加入 VSAN 1。 [SwitchC] interface Vfc 1 [SwitchC-Vfc1] bind interface ten-gigabitethernet1/0/1 [SwitchC-Vfc1] fc mode f [SwitchC-Vfc1] port trunk vsan 1 [SwitchC-Vfc1] quit # 创建 VFC 2 接口并将其与物理端口 Ten-GigabitEthernet1/0/2 绑定:将 VFC 2 接口配置为 E 模式、 并以 Trunk 方式加入 VSAN 1。 [SwitchC] interface Vfc 2 [SwitchC-Vfc2] bind interface ten-gigabitethernet1/0/2 [SwitchC-Vfc2] fc mode e [SwitchC-Vfc2] port trunk vsan 1 [SwitchC-Vfc2] quit #创建VFC3接口并将其与物理端口Ten-GigabitEthernet1/0/3绑定;将VFC3接口配置为E模式、 并以 Trunk 方式加入 VSAN 1。 [SwitchC] interface Vfc 3 [SwitchC-Vfc3] bind interface ten-gigabitethernet1/0/3 [SwitchC-Vfc3] fc mode e [SwitchC-Vfc3] port trunk vsan 1 [SwitchC-Vfc3] quit #缺省情况下,服务器和磁盘设备属于默认 Zone,为了实现两者互通,需要配置允许默认 Zone 内 的成员互相访问。关于 Zone 的介绍,请参见"8 FC Zone"。 [SwitchC] vsan 1 [SwitchC-vsan1] zone default-zone permit [SwitchC-vsan1] quit (4) 配置 Switch D

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchD> system-view

[SwitchD] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchD] save

[SwitchD] quit

<SwitchD> reboot

#开启 Fabric 配置功能(本步骤可选, Fabric 配置功能缺省开启),并把交换机模式配置为 FCF 模式。

<SwitchD> system-view

[SwitchD] fcoe-mode fcf

[SwitchD] vsan 1

[SwitchD-vsan1] domain configure enable

配置域 ID 为 14。

[SwitchD-vsan1] domain-id 14 preferred

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[Y/N]\!:\!y$

#开启 VLAN 10 的 FCoE 功能、并将其与 VSAN 1 进行映射。

[SwitchD] vlan 10

[SwitchD-vlan10] fcoe enable vsan 1

[SwitchD-vlan10] quit

#创建VFC1接口并将其与物理端口Ten-GigabitEthernet1/0/1绑定;将VFC1接口配置为F模式、

并以 Trunk 方式加入 VSAN 1。

[SwitchD] interface Vfc 1

[SwitchD-Vfc1] bind interface ten-gigabitethernet1/0/1

[SwitchD-Vfc1] fc mode f

[SwitchD-Vfc1] port trunk vsan 1

[SwitchD-Vfc1] quit

#创建VFC2接口并将其与物理端口Ten-GigabitEthernet1/0/2绑定;将VFC2接口配置为E模式、

并以 Trunk 方式加入 VSAN 1。

[SwitchD] interface Vfc 2

[SwitchD-Vfc2] bind interface ten-gigabitethernet1/0/2

[SwitchD-Vfc2] fc mode e

[SwitchD-Vfc2] port trunk vsan 1

[SwitchD-Vfc2] quit

#缺省情况下,服务器和磁盘设备属于默认 Zone,为了实现两者互通,需要配置允许默认 Zone 内的成员互相访问。关于 Zone 的介绍,请参见 "8 FC Zone"。

[SwitchD] vsan 1

[SwitchD-vsan1] zone default-zone permit

[SwitchD-vsan1] quit

4. 验证配置

在 Switch A 上进行验证。

#显示 VSAN 1 内的域信息。

```
[SwitchA-vsan1] display fc domain vsan 1
Domain Information of VSAN 1:
   Running time information:
       State: Stable
       Switch WWN: 48:33:43:2d:46:43:1A:1A
       Fabric name: 48:33:43:2d:46:43:1B:1B
       Priority: 128
       Domain ID: 11
   Configuration information:
       Domain configure: Enabled
       Domain auto-reconfigure: Disabled
       Fabric name: 48:33:43:2d:46:43:1A:1A
       Priority: 128
       Domain ID: 11 (preferred)
   Principal switch running time information:
       Priority: 1
   Path
                 Interface
   Upstream
                 Vfc1
                 Vfc2
   Downstream
从上述信息可以看出,Switch A的配置已经结束,主交换机为Switch A分配的域 ID为 11。
#显示 VSAN 1 内的域列表。
[SwitchA-vsan1] display fc domain-list vsan 1
Domain list of VSAN 1:
 Number of domains: 4
 Domain ID
                WWN
 0x01(5)
                48:33:43:2d:46:43:1B:1B [Principal]
 0x0b(11)
                48:33:43:2d:46:43:1A:1A [Local]
                48:33:43:2d:46:43:1C:1C
 0x0d(13)
 0x0e(14)
                48:33:43:2d:46:43:1D:1D
```

从上述信息可以看出,Switch B成为主交换机,主交换机给自己随机分配了一个域 ID 5。

7 FC 路由与转发

7.1 FC路由与转发简介

在 FC SAN 中进行路由选择和报文转发要使用 FCF 交换机,FCF 交换机根据所收到的报文的目的 地址选择一条合适的路径,并将报文转发到下一台 FCF 交换机。路径中最后的 FCF 交换机负责将 报文转发给目的节点。

路由就是报文在转发过程中的路径信息,用来指导报文转发。

7.1.1 路由表和 FIB 表

1. 路由表和 FIB 表简介

FCF 交换机通过路由表选择路由,把优选路由下发到 FIB(Forwarding Information Base,转发信息库)表中,通过 FIB 表指导报文转发。

每台 FCF 交换机的每个 VSAN 都对应着一张路由表和一张 FIB 表。

2. 路由表内容

路由表中保存了各种路由协议发现的路由,根据来源不同,分为以下几类:

- 直连路由:链路层协议发现的路由。
- 静态路由:网络管理员手工配置的路由。
- FSPF 路由: FSPF(Fabric Shortest Path First,光纤最短路径优先)协议发现的路由。

通过命令 display fc routing-table 可以显示路由表的摘要信息,例如:

```
<Sysname> display fc routing-table vsan 1
```

Routing Table: VSAN	1			
Destinations : 6	Rou	ites : 6		
Destination/mask	Protocol	Preference	Cost	Interface
0x020000/8	FSPF	20	265	Vfcl
0x120000/8	STATIC	10	0	Vfc2
0xfffc01/24	DIRECT	0	0	InLoop0
0xfffffa/24	DIRECT	0	0	InLoop0
0xffffc/24	DIRECT	0	0	InLoop0
0xfffffd/24	DIRECT	0	0	InLoop0

.....(省略部分显示信息)

路由表中包含了下列关键项:

- Destination: 目的地址。用来标识 FC 报文的目的 FC 地址。
- mask: 网络掩码。与目的地址一起来标识目的节点或 FCF 交换机所在域的地址。将目的地址和网络掩码"逻辑与"后可得到目的节点或 FCF 交换机所在域的地址。例如:目的地址为0x010001、掩码为 0xff0000 的节点或 FCF 交换机所在域的地址为 0x010000。掩码由若干个连续"1"构成,既可以用十六进制表示,也可以用掩码中连续"1"的个数来表示。
- Protocol: 协议类型。可以为 DIRECT(直连路由)、STATIC(静态路由)、FSPF(FSPF路由)。

- Preference:路由优先级。对于相同的目的地,直连路由、静态路由、FSPF可能会发现不同的路由,但这些路由并不都是最优的。为了判断最优路由,直连路由、静态路由、FSPF都被赋予了一个优先级,具有最高优先级的路由协议发现的路由将成为当前路由。直连路由的优先级为0,静态路由的优先级为10,FSPF的优先级为20。数值越小表明优先级越高。
- Cost: 路由的度量值。当到达同一目的地的多条路由具有相同的优先级时,路由的度量值越小的路由将成为当前的最优路由。直连路由的度量值为 0;静态路由、FSPF 路由的度量值可以配置。
- Interface:出接口。指明 FC 报文将从该 FCF 交换机哪个接口转发。

3. FIB 表内容

FIB 表中每条转发项都指明了要到达某 FCF 交换机或某节点的报文应通过 FCF 交换机的哪个物理 接口发送,就可到达该路径的下一台 FCF 交换机,或者目的节点。

通过命令 display fc fib 可以查看 FIB 表的信息,例如:

```
<Sysname> display fc fib vsan 1
FC FIB information in VSAN 1:
Destination count: 6
```

FIB entry count: 6

Destination/Mask	Interface
0x020000/8	Vfcl
0x120000/8	Vfc2
0xfffc01/24	InLoop0
0xffffa/24	InLoop0
0xffffc/24	InLoop0
0xffffd/24	InLoop0

FIB 表中包含的 Destination、Mask、Interface 关键项的含义与路由表中对应关键项的含义相同。

7.1.2 直连路由

直连路由的来源包括:知名地址、本机给直连的 N_Port 分配的 FC 地址。

- 对 FCF 交换机的访问通常使用知名地址,常见知名地址的用途介绍请参见"<u>16.2 附录 B Fabric</u> <u>知名地址</u>"。所有知名地址均作为直连路由加入路由表中,路由的目的地址为知名地址,掩码 为 0xfffff,出接口为 InLoop0。
- 在 FCF 交换机给直连的 N_Port 分配 FC 地址时添加该 FC 地址的直连路由到路由表中,路由的目的地址为分配的 FC 地址,掩码为 0xfffff,出接口为连接 N_Port 的 VFC 接口。

7.1.3 静态路由

静态路由是由管理员手工配置的。配置静态路由后,去往指定目的地的 FC 报文将按照管理员指定的路径进行转发。

在组网结构比较简单的网络中,只需配置静态路由就可以实现网络互通。恰当地设置和使用静态路 由可以改善网络的性能,并可为重要的网络应用保证带宽。

静态路由的缺点在于:不能自动适应网络拓扑结构的变化,当网络发生故障或者拓扑发生变化后,可能会出现路由不可达,导致网络中断,此时必须由网络管理员手工修改静态路由的配置。

静态路由支持等价路由,如果先后配置多条目的地址相同、出接口不同的静态路由且度量值相同,则生成等价路由。

7.1.4 FSPF 路由

FSPF 是一个基于链路状态的动态路由选择协议,它可以自动计算 Fabric 网络中任意两台交换机之间的最短路径。

FSPF 具有如下特点:

- 可用于任何组网。
- 支持等价路由。
- 基于每个 VSAN 进行拓扑计算。
- 只在 E 模式端口运行,提供无环路的拓扑。
- 在每个交换机上都有一个拓扑数据库,跟踪每条链路的状态。
- 使用 Dijkstra 算法计算路由。
- 网络拓扑改变时可以快速收敛。

1. FSPF 基本概念

在介绍 FSPF 的工作机制之前,先介绍几个基本概念。

(1) LSDB

LSDB(Link State Database,链路状态数据库)是交换机保存全网拓扑信息的数据库。在 LSDB 中,以 LSR(Link State Record,链路状态记录)的形式来存储各交换机的链路状态信息。

(2) LSR

LSR 完整地描述了一个交换机与其它直连交换机的所有链路状态信息。

交换机每次生成的 LSR,都统称为交换机生成的 LSR 实例,所有交换机产生的 LSR 构成 LSDB。 LSR 中可以包含一个或多个链路的描述信息。LSR 中的信息主要包括:

- LSR 的生存时间。
- 通告此 LSR 的交换机域 ID。
- LSR 实例号:每刷新一次 LSR,实例号加一。
- 链路 ID: 用来标识链路。链路 ID 中包含链路对端的邻居交换机的域 ID。
- 链路的源接口和目的接口。
- 链路的类型。例如点对点连接。
- 链路上传输报文的开销。每一条链路会有不同的开销,接口开销越小说明链路越好。在路由 优选算法中将使用这些值来确定最有效的路由。接口的开销值可以配置。

2. FSPF 报文类型

FSPF 中用到如下协议报文:

- Hello 报文:周期性发送,用来发现和维持 FSPF 邻居关系。
- LSU(Link State Update,链路状态更新)报文:用于向邻居交换机通告本机的链路状态信息,即每次报文交互时通过它来携带 LSR 的详细信息。
- LSA(Link State Acknowledgment,链路状态确认)报文:对接收到的LSR做确认回应。接收到LSU后,需要对其中的LSR以LSA报文进行确认,否则邻居将重传该LSR。

3. FSPF 工作机制

FSPF 工作机制可简单描述如下:

- 交换机周期性向外发送 Hello 报文,与其它交换机建立邻居关系。
- 建立邻居关系之后,交换机之间开始进行 LSDB 的初始化同步,即交换彼此 LSDB 中的所有 LSR。通过 LSU 报文来携带 LSR, LSA 报文来确认 LSR 的接收。
- LSDB 初始化同步完成之后,每台交换机存储的 LSDB 中都包含了整个 Fabric 网络中各交换 机的所有链路信息(即 LSR)。
- 交换机依据存储在本地的 LSDB,使用 Dijkstra 算法计算出到其它交换机的最短路径。据此,可以确定从源交换机到目的交换机的输出接口,生成 FSPF 路由表。
- 当网络拓扑改变、链路状态发生变化时,交换机会向整个 Fabric 网络泛洪新的 LSR,进行 LSDB 更新同步。邻居交换机收到泛洪的 LSR 时,一方面加到自己的 LSDB 中,一方面将它泛洪给 它的邻居,这样 Fabric 网络中所有的交换机都会同步更新此 LSR。
- 本地的 LSDB 更新将产生路由计算,当计算完成,会将计算得到的最短路径树列表结果更新进 FSPF 路由表。

7.2 配置FC静态路由

配置 FC 静态路由时,需要注意:

- FC 静态路由允许配置的目的地址范围是 010000~EFFFFF (十六进制),不允许配置目的地址为知名服务地址的路由。
- FC 静态路由的出接口允许配置为 VFC 接口。
- 如果先后配置两条目的地址、掩码和出接口均相同而 cost 值不同的静态路由,最后保留在静态路由表内的静态路由的 cost 值将是后者。
- 每个 VSAN 中允许配置的静态路由条数为 256。

表7-1 配置 FC 静态路由

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置FC静态路由	<pre>fc route-static fcid { mask mask-length } interface-type interface-number [cost cost-value]</pre>	缺省情况下,不存在 FC 静态路由

7.3 配置FSPF

7.3.1 FSPF 配置任务简介

FSPF 功能缺省开启,用户一般不需要进行特别的配置。 在实际使用过程中,用户可以根据网络的实际情况,调整某个 VSAN 或者某个接口的 FSPF 运行参数,以便达到更好的运行效果。

表7-2 FSPF 配置任务简介

配置任务		说明	详细配置
调整某个VSAN的运行参数 (这些参数在VSAN视图下进行 配置)	开启 FSPF 功能	必选	<u>7.3.2</u>
	配置最短SPF计算间隔	可选	<u>7.3.3</u>
	配置LSR最小接收间隔	可选	<u>7.3.4</u>
	配置LSR最小刷新间隔	可选	<u>7.3.5</u>
	配置接口的FSPF开销	可选	<u>7.3.6</u>
调整某个接口的运行参数	配置接口的Hello时间间隔	可选	<u>7.3.7</u>
(这些参数必须在E模式接口下	配置接口的Dead时间间隔	可选	<u>7.3.8</u>
进行配置)	配置接口的LSR重传间隔	可选	<u>7.3.9</u>
	关闭接口的FSPF功能	可选	<u>7.3.10</u>
配置FSPF GR (本功能在系统视图下进行配 置)	配置GR Restarter	可选	<u>7.3.11 1.</u>
	配置GR Helper	可选	<u>7.3.11 2.</u>

7.3.2 开启 FSPF 功能

开启了指定 VSAN 的 FSPF 功能后,该 VSAN 才可以运行 FSPF 相关的功能。

表7-3 开启 FSPF 功能

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
开启FSPF功能	fspf enable	缺省情况下,VSAN创建后,FSPF功能处于开启状态

7.3.3 配置最短 SPF 计算间隔

当 LSDB 发生改变时,需要进行 SPF 计算。SPF 计算需要耗费一定的 CPU,如果网络频繁变化, 且每次变化都立即进行 SPF 计算,将会占用大量的 CPU。为了避免交换机过于频繁的进行路由计 算而浪费 CPU,用户可以配置最短的 SPF 计算间隔。

最短 SPF 计算间隔决定了指定 VSAN 内两次连续的 SPF 计算之间的最小时间间隔。最短 SPF 计算间隔配置的小,意味着 FSPF 对于 Fabric 的变化可以快速反应,重新计算 VSAN 内的路由。一个更小的 SPF 计算间隔会耗费更多的 CPU。

表7-4 配置最短 SPF 计算间隔

操作	命令	说明
进入系统视图	system-view	-

操作	命令	说明
进入VSAN视图	vsan vsan-id	-
配置最短SPF计算间隔	fspf spf-hold-time value	缺省情况下,最短SPF计算间隔为0秒

7.3.4 配置 LSR 最小接收间隔

LSR 最小接收间隔决定了指定 VSAN 内接收 LSR 的间隔。为了避免过于频繁的从邻居接收到同一个 LSR 的新实例、更新本地 LSDB 而频繁触发路由计算。在 LSR 最小接收间隔时间内,如果又一次接收到了这个 LSR 的新实例,则直接丢弃,不做处理。

表7-5 配置 LSR 最小接收间隔

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置LSR最小接收间隔	fspf min-ls-arrival value	缺省情况下,LSR最小接收间隔为1秒

7.3.5 配置 LSR 最小刷新间隔

LSR 最小刷新间隔决定了指定 VSAN 内 LSR 刷新间隔。为了避免本机 LSR 被频繁的刷新,从而降低路由计算的频率和减少 Fabric 中 LSR 的泛洪,在 LSR 最小刷新间隔内,交换机不能再次刷新本机 LSR。

表7-6 配置 LSR 最小刷新间隔

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置LSR最小刷新间隔	fspf min-ls-interval interval	缺省情况下,LSR最小刷新间隔为5秒

7.3.6 配置接口的 FSPF 开销

网络中,每一条链路会有不同的开销,在路由优选算法中将使用开销值来确定最有效的路由,接口的 FSPF 开销越小说明链路的开销越小。

表7-7 配置接口的 FSPF 开销

操作	命令	说明
进入系统视图	system-view	-
进入VFC接口视图	interface vfc interface-number	-
配置指定VSAN内接口的FSPF 开销	fspf cost cost-value vsan vsan-id	缺省情况下,VFC接口的FSPF开销根 据接口波特率计算得到,计算公式为

操作	命令	说明
		(1.0e12/波特率)

7.3.7 配置接口的 Hello 时间间隔

交换机通过周期性向外发送 Hello 报文,来发现和维护邻居关系。Hello 间隔值决定了接口在指定 VSAN 内发送 Hello 报文的时间间隔。

₩ 提示

配置的 Hello 间隔值必须小于 Dead 间隔值,且邻居双方配置的 Hello 间隔值必须一致。

表7-8 配置接口的 Hello 间隔值

操作	命令	说明
进入系统视图	system-view	-
进入VFC接口视图	interface vfc interface-number	-
配置指定VSAN内接口的 Hello间隔值	fspf hello-interval interval vsan vsan-id	缺省情况下,接口的Hello间隔 值为20秒

7.3.8 配置接口的 Dead 时间间隔

两台交换机之间建立起邻居关系后,需要以 Hello 间隔值为周期向对方发送 Hello 报文来维护邻居 关系。若在 Dead 间隔内仍未收到对方的 Hello 报文,则认为邻居不存在,需要删除该邻居。

₩ 提示

配置的 Dead 间隔值必须大于 Hello 间隔值,且邻居双方配置的 Dead 间隔值必须一致。

表7-9 配置接口的 Dead 间隔值

操作	命令	说明
进入系统视图	system-view	-
进入VFC接口视图	interface vfc interface-number	-
配置指定VSAN内接口的 Dead间隔值	fspf dead-interval interval vsan vsan-id	缺省情况下,接口的Dead间隔 值为80秒

7.3.9 配置接口的 LSR 重传间隔

LSDB 的同步需要交互 LSR。在发送 LSR 后,等待邻居回应报文确认,如果过了 LSR 重传间隔还 没有接收到邻居的确认,那么需要再次发送该 LSR。

表7-10 配置接口的 LSR 重传间隔

操作	命令	说明
进入系统视图	system-view	-
进入VFC接口视图	interface vfc interface-number	-
配置指定VSAN内接口的LSR 重传间隔	fspf retransmit-interval interval vsan vsan-id	缺省情况下,接口的LSR重传间隔为5秒

7.3.10 关闭接口的 FSPF 功能

开启接口的 FSPF 功能后,接口才可以参与 FSPF 路由运算,如果某接口不参与 FSPF 路由运算,则需关闭该接口的 FSPF 功能。

表7-11 关闭接口的 FSPF 功能

操作	命令	说明
进入系统视图	system-view	-
进入VFC接口视图	interface vfc interface-number	-
关闭指定VSAN内接口的 FSPF功能	fspf silent vsan vsan-id	缺省情况下,所有接口的FSPF功能 均处于开启状态

7.3.11 配置 FSPF GR

GR(Graceful Restart,平滑重启)是一种通过备份 FSPF 配置信息,在协议重启(比如通过 process 命令重启 FSPF 进程等情况)或主备倒换时 FSPF 进行平滑重启,从邻居那里获得邻居关系,并对 LSDB 进行同步,从而保证转发业务不中断的机制。

GR 有两个角色:

- GR Restarter:发生协议重启或主备倒换事件且具有 GR 能力的设备。
- GR Helper: 和 GR Restarter 具有邻居关系,协助完成 GR 流程的设备。

1. 配置 GR Restarter

在作为 GR Restarter 的设备上进行如下配置:

表7-12 配置 GR Restarter

操作	命令	说明
进入系统视图	system-view	-
开启FSPF的GR能力	fspf graceful-restart	缺省情况下,FSPF的GR能力 处于关闭状态
配置FSPF的GR最大间隔时间	fspf graceful-restart interval interval	缺省情况下,FSPF的GR最大间隔时间为120秒

2. 配置 GR Helper

在作为 GR Helper 的设备上进行如下配置:

表7-13 配置 GR Helper

操作	命令	说明
进入系统视图	system-view	-
开启FSPF的GR Helper能力	fspf graceful-restart helper	缺省情况下,FSPF的GR Helper能力处于开 启状态

7.4 FC路由与转发显示和维护

在完成上述配置后,在任意视图下执行 display 命令可以显示配置后 FC 路由与转发的运行情况, 通过查看显示信息验证配置的效果。

在用户视图下执行 reset 命令可以清除 FSPF 统计信息。

表7-14 FC 路由与转发显示和维护

操作	命令	
显示FC路由表信息	display fc routing-table [vsan vsan-id] [statistics verbose] display fc routing-table vsan vsan-id fc-id [mask mask-length] [verbose]	
显示FC FIB表项信息	display fc fib [fcid [mask-length]] vsan vsan-id	
显示 FC Exchange 表项信 息(独立运行模式)	<pre>display fc exchange { link protocol } [slot slot-number] display fc exchange link verbose [slot slot-number [exid exid]]</pre>	
显示FC Exchange表项信 息(IRF模式)	display fc exchange { link protocol } [chassis chassis-number slot slot-number] display fc exchange link verbose [chassis chassis-number slot slot-number [exid exid]]	
显示FSPF邻居信息	display fspf neighbor [vsan vsan-id]	
显示 FSPF 链路状态数据库 信息	display fspf lsdb [vsan vsan-id]	
显示FSPF GR状态信息	display fspf graceful-restart [vsan vsan-id]	
显示FSPF统计信息	display fspf statistics [vsan vsan-id]	
清除FSPF统计信息	reset fspf counters [vsan vsan-id]	

7.5 FC路由与转发典型配置举例

7.5.1 FC 静态路由配置举例

1. 组网需求

网络由三台 FCF 交换机 Switch A、Switch B 和 Switch C 组成。 要求:配置静态路由,使任意两台 FCF 交换机之间都能互通。

2. 组网图

图7-1 配置 FC 静态路由组网图



3. 配置步骤

(1) 配置 Switch A

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view

[SwitchA] system-working-mode advance

Do you want to change the system working mode? $[{\tt Y}/{\tt N}]\!:\!{\tt y}$

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchA] save

[SwitchA] quit

<SwitchA> reboot

配置 FCoE 模式为 FCF 模式。

<SwitchA> system-view

[SwitchA] fcoe-mode fcf

#开启 VSAN 1的 Fabric 配置功能。

[SwitchA] vsan 1

[SwitchA-vsan1] domain configure enable

配置 Switch A 的域 ID 为 1。

[SwitchA-vsan1] domain-id 1 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[Y/N]\!:\!y$

[SwitchA-vsan1] quit

创建 VFC 接口 VFC1, 配置 VFC1 接口工作在 E 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC1 接口。

[SwitchA] interface vfc 1 [SwitchA-Vfc1] fc mode e [SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1 [SwitchA-Vfc1] port trunk vsan 1 [SwitchA-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/1

[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[SwitchA-Ten-GigabitEthernet1/0/1] quit

#开启 VLAN 10的 FCoE 功能,并将其与 VSAN 1进行映射。

[SwitchA] vlan 10

[SwitchA-vlan10] fcoe enable vsan 1

[SwitchA-vlan10] quit

#在 Switch A 上配置两条静态路由。

[SwitchA] vsan 1 [SwitchA-vsan1] fc route-static 020000 8 vfc 1 [SwitchA-vsan1] fc route-static 030000 8 vfc 1

(2) 配置 Switch B

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchB> system-view

[SwitchB] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchB] save

[SwitchB] quit

<SwitchB> reboot

配置 FCoE 模式为 FCF 模式。

<SwitchB> system-view

[SwitchB] fcoe-mode fcf

#开启 VSAN 1的 Fabric 配置功能。

[SwitchB] vsan 1

[SwitchB-vsan1] domain configure enable

配置 Switch B 的域 ID 为 2。

[SwitchB-vsan1] domain-id 2 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[\rm Y/N]:y$

[SwitchB-vsan1] quit

创建 VFC 接口 VFC1, 配置 VFC1 接口工作在 E 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC1 接口。

[SwitchB] interface vfc 1

[SwitchB-Vfc1] fc mode e

[SwitchB-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchB-Vfc1] port trunk vsan 1

[SwitchB-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过。

[SwitchB] interface ten-gigabitethernet 1/0/1

[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[SwitchB-Ten-GigabitEthernet1/0/1] quit

创建 VFC 接口 VFC2, 配置 VFC2 接口工作在 E 模式,将 VFC2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2 上,并将 VFC2 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC2 接口。

[SwitchB] interface vfc 2

[SwitchB-Vfc2] fc mode e

[SwitchB-Vfc2] bind interface ten-gigabitethernet 1/0/2

[SwitchB-Vfc2] port trunk vsan 1

[SwitchB-Vfc2] quit

配置以太网接口 Ten-GigabitEthernet1/0/2 允许 VLAN 10 的报文通过。

[SwitchB] interface ten-gigabitethernet 1/0/2

[SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk

[SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10

[SwitchB-Ten-GigabitEthernet1/0/2] quit

#开启 VLAN 10 的 FCoE 功能,并将其与 VSAN 1 进行映射。

[SwitchB] vlan 10

[SwitchB-vlan10] fcoe enable vsan 1

[SwitchB-vlan10] quit

#在 Switch B上配置两条静态路由。

[SwitchB] vsan 1

[SwitchB-vsan1] fc route-static 010000 8 vfc 1

[SwitchB-vsan1] fc route-static 030000 8 vfc 2

(3) 配置 Switch C

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchC> system-view

[SwitchC] system-working-mode advance

Do you want to change the system working mode? $[{\rm Y}/{\rm N}]{\rm :}{\rm y}$

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchC] save

[SwitchC] quit

<SwitchC> reboot

配置 FCoE 模式为 FCF 模式。

<SwitchC> system-view

[SwitchC] fcoe-mode fcf

#开启 VSAN 1的 Fabric 配置功能。

[SwitchC] vsan 1

[SwitchC-vsan1] domain configure enable

配置 Switch C 的域 ID 为 3。

[SwitchC-vsan1] domain-id 3 static Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? [Y/N]:y [SwitchC-vsan1] quit # 创建 VFC 接口 VFC2, 配置 VFC2 接口工作在 E 模式,将 VFC2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2 上,并将 VFC2 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC2 接口。

[SwitchC] interface vfc 2

[SwitchC-Vfc2] fc mode e

[SwitchC-Vfc2] bind interface ten-gigabitethernet 1/0/2

[SwitchC-Vfc2] port trunk vsan 1

[SwitchC-Vfc2] quit

配置以太网接口 Ten-GigabitEthernet1/0/2 允许 VLAN 10 的报文通过。

[SwitchC] interface ten-gigabitethernet 1/0/2

[SwitchC-Ten-GigabitEthernet1/0/2] port link-type trunk

[SwitchC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10

[SwitchC-Ten-GigabitEthernet1/0/2] quit

开启 VLAN 10 的 FCoE 功能,并将其与 VSAN 1 进行映射。

[SwitchC] vlan 10

[SwitchC-vlan10] fcoe enable vsan 1

[SwitchC-vlan10] quit

#在 Switch C 上配置两条静态路由。

[SwitchC] vsan 1 [SwitchC-vsan1] fc route-static 010000 8 vfc 2 [SwitchC-vsan1] fc route-static 020000 8 vfc 2

4. 验证配置

#显示 Switch A的 VSAN 1的 FC 路由表。

```
[SwitchA-vsan1] display fc routing-table vsan 1
Routing Table: VSAN 1
 Destinations : 6
                         Routes : 6
 Destination/mask
                  Protocol Preference
                                                  Interface
                                          Cost
                   STATIC
 0x020000/8
                                          0
                             10
                                                  Vfc1
 0x030000/8
                   STATIC
                            10
                                          0
                                                  Vfcl
 0xfffc01/24
                   DIRECT
                            0
                                          0
                                                  InLoop0
 0xfffffa/24
                   DIRECT
                            0
                                          0
                                                  InLoop0
 0xfffffc/24
                   DIRECT
                             0
                                          0
                                                  InLoop0
```

#显示 Switch B的 VSAN 1的 FC 路由表。

[SwitchB-vsan1] display fc routing-table vsan 1

DIRECT

Routing Table: VSAN 1

0xfffffd/24

Destinations : 6	Rou	ites : 6		
Destination/mask	Protocol	Preference	Cost	Interface
0x010000/8	STATIC	10	0	Vfcl
0x030000/8	STATIC	10	0	Vfc2
0xfffc02/24	DIRECT	0	0	InLoop0
0xfffffa/24	DIRECT	0	0	InLoop0
0xfffffc/24	DIRECT	0	0	InLoop0
0xfffffd/24	DIRECT	0	0	InLoop0

0

#显示 Switch C的 VSAN 1的 FC 路由表。

[SwitchC-vsan1] display fc routing-table vsan 1

0

InLoop0

```
Routing Table: VSAN 1
  Destinations : 6
                            Routes : 6
  Destination/mask
                     Protocol
                                 Preference
                                               Cost
                                                        Interface
  0x010000/8
                      STATIC
                                               0
                                                        Vfc2
                                 10
  0x020000/8
                                                        Vfc2
                      STATIC
                                 10
                                               0
  0xfffc03/24
                      DIRECT
                                 0
                                               0
                                                        InLoop0
  0xfffffa/24
                      DIRECT
                                 0
                                               0
                                                        InLoop0
  0xffffc/24
                      DIRECT
                                 0
                                               0
                                                        InLoop0
  0xffffd/24
                      DIRECT
                                 0
                                               0
                                                        InLoop0
```

在 Switch A 上使用 fcping 命令验证 Switch C 是否可达。

```
[SwitchA-vsan1] fcping fcid fffc03 vsan 1
FCPING fcid 0xfffc03: 128 data bytes, press CTRL_C to break
Reply from 0xfffc03: bytes = 128 time = 23 ms
Reply from 0xfffc03: bytes = 128 time = 9 ms
Reply from 0xfffc03: bytes = 128 time = 19 ms
Reply from 0xfffc03: bytes = 128 time = 14 ms
Reply from 0xfffc03: bytes = 128 time = 25 ms
```

```
--- 0xfffc03 fcping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 9/18/25 ms
```

7.5.2 FSPF 配置举例

1. 组网需求

网络由两台 FCF 交换机组成,要求通过动态路由协议 FSPF,使两台 FCF 交换机之间可以互通。

2. 组网图

图7-2 配置 FSPF 组网图



3. 配置步骤



本例中只列出 FC 路由的相关配置,其它配置步骤略。

(1) 配置 Switch A

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view

[SwitchA] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the system to make it effective. [SwitchA] save [SwitchA] guit

<SwitchA> reboot

配置 FCoE 模式为 FCF 模式。

<SwitchA> system-view

[SwitchA] fcoe-mode fcf

创建 VSAN 2 并开启 VSAN 2 的 Fabric 配置功能。

[SwitchA] vsan 2

[SwitchA-vsan2] domain configure enable

配置域 ID 为 1。

[SwitchA-vsan2] domain-id 1 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[Y/N]\!:\!y$

全局开启 FSPF 功能。

[SwitchA-vsan2] fspf enable

[SwitchA-vsan2] quit

创建 VFC 接口 VFC1, 配置 VFC1 接口工作在 E 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 2, 即允许 VSAN 1 的报文 通过 VFC1 接口。

[SwitchA] interface vfc 1

[SwitchA-Vfc1] fc mode e

[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchA-Vfc1] port trunk vsan 2

[SwitchA-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/1

[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[SwitchA-Ten-GigabitEthernet1/0/1] quit

#开启 VLAN 10的 FCoE 功能,并将其与 VSAN 2进行映射。

[SwitchA] vlan 10

[SwitchA-vlan10] fcoe enable vsan 2

[SwitchA-vlan10] quit

#开启 VFC1 接口的 FSPF 功能。

[SwitchA] interface vfc 1

[SwitchA-Vfc1] undo fspf silent vsan 2

[SwitchA-Vfc1] quit

(2) 配置 Switch B

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchB> system-view

[SwitchB] system-working-mode advance

Do you want to change the system working mode? $[\,Y/N\,]\,{:}\,y$

The system working mode is changed, please save the configuration and reboot the system to make it effective.

[SwitchB] save [SwitchB] quit <SwitchB> reboot

配置 FCoE 模式为 FCF 模式。

<SwitchB> system-view

[SwitchB] fcoe-mode fcf

创建 VSAN 2 并开启 VSAN 2 的 Fabric 配置功能。

[SwitchB] vsan 2

[SwitchB-vsan2] domain configure enable

配置域 ID 为 2。

[SwitchB-vsan2] domain-id 2 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[Y/N]\!:\!y$

全局开启 FSPF 功能。

[SwitchB-vsan2] fspf enable [SwitchB-vsan2] quit

创建 VFC 接口 VFC1, 配置 VFC1 接口工作在 E 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 2, 即允许 VSAN 1 的报文 通过 VFC1 接口。

[SwitchB] interface vfc 1

[SwitchB-Vfc1] fc mode e

[SwitchB-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchB-Vfc1] port trunk vsan 2

[SwitchB-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过。

[SwitchB] interface ten-gigabitethernet 1/0/1

[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[SwitchB-Ten-GigabitEthernet1/0/1] quit

开启 VLAN 10 的 FCoE 功能,并将其与 VSAN 2 进行映射。

[SwitchB] vlan 10

[SwitchB-vlan10] fcoe enable vsan 2

[SwitchB-vlan10] quit

#开启 VFC1 接口的 FSPF 功能。

[SwitchB] interface vfc 1

[SwitchB-Vfc1] undo fspf silent vsan 2

[SwitchB-Vfc1] quit

4. 验证配置

#显示 Switch A的 FSPF 邻居信息。

 [SwitchA] display fspf neighbor

 FSPF neighbor information of VSAN 2(01):

 Interface
 NbrDomain

 IfIndex
 NbrIfIndex

 Dead Time
 State

 Vfc1
 2
 0x68
 00:01:06

 Full
 Full
 Full

#显示 Switch A 路由表相关信息。

[SwitchA] display fc routing-table vsan 2

Routing Table: VSAN 2

Destinations : 5	Rou	ites : 5		
Destination/mask	Protocol	Preference	Cost	Interface
0x020000/8	FSPF	20	100	Vfcl
0xfffc01/24	DIRECT	0	0	InLoop0
0xfffffa/24	DIRECT	0	0	InLoop0
0xffffc/24	DIRECT	0	0	InLoop0
0xfffffd/24	DIRECT	0	0	InLoop0

在 Switch A 上执行 FC Ping,验证能否到达交换机 Switch B。

```
[SwitchA] fcping fcid fffc02 vsan 2
FCPING fcid 0xfffc02: 128 data bytes, press CTRL_C to break.
Reply from 0xfffc02: bytes = 128 time = 1.102 ms
Reply from 0xfffc02: bytes = 128 time = 0.276 ms
Reply from 0xfffc02: bytes = 128 time = 0.253 ms
Reply from 0xfffc02: bytes = 128 time = 0.270 ms
Reply from 0xfffc02: bytes = 128 time = 0.247 ms
```

```
--- 0xfffc02 fcping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 0.247/0.430/1.102 ms
```

8 FC Zone

8.1 FC Zone简介

8.1.1 FC Zone 概述

VSAN 的划分实现了将一个物理连通的 SAN 分割成多个逻辑上的虚拟 SAN。每个 VSAN 相互隔离, 并独立提供服务,增强了网络的适应性和安全性,使其能够为用户提供更有效的服务。但仅通过 VSAN 却不能对接入 Fabric 的服务器及磁盘设备(即 N_Port)进行访问控制,它们发送的报文不 会带有 VSAN 信息,所以其所属的 VSAN 只能由与其连接的 FCF 交换机的端口(F_Port)所在的 VSAN 决定,如果 F_Port 所在 VSAN 相同,表明对应 N_Port 属于同一个 VSAN。相同 VSAN 内的 N_Port,只要注册了名称服务就可以相互访问,这样给数据安全带来隐患,尤其是在不同的操作系 统环境下,很容易对磁盘数据造成破坏。

Zone 特性则可以有效解决上述问题,其原理是:在 VSAN 内进一步划分区域(Zone),在 Zone 内 根据不同的目的添加不同的 N_Port 成员或 F_Port 成员。使不同 Zone 内的 N_Port 成员之间相互隔 离,以达到访问控制的目的。

将一个F_Port添加到某个Zone内的效果是将该F_Port下登录的所有N_Port批量加入该Zone内, 方便配置。

8.1.2 Zone 模式

Zone 分为两种模式:基本 Zone 模式和增强 Zone 模式。两者主要的区别是:

- 基本 Zone 不负责同步默认 Zone 策略和硬件 Zone 配置,需要用户通过手工配置的方式保证 全网默认 Zone 策略和硬件 Zone 配置一致;增强 Zone 会在扩散过程中携带默认 Zone 策略 和硬件 Zone 配置,通过数据同步的方式保证全网默认 Zone 策略和硬件 Zone 配置一致。
- 在 Zone 数据合并或扩散时,当一个 Zone 同时属于多个 Zone set 时,在同步报文中,基本 Zone 需要为每个 Zone set 都生成一个 Zone 实例,而增强 Zone 的 Zone set 引用已定义的 Zone,从而大幅减少了数据同步时报文的负载。
- 基本 Zone 中无合并控制特性,合并规则较为简单;增强 Zone 有合并控制特性,通过对合并 控制的配置加强了对 Zone 数据合并的管理,合并规则更加严格。

关于上述内容的详细描述,请看下面的工作机制介绍。

8.1.3 Zone 数据库

为了控制 N_Port 之间的访问权限,可以将 N_Port 按照应用的需要划分到不同的 Zone 中,这些 Zone 形成一个集合 Zone set。同样的 N_Port 集合,如果划分 Zone 的策略不同,将会形成多个 Zone set。 这些按照不同策略划分出来的各个 Zone 以及 Zone set 组成了 Zone 数据库。

1. Zone 数据库结构

Zone 数据库是按照 Zone set、Zone、Zone member 三级基本对象进行组织的,如图 8-1 所示。

图8-1 Zone 数据库结构



- Zone set 是 Zone 的集合; Zone 是 Zone member 的集合; Zone member 是 Zone 的成员, 每个成员都是一个 N_Port 或 F_Port,称为 N_Port 成员或 F_Port 成员。N_Port 成员可以通 过 PWWN(即 N_Port 的 WWN)、FC 地址进行标识,F_Port 成员可以通过 FWWN(即 F_Port 的 WWN)进行标识。
- 每个 VSAN 内可以配置多个 Zone set,每个 Zone set 内可以包含多个 Zone,每个 Zone 内可 以包含多个 Zone member。
- 为了配置方便, Zone 成员配置还支持使用 Zone 别名,即 Zone alias。Zone 别名为 N_Port 的集合,可以将其作为一个整体使用。如果多个 Zone 内包含很多相同的公共 Zone member,可以将这些公共 Zone member 先加入到同一个 Zone 别名中,再通过在不同的 Zone 中引用 该 Zone 别名,达到简化配置的目的。

2. Active Zone set

虽然每个 VSAN 内可以配置多个 Zone set,但只有一个可以生效,称为 Active Zone set。最终 N_Port 成员的访问控制都由 Active Zone set 决定。

为了让网络中的各交换机对 N_Port 的访问控制有一致的行为,需要通过命令在本地交换机上指定 Active Zone set,并向整个 Fabric 进行同步,使其在全网范围内保持一致。

当一个 Zone set 被激活时,实际上是将激活时刻的 Zone set 生成一个独立的副本,该副本即是 Active Zone set。当再对该 Zone set 进行修改时,不会对生成的副本造成影响。只有再次激活时, 才会将修改的内容更新到副本中。图 8-2 描述了对 Zone set zs2 进行激活配置,并修改其配置后重 新激活的数据库变化流程。

需要注意的是,在基本 Zone 中,激活指定的 Zone set 时,系统会对 Zone set 激活后将要发送的 封装报文的大小进行判断,如果超过最大规格,则激活失败,并打印相应的提示信息,但在增强 Zone 中激活 Zone set 不受此限制。

图8-2 Active Zone set 与 Zone 数据库关系图



3. 默认 Zone

Active Zone set 中通过包含 Zone,将 Zone 中的 N_Port 纳入了 Active Zone set 的范围。对于不在 Active Zone set 范围内,且已经注册的 N_Port 则自动属于默认 Zone。

如果配置了允许默认 Zone 内的成员互相访问,可以将默认 Zone 也当做 Active Zone set 内的一个 Zone,参与 N_Port 成员之间的访问控制;否则,默认 Zone 不在 Active Zone set 内,不参加 N_Port 成员之间的访问控制。

基本 Zone 不负责默认 Zone 策略在 Fabric 中的同步,需要用户通过手工配置保证 Fabric 中的默认 Zone 策略一致;而增强 Zone 会在扩散过程中携带默认 Zone 策略,使得 Fabric 中默认 Zone 策略 的一致性得到更好的保障。

4. Peer Zone

Zone 类型分为普通 Zone 类型和 Peer Zone 类型。本文中未明确为 Peer Zone 时,均表示普通 Zone。 Peer Zone 是增强 Zone 中一种 Zone 控制类型,用户可以在 Target 设备(访问目的端,一般为存 储设备)上定义 Peer Zone,包括 Peer Zone 名称、主成员(Principal member)和副成员(Peer members)。Target 设备通过向交换机发送相关报文,使交换机创建用户定制的 Peer Zone。每一个 Peer Zone 内可以定义一个主成员和多个副成员,成员之间互通规则如下:

- 主成员可以和其他所有副成员通信。
- 副成员之间不可以互相通信,除非在其他 Zone 内被允许通信。

8.1.4 Zone 的 Pairwise 特性

💕 说明

Zone 的 Pairwise 特性仅支持在增强 Zone 模式下配置,基本 Zone 模式不支持此特性。

在实际应用中,通常将访问发起端(一般是服务器)以及需要访问的目的端(一般是存储设备)划 分到同一个 Zone 中,然后加入一个 Zone set 中并激活该 Zone set。只要是属于 Active Zone set 中同一个 Zone 的成员,它们就可以互相访问。Zone 功能在实现时,为所有划分到同一个 Zone 中 的成员都生成了两两间的硬件访问规则。但在实际的操作中,一般是由服务器访问存储设备,而服 务器与服务器之间、存储设备与存储设备之间并不需要互相访问。当同一个 Zone 中包含多个服务 器或存储设备时,这种生成规则的方式就会产生硬件资源的浪费。Pairwise 特性可以很好地解决这 个问题。

1. Pairwise 特性的机制

Pairwise 特性的原理是:为 Zone 中的成员指明角色,以限定成员的访问行为。成员角色分为两类:

- Initiator: 访问发起端, 一般为服务器。
- Target: 访问目的端, 一般为存储设备。

当某成员是 Initiator 角色时,它只能与具有 Target 角色的成员互相访问;当某成员是 Target 角色时, 它只能与具有 Initiator 角色的成员互相访问。成员可以兼具两种角色,即同时具有 Initiator 和 Target 角色,兼具两种角色的成员既可以访问角色为 Initiator 的发起端,也可以访问角色为 Target 的目的 端,如果未指明成员的角色,则默认同时兼具两种角色。

2. Pairwise 特性的影响范围

Pairwise 特性是以 Zone 为单位进行配置的。当 Pairwise 特性关闭时,成员角色信息不生效;当开 启某个 Zone 的 Pairwise 特性时,该 Zone 的成员携带的角色信息仅在当前 Zone 生效,对于其它 Zone 而言,成员可能拥有不同的角色信息。

8.1.5 基本 Zone 的扩散

扩散是由一台交换机将自己的 Zone 数据向全网同步的过程。发起扩散的交换机称作管理交换机, 网络内的其它所有交换机称作被管理交换机。

对于基本 Zone 而言,会涉及到扩散的数据只有 Active Zone set 和 Zone 数据库两部分,具体扩散 哪些部分,取决于扩散类型。

1. 基本 Zone 的扩散类型

基本 Zone 的扩散类型分为两种:

- 完全扩散:会将 Active Zone set 以及 Zone 数据库都进行扩散。
- 非完全扩散: 仅将 Active Zone set 进行扩散。

2. 基本 Zone 激发扩散的途径

基本 Zone 中有两种途径可以激发扩散过程:

- 一种是通过激活命令 zoneset activate 将一个 Zone set 激活成 Active Zone set,此 Active Zone set 在本地生效的同时还将被同步到其它交换机;但若该 Zone set 在激活时,因超规格导致激活失败,则不会发生激活扩散。
- 另一种是通过扩散命令 **zoneset distribute**,直接将本交换机上的 Active Zone set 以及 Zone 数据库向全网同步。

通过激活命令激发的扩散将根据扩散类型决定是否携带 Zone 数据库,通过扩散命令激发的扩散不 受扩散类型的约束,为完全扩散。

被管理交换机使用收到的数据替换本地的 Active Zone set 或 Zone 数据库。替换的内容以接收到的数据为准,不受本交换机上扩散类型的影响。例如,接收到的数据为 Active Zone set 和 Zone 数据库,则替换本地的 Active Zone set 和 Zone 数据库,不管本地配置的扩散类型是否为完全同步。如果接收到的数据只有 Zone 数据库,则替换之后,本地交换机将只有 Zone 数据库,不管之前本地 是否存在 Active Zone set。

3. 基本 Zone 的扩散过程

管理交换机和每台被管理交换机之间都经过下列四类报文的交互,来完成报文传输与数据同步:

- ACA(Acquire Change Authorization, 获取修改授权)
- SFC (Stage Fabric Configuration Update, 进行 Fabric 配置更新)
- UFC(Update Fabric Configuration,更新 Fabric 配置)
- RCA (Release Change Authorization,释放修改授权)

这四类报文的作用分别相当于加锁、数据同步、提交和解锁的过程,可以保证不同的用户在不同交换机上同时输入命令触发数据扩散时,只有一台交换机作为管理交换机进行数据扩散。数据扩散过程如图 8-3 所示。

图8-3 扩散过程报文交互图



- (1) 首先,管理交换机要通过 ACA 请求报文,获取各被管理交换机的状态,该报文带有管理交换 机所知道的全网的 Domain ID 列表,即 Fabric 中所有交换机的地址。管理交换机向各被管理 交换机发送 ACA 请求报文后进入锁定状态。各被管理交换机收到 ACA 请求报文后,将报文 中的 Domain ID 列表与本地所知道的 Domain ID 列表进行比较。如果列表一致,表示 Fabric 处于稳定状态^[1]。这时可以进行同步并回应 ACC(确认)报文,同时进入修改授权状态,即 进行锁定。否则,如果交换机已经处于修改授权状态,或由于其它原因导致不能处理该报文,则回应 RJT(拒绝)报文。
- (2) 管理交换机只有等到所有被管理交换机都回应 ACC 报文后,才开始通过发送 SFC 请求报文进行数据同步。否则发送 RCA 请求报文,使各交换机解除修改授权状态^[2]。
- (3) 管理交换机向所有被管理交换机发送 SFC 请求报文,报文携带了要同步的数据,包括 Active Zone set、Zone 数据库内容。各个被管理交换机收到 SFC 请求报文后,如果发现携带有 Zone 数据库内容,则计算本地 Zone 数据库被替换后整机 Zone set、Zone、Zone 别名的总数是否 超过各自的规格限制,如果没有超过规格限制则回应 ACC 报文,否则回应 RJT 报文。
- (4) 管理交换机只有等到所有被管理交换机都回应 ACC 报文后,才向所有被管理交换机发送 UFC 请求报文,通知其根据收到的数据更新各自的本地数据。否则发送 RCA 请求报文,使各交换 机解除修改授权状态。
- (5) 各个被管理交换机收到 UFC 请求报文后,开始更新本地的 Zone set 数据库,如果更新成功回应 ACC 报文,否则回应 RJT 报文。
- (6) 管理交换机在收到所有交换机的响应后,发送 RCA 请求报文,使各交换机解除修改授权状态。
- (7) 各个被管理交换机收到 RCA 请求报文后,解除本机的修改授权状态,并回应 ACC 报文。
- (8) 管理交换机收到所有被管理交换机的 ACC 报文后解除本机的锁定状态。



- [1]: 这实际上要求全网的路由信息一定要正确且保持一致,并且不能有多余的不可达路由。尤 其是使用静态路由配置时要特别注意这一点,否则,不能正确进行数据扩散。
- •[2]:为防止由于被管理交换机状态异常而不回应 ACC 报文也不回应 RJT 报文,从而造成管理交换机锁定状态无法解除的情况,管理交换机上启用报文重传机制,在发送扩散请求报文时,最多发送3次。如果一直收不到回应,将解除本机的锁定状态。而管理交换机如果在发送 ACA 请求后出现异常,导致被管理交换机已经处于锁定状态但接收不到后续的报文,被管理交换机在等待一段时间后解除锁定状态。

8.1.6 增强 Zone 的扩散

增强 Zone 的扩散与基本 Zone 的扩散机制基本相同,但有如下几点不同:

- 参与扩散的数据不同:增强 Zone 扩散的数据除了 Active Zone set 和 Zone 数据库,还包括
 Zone 策略和硬件 Zone 开启情况。Zone 策略包括合并控制模式和默认 Zone 策略。关于合并
 控制模式的介绍请参见 "<u>8.1.8 增强 Zone 的合并</u>"。
- 扩散类型不同:增强 Zone 不再受扩散类型的影响,始终会进行完全扩散,也不支持 zoneset distribute full 命令的配置。

增强 Zone 中激发扩散过程的途径和基本 Zone 激发扩散过程的途径相同,只是激活命令 zoneset activate 激发的扩散始终为完全扩散。具体激发扩散的途径介绍请参见"<u>8.1.5</u><u>2</u>.基本 Zone 激发 扩散的途径"。

除了基本 Zone 和增强 Zone 模式下激发扩散的途径外,Zone 模式的切换也会引发 Zone 数据的扩散,无论是基本 Zone 切换到增强 Zone,还是增强 Zone 切换到基本 Zone。Zone 模式切换引发的 扩散所携带的数据和增强 Zone 模式下的扩散类似,除了 Active Zone set 和 Zone 数据库,还包括 Zone 策略和硬件 Zone 开启情况。

无论是增强 Zone 模式下的扩散还是 Zone 模式切换引发的扩散,扩散报文始终都会携带 Zone 策略, 无论是否有 Active Zone set 或 Zone 数据库。硬件 Zone 开启情况有些特殊,在增强 Zone 模式下 的扩散中,扩散报文始终都会携带硬件 Zone 开启情况,Zone 模式切换时则要区别切换方式对待, 如果是由基本 Zone 模式切换到增强 Zone 模式,则携带硬件 Zone 开启情况,如果是由增强 Zone 模式切换到基本 Zone 模式,则不携带硬件 Zone 开启情况。

8.1.7 基本 Zone 的合并

当两个 Fabric 合并到一起时,可能每个 Fabric 内部都存在 Zone 数据,这时要将 Zone 相关配置数 据进行合并。基本 Zone 合并的 Zone 数据包括 Active Zone set 和 Zone 数据库。 基本 Zone 合并时受合并类型的影响,合并类型分为两种:

- 完全合并: 会将 Active Zone set 以及 Zone 数据库都进行合并。
- 非完全合并: 仅将 Active Zone set 进行合并。

由发起合并的交换机,检查本地配置的数据合并类型,如果为非完全合并,发送的报文就只携带 Active Zone set,如果为完全合并,则同时携带 Active Zone set 和整个 Zone 数据库。



- Zone 合并发起方根据当前本地配置的数据合并类型决定合并的数据内容,合并接收方对接收到的所有数据进行合并处理而不受本地数据合并类型限制。
- Zone 成员可以通过 FC 地址进行区分,但是当 Fabric 合并时,FC 地址有可能发生变化,最终 合并出的结果可能并不是用户期望的,所以应该尽量使用端口 PWWN 作为成员标识。

1. 基本 Zone 的合并过程

当交换机发现新增的邻居(由链路模块负责发现邻居并通知给 Zone 模块)时,就开始与该邻居进 行合并过程,如果合并后的数据发生了变化,就将变化后的数据发送给所有邻居交换机进行再次 Zone 合并,直到全网所有交换机的数据都得到更新。

合并过程中,先使用 MRRA(Merge Request Resource Allocation,合并请求资源分配)报文协商 传输数据的规模,之后再使用 MR(Merge Request,合并请求)报文携带需要合并的数据发送到 邻居节点。

两台交换机 Zone 合并过程如图 8-4 所示。

图8-4 两台交换机 Zone 合并过程图



(1) A和B互为新邻居,且假设首先由A向B发起合并:

a. A向B发送MRRA请求报文,该报文中携带着本地需要合并的数据的规模;

- b. B 接收到 A 发送的 MRRA 请求报文后,根据报文中的数据规模并结合本地数据规模判断是 否能够接受此次合并,如果能接受,则回应 ACC 报文,否则回应 RJT 报文;
- c. A 收到 B 回复的 ACC 报文后,向 B 发送 MR 请求报文,该报文中携带了 A 的 Zone 数据;

- d. B收到A发送的MR请求报文后,获取报文中的Zone数据并与本地的Zone数据进行合并。 合并成功向 A 回应 ACC 报文,否则回应 RJT 报文并携带合并失败的原因。
- (2) A向B发起的合并过程完成之后,如果B发现本地数据与从A同步过来的数据完全一致,或 者本地数据是从A同步过来的数据的子集,则结束A和B之间的合并过程,否则,B将继续 发起向A的合并。由B向A发起的合并过程与由A向B发起的合并过程类似,如图中5、6、 7、8所示。
- (3) A向B发起的合并过程完成之后,如果B发现本地数据库因为合并发生了变化,将会试图将 这种变化同步到整个网络,这种同步是通过B向自己的所有邻居发起合并过程完成的。
- (4) A和B之间,至多经过两个单向的合并过程即可保证两台交换机之间数据的一致性。

🕑 说明

合并过程可以保证相互合并的交换机间 Active Zone set 的一致性,但是数据库是否一致则决定于各 台交换机上配置的同步类型是否均为完全同步。当各台交换机上均配置了完全同步,经过合并,可 以让多台交换机上的 Zone 数据库达到一致。

2. 基本 Zone 的合并规则

基本 Zone 数据合并具体规则如表 8-1 所示。

表8-1 基本 Zone 数据合并规则

本地数据库	邻居数据库	合并状态	合并结果
Zone数据库包含同名的Zone s	et但其中的Zone名称不同	成功	本地数据库与邻居数据库的并集, 同名Zone set进行合并
Zone数据库包含不同名的Zone	e set	成功	本地数据库与邻居数据库的并集, 不同名Zone set均存在
Zone数据库包含不同名的Zone	e或Zone别名	成功	本地数据库与邻居数据库的并集, 不同名Zone或Zone别名均存在
Active Zone set 或Zone数据库中同名Zone的Pairwise特性 开启情况不一致		失败	邻居数据库和本地数据库无变化
Zone数据库包含同名的Zone或Zone别名,但其中的成员不同		失败	邻居数据库和本地数据库无变化
Active Zone set中同名的Zone的成员相同,但成员角色不同, 或Zone数据库中同名的Zone或Zone别名的成员相同,但成 员角色不同		失败	邻居数据库和本地数据库无变化
空	非空	成功	邻居数据库覆盖本地数据库
非空	空	成功	本地数据库覆盖邻居数据库



- 若发生合并的两台交换机上配置的 Active Zone set 名字不同,则通过字符串比较的方式得到 Active Zone set 名字较大的一个作为合并之后的 Active Zone set 名字。
- 按照表 8-1 中的规则合并后,如果 Active Zone set 合并失败,则会将发生合并的两台交换机之间的链路隔离(端口在该 VSAN 内处于 down 状态),合并双方的数据库不发生改变;如果 Zone 数据库合并失败,则不会隔离发生合并的两台交换机之间的链路,仅仅是合并双方的数据库不发生改变。

8.1.8 增强 Zone 的合并

增强 Zone 的合并触发条件和合并过程与基本 Zone 一致,但有如下几点不同:

- 合并类型不同:增强 Zone 不再受合并类型的影响,始终会进行完全合并。
- 报文携带的数据不同:增强 Zone 的 MR 报文中除了携带 Active Zone set 和 Zone 数据库,还 携带了硬件 Zone 开启情况和一个合并标志字段。合并标志字段中的合并控制模式和默认 Zone 策略参数是能否进行合并的重要条件。
- 合并规则不同:相比基本 Zone 的合并,增强 Zone 对数据合并的管理更加严格。

增强 Zone 的合并规则如下:

- (1) 如果合并控制模式和默认 Zone 策略有一个与本地不一致,则合并失败。
- (2) 如果合并控制模式和默认 Zone 策略与本地全部一致,且合并控制模式为 Restrict,则检查报 文中携带的数据和本地数据是否完全一致,如果完全一致,则合并成功,两端数据库不发生 变化。如果有任何数据不一致,则合并失败。
- (3) 如果合并控制模式和默认 Zone 策略与本地全部一致,且合并控制模式为 Allow,则按如下原则处理:
- 如果 Active Zone set 中包含同名的 Zone 但 Zone 内成员不同,则合并失败;
- 如果 Zone 数据库中包含同名的 Zone set、Zone 或 Zone alias,但其成员不同,则合并失败;
- 如果 Zone 数据中有同名的端口但是端口的成员角色不同,则合并失败;
- 如果 Zone 数据中有同名的 Zone, 但该 Zone 的 Pairwise 特性开启情况不同,则合并失败;
- 如果 Zone 数据中携带的硬件 Zone 开启情况不同,则合并失败;
- 如果 Active Zone set 包含不同名的 Zone,同时不违反上述其它条件时,则合并成功,Active Zone set 取两端数据的并集;
- 如果 Zone 数据库中包含不同名的 Zone set、Zone 或 Zone alias,同时不违反上述其它条件时,则合并成功,Zone 数据库取两端数据的并集。

🕑 说明

不同于基本 Zone, 增强 Zone 在所有合并失败的情况都会隔离两台交换机之间的链路, 且两端 Zone 数据不发生改变。

8.1.9 访问控制

当用户所在服务器需要使用名称服务访问磁盘时,需要确认该服务器与要访问的磁盘是否同时属于 Active Zone set 内的某个 Zone 的 N_Port 成员。只有属于同一个 Zone 的成员才允许互相访问,否则不允许互相访问。

8.2 FC Zone配置任务简介

表8-2 FC Zone 配置任务简介

配置任务	说明	详细配置
配置Zone模式	必选	<u>8.3.1</u>
配置Zone的Pairwise特性	必选 只允许在增强 Zone 模式下配置	<u>8.3.2</u>
配置Zone别名	可选	<u>8.3.3</u>
配置Zone	必选	<u>8.3.4</u>
配置Zone set	必选	<u>8.3.6</u>
配置默认Zone策略	必选	<u>8.3.7</u>
配置Zone扩散和合并类型	必选 只允许在基本 Zone 模式下配置	<u>8.3.8</u>
配置Zone的合并控制模式	必选 只允许在增强 Zone 模式下配置	<u>8.3.9</u>
开启硬件Zone	可选	<u>8.3.10</u>
激活Zone set并发起向全网的扩散过程	必选	<u>8.3.11</u>
激发完全扩散过程	可选	<u>8.3.12</u>
重命名Zone别名、Zone、Zone set	可选	<u>8.3.13</u>
复制Zone别名、Zone、Zone set	可选	<u>8.3.14</u>
清除Zone数据库	可选	<u>8.3.15</u>
开启FC Zone告警功能	可选	<u>8.3.16</u>

🕑 说明

- 在交换机进行扩散或合并的过程中,用户无法修改 Zone 的配置。
- 一个 Fabric 网络中同时只能有一个管理交换机正在发起扩散,只有当一次扩散完成后才能发起下一次扩散。

8.3 配置FC Zone

8.3.1 配置 Zone 模式

Zone 有两种工作模式:基本 Zone 模式和增强 Zone 模式。缺省工作在基本 Zone 模式。当进行 Zone 模式切换时,将进行 Fabric 内的扩散操作,以保证 Fabric 内的所有交换机的 Zone 模式的一致性。因此从基本 Zone 模式切换为增强 Zone 模式时,需要满足以下限制:

- Fabric 中的所有交换机都支持增强 Zone 模式。
- Fabric 中不能存在无效的静态路由。因为交换机配置增强 Zone 模式后,会检查 ESS 协商结果。ESS 协商是根据交换机上的路由表进行的,存在无效静态路由的交换机依然会与目的交换机进行 ESS 协商,协商结果默认目的交换机不支持增强 Zone 模式。

进行 Zone 模式切换时,系统将打印提示信息,提醒用户 Zone 模式切换将引发 Zone 数据扩散,是 否要切换模式。如果用户输入 No,则直接返回,不做任何操作;如果用户输入 Yes,则将本地交换 机切换模式,并生成相应配置。完成本地模式切换和配置之后,将向 Fabric 内所有交换机发起扩散。 如果扩散失败,系统将打印日志信息,告知用户扩散失败,但 Zone 模式切换后生成的本地配置不 再回退。此时需要用户主动激发一次完全扩散,以保证 Fabric 内所有交换机的 Zone 模式的一致性。 当从增强 Zone 模式切换为基本 Zone 模式时,若存在激活 Zone set,且激活 Zone set 大小超过了 基本 Zone 模式下激活 Zone set 的最大规格,则切换失败,本交换机的 Zone 模式不变。

表8-3 配置 Zone 模式

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置当前VSAN工作在增强Zone模式	zone mode enhanced	二者选其一
配置当前VSAN工作在基本Zone模式	undo zone mode enhanced	缺省情况下,当前VSAN工作 在基本Zone模式

8.3.2 配置 Zone 的 Pairwise 特性

在 Zone 中开启 Pairwise 特性后,该 Zone 内节点间的访问会受到成员角色的影响,即同一 Zone 内具有不同角色的成员可以互相访问,角色相同的成员间不允许互相访问,兼具两种角色的成员可 以和任意角色的成员互相访问。

在 Zone 中关闭 Pairwise 特性后,该 Zone 内节点间的访问不会受到成员角色的影响,即同一 Zone 内的所有成员之间都可以互相访问。

只允许在增强 Zone 模式下配置

表8-4	配置	Zone	的	Pairwise	特性
------	----	------	---	----------	----

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
进入Zone视图	zone name zone-name	-

操作	命令	说明
开启Zone的Pairwise特性	pairwise-zoning enable	二者选其一
关闭Zone的Pairwise特性	undo pairwise-zoning enable	缺省情况下,Zone的Pairwise特性处于关闭状态

8.3.3 配置 Zone 别名

Zone 别名中的成员可以通过 FC 地址、PWWN 或 FWWN 的方式配置,其中:FWWN 为交换机上 F 端口的 WWN,代表通过该 F 端口 Login 网络的所有 N_Port;而通过 FC 地址和 PWWN 方式所 配置的 N_Port 成员可以不是本机直连的 N_Port,允许任意配置。

用户在配置成员时,可以指定成员的角色(Initiator/Target),成员角色仅支持在增强 Zone 模式下 配置,并且在开启 Pairwise 特性时才生效。

表8-5 配置 Zone 别名

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
创建Zone别名,并进入其视图	zone-alias name zone-alias-name	缺省情况下,不存在Zone别名
在Zone别名内添加成员	member { fcid fcid fwwn fwwn pwwn pwwn } [initiator target]	缺省情况下,新建的Zone别名内不存 在成员

8.3.4 配置 Zone

Zone 中的成员可以通过 FC 地址、PWWN、FWWN 或 Zone 别名的方式配置,其中:FWWN 为交换机上 F 端口的 WWN,代表通过该 F 端口 Login 网络的所有 N_Port; Zone 别名则代表其下配置的一组 N_Port 成员。而无论以何种方式配置的 N_Port 成员,都可以不是本机直连的 N_Port,允许任意配置。一个成员可以同时属于多个 Zone。

用户在配置成员时,可以指定成员的角色(Initiator/Target),成员角色仅支持在增强 Zone 模式下 配置,并且在开启 Pairwise 特性时才生效。

表8-6 配置 Zone

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
创建Zone,并进入其视图	zone name zone-name	缺省情况下,不存在 Zone
在Zone内添加成员	<pre>member { { fcid fcid fwwn fwwn pwwn pwwn } [initiator target] zone-alias zone-alias-name }</pre>	缺省情况下,新建的Zone内不存在成员

8.3.5 配置 Peer Zone

Peer Zone 可以通过 Smart SAN 协议报文自动创建或通过命令行配置将普通 Zone 转换为 Peer Zone。

当需要将一个普通 Zone 转换为 Peer Zone,可以通过表 8-7 所示方式进行配置。

将普通 Zone 转换为 Peer Zone 之前,需要先开启 Smart SAN 功能并指定其应用类型为 FC/FCoE 类型,否则将配置失败。

已开启 Pairwise 特性的 Zone 不能通过本功能切换为 Peer Zone。

表8-7 将普通 Zone 转换为 Peer Zone

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
进入Zone视图	zone name zone-name	缺省情况下,用户创建的Zone为普通 Zone
悠普通 Zone 转拖为		被指定的主成员必须为节点设备上 端口
N 目 远 Z One 积 换 为 Peer Zone,并为其指 定主成员	zone-type peer-zone principal-member wwn	执行本命令后会自动将主成员的成 员角色指定为目的端
庄主成 贝		使用本命令行修改Zone类型时,会同时删除该Zone下已有的配置

8.3.6 配置 Zone set

表8-8 配置 Zone set

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
创建Zone set,并进入其视图	zoneset name zoneset-name	缺省情况下,不存在Zone set
在Zone set内添加Zone	member zone-name	缺省情况下,新建的Zone set内不存在Zone

8.3.7 配置默认 Zone 策略

在增强 Zone 模式下,需要通过激活 Zone set 或扩散命令显式地触发扩散,使默认 Zone 策略随同 其它数据一同向全网扩散。但是在基本 Zone 模式下,必须手动配置全网默认 Zone 策略一致。 在 Zone 模式切换时,无论是基本 Zone 向增强 Zone 切换,还是增强 Zone 向基本 Zone 扩散,默 认 Zone 策略也会随同其它数据一同向全网扩散。

表8-9 配置默认 Zone 策略

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置允许默认Zone内的成员互相访问	zone default-zone permit	二者选其一
配置禁止默认Zone内的成员互相访问	undo zone default-zone permit	缺省情况下,默认Zone内的成员 禁止互相访问

8.3.8 配置 Zone 扩散和合并类型

完全扩散和完全合并会将 Active Zone Set 以及数据库都进行扩散和合并;非完全扩散和非完全合并仅将 Active Zone Set 进行扩散和合并。

需要注意的是:

- 本功能只允许在基本 Zone 模式下配置。在增强 Zone 模式下,扩散和合并类型固定为完全扩 散和完全合并,因此不支持本配置。
- 基本 Zone 模式下,扩散类型仅会对使用 zoneset activate 命令激发的扩散过程产生影响,对 使用 zoneset distrbute 命令激发的扩散不会产生影响。
- 基本 Zone 模式下,合并类型会对所有合并过程产生影响。

表8-10 配置 Zone 扩散和合并类型

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置扩散和合并类型为完全扩散和完全合并	zoneset distribute full	缺省情况下,扩散和合并类型为非 完全扩散和非完全合并

8.3.9 配置 Zone 的合并控制模式

合并控制模式分为两种: Restrict 和 Allow。在增强 Zone 模式下,当 VSAN 内的两台交换机发生合并时,合并操作的结果受其所配置的合并控制模式的影响。并且,只有当发生合并的交换机具有相同的合并控制模式时才允许进行合并,否则合并失败,链路将被隔离。

需要注意的是,本功能仅支持在增强 Zone 模式下配置,该配置需要通过激活 Zone set 或扩散命令 显式地触发扩散,保证全网一致性。

表8-11 配置 Zone 的合并控制模式

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置合并控制模式为Restrict	zone merge-control restrict	二者选其一

操作	命令	说明
配置合并控制模式为Allow	undo zone merge-control restrict	缺省情况下,合并控制模式为Allow

8.3.10 开启硬件 Zone

交换机通过两种方式实现 Zone 访问控制:软件 Zone 和硬件 Zone。

- 软件 Zone 是指当注册后的节点通过通用服务报文查询当前 Fabric 中存在哪些节点时,交换 机将根据 Zone 规则进行过滤,只返回符合 Zone 规则的查询结果。由于软件 Zone 只是一种 针对节点接入时的控制手段,仅能限制节点向交换机进行查询的结果,不能直接控制底层流 量。当节点直接针对应该被 Zone 规则过滤掉的节点进行流量攻击时,软件 Zone 无法对其进 行访问控制。
- 硬件 Zone 是将 Zone 配置转化为底层驱动规则并下发到硬件,形成硬件 Zone 规则,通过硬 件 Zone 规则可以直接控制交换机上的报文流量按照 Zone 规则转发,是一种严密的控制手段。

两种方式各自独立存在,相辅相成,共同完成按照 Zone 配置进行节点访问控制的功能。

当底层资源足够下发 Zone 规则时,硬件 Zone 才能生效,而软件 Zone 一直处于生效状态。当底层 资源足够下发当前 VSAN 的硬件 Zone 规则时,该 VSAN 的软件 Zone 和硬件 Zone 一起生效: 当 底层资源不够下发当前 VSAN 的硬件 Zone 规则时,为了保证规则的完整性,系统会清空该 VSAN 已经下发的硬件 Zone 规则,自动切换为硬件 Zone 未生效状态,此时该 VSAN 下只有软件 Zone 继续生效。

当用户希望增强某 VSAN 的安全性时,可以开启该 VSAN 的硬件 Zone。当用户认为软件 Zone 能 够满足某 VSAN 的节点访问控制要求时,可以关闭该 VSAN 的硬件 Zone,节约硬件表项资源供其 它重要 VSAN 使用。

开启某VSAN的硬件Zone后,系统将触发一次下发该VSAN的所有Zone规则的操作;关闭某VSAN 的硬件 Zone 后,系统会清空该 VSAN 当前已经下发的硬件 Zone 规则,并且后续不会下发任何新 的硬件 Zone 规则。

在增强 Zone 模式下,需要通过激活 Zone set 或扩散命令显式地触发扩散,使硬件 Zone 配置随同 其它数据一同向全网扩散。但是在基本 Zone 模式下,必须手动配置保证全网硬件 Zone 配置的一 致性。

用户可以通过 display zone status 命令查询当前硬件 Zone 的生效状态。

需要注意的是,当交换机处于合并或扩散状态时,不能配置本命令。

表8-12 开启硬件 Zone		
操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
开启硬件Zone	zone hard-zoning enable	缺省情况下,硬件Zone处于开启状态

8.3.11 激活 Zone set 并发起向全网的扩散过程

激活指定 Zone set,使其成为 Active Zone set,同时向全网进行扩散,并以此 Zone set 配置进行 访问控制。用户执行的后续配置不会影响当前 Active Zone set数据,直到去激活当前 Active Zone set、 重新配置激活命令、进行数据扩散或进行合并。

激活 Zone set 时,用户需保证所激活的 Zone set 必须已经存在,且被激活的 Zone set 中至少要包含一个 N_Port 成员。如果当前 Zone 模式为基本 Zone,则激活成功与否还会受到基本 Zone 下 Active Zone set 最大规格的限制,若超过了最大规格,则激活失败。

同一 VSAN 内只能够存在一个 Active Zone set。

在基本 Zone 模式下,将 Active Zone set 进行全网扩散时,交换机会根据 zoneset distribute full 命令配置的扩散类型来决定扩散时要携带的数据。但在增强 Zone 模式下,不支持 zoneset distribute full 命令,激活扩散为完全扩散。

无论是在增强 Zone 模式下还是在基本 Zone 模式下,如果扩散失败,系统将打印日志信息,告知 用户扩散失败。用户解决了网络故障后,用户需要重新激活该 Zone set,以保证 Fabric 内所有交换 机的 Active Zone set 数据的一致性。

表8-13 激活 Zone set 并发起向全网的扩散过程

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
激活指定Zone set生成Active Zone Set, 并发起向全网的扩散过程	zoneset activate name zoneset-name	-

🕑 说明

不支持在 Active Zone set 信息中以 Zone 别名显示成员。配置激活 Zone set 后,如果该 Zone set 中的 Zone 存在 Zone 别名类型成员,会直接将 Zone 别名中的非重复 N_Port 成员添加到 Zone。用 户能够通过显示命令 display zoneset active 观察这一变化。

8.3.12 激发完全扩散过程

配置该命令会触发一次 Zone 数据扩散流程,且为完全扩散,即将 Active Zone set 和 Zone 数据库 (增强 Zone 模式下还会携带 Zone 策略和硬件 Zone 开启情况)均携带在报文中进行扩散。

使用激活命令 **zoneset activate** 激活一个 Zone set 成为 Active Zone set 后,用户可以继续修改数 据库的配置,本命令可以在不改变 Active Zone set 的同时将 Active Zone set 以及修改后的数据库 向全网扩散。

如果扩散失败,系统将打印日志信息,告知用户扩散失败。用户解决了网络故障后,用户需要重新 激发一次完全扩散,以保证 Fabric 内所有交换机的 Zone 数据的一致性。

表8-14 激发完全扩散过程

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
激发完全扩散过程	zoneset distribute	-

8.3.13 重命名 Zone 别名、Zone、Zone set

用户可以通过下面的配置修改 Zone 别名、Zone、Zone set 的名称。

```
表8-15 重命名 Zone 别名、Zone、Zone set
```

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
修改Zone别名的名称	zone-alias rename old-name new-name	待重命名的Zone别名必须已创建,新的 Zone别名必须未被创建
修改Zone的名称	zone rename old-name new-name	待重命名的Zone必须已创建,新的 Zone必须未被创建
修改Zone set的名称	zoneset rename old-name new-name	待重命名的Zone set必须已创建,新的 Zone set必须未被创建

8.3.14 复制 Zone 别名、Zone、Zone set

用户可以通过复制一个已经存在的 Zone 别名、Zone、Zone set,产生新的 Zone 别名、Zone、Zone set。二者名称不同,但包含的内容相同。

表8-16 复制 Zone 别名、Zone、Zone set

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
复制Zone别名	zone-alias clone src-name dest-name	被复制的Zone别名必须已创建,复制后的目的Zone别名必须未被创建
复制Zone	zone clone src-name dest-name	被复制的Zone必须已创建,复制后的目的Zone必须未被创建
复制Zone set	zoneset clone src-name dest-name	被复制的Zone set必须已创建,复制后的目的Zone set必须未被创建

8.3.15 清除 Zone 数据库信息

通过本命令可以删除指定 VSAN 内的 Zone 数据库信息,包括所有 Zone set、Zone 以及 Zone 别名, 但是 Active Zone set 不会被删除。

表8-17 清除 Zone 数据库信息

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
清除Zone数据库信息	delete zone database all	-

8.3.16 开启 Zone 的告警功能

开启了 Zone 的告警功能后, Zone 会生成告警信息,以向网管软件报告本模块的重要事件。该信息 将发送至 SNMP 模块,通过设置 SNMP 中告警信息的发送参数,来决定告警信息输出的相关属性。 有关告警信息的详细介绍,请参见"网络管理和监控配置指导"中的"SNMP"。

表8-18 开启 Zone 告警功能

操作	命令	说明
进入系统视图	system-view	-
开启Zone模块的告警功能	snmp-agent trap enable fc-zone [activation-completed defaultzone-change hardzone-change merge-failed merge-succeeded] *	缺省情况下,Zone的告警功能 处于关闭状态

8.4 FC Zone显示和维护

在完成上述配置后,在任意视图下执行 display 命令可以显示配置后 FC Zone 的运行情况,通过查看显示信息验证配置的效果。

表8-19 FC Zone 显示和维护

操作	命令
显示Zone别名的相关信息	display zone-alias [[name zone-alias-name] vsan vsan-id]
显示Zone的相关信息	display zone [[name zone-name] vsan vsan-id]
显示Zone set的相关信息	display zoneset [[name zoneset-name] vsan vsan-id]
显示Active Zone set的相关信息	display zoneset active [vsan vsan-id]
显示指定Zone成员所属的父亲信息(父亲 信息包括:成员所属的Zone和Zone别名, 以及Zone别名所属的Zone)	display zone member { fcid fcid pwwn pwwn zone-alias zone-alias-name } [vsan vsan-id]
显示FC Zone的配置信息以及运行状态	display zone status [vsan vsan-id]
显示Zone报文统计信息	display zone statistics [vsan vsan-id]

操作	命令
清除Zone报文统计信息	reset zone statistics [vsan vsan-id]

8.5 FC Zone典型配置举例

1. 组网需求

VSAN 1 内 3 台服务器和 3 个磁盘设备共同接入一个 Fabric 中,节点设备分别以 FC 地址或 PWWN 进行标识,如图 8-5 所示。所有节点设备均已向交换机完成注册。 VSAN 1 中需要对访问权限进行控制,具体需求如下:

- 服务器 Server A 不访问磁盘,但以后有可能添加访问磁盘需求。
- 服务器 Server B 能访问磁盘 Disk A、Disk B、Disk C 的数据。
- 服务器 Server C 能访问磁盘 Disk B、Disk C 的数据。
- 服务器之间不能相互访问。

2. 组网图

图8-5 配置 FC Zone 组网图 Disk A Server A PWWN: Zone 1 FC ID: 11:22:33:44:55:66:77:88 010001 (FC_ID:020006) Switch A Switch B Disk B Server B PWWN: FC ID: 22:33:44:55:66:77:88:99 010002 (FC ID:020005) Zone 2 Alias 1 Server C Disk C Zone 3 FC ID: FC_ID: 020004 010003

3. 配置思路

为实现上述需求,考虑将 VSAN 1 划分为 3 个 Zone,其中:

- Zone1 包括 Server A
- Zone2 包括 Server B、Disk A、Disk B、Disk C
- Zone3 包括 Server C、Disk B、Disk C
- Zone2 开启 Pairwise 特性, 配置 Server B 角色为 Initiator, Disk A、Disk B、Disk C 角色为 Target
- Zone3 开启 Pairwise 特性, 配置 Server C 角色为 Initiator, Disk B、Disk C 角色为 Target

同时创建 Zone 别名 Alias1 包含 Disk B、Disk C,以简化配置。 创建 Zone set Zoneset1 包括 Zone1、Zone2、Zone3 并激活生效。 在 Switch A 上进行配置并激活,将当前完整数据库配置同步到 Switch B。

4. 配置步骤

💕 说明

- 只需在 Switch A 上进行如下配置, Switch B 上不需要进行 Zone 相关配置。
- 本例中只列出 Zone 相关配置, 其它配置步骤略。

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view

[SwitchA] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchA] save

[SwitchA] quit

<SwitchA> reboot

配置 FCoE 模式为 FCF 模式。

<SwitchA> system-view

[SwitchA] fcoe-mode fcf

配置 VSAN 1 工作在增强 Zone 模式。

[SwitchA] vsan 1

[SwitchA-vsan1] zone mode enhanced

The zoning database in this switch would be distributed throughout the fabric. Continue? $[{\tt Y}/{\tt N}]\!:\!{\tt y}$

[SwitchA-vsan1]

创建 Zone 别名 Alias1,添加 PWWN 为 22:33:44:55:66:77:88:99、FC 地址为 020004 的两个成员,即 Disk B 和 Disk C,角色均为 Target。

[SwitchA-vsan1] zone-alias name Alias1

[SwitchA-vsan1-zone-alias-Alias1] member pwwn 22:33:44:55:66:77:88:99 target

[SwitchA-vsan1-zone-alias-Alias1] member fcid 020004 target

[SwitchA-vsan1-zone-alias-Alias1] quit

创建 Zone1, 添加 FC 地址为 010001 的成员。创建 Zone2,开启其 Pairwise 特性,添加 FC 地 址为 010002 的成员,角色为 Initiator;添加 PWWN 为 11:22:33:44:55:66:77:88 的成员,角色为 Target;添加 Zone 别名为 Alias1 的成员。创建 Zone3,开启其 Pairwise 特性,添加 FC 地址为 010003 的成员,角色为 Initiator;添加 Zone 别名为 Alias1 的成员。

[SwitchA-vsan1] zone name Zone1

[SwitchA-vsan1-zone-Zone1] member fcid 010001

[SwitchA-vsan1-zone-Zone1] quit

[SwitchA-vsan1] zone name Zone2

[SwitchA-vsan1-zone-Zone2] pairwise-zoning enable

[SwitchA-vsan1-zone-Zone2] member fcid 010002 initiator

[SwitchA-vsan1-zone-Zone2] member pwwn 11:22:33:44:55:66:77:88 target

```
[SwitchA-vsan1-zone-Zone2] member zone-alias Alias1
[SwitchA-vsan1-zone-Zone2] quit
[SwitchA-vsan1] zone name Zone3
[SwitchA-vsan1-zone-Zone3] pairwise-zoning enable
[SwitchA-vsan1-zone-Zone3] member fcid 010003 initiator
[SwitchA-vsan1-zone-Zone3] member zone-alias Alias1
[SwitchA-vsan1-zone-Zone3] quit
# 创建 Zone set Zoneset1,添加 Zone1、Zone2、Zone3 为其成员。
[SwitchA-vsan1] zoneset name Zoneset1
[SwitchA-vsanl-zoneset-Zoneset1] member Zone1
[SwitchA-vsan1-zoneset-Zoneset1] member Zone2
[SwitchA-vsan1-zoneset-Zoneset1] member Zone3
[SwitchA-vsan1-zoneset-Zoneset1] quit
# 配置扩散和合并类型为完全扩散和完全合并,即携带完整数据库信息进行数据同步。
[SwitchA-vsan1] zoneset distribute full
# 激活 Zone set 并发起向全网的扩散过程。
[SwitchA-vsan1] zoneset activate name Zoneset1
```

5. 验证配置

在 Switch A 和 Switch B 上通过显示命令都能够观察到 Zone 配置结果和数据同步结果。下面以 Switch B 上的显示为例:

查看 VSAN 1 内的 Zone set 相关信息。

```
<SwitchB> display zoneset vsan 1
VSAN 1:
  zoneset name Zoneset1
    zone name Zonel
      fcid 0x010001
    zone name Zone2
      fcid 0x010002 initiator
      pwwn 11:22:33:44:55:66:77:88 target
      zone-alias Alias1
        fcid 0x020004 target
        pwwn 22:33:44:55:66:77:88:99 target
    zone name Zone3
      fcid 0x010003 initiator
      zone-alias Alias1
        fcid 0x020004 target
        pwwn 22:33:44:55:66:77:88:99 target
```

查看 VSAN 1 内 Zone2 的相关信息。

```
<SwitchB> display zone name Zone2 vsan 1
VSAN 1:
zone name Zone2
fcid 0x010002 initiator
pwwn 11:22:33:44:55:66:77:88 target
zone-alias Alias1
fcid 0x020004 target
pwwn 22:33:44:55:66:77:88:99 target
```

```
#查看所有 Zone 别名的相关信息。
```

```
<SwitchB> display zone-alias
VSAN 1:
zone-alias name Alias1
fcid 0x020004 target
```

pwwn 22:33:44:55:66:77:88:99 target

查看 FC 地址类型成员 020004 所属于的 Zone 或 Zone 别名。

```
<SwitchB> display zone member fcid 020004
```

fcid 0x020004

```
VSAN 1:
```

zone-alias Alias1

zone Zone2

zone Zone3

查看 VSAN 1 内的 Active Zone set 相关信息。

```
<SwitchB> display zoneset active vsan 1
VSAN 1:
zoneset name Zoneset1
zone name Zone1
 *fcid 0x010001
zone name Zone2
 *fcid 0x020004
 *fcid 0x020005 [pwwn 22:33:44:55:66:77:88:99]
 *fcid 0x020006 [pwwn 11:22:33:44:55:66:77:88]
zone name Zone3
 *fcid 0x010003
 *fcid 0x020004
 *fcid 0x020005 [pwwn 22:33:44:55:66:77:88:99]
```

9 NPV

9.1 NPV简介

NPV 功能可以使 FC SAN 中的交换机突破 239 台最大数目的限制,扩充网络的规模。 NPV 交换机位于 Fabric 网络边缘,处于节点设备与核心交换机之间,将节点设备的流量转发到核 心交换机。NPV 的典型组网如图 9-1 所示。



🗑 提示

NPV 交换机和核心交换机之间必须直连。

9.1.1 下行口和下行链路

NPV 交换机上,和节点设备相连的接口称为下行口,也称之为 server interface。

下行口是 VFC 接口,且接口必须配置为 F 模式。

下行链路是 NPV 交换机和节点设备之间的链路。

每个下行口会唯一映射到一个生效(链路 up)的上行口,所有和该下行口相连的节点设备的数据都 会通过映射的上行口转发到核心交换机。

9.1.2 上行口和上行链路

NPV 交换机上,和核心交换机相连的接口称为上行口,也称之为 external interface。

上行口是 VFC 接口,且接口必须配置为 NP 模式。

上行链路是 NPV 交换机和核心交换机之间的链路。

在上行链路生效后,NPV 交换机向核心交换机发送 FLOGI 报文进行注册,核心交换机将为上行口 (NP 端口)分配一个 FC 地址。随后,NPV 交换机将向核心交换机的名称服务进行注册。后续, 当 NPV 交换机从下行口上收到节点设备发送的报文(包括注册报文在内的所有报文)时,NPV 交 换机负责将报文从该下行口映射的上行口发送给核心交换机,并将回应报文从下行口转发给节点设备。

9.1.3 上下行口流量映射

NPV 交换机会自动的进行上下行口的映射,在下行口生效前,NPV 交换机会从当前所有生效的上行口中选择一个负载最小的上行口,将下行口映射到选中的上行口。这里的负载是指上行口上映射的下行口的数目。

在自动映射不能满足组网需求(比如需要下行口通过指定的上行口连接到 Fabric 网络)时,可以通 过配置上下行口映射关系来将下行口映射到指定的上行口或上行口的集合。一旦配置了映射关系, 则下行口就只能映射到用户配置的上行口,如果配置的上行口都没有生效,则下行口也无法生效。 在有配置的映射关系时,进行上下行口映射是从用户配置的上行口集合中选择负载最小的上行口, 然后将下行口映射到选中的上行口。

上下行口建立映射关系后,从下行口过来的流量均通过映射的上行口进行转发。

9.1.4 负载均衡

1. 手动负载均衡

缺省情况下,当有新的上行口生效时,NPV 交换机并不会自动对已有的上下行口映射进行重新映射, 以达到负载均衡。因为重新映射时,NPV 交换机将对下行口进行链路初始化,会破坏已经稳定的上 下行口的映射关系,以及要求和下行口相连的节点设备重新进行注册,这样会导致流量中断。 当有新的上行口生效时,如果用户希望重新进行上下行口映射,以达到更好的负载均衡效果,可以 通过命令行立即触发一次重新映射,此时会对部分下行口进行链路初始化。

部分进行链路初始化的下行口选择步骤如下:

- (1) NPV 交换机计算出上行口负载平均值,上行口负载平均值=所有下行口数/所有上行口数。
- (2) NPV 交换机遍历出超过该负载平均值的上行口。
- (3) 这些上行口若存在自动映射的下行口,则 NPV 交换机会按先后自动映射顺序将先自动映射的 下行口进行链路初始化。需要进行链路初始化的下行口数=该上行口的所有下行口数-上行口负 载平均值,从而使得上行口的下行口数量不超过上行口负载平均值。
- (4) 这些上行口若不存在自动映射的下行口,则 NPV 交换机不会对这些上行口的下行口进行链路 初始化。

2. 自动负载均衡

自动负载均衡与手动负载均衡对下行口重新映射的策略是相同的。开启自动负载均衡后,当系统检测到 up 的上行口时,会自动创建一个延迟定时器,待定时器超时后,系统将自动进行一次负载均衡。如果在定时器超时前又有新的上行口 up,则重置该定时器。

可以通过配置自动负载均衡的延迟时间来缓冲上行口的 up、down 而引起震荡,以减少对自动负载 均衡的影响。

9.2 NPV配置任务简介

表9-1 NPV 配置任务简介

配置任务	说明	详细配置
配置交换机工作在NPV模式	必选	<u>2.2</u>
配置上下行口	必选	<u>9.3</u>
配置上下行口映射关系	可选	<u>9.4</u>
配置发起手动负载均衡功能	可选	<u>9.5</u>
配置自动负载均衡功能	可选	<u>9.6</u>

9.3 配置上下行口

交换机工作在 NPV 模式后,用户需要配置上行口和下行口。

9.3.1 配置上行口

上行口是 VFC 接口,且接口必须配置为 NP 模式。

表9-2 配置上行口

操作	命令	说明
进入系统视图	system-view	-
进入VFC接口视图	interface vfc interface-number	该接口与核心交换机相连
配置接口为NP模式	fc mode np	缺省情况下,NPV模式交换机的VFC 接口为F模式

9.3.2 配置下行口

下行口是 VFC 接口,且接口必须配置为 F 模式。

表9-3 配置下行口

操作	命令	说明
进入系统视图	system-view	-
进入VFC接口视图	interface vfc interface-number	该接口与节点设备相连
配置接口为F模式	fc mode f	缺省情况下,NPV模式交换机的VFC 接口为F模式

9.4 配置上下行口映射关系



配置上下行口的映射关系后,如果下行口当前映射的上行口不在配置的映射关系中,则触发下行口 链路初始化,流量中断。

NPV 交换机会自动进行上下行口的映射,当上下行口自动映射不能满足组网需求(比如需要下行口通过指定的上行口连接到 Fabric 网络)时,可以通过配置上下行口映射关系来将下行口映射到指定的上行口或上行口的集合。

一旦配置了映射关系,则下行口就只能映射到用户配置的上行口,如果配置的上行口都没有生效,则下行口也无法生效。在有配置的映射关系时,进行上下行口映射是从用户配置的上行口集合中选择负载最小的上行口,然后将下行口映射到选中的上行口。

表9-4 配置上下行口映射关系

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置上下行口的 映射关系	npv traffic-map server-interface interface-type interface-number external-interface interface-type interface-number	缺省情况下,上下行口 之间不存在映射关系

9.5 配置发起手动负载均衡功能

表9-5 配置发起手动负载均衡功能

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
配置发起一次手动负载均衡 过程	npv load-balance disruptive	-

9.6 配置自动负载均衡功能

如果上行口的链路层状况良好,可适当将减小延迟时间;否则,需增大延迟时间。

🖞 提示

开启了自动负载均衡功能后,上行口的 up 可能引起负载均衡的发生,从而可能导致流量中断。 关闭了自动负载均衡功能后,不会影响现有的上下行口映射关系。

表9-6 配置自动负载均衡功能

操作	命令	说明
进入系统视图	system-view	-
进入VSAN视图	vsan vsan-id	-
开启自动负载均衡功能	npv auto-load-balance enable	缺省情况下,自动负载均衡功能处于关闭状态
配置自动负载均衡的延迟 时间	npv auto-load-balance-interval interval	缺省情况下,自动负载均衡的延迟时间为30秒

9.7 NPV显示和维护

在完成上述配置后,在任意视图下执行 **display** 命令可以显示配置后 NPV 的运行情况,通过查看显示信息验证配置的效果。

表9-7 NPV 显示和维护

操作	命令
显示NPV交换机向FCF交换机进行注册 的信息以及获取到的管理地址	display fc nport [interface interface-type interface-number]
显示NPV交换机的下行口上相连的节点 设备的注册信息和映射的上行口	display npv login [vsan vsan-id] [interface interface-type interface-number] display npv login [vsan vsan-id] count
显示NPV交换机上的流量映射信息	display npv traffic-map [vsan <i>vsan-id</i>] [interface <i>interface-type interface-number</i>]
显示NPV交换机的状态信息	display npv status [vsan vsan-id]

9.8 NPV典型配置举例

9.8.1 NPV 配置举例

1. 组网需求

如<u>图 9-2</u>所示,网络由边缘交换机 Switch A、核心交换机 Switch B 和两个服务器组成。 要求:将边缘交换机 Switch A 配置为 NPV 交换机,以便扩充网络规模。

2. 组网图

图9-2 配置 NPV 组网图 Server A VFC1 Switch A VFC3 XGE1/0/3 VFC3 XGE1/0/3 XGE1/0/3 XGE1/0/3 Switch B Fabric Switch B

3. 配置步骤

(1) 配置 Switch A

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view

[SwitchA] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchA] save

[SwitchA] quit

<SwitchA> reboot

配置 Switch A 的 FCoE 模式为 NPV 模式,进入 VSAN 1 的视图。

<SwitchA> system-view

[SwitchA] fcoe-mode npv

[SwitchA] vsan 1

[SwitchA-vsan1] quit

创建 VFC 接口 VFC1,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文通过 VFC1 接口。

[SwitchA] interface vfc 1

[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchA-Vfc1] port trunk vsan 1

[SwitchA-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/1

[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[SwitchA-Ten-GigabitEthernet1/0/1] quit

创建 VFC 接口 VFC2,将 VFC2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2 上,并将 VFC2 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文通过 VFC2 接口。

[SwitchA] interface vfc 2

[SwitchA-Vfc2] bind interface ten-gigabitethernet 1/0/2

[SwitchA-Vfc2] port trunk vsan 1

```
[SwitchA-Vfc2] quit
```

配置以太网接口 Ten-GigabitEthernet1/0/2 允许 VLAN 10 的报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/2

[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10

[SwitchA-Ten-GigabitEthernet1/0/2] quit

```
# 创建 VFC 接口 VFC3,将 VFC3 接口绑定到以太网接口 Ten-GigabitEthernet1/0/3 上,并将 VFC3 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文通过 VFC3 接口。
```

[SwitchA] interface vfc 3

[SwitchA-Vfc3] bind interface ten-gigabitethernet 1/0/3

[SwitchA-Vfc3] port trunk vsan 1

[SwitchA-Vfc3] quit

配置以太网接口 Ten-GigabitEthernet1/0/3 允许 VLAN 10 的报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/3

[SwitchA-Ten-GigabitEthernet1/0/3] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10

[SwitchA-Ten-GigabitEthernet1/0/3] quit

#开启 VLAN 10 的 FCoE 功能,并将其与 VSAN 1 进行映射。

[SwitchA] vlan 10

[SwitchA-vlan10] fcoe enable vsan 1

[SwitchA-vlan10] quit

配置上行口。

[SwitchA] interface vfc 3 [SwitchA-Vfc3] fc mode np [SwitchA-Vfc3] quit

配置下行口。

[SwitchA] interface vfc 1 [SwitchA-Vfc1] fc mode f [SwitchA-Vfc1] quit [SwitchA] interface vfc 2 [SwitchA-Vfc2] fc mode f [SwitchA-Vfc2] quit

(2) 配置 Switch B

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchB> system-view

[SwitchB] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the

system to make it effective.

[SwitchB] save

[SwitchB] quit

<SwitchB> reboot

配置 Switch B 的 FCoE 模式为 FCF 模式,进入 VSAN 1 的视图。

<SwitchB> system-view [SwitchB] fcoe-mode fcf [SwitchB] vsan 1
[SwitchB-vsan1] quit

创建 VFC 接口 VFC3, 配置 VFC3 接口工作在 F 模式,将 VFC3 接口绑定到以太网接口 Ten-GigabitEthernet1/0/3 上,并将 VFC3 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC3 接口。

[SwitchB] interface vfc 3

[SwitchB-Vfc3] fc mode f

[SwitchB-Vfc3] bind interface ten-gigabitethernet 1/0/3

[SwitchB-Vfc3] port trunk vsan 1

[SwitchB-Vfc3] quit

配置以太网接口 Ten-GigabitEthernet1/0/3 允许 VLAN 10 的报文通过。

[SwitchB] interface ten-gigabitethernet 1/0/3

[SwitchB-Ten-GigabitEthernet1/0/3] port link-type trunk

[SwitchB-Ten-GigabitEthernet1/0/3] port trunk permit vlan 10

[SwitchB-Ten-GigabitEthernet1/0/3] quit

#开启 VLAN 10的 FCoE 功能,并将其与 VSAN 1进行映射。

[SwitchB] vlan 10

[SwitchB-vlan10] fcoe enable vsan 1

[SwitchB-vlan10] quit

4. 验证配置

#显示 NPV 交换机 Switch A 的下行口上连接的节点设备的 Login 信息和映射的上行口。

[SwitchA] display npv login

Server					External
Interface	VSAN	FCID	Node WWN	Port WWN	Interface
Vfcl	1	0x010001	21:00:00:c8:00:e4:30	20:00:00:00:c8:60:e4:9a	Vfc3
Vfc2	1	0x010002	21:00:00:c9:00:e4:30	20:00:00:00:c9:60:e4:9a	Vfc3

#显示 NPV 交换机 Switch A 的状态信息。

[SwitchA] display npv status External Interfaces: Interface: Vfc3 VSAN tagging mode: Tagging VSAN State FCID 1 Up 0x010000 Number of External Interfaces: 1 Server Interfaces: Interface : Vfc1 VSAN tagging mode: Tagging VSAN State 1 Up Interface : Vfc2 VSAN tagging mode: Tagging VSAN State 1 IJρ

Number of Server Interfaces: 2 # 显示 NPV 交换机 Switch A 上的流量映射信息。 [SwitchA] display npv traffic-map NPV traffic map information of VSAN 1: Server Interface External Interface Vfc1 Vfc3 Vfc2 Vfc3

$10\,$ FIP Snooping

10.1 FIP Snooping简介

在 FC Fabric 网络中,节点设备必须向 Fabric 注册后才能和 FC SAN 中设备进行通信。节点设备和 FCF 交换机之间的物理连接是点对点的,只有节点设备成功注册后,FCF 交换机上连接这个节点设备的接口才能 up,所以 FCF 交换机可以控制只有成功注册的节点设备才可以和 FC SAN 中的设备 进行通信。

FCoE 增加了组网的灵活性,在 ENode 和 FCF 交换机之间可以存在 Transit 交换机,这就使得 FCF 交换机和 ENode 之间的物理连接不再是点对点连接,这样则会出现即使没有注册的 ENode 设备也 可能通过 FCF 交换机和 FC SAN 中的设备进行通信。比如,两个 ENode 通过一台 Transit 交换机 接入到同一台 FCF 交换机,其中一个 ENode 在 FCF 交换机上成功注册后,FCF 交换机上的接口 变为 up,此时,另外一个没有注册的 ENode 就可以通过该 FCF 交换机和 FC SAN 中的设备进行 通信了。

FIP Snooping(FCoE Initialization Protocol Snooping, FCoE 初始化探测协议)可以解决上述问题, 它是应用在 FCoE 网络边缘设备上的一种安全特性,该特性只能运行在 Transit 交换机上。FIP Snooping 通过对报文 MAC 地址的检查来限定 ENode 发送的报文仅能转发给 FCF 交换机,不能转 发给 ENode,且只有成功注册的 ENode 发送的 FCoE 报文才能被 Transit 交换机转发给 FCF 交换 机,以及限定 FCF 交换机发送的 FCoE 报文仅能被 Transit 交换机转发给已经注册的 ENode。

10.1.1 FIP Snooping 典型组网

FIP Snooping 典型组网如图 10-1 所示。ENode 通过 Transit 交换机接入 FCF 交换机。



图10-1 FIP Snooping 组网

Transit 交换机上的以太网接口有两种模式: FCF 模式和 ENode 模式。与 ENode 相连的以太网接口需要配置为 ENode 模式; 与 FCF 交换机相连的以太网接口需要配置为 FCF 模式。

在 Transit 交换机上开启 FIP Snooping 功能,并将以太网接口配置为正确的模式后,就可以控制 ENode 和 FCF 交换机之间报文的交互,以达到安全接入和通信的目的。

10.1.2 FIP Snooping 工作机制

开启 VLAN 的 FIP Snooping 功能后,Transit 交换机上的以太网接口开始根据 FIP 协议报文(以太 网报文类型为 0x8914)来建立 FIP Snooping 规则,然后根据 FIP Snooping 规则来控制 FCoE 报 文(以太网报文类型为 0x8906)的转发。

为方便描述,做如下定义:

- FCF 模式以太网接口生成的 FIP Snooping 规则称为 FCF FIP Snooping 规则。
- ENode 模式以太网接口生成的 FIP Snooping 规则称为 ENode FIP Snooping 规则。

1. 建立 FIP Snooping 规则

FIP Snooping 规则是在 ENode 和 FCF 交换机之间通过 FIP 协议建立虚链路的过程中建立的,其建立过程简单描述如下:

- (1) Transit 交换机 FCF 模式以太网接口收到 FCF 交换机的非请求发现通告报文后,据其生成 FCF FIP Snooping 规则并将该报文转发给 ENode。生成的 FCF FIP Snooping 规则为:允许源 MAC 地址为该非请求发现通告报文中的源 MAC 地址(即 FCF 交换机的 FCoE MAC 地址)、目的 MAC 地址高三个字节为 FC-MAP 的 FCoE 报文通过。
- (2) Transit 交换机 ENode 模式以太网接口收到 ENode 向 FCF 交换机发送的发现请求报文后,转 发该报文给 FCF 交换机。
- (3) Transit 交换机 ENode 模式以太网接口接收到 FIP FLOGI 请求报文后,将该报文转发给 FCF 交换机。
- (4) Transit 交换机 ENode 模式以太网接口在转发来自 FCF 交换机的 FLOGI LS_ACC 报文时,据 其获取 FCF 交换机分配给 ENode 的 FC 地址以及 FCF 交换机的 FCoE MAC 地址,并生成 ENode FIP Snooping 规则。该规则允许源 MAC 地址为 FC 地址对应的 MAC 地址(即高三个 字节为 FC-MAP,低三个字节为 FC 地址)、目的 MAC 地址为 FCF 交换机的 FCoE MAC 地 址的 FCoE 报文通过。

FIP Snooping 规则建立后,如果虚链路存在,则规则会一直存在,如果虚链路被删除,则规则会被同步删除。

2. 控制 FCoE 报文的转发

建立 FIP Snooping 规则后, Transit 交换机就可以根据 FIP Snooping 规则来控制 ENode 和 FCF 交换机之间 FCoE 报文的转发:对于接收的 FCoE 报文,如果能够匹配学习到的 FIP Snooping 规则则转发,否则,丢弃该 FCoE 报文。从而,可以保证只有成功注册的 ENode 可以和 FCF 交换机进行 FCoE 报文的交互。

10.2 FIP Snooping配置任务简介

只有 Transit 交换机支持 FIP Snooping 功能。

表10-1 FIP Snooping 配置任务简介

配置任务	说明	详细配置
配置交换机工作在Transit模式	必选	<u>2.2</u>
开启FIP Snooping功能	必选	<u>10.3</u>
配置以太网接口的模式	必选	<u>10.4</u>

配置任务	说明	详细配置
配置FC-MAP值	可选	<u>10.5</u>

10.3 开启FIP Snooping功能

开启 VLAN 的 FIP Snooping 功能后, Transit 交换机开始根据 FIP 协议报文建立 FIP Snooping 规则, 然后根据 FIP Snooping 规则来控制 FCoE 报文的转发。

表10-2 开启 FIP Snooping 功能

操作	命令	说明
进入系统视图	system-view	-
进入VLAN视图	vlan vlan-id	-
开启FIP Snooping功能	fip-snooping enable	缺省情况下,FIP Snooping功能处于关闭状态

10.4 配置以太网接口的模式

Transit 交换机上的以太网接口有两种模式: FCF 模式和 ENode 模式。与 ENode 相连的以太网接口需要配置为 ENode 模式; 与 FCF 交换机相连的以太网接口需要配置为 FCF 模式。

表10-3 配置以太网接口的模式

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网接口视图 /二层聚合接口视图	interface interface-type interface-number	-
配置以太网接口的模式	fip-snooping port-mode { enode fcf }	缺省情况下,以太网接口为ENode模式

10.5 配置FC-MAP值

FC-MAP值用来标识一个FCoE网络,同一个FCoE网络中的所有交换机(包括FCF交换机和Transit 交换机)必须具有相同的FC-MAP值。

Transit交换机上某 VLAN 中的以太网接口从 FCF 交换机接收到报文后,会检查接收报文的 FC-MAP 值(此 FC-MAP 值可以在 FCF 交换机上通过 fcoe fcmap 命令配置)和 Transit 交换机上该 VLAN 下配置的 FC-MAP 值是否一致:如果一致,则转发报文;如果不一致,则丢弃报文。

表10-4	配置	FC-MAP1	直
-------	----	---------	---

操作	命令	说明
进入系统视图	system-view	-
进入VLAN视图	vlan vlan-id	-

操作	命令	说明
配置FC-MAP值	fip-snooping fc-map fc-map	缺省情况下,FC-MAP值为0x0efc00

10.6 FIP Snooping显示和维护

在完成上述配置后,在任意视图下执行 **display** 命令可以显示配置后 **FIP** Snooping 的运行情况,通过查看显示信息验证配置的效果。

表10-5 FIP Snooping 显示和维护

操作	命令
显示Transit交换机获取到的ENode信息	display fip-snooping enode [vlan vlan-id]
显示Transit交换机获取到的FCF交换机信息	display fip-snooping fcf [vlan vlan-id]
显示已经下刷的FIP Snooping规则(独立运行模式)	display fip-snooping rules [enode fcf] [vlan vlan-id] [slot slot-number]
显示已经下刷的FIP Snooping规则(IRF模式)	display fip-snooping rules [enode fcf] [vlan vlan-id] [chassis chassis-number slot slot-number]
显示正在下刷的FIP Snooping规则	display fip-snooping flushing-rules [enode fcf] [vlan vlan-id]
显示FIP Snooping的会话信息,即ENode和FCF 交换机的连接信息	display fip-snooping sessions [vlan vlan-id]

10.7 FIP Snooping典型配置举例

1. 组网需求

网络由两台分别工作在 Transit 模式和 FCF 模式的交换机以及 ENode 节点组成。 要求配置 FIP Snooping 功能,使 ENode 和 FCF 交换机之间可以进行可靠的通信。

2. 组网图

图10-2 配置 FIP Snooping 组网图



3. 配置步骤

(1) 配置 Transit 交换机

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<Transit> system-view

[Transit] system-working-mode advance

Do you want to change the system working mode? $[{\rm Y}/{\rm N}]{\rm\, :y}$

The system working mode is changed, please save the configuration and reboot the system to make it effective.

[Transit] save

[Transit] quit

<Transit> reboot

配置 FCoE 模式为 Transit 模式。

<Transit> system-view

[Transit] fcoe-mode transit

#开启 VLAN 10的 FIP Snooping 功能。

[Transit] vlan 10

[Transit-vlan10] fip-snooping enable

配置 VLAN 10 的 FC-MAP 值为 0x0EFC01。

[Transit-vlan10] fip-snooping fc-map 0efc01

Changing the FC-MAP will flap all interfaces. Continue? $[\,Y/N\,]\!:\!y$

[Transit-vlan10] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过,并将该接口配置为 ENode 模式。

[Transit] interface ten-gigabitethernet 1/0/1

[Transit-Ten-GigabitEthernet1/0/1] port link-type trunk

[Transit-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[Transit-Ten-GigabitEthernet1/0/1] fip-snooping port-mode enode

[Transit-Ten-GigabitEthernet1/0/1] quit

配置以太网接口 Ten-GigabitEthernet1/0/2 允许 VLAN 10 的报文通过,并将该接口配置为 FCF 模式。

[Transit] interface ten-gigabitethernet 1/0/2

[Transit-Ten-GigabitEthernet1/0/2] port link-type trunk

[Transit-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10

[Transit-Ten-GigabitEthernet1/0/2] fip-snooping port-mode fcf

[Transit-Ten-GigabitEthernet1/0/2] quit

(2) 配置 FCF 交换机

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<FCF> system-view

[FCF] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the system to make it effective.

- [FCF] save
- [FCF] quit

<FCF> reboot

配置 FCoE 模式为 FCF 模式。

<FCF> system-view [FCF] fcoe-mode fcf # 配置 FC-MAP 值为 0x0EFC01。

[FCF] fcoe fcmap 0efc01

Changing the FC-MAP will flap all VFC interfaces. Continue? [Y/N]:y

创建 VSAN 10。

```
[FCF] vsan 10
```

[FCF-vsan10] quit

创建 VFC 接口 VFC2, 配置 VFC2 接口工作在 F 模式,将 VFC2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2 上,并将 VFC2 接口以 Trunk 方式加入 VSAN 10,即允许 VSAN 10 的报 文通过 VFC2 接口。

[FCF] interface vfc 2

[FCF-vfc2] fc mode f

[FCF-vfc2] port trunk vsan 10

[FCF-vfc2] bind interface ten-gigabitethernet 1/0/2

[FCF-Vfc2] quit

配置以太网接口 Ten-GigabitEthernet1/0/2 允许 VLAN 10 的报文通过。

```
[FCF] interface ten-gigabitethernet 1/0/2
```

[FCF-Ten-GigabitEthernet1/0/2] port link-type trunk

[FCF-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10

[FCF-Ten-GigabitEthernet1/0/2] quit

开启 VLAN 10 的 FCoE 功能,并将其与 VSAN 10 进行映射。

[FCF] vlan 10

[FCF-vlan10] fcoe enable vsan 10

4. 验证配置

#显示 Transit 交换机获取到的 ENode 信息。 [Transit] display fip-snooping enode VLAN 10: Interface ENode WWN ENode MAC 10:00:00:11:22:00:0d:01 XGE1/0/1 dc2d-cb34-0d01 #显示 Transit 交换机获取到的 FCF 交换机信息。 [Transit] display fip-snooping fcf VLAN 10: Interface FCF MAC FCF WWN Fabric Name ENode XGE1/0/2 dc2d-cb34-0e01 10:00:00:11:22:00:0e:01 10:00:00:11:22:00:0e:01 1 # 显示 FIP Snooping 的会话信息。 [Transit] display fip-snooping sessions VLAN 10: FCF MAC ENode MAC VN_Port MAC VN_Port WWN dc2d-cb34-0e01 dc2d-cb34-0d01 dc2d-cb01-0000 af:10:01:11:22:00:0d:01 #显示已经下刷的 FIP Snooping 规则。 [Transit] display fip-snooping rules Slot 1: VLAN 10: FCF rules information: Interface Source MAC/Mask Destination MAC/Mask Context XGE1/0/2 dc2d-cb34-0e01/48 dc2d-cb00-0000/24 fffffff ENode rules information: Interface Source MAC/Mask Destination MAC/Mask Context XGE1/0/1 dc2d-cb01-0000/48 dc2d-cb34-0e01/48 fffffff

11 FCS

🕑 说明

仅 FCF 模式的交换机支持 FCS。本章中的交换机均指 FCF 交换机。

11.1 FCS简介

FCS(Fabric Configuration Server, Fabric 配置服务)使得用户可以通过命令行或者 MIB,在指定 VSAN 下发起拓扑发现过程来获取 Fabric 网络的拓扑信息,即 Fabric 网络中包含的交换机信息以 及交换机上的端口信息。运行在服务器上的管理应用程序(例如 SNMP 网管软件)使用管理协议(例 如 SNMP)根据 FCS 获取到的拓扑信息来确定 Fabric 网络的物理和逻辑拓扑,对 Fabric 网络中的 交换机实施管理(例如可以根据 FCS 获取到的拓扑信息中的其它交换机的管理地址信息,通过 SNMP 网管软件连接到对应的交换机上,并对该交换机实施进一步的管理和配置)。

FCS 通过下列对象描述 Fabric 网络的拓扑:

- IE(Interconnect Element, 互联设备)对象: Fabric 网络中的每台交换机对应一个 IE 对象。 一个或多个 IE 对象互联构成了一个 Fabric 网络。IE 对象具备一系列属性, 如<u>表 11-1</u> 所示。
- 端口对象: IE 对象上的每个 VFC 接口对应一个端口对象。每个 IE 对象包含一个或多个端口 对象。端口对象具备一系列属性,如<u>表 11-2</u>所示。

属性	说明
IE名称	IE的WWN
IE类型	IE的类型,目前仅支持交换机一种类型
IE域ID	IE的域ID
IE的Fabric名称	IE所在Fabric网络的名称
IE的逻辑名称	IE的设备名称,可以通过sysname命令配置设备的名称
	IE支持的管理协议和管理IP地址,目前仅支持SNMP(Simple Network Management Protocol,简单网络管理协议)一种管理协议
IE管理地址	管理地址以URL(Uniform Resource Locator,统一资源定位符)的格式表示,例如: snmp://192.168.6.100,表示管理协议为SNMP,对应的管理IP地址为192.168.6.100
	一个IE可能存在一个或多个管理地址
IE信息列表	包含:厂商名称、产品名称/编号、发布编码和其他厂商指定信息

表11-1 IE 对象的属性

表11-2 端口对象的属性

属性	说明
Port名称	端口的WWN

属性	说明
Port类型	端口的模式,包括: E端口、F端口
Port TX类型	端口的传输类型,包括: Long wave laser-LL(1550nm)、Short wave laser-SN(850nm)、 Long wave laser cost reduced-LC(1310nm)、Electrical-EL、10GBASE-SR 850nm laser、10GBASE-LR 1310nm laser、10GBASE-ER 1550nm laser、10GBASE-LX4 WWDM 1300nm laser、10GBASE-SW 850nm laser、10GBASE-LW 1310nm laser、 10GBASE-EW 1550nm laser和10GBASE-CX4
Port模块类型	端口采用的光模块类型,比如:GLM、GBIC with serial ID、GBIC without serial ID、 SFP with serial ID、SFP without serial ID、XFP、X2 short、X2 Medium、X2 Tall、 XPAX short、XPAX Medium、XPAX Tall、XENPAK、SFP-DWDM、QSFP和X2-DWDM
Port接口索引	端口的索引值
Attached Port列表	与端口相连的对端端口列表(如果节点通过NPV交换机注册,就可能有多个对端端口)
Port状态	端口当前的状态,包括:端口链路已连接、端口链路未连接
Port速率能力	端口支持的所有速率,包括:1Gbps、2Gbps、4Gbps、8Gbps、10Gbps、16Gbps 和20Gbps(可包含其中一项或多项)
Port协商速率	端口当前的运行速率,包括:1Gbps、2Gbps、4Gbps、8Gbps、10Gbps、16Gbps 和20Gbps(只可包含其中一项)
Port的Zone支持状态	端口支持的Zone类型,包括:软件Zone、硬件Zone

11.2 配置FCS

11.2.1 发起拓扑发现

用户可以在 Fabric 网络中的任意一台交换机上发起拓扑发现。拓扑发现的工作机制如下:

- Fabric 网络中的每台交换机上都会维护 Fabric 网络中所有 IE 的列表。当没有发起拓扑发现时, 对应 VSAN 下拓扑发现状态为 localOnly,表示未进行拓扑发现。交换机只保存有本 IE 的所有 属性信息及其端口信息,非本地 IE 的属性只包含 IE 的 WWN、类型和域 ID 信息,无非本地 IE 的端口信息。
- 当发起拓扑发现后,对应 VSAN 下的拓扑发现状态更新为 InProgress,表示正在进行拓扑发现。交换机会从 Fabric 网络内所有非本地交换机获取最新的 IE 属性和 IE 的端口信息,并更新本地 FCS 数据库中对应的 IE 和 IE 下端口信息。
- 获取完所有的拓扑信息,交换机更新指定 VSAN 下的拓扑发现状态为 completed,表示已完成拓扑发现,同时启动拓扑发现数据老化定时器,用于限制本次拓扑发现信息的有效时间。
- 当拓扑发现数据老化定时器超时,交换机会删除非本地交换机的拓扑发现数据,恢复 VSAN 下的拓扑发现状态为 localOnly。

Fabric 网络的拓扑信息有可能发生变化,因此拓扑发现获取到的只能是某一个时刻整个 Fabric 网络的拓扑信息。在拓扑发现过程中,处理非本地交换机的拓扑信息变化的原则如下:

- 如果在新的 IE 加入 Fabric 网络之前,交换机已经开始获取其它 IE 的详细属性和端口列表, 则对于新加入 IE 的详细属性和端口数据在本次拓扑发现中不会去获取。
- 获取完某 IE 的详细属性和端口数据之后,该 IE 的某些属性和状态又发生了变化,对于这些数据在本次拓扑发现中也不会重新获取。

对于本地交换机的拓扑相关信息变化则会实时处理,不管是否进行拓扑发现,获取的本地交换机拓 扑相关信息总是最新的。

表1-1 发起拓扑发现

操作	命令	说明
进入系统视图	system-view	-
发起拓扑发现	fcs discovery start [age interval] vsan vsan-list	对某VSAN来说,只有等本次拓扑发现过程结 束后,才能发起下一次的拓扑发现,否则,系 统会提示正在进行拓扑发现

11.2.2 取消拓扑发现

用户可以通过下面的配置取消拓扑发现。配置本命令后,系统将终止本次拓扑发现,并删除已获取的非本地交换机拓扑发现数据,恢复对应 VSAN 下的拓扑发现状态为 localOnly。

表1-2 取消拓扑发现

操作	命令	说明
进入系统视图	system-view	-
取消拓扑发现	fcs discovery stop vsan vsan-list	-

11.3 FCS显示和维护

在完成上述配置后,在任意视图下执行 display 命令可以显示拓扑发现的状态以及获取的拓扑信息。

表1-3 FCS 显示和维护

操作	命令	
显示当前的拓扑发现状态	display fcs discovery status [vsan vsan-id]	
显示FCS数据库信息	display fcs database [vsan vsan-id]	
显示FCS的IE信息	display fcs ie [vsan vsan-id [nwwn wwn]] [verbose]	
显示FCS的端口信息	display fcs port [vsan vsan-id [pwwn wwn]] [verbose]	

11.4 FCS典型配置举例

1. 组网需求

通过 FCS 获取 Fabric 网络的拓扑信息,以供管理应用程序使用。

2. 组网图

图11-1 配置 FCS 组网图



3. 配置步骤



<SwitchA> system-view

本例中只列出 FCS 相关配置,其它配置步骤略。

[SwitchA] system-working-mode advance

配置 Switch A 工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

Do you want to change the system working mode? [Y/N]:y The system working mode is changed, please save the configuration and reboot the system to make it effective. [SwitchA] save [SwitchA] quit <SwitchA> reboot # 配置 Switch A 的 FCoE 模式为 FCF 模式。 <SwitchA> system-view [SwitchA] fcoe-mode fcf #在 Switch A 上发起拓扑发现。 [SwitchA] fcs discovery start vsan 1 4. 验证配置 #显示 Switch A 上 VSAN 1 下的 FCS 数据库信息。 [SwitchA] display fcs database vsan 1 FCS Local Database in VSAN 1: : 10:00:00:11:22:00:01:01 IE WWN Domain ID : 0x01 Management address list : snmp://192.168.0.1 : 10:00:00:11:22:00:01:01 Fabric name Logical name : SwitchA : UNIS#UNIS S10600X-06#Version 7.1.045, Beta 7143 Information list

```
IE ports:
   Interface Port WWN
                                        Port type Attached port WWNs
   Vfc1
              e1:01:00:11:22:00:01:01
                                        E Port
                                                    e2:01:00:11:22:00:01:01
   Vfc2
              e1:01:00:11:22:00:01:02
                                        E Port
                                                    e3:01:00:11:22:00:01:01
  IE WWN
                          : 10:00:00:11:22:00:01:02
  Domain ID
                          : 0x02
  Management address list : snmp://192.168.0.2
                         : 10:00:00:11:22:00:01:01
  Fabric name
  Logical name
                         : SwitchB
  Information list
                         : UNIS#UNIS S10600X-06#Version 7.1.045, Beta 7143
  IE ports:
   Interface Port WWN
                                        Port type Attached port WWNs
              e2:01:00:11:22:00:01:01
                                                    e1:01:00:11:22:00:01:01
                                        E_Port
               e2:01:00:11:22:00:01:02
                                        E_Port
                                                    e3:01:00:11:22:00:01:02
               e2:01:00:11:22:00:01:03
                                        E_Port
                                                    e4:01:00:11:22:00:01:01
                          : 10:00:00:11:22:00:01:03
  IE WWN
  Domain ID
                         : 0x03
  Management address list : snmp://192.168.0.3
  Fabric name
                         : 10:00:00:11:22:00:01:01
  Logical name
                         : SwitchC
  Information list
                         : UNIS#UNIS S10600X-06#Version 7.1.045, Beta 7143
  IE ports:
   Interface Port WWN
                                        Port type Attached port WWNs
              e3:01:00:11:22:00:01:01
                                                    e1:01:00:11:22:00:01:02
                                        E_Port
               e3:01:00:11:22:00:01:02
                                        E_Port
                                                    e2:01:00:11:22:00:01:02
               e3:01:00:11:22:00:01:03
                                        F Port
                                                    48:33:43:2d:46:43:1A:1A
  IE WWN
                          : 10:00:00:11:22:00:01:04
  Domain ID
                          : 0x04
  Management address list : snmp://192.168.0.4
                         : 10:00:00:11:22:00:01:01
  Fabric name
  Logical name
                         : SwitchD
  Information list
                         : UNIS#UNIS S10600X-06#Version 7.1.045, Beta 7143
  IE ports:
   Interface Port WWN
                                         Port type Attached port WWNs
               e4:01:00:11:22:00:01:01
                                        E_Port
                                                    e2:01:00:11:22:00:01:03
               e4:01:00:11:22:00:01:02
                                         F_Port
                                                    48:33:43:2d:46:43:1B:1B
#显示 Switch A 上 VSAN 1 下 FCS 的 IE 简要信息。
[SwitchA] display fcs ie vsan 1
```

IE List for VSAN 1:

IE WWN	Domain ID	Mgmt addr list	Logical name
10:00:00:11:22:00:01:01	0x01	snmp://192.168.0.1	SwitchA
10:00:00:11:22:00:01:02	0x02	snmp://192.168.0.2	SwitchB
10:00:00:11:22:00:01:03	0x03	snmp://192.168.0.3	SwitchC
10:00:00:11:22:00:01:04	0x04	snmp://192.168.0.4	SwitchD

Total 4 IEs in Fabric. #显示 Switch A 上 VSAN 1 下 FCS 的端口简要信息。 [SwitchA] display fcs port vsan 1 Port List for VSAN 1: IE WWN: 10:00:00:11:22:00:01:01 Port WWN Port type Tx type Module type e1:01:00:11:22:00:01:01 E_Port 10GBASE-CX4 SFP with serial ID SFP with serial ID e1:01:00:11:22:00:01:02 E_Port 10GBASE-CX4 Total 2 switch-ports in IE. IE WWN: 10:00:00:11:22:00:01:02 Port WWN Port type Tx type Module type e2:01:00:11:22:00:01:01 E_Port 10GBASE-CX4 SFP with serial ID SFP with serial ID e2:01:00:11:22:00:01:02 E_Port 10GBASE-CX4 e2:01:00:11:22:00:01:03 E Port 10GBASE-CX4 SFP with serial ID Total 3 switch-ports in IE. IE WWN: 10:00:00:11:22:00:01:03 Port WWN Port type Tx type Module type e3:01:00:11:22:00:01:01 E Port 10GBASE-CX4 SFP with serial ID e3:01:00:11:22:00:01:02 E_Port 10GBASE-CX4 SFP with serial ID e3:01:00:11:22:00:01:03 F_Port 10GBASE-CX4 SFP with serial ID Total 3 switch-ports in IE. IE WWN: 10:00:00:11:22:00:01:04 Port WWN Port type Tx type Module type e4:01:00:11:22:00:01:01 E_Port 10GBASE-CX4 SFP with serial ID e4:01:00:11:22:00:01:02 F Port 10GBASE-CX4 SFP with serial ID

Total 2 switch-ports in IE.

12 FDMI

🕑 说明

仅 FCF 模式的交换机支持 FDMI。本章中的交换机均指 FCF 交换机。

12.1 FDMI简介

通过 FDMI(Fabric Device Management Interface, Fabric 设备管理接口),用户可以查看 Fabric 网络中所有已经注册节点设备上的 HBA(Host Bus Adapter,主机总线适配器)信息,包括 HBA 和 HBA 上的端口信息。

HBA 是一种 FC 存储网卡。对交换机来说,每个 HBA 是一个对象。HBA 对象具备一系列属性,如 表 12-1 所示。HBA 对象上的每个物理端口对应一个端口对象。每个 HBA 对象包含一个或多个端口 对象,最多可以包含 256 个端口对象。端口对象具备一系列属性,如<u>表 12-2</u>所示。

当 HBA 上的端口对象进行注册的 RPRT/RPA 报文携带 Smart SAN 属性时,如果交换机开启了 Smart SAN 功能,则通过 FDMI 显示节点设备的 HBA 信息时,端口对象会带有 Smart SAN 属性; 如果交换机没有开启 Smart SAN 功能,则不会显示节点设备的 HBA 信息和端口对象信息。

当节点设备在 HBA 下的端口对象进行注册的 RPRT/RPA 报文未携带 Smart SAN 属性时,不论交换机是否开启 Smart SAN 功能,通过 FDMI 显示节点设备的 HBA 信息时,端口对象都不会带有 Smart SAN 属性。

属性	说明
HBA ID	HBA的编号(HBA ID用来标识一个HBA。如果HBA上有一个物理端口,则采 用该物理端口的WWN作为HBA ID;如果HBA上有多个物理端口,则选择其 中一个物理端口的WWN作为HBA ID)
Manufacturer	HBA制造商信息
Serial Numbe	HBA序列号
Model HBA型뮥	
Model Description	HBA型号描述
Node Name	HBA所属节点的WWN
Node Symbolic Name	节点的符号名称,用于描述此节点
Hardware Version	HBA的硬件版本号
Driver Version HBA的驱动程序版本号 Option ROM Version HBA的ROM版本号	

表12-1 HBA 对象的属性

属性	说明	
OS ame and Version	HBA所在操作系统名称和版本号	
Maximum CT Payload	HBA允许的CT负载的最大长度,包括CT类型报文的基本头和扩展头,但不包括FC头	
Vendor Identifier	HBA制造厂商的T10编码,或HBA的OEM(Original Equipment Manufacturer, 原始设备制造商)	
Vendor Specific Information	厂商自定义信息,为十六进制数值形式	
Number of Ports	HBA上端口的数量	
Fabric Name	HBA所在的网络名称	
Boot BIOS Version HBA的Boot BIOS版本号		
	HBA的Boot BIOS状态,包括:	
Boot BIOS State	• Enabled: 开启	
	• Disabled: 关闭	

表12-2 端口对象的属性

属性	说明	
Port Name	端口的WWN	
Port Symbolic Name	N端口的符号名称,用于描述此端口	
Port Identifier	端口的FC_ID	
Port Type	端口类型	
Supported Class of Service	端口支持的服务等级,包括: Class 2, Class 3	
Supported FC-4 Types	 端口支持的FC4类型,包括以下几种类型: FCP:光纤通道协议 IP:因特网协议 LLC/SNAP:链路控制/子网访问协议 SW_ILS:交换机 Fabric 网内部链接服务 SNMP:简单网络管理协议 GS3:通用服务版本 3 VI:接口虚拟化 NPV:N端口虚拟化 NVMeoFC:基于光纤通道的 NVMe 协议 	
Port Active FC-4 Types	 端口生效的FC4类型,包括以下几种类型: FCP:光纤通道协议 IP:因特网协议 LLC/SNAP:链路控制/子网访问协议 SW_ILS:交换机 Fabric 网内部链接服务 SNMP:简单网络管理协议 	

属性	说明		
	• GS3: 通用服务 3		
	• VI: 接口虚拟化		
	● NPV: N 端口虚拟化		
	• NVMeoFC: 基于光纤通道的 NVMe 协议		
	端口支持的速率,包括:		
	• 1 Gbps		
	• 2 Gbps		
	• 4 Gbps		
	• 8 Gbps		
Supported Speed	• 10 Gbps		
	• 16 Gbps		
	• 20 Gbps		
	• 32 Gbps		
	• 40 Gbps		
	非以上迷学则亚小UNKNOWN		
	• 2 Gbps		
	• 8 Gbps		
	• 10 Gbps		
Current Speed	• 16 Gbps		
	• 20 Gbps		
	• 32 Gbps		
	• 40 Gbps		
	非以上速率则显示Unknown		
	如果不能确定端口当前的速率,则显示 Speed not obtained		
Maximum Frame Size	端口支持的最大帧大小		
OS Device Name	端口所在操作系统的名称		
Host Name	端口所在节点设备的名称		
Node Name	端口所在的节点的WWN		
Port Fabric Name	端口所在的网络名称		
Port State	端口当前状态		
Number of Discovered Ports	已发现的端口数量		
	端口上的Smart SAN服务类别,包括:		
Smart SAN Service Category	• Smart SAN Initiator: 服务器		
	• Smart SAN Target: 存储设备		

属性	说明
Smart SAN GUID	端口上的Smart SAN服务的GUID
Smart SAN Version	端口上的Smart SAN服务的版本号
Smart SAN Product Name (Model)	端口上的Smart SAN服务的型号
	端口信息,包括:
Smart SAN Dart Info	• 0x01 (Physical): 端口为物理接口
Small SAN Foll Inio	• 0x02 (NPIV):端口支持 NPIV 功能
	• 0x03 (SRIOV):端口支持 SRIOV 功能
	端口支持QoS状态,包括:
Smart SAN QoS Support	• 0x00 (Not supported):不支持
	• 0x01 (Supported): 支持
	端口支持的安全类别,包括:
	0x00 (Not Supported)
Smart SAN Security Support	• 0x01 (Tier-1)
	• 0x02 (Tier-2)
	• 0x03 (Tier-3)
Smart SAN Connected Ports 该端口发现的远端节点上的端口	



端口对象的 Smart SAN 属性包括 Smart SAN Service Category、Smart SAN GUI、Smart SAN Version、Smart SAN Product Name (Model)、Smart SAN Port Info、Smart SAN QoS Support、Smart SAN Security Support、Smart SAN Connected Ports。

每台交换机都会获取到与它直连的、已注册节点设备上的 HBA 信息,并向 Fabric 网络中的其它交换机进行同步。最终 Fabric 网络中的每台交换机上都会保存所有已经注册到 Fabric 网络的节点设 备上的 HBA 信息。

12.2 FDMI显示和维护

在任意视图下执行 **display** 命令可以显示 FDMI 数据库信息,包括整个 Fabric 网络中所有已经注册 节点设备上的 HBA 信息。

表1-4 FDMI显示和维护

操作	命令
显示FDMI数据库信息	display fdmi database [vsan vsan-id [hba-id hba-id]] [verbose]

13 FC Ping

13.1 FC Ping简介

在 FC SAN 中,用户可以使用 FC Ping 检查目的地址是否可达,测试网络连接是否出现故障。 FC Ping 的工作原理是:源端向目的端发送 ECHO 请求报文后,根据是否收到目的端的 ECHO 回应报文来判断目的端是否可达。对于可达的目的端,用户可以根据发送报文个数、接收到回应报文 个数来判断链路的质量;根据 FC Ping 报文的往返时间来判断源端与目的端之间的"距离"。

目前,交换机可以实现下列 FC Ping 功能:

- FC Ping N_Port: 在交换机上执行命令, FC Ping 远端的 N_Port。FC Ping 的目的地址为 N_Port 的 FC 地址。
- FC Ping 交换机: 在交换机上执行命令, FC Ping 远端交换机。FC Ping 的目的地址为目的交换机的域控制器地址 FFFCxx, 其中, xx 为目的交换机的域 ID。

13.2 配置FC Ping

表13-1 配置 FC Ping

操作	命令	说明
检查指定目的地址是否可达	fcping [-c count -t timeout] * fcid fcid vsan vsan-id	本命令可在任意视图下执行 在执行命令过程中,键入 <ctrl+c>可终 止FC Ping操作</ctrl+c>

13.3 FC Ping典型配置举例

13.3.1 FC Ping 配置举例

1. 组网需求

检查 Switch A 和 Switch B 之间是否可达。

2. 组网图

图13-1 配置 FC Ping 组网图



3. 配置步骤

(1) 配置 Switch A

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view

[SwitchA] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the system to make it effective.

[SwitchA] save

[SwitchA] quit

<SwitchA> reboot

配置 FCoE 模式为 FCF 模式。

<SwitchA> system-view

[SwitchA] fcoe-mode fcf

#开启 VSAN 1的 Fabric 配置功能。

[SwitchA] vsan 1

[SwitchA-vsan1] domain configure enable

配置 Switch A 的域 ID 为 1。

[SwitchA-vsan1] domain-id 1 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? [Y/N]:y

[SwitchA-vsan1] quit

创建 VFC 接口 VFC1, 配置 VFC1 接口工作在 E 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC1 接口。

[SwitchA] interface vfc 1

[SwitchA-Vfc1] fc mode e

[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchA-Vfc1] port trunk vsan 1

[SwitchA-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/1

[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[SwitchA-Ten-GigabitEthernet1/0/1] quit

开启 VLAN 10 的 FCoE 功能,并将其与 VSAN 1 进行映射。

[SwitchA] vlan 10

[SwitchA-vlan10] fcoe enable vsan 1

[SwitchA-vlan10] quit

#在 Switch A 上配置静态路由。

[SwitchA] vsan 1 [SwitchA-vsan1] fc route-static 020000 8 vfc 1 [SwitchA-vsan1] quit

(2) 配置 Switch B

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchB> system-view

[SwitchB] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the

```
system to make it effective.
[SwitchB] save
[SwitchB] quit
<SwitchB> reboot
```

配置 FCoE 模式为 FCF 模式。

<SwitchB> system-view [SwitchB] fcoe-mode fcf

#开启 VSAN 1的 Fabric 配置功能。

[SwitchB] vsan 1

[SwitchB-vsan1] domain configure enable

配置 Switch B 的域 ID 为 2。

[SwitchB-vsan1] domain-id 2 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[Y/N]\!:\!y$

[SwitchB-vsan1] quit

创建 VFC 接口 VFC1, 配置 VFC1 接口工作在 E 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC1 接口。

[SwitchB] interface vfc 1

[SwitchB-Vfc1] fc mode e

[SwitchB-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchB-Vfc1] port trunk vsan 1

[SwitchB-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过。

[SwitchB] interface ten-gigabitethernet 1/0/1

[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[SwitchB-Ten-GigabitEthernet1/0/1] quit

#开启 VLAN 10的 FCoE 功能,并将其与 VSAN 1进行映射。

[SwitchB] vlan 10

[SwitchB-vlan10] fcoe enable vsan 1

[SwitchB-vlan10] quit

#在 Switch B上配置静态路由。

[SwitchB] vsan 1 [SwitchB-vsan1] fc route-static 010000 8 vfc 1 [SwitchB-vsan1] quit

4. 验证配置

检查 Switch A 和 Switch B 之间是否可达。

在 Switch A 上使用 fcping 命令验证 Switch B 是否可达。

[SwitchA] fcping fcid fffc02 vsan 1
FCPING fcid 0xfffc02: 128 data bytes, press CTRL_C to break.
Reply from 0xfffc02: bytes = 128 time = 23 ms
Reply from 0xfffc02: bytes = 128 time = 9 ms
Reply from 0xfffc02: bytes = 128 time = 19 ms
Reply from 0xfffc02: bytes = 128 time = 14 ms

Reply from 0xfffc02: bytes = 128 time = 25 ms
--- 0xfffc02 fcping statistics --5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 9/18/25 ms

14 FC Tracert

14.1 FC Tracert简介

用户可以通过 FC Tracert 功能获取本端到目的端之间的双向路由信息,从而检查网络连接是否可用。 当网络出现故障时,用户可以使用该功能分析出现故障的网络节点。

FC Tracert 的目的端可以是 N 节点,也可以是 FCF 交换机。

FC Tracert 过程分为上行、下行两个子过程:

- 在上行过程中,从本端开始,逐跳向到达目的端经过的所有交换机发送 STR (Switch Trace Route, FCF 交换机路由探测)报文,直至目的交换机(如果 FC Tracert 的目的端是 N 节点,目的交换机指的是与 N 节点直连的 FCF 交换机)。在这个过程中,每台交换机都会向 STR 报文中添加本机的上行路径信息,包括交换机的 WWN、域 ID 等信息。STR 报文到达目的交换机后,将开始下行过程。
- 在下行过程中,从目的端开始,逐跳向到达源端经过的所有交换机发送 STR 报文,直至源交换机。同样,在这个过程中,每台交换机都会向 STR 报文中添加本机的下行路径信息,包含的信息内容与上行路径信息相同。当源交换机收到下行的 STR 报文后,表示整个 FC Tracert 过程结束。源交换机将输出 STR 报文中携带的所有经过的上行和下行交换机信息。如果在 FC Tracert 过程中的任一中间交换机上处理失败,会在 STR 报文中设置相应的错误原因,并将该 STR 报文(报文中包含已经通过的交换机的信息)直接发给源交换机。

下面以图 14-1 为例,介绍一下 FC Tracert 的基本过程。



图14-1 FC Tracert 过程示意图

Switch A FC Tracert Switch C 的基本过程如下:

1. 上行过程

- (1) 源交换机 Switch A 将自己的上行路径信息(包括交换机的 WWN 和域 ID)填入 STR 请求报 文,并将该 STR 请求报文发给下一跳交换机 Switch B。Switch B 收到 STR 请求报文后,向 Switch A 回 STR ACC 报文,表明自己收到了 STR 请求报文;
- (2) Switch B 将自己的上行路径信息添加到收到的 STR 请求报文中以后,将该 STR 请求报文发 给目的交换机 Switch C。Switch C 收到 STR 请求报文后,向 Switch B 回 STR ACC 报文;
- (3) 目的交换机 Switch C 将自己的上行路径信息也添加到收到的 STR 请求报文中,完成上行路径 信息收集。

2. 下行过程

- (1) 目的交换机 Switch C 以相同方式逐跳发送 STR 请求报文到源交换机 Switch A,完成下行路 径信息收集;
- (2) 源交换机 Switch A 收到携带下行标志的 STR 请求报文后,将输出 STR 请求报文中携带的所 有上行和下行交换机信息。

14.2 配置FC Tracert

表14-1 配置 FC Tracert

操作	命令	说明
探测本端到目的端的双向路由 信息	fctracert [-t <i>timeout</i>] fcid fcid vsan vsan-id	本命令可在任意视图下执行 在执行命令过程中,键入 <ctrl+c> 可终止FC Tracert操作</ctrl+c>

14.3 FC Tracert典型配置举例

14.3.1 FC Tracert 配置举例

1. 组网需求

通过 FC Tracert 功能获取 Switch A 到 Switch C 的双向路由信息。如果路由不可达,需要确定故障的网络节点。

2. 组网图

图14-2 配置 FC Tracert 组网图



3. 配置步骤

(1) 配置 Switch A

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view

[SwitchA] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the system to make it effective.

[SwitchA] save

[SwitchA] quit

<SwitchA> reboot

配置 FCoE 模式为 FCF 模式。

<SwitchA> system-view

[SwitchA] fcoe-mode fcf

#开启 VSAN 1的 Fabric 配置功能。

[SwitchA] vsan 1

[SwitchA-vsan1] domain configure enable

配置域 ID 为 1。

[SwitchA-vsan1] domain-id 1 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? [Y/N]:y

关闭 FSPF 功能。

[SwitchA-vsan1] undo fspf enable

配置静态路由。

[SwitchA-vsan1] fc route-static 020000 8 vfc 1

[SwitchA-vsan1] fc route-static 030000 8 vfc 1

[SwitchA-vsan1] quit

创建 VFC 接口 VFC1, 配置 VFC1 接口工作在 E 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC1 接口。

[SwitchA] interface vfc 1

[SwitchA-Vfc1] fc mode e

[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchA-Vfc1] port trunk vsan 1

[SwitchA-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过。

[SwitchA] interface ten-gigabitethernet 1/0/1

[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[SwitchA-Ten-GigabitEthernet1/0/1] quit

#开启 VLAN 10的 FCoE 功能,并将其与 VSAN 1进行映射。

[SwitchA] vlan 10

[SwitchA-vlan10] fcoe enable vsan 1

[SwitchA-vlan10] quit

(2) 配置 Switch B

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchB> system-view

[SwitchB] system-working-mode advance

Do you want to change the system working mode? $[\,Y/N\,]\,{:}\,y$

The system working mode is changed, please save the configuration and reboot the system to make it effective.

[SwitchB] save

[SwitchB] quit <SwitchB> reboot

配置 FCoE 模式为 FCF 模式。

<SwitchB> system-view

[SwitchB] fcoe-mode fcf

#开启 VSAN 1的 Fabric 配置功能。

[SwitchB] vsan 1

[SwitchB-vsan1] domain configure enable

配置域 ID 为 2。

[SwitchB-vsan1] domain-id 2 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[Y/N]\!:\!y$

关闭 FSPF 功能。

[SwitchB-vsan1] undo fspf enable

配置静态路由。

[SwitchB-vsan1] fc route-static 010000 8 vfc 1

[SwitchB-vsan1] quit

创建 VFC 接口 VFC1, 配置 VFC1 接口工作在 E 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC1 接口。

[SwitchB] interface vfc 1

[SwitchB-Vfc1] fc mode e

[SwitchB-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchB-Vfc1] port trunk vsan 1

[SwitchB-Vfc1] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 允许 VLAN 10 的报文通过。

[SwitchB] interface ten-gigabitethernet 1/0/1

[SwitchB-Ten-GigabitEthernet1/0/1] port link-type trunk

[SwitchB-Ten-GigabitEthernet1/0/1] port trunk permit vlan 10

[SwitchB-Ten-GigabitEthernet1/0/1] quit

创建 VFC 接口 VFC2, 配置 VFC2 接口工作在 E 模式,将 VFC2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2 上,并将 VFC2 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC2 接口。

[SwitchB] interface vfc 2

[SwitchB-Vfc2] fc mode e

[SwitchB-Vfc2] bind interface ten-gigabitethernet 1/0/2

[SwitchB-Vfc2] port trunk vsan 1

[SwitchB-Vfc2] quit

配置以太网接口 Ten-GigabitEthernet1/0/2 允许 VLAN 10 的报文通过。

[SwitchB] interface ten-gigabitethernet 1/0/2 [SwitchB-Ten-GigabitEthernet1/0/2] port link-type trunk [SwitchB-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10 [SwitchB-Ten-GigabitEthernet1/0/2] quit

#开启 VLAN 10的 FCoE 功能,并将其与 VSAN 1进行映射。

[SwitchB] vlan 10

[SwitchB-vlan10] fcoe enable vsan 1

[SwitchB-vlan10] quit

(3) 配置 Switch C

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchC> system-view

[SwitchC] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the system to make it effective.

[SwitchC] save

[SwitchC] quit

<SwitchC> reboot

配置 FCoE 模式为 FCF 模式。

<SwitchC> system-view

[SwitchC] fcoe-mode fcf

#开启 VSAN 1的 Fabric 配置功能。

[SwitchC] vsan 1

[SwitchC-vsan1] domain configure enable

配置域 ID 为 3。

[SwitchC-vsan1] domain-id 3 static

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? [Y/N]:y

关闭 FSPF 功能。

[SwitchC-vsan1] undo fspf enable

[SwitchC-vsan1] quit

#创建 VFC 接口 VFC2, 配置 VFC2 接口工作在 E 模式,将 VFC2 接口绑定到以太网接口 Ten-GigabitEthernet1/0/2 上,并将 VFC2 接口以 Trunk 方式加入 VSAN 1,即允许 VSAN 1 的报文 通过 VFC2 接口。

[SwitchC] interface vfc 2

[SwitchC-Vfc2] fc mode e

[SwitchC-Vfc2] bind interface ten-gigabitethernet 1/0/2

[SwitchC-Vfc2] port trunk vsan 1

[SwitchC-Vfc2] quit

配置以太网接口 Ten-GigabitEthernet1/0/2 允许 VLAN 10 的报文通过。

```
[SwitchC] interface ten-gigabitethernet 1/0/2
```

[SwitchC-Ten-GigabitEthernet1/0/2] port link-type trunk

[SwitchC-Ten-GigabitEthernet1/0/2] port trunk permit vlan 10

[SwitchC-Ten-GigabitEthernet1/0/2] quit

#开启 VLAN 10的 FCoE 功能,并将其与 VSAN 1进行映射。

[SwitchC] vlan 10

[SwitchC-vlan10] fcoe enable vsan 1

[SwitchC-vlan10] quit

(4) 使用 fcping 命令查看 SwitchA 和 Switch C 之间的路由是否可达

[SwitchA] fcping fcid fffc03 vsan 1
FCPING fcid 0xfffc03: 128 data bytes, press CTRL_C to break.
Request time out
Request time out
Request time out
--- 0xfffc03 fcping statistics --5 packet(s) transmitted
0 packet(s) received
100.00% packet loss

(5) Switch A 和 Switch C 之间的路由不可达,使用 fctracert 命令确定故障的网络节点

[SwitchA] fctracert fcid fffc03 vsan 1

Route present for: 0xfffc03, press CTRL_C to break

20:00:00:0b:46:00:02:82(0xfffc01)

20:00:00:05:30:00:18:db(0xfffc02)

Fctracert uncompleted: no route to destination port.

从上面的结果可以看出,Switch A 和 Switch C 之间路由不可达,Switch A 和 Switch B 之间路由可达,Switch B 和 Switch C 之间的连接出了问题。此时可以在 Switch B 上使用 display fc routing-table 命令查看有没有到 Switch C 的路由。

15 FCoE 综合配置举例

15.1 非IRF模式的FCoE配置举例

15.1.1 组网需求

如<u>图 15-1</u>所示, Switch A 和 Switch B 与以太网交换机连接,作为 LAN 网络的接入层; Switch A 和 Switch B 分别与 Switch C 和 Switch D 连接,作为 SAN 网络的 FCF 交换机。 要求实现:

- Switch A 和 Switch B 与以太网交换机所组成的传输网络能够使服务器为 LAN 网络提供业务服务; Switch A~Switch D 所组成的传输网络能够使服务器访问磁盘设备内的存储资源。
- 满足用户对服务器、磁盘设备等设备收发报文的高可靠性要求,需要实现链路备份功能。
- 提高 Switch A 和 Switch C 之间、Switch B 和 Switch D 之间链路的带宽,并实现链路备份和 负载分担。

15.1.2 组网图

图15-1 配置非 IRF 模式的 FCoE 组网图



15.1.3 配置思路

- 为了实现 SAN 网络中的存储数据流量能够在无损以太网链路上传输,建议用户在交换机上与服务器连接的以太网接口上配置 DCBX、自动协商模式的 PFC、ETS 功能;在交换机上与磁盘设备连接的以太网接口上配置 DCBX、自动协商模式的 PFC 功能;在交换机之间连接的以太网接口上要强制开启 PFC 功能。
- 为了实现服务器到磁盘设备间的链路备份,使用互相隔离的两个 SAN 网络(服务器、Switch A、 Switch C 和磁盘设备所组成的 SAN 网络与服务器、Switch B、Switch D 和磁盘设备所组成的 SAN 网络是两个不同的物理 SAN 网络)为服务器提供到存储设备的连接,两个 SAN 网络可 以使用相同的 VSAN。
- LAN 网络的以太网数量流量在 VLAN 1001 中传输, Switch A 和 Switch B 与 LAN 网络/服务器 所连接的以太网接口上需要允许 VLAN 1001 中的报文通过。
- SAN 网络的存储数据流量在 VSAN 100 中传输,4 台 FCF 交换机上接入 SAN 网络的接口上 需要允许 VSAN 100 中的报文通过。配置 VLAN 4001 与 VSAN 100 进行映射,使得 VSAN 100 内的存储数据流量在 VLAN 4001 中传输。
- 为了防止 LAN 网络存在物理环路,需要在 Switch A 和 Switch B 与 LAN 网络/服务器所连接的 以太网接口开启 STP 功能。为了避免 STP 功能阻塞 Switch A 和 Switch B 负责转发存储流量 的接口,需要保证 4 台 FCF 交换机之间的接口上没有开启 STP 功能。
- 由于 SAN 网络结构比较复杂,建议用户采用动态方式建立 Fabric 网络,使用 FSPF 协议建立 FC 路由。
- 为了实现服务器能够访问磁盘设备内的存储资源,需要配置允许默认 Zone 内的成员互相访问。
- 为了提高 Switch A 和 Switch C 之间、Switch B 和 Switch D 之间链路的带宽,并实现链路备 份和负载分担,分别配置以太网聚合链路 1 和以太网聚合链路 2。

15.1.4 配置步骤

1. 配置 Switch A

(1) 开启高级模式

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view

[SwitchA] system-working-mode advance

Do you want to change the system working mode? $[{\rm Y}/{\rm N}]{\rm :}{\rm y}$

The system working mode is changed, please save the configuration and reboot the system to make it effective.

[SwitchA] save

The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(*.cfg)[flash:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

Slot 1:

Save next configuration file successfully.

[SwitchA] quit

<SwitchA> reboot

Start to check configuration with next startup configuration file, please wait.....DONE! Current configuration will be lost after the reboot, save current configuration? [Y/N]:y Please input the file name(*.cfg)[flash:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

flash:/startup.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait...

Configuration is saved to flash successfully.

This command will reboot the device. Continue? [Y/N]:y

Now rebooting, please wait...

(2) VLAN 和接口部署

创建 VLAN 1001、4001,分别用来传输以太网数据流量和存储数据流量。

<SwitchA> system-view

[SwitchA] vlan 1001

[SwitchA-vlan1001] description ToLAN

[SwitchA-vlan1001] quit

[SwitchA] vlan 4001

[SwitchA-vlan4001] description ToSAN

[SwitchA-vlan4001] quit

#开启全局 STP 功能。

[SwitchA] stp global enable

配置以太网接口 Ten-GigabitEthernet1/0/1 为 Hybrid 接口, 允许 VLAN 1001 的以太网数据报文不带 Tag 标签通过, 允许 VLAN 4001 的存储数据报文带 Tag 标签通过, 设置接口的 PVID 为 VLAN 1001, 并开启 STP 功能。

[SwitchA] interface ten-gigabitethernet 1/0/1

[SwitchA-Ten-GigabitEthernet1/0/1] port link-type hybrid

[SwitchA-Ten-GigabitEthernet1/0/1] port hybrid vlan 1001 untagged

[SwitchA-Ten-GigabitEthernet1/0/1] port hybrid vlan 4001 tagged

[SwitchA-Ten-GigabitEthernet1/0/1] port hybrid pvid vlan 1001

[SwitchA-Ten-GigabitEthernet1/0/1] stp enable

[SwitchA-Ten-GigabitEthernet1/0/1] quit

配置以太网接口 Ten-GigabitEthernet1/0/10 为 Trunk 接口, 允许 VLAN 1001 的以太网数据报文 通过, 并开启 STP 功能。

[SwitchA] interface ten-gigabitethernet 1/0/10

[SwitchA-Ten-GigabitEthernet1/0/10] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/0/10] port trunk permit vlan 1001

[SwitchA-Ten-GigabitEthernet1/0/10] stp enable

[SwitchA-Ten-GigabitEthernet1/0/10] quit

创建二层聚合接口 1, 配置其对应的聚合组工作在动态聚合模式下, 并关闭 STP 功能。

[SwitchA] interface bridge-aggregation 1

[SwitchA-Bridge-Aggregation1] link-aggregation mode dynamic

[SwitchA-Bridge-Aggregation1] undo stp enable

[SwitchA-Bridge-Aggregation1] quit

#将以太网接口Ten-GigabitEthernet1/0/5~Ten-GigabitEthernet1/0/8共4个接口加入二层聚合组1。

[SwitchA] interface ten-gigabitethernet 1/0/5

[SwitchA-Ten-GigabitEthernet1/0/5] port link-aggregation group 1

[SwitchA-Ten-GigabitEthernet1/0/5] quit

[SwitchA] interface ten-gigabitethernet 1/0/6 [SwitchA-Ten-GigabitEthernet1/0/6] port link-aggregation group 1 [SwitchA-Ten-GigabitEthernet1/0/6] guit [SwitchA] interface ten-gigabitethernet 1/0/7 [SwitchA-Ten-GigabitEthernet1/0/7] port link-aggregation group 1 [SwitchA-Ten-GigabitEthernet1/0/7] quit [SwitchA] interface ten-gigabitethernet 1/0/8 [SwitchA-Ten-GigabitEthernet1/0/8] port link-aggregation group 1 [SwitchA-Ten-GigabitEthernet1/0/8] quit # 配置二层聚合接口 1 为 Trunk 接口, 允许 VLAN 4001 的存储数据报文通过。 [SwitchA] interface bridge-aggregation 1 [SwitchA-Bridge-Aggregation1] port link-type trunk [SwitchA-Bridge-Aggregation1] port trunk permit vlan 4001 [SwitchA-Bridge-Aggregation1] quit (3) DCBX 部署 # 全局开启 LLDP 功能。 [SwitchA] lldp global enable # 创建编号为 4000 的二层 ACL, 并为其创建规则来匹配 FCoE 报文(协议号为 0x8906) 和 FIP 报 文(协议号为0x8914)。 [SwitchA] acl mac 4000 [SwitchA-acl-mac-4000] rule 0 permit type 8906 ffff [SwitchA-acl-mac-4000] rule 5 permit type 8914 ffff [SwitchA-acl-mac-4000] quit # 定义名为 DCBX 的类,其下各规则间的关系为逻辑或,并定义其匹配 ACL 4000。 [SwitchA] traffic classifier DCBX operator or [SwitchA-classifier-DCBX] if-match acl 4000 [SwitchA-classifier-DCBX] quit # 定义名为 DCBX 的流行为,并配置标记报文的 802.1p 优先级为 3。 [SwitchA] traffic behavior DCBX [SwitchA-behavior-DCBX] remark dot1p 3 [SwitchA-behavior-DCBX] quit # 定义名为 DCBX 的 QoS 策略,为类 DCBX 指定采用的流行为是 DCBX,并指定该策略为 DCBX 模式。 [SwitchA] gos policy DCBX [SwitchA-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx [SwitchA-qospolicy-DCBX] quit # 在以太网接口 Ten-GigabitEthernet1/0/1 上开启 LLDP 功能,并允许该接口发送 LLDP 报文时携带 **DCBX TLV** 字段。 [SwitchA] interface ten-gigabitethernet 1/0/1 [SwitchA-Ten-GigabitEthernet1/0/1] lldp enable [SwitchA-Ten-GigabitEthernet1/0/1] lldp tly-enable dot1-tly dcbx # 在以太网接口 Ten-GigabitEthernet1/0/1 的出方向上应用 QoS 策略。 [SwitchA-Ten-GigabitEthernet1/0/1] gos apply policy DCBX outbound (4) PFC 部署

15-4

在以太网接口 Ten-GigabitEthernet1/0/1 上配置与服务器自动协商是否开启 PFC 功能,且设置对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control auto

[SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dotlp 3

[SwitchA-Ten-GigabitEthernet1/0/1] qos trust dotlp

[SwitchA-Ten-GigabitEthernet1/0/1] quit

在以太网接口 Ten-GigabitEthernet1/0/5~Ten-GigabitEthernet1/0/8 上配置强制开启 PFC 功能, 且设置对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

```
[SwitchA] interface ten-gigabitethernet 1/0/5
[SwitchA-Ten-GigabitEthernet1/0/5] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet1/0/5] priority-flow-control no-drop dot1p 3
[SwitchA-Ten-GigabitEthernet1/0/5] gos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/5] guit
[SwitchA] interface ten-gigabitethernet 1/0/6
[SwitchA-Ten-GigabitEthernet1/0/6] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet1/0/6] priority-flow-control no-drop dot1p 3
[SwitchA-Ten-GigabitEthernet1/0/6] gos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/6] guit
[SwitchA] interface ten-gigabitethernet 1/0/7
[SwitchA-Ten-GigabitEthernet1/0/7] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet1/0/7] priority-flow-control no-drop dot1p 3
[SwitchA-Ten-GigabitEthernet1/0/7] gos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/7] quit
[SwitchA] interface ten-gigabitethernet 1/0/8
[SwitchA-Ten-GigabitEthernet1/0/8] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet1/0/8] priority-flow-control no-drop dot1p 3
[SwitchA-Ten-GigabitEthernet1/0/8] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/0/8] quit
(5) ETS 部署
```

配置 802.1p 优先级到本地优先级的映射,将 802.1p 优先级 3 映射到本地优先级 1,配置其它的 802.1p 优先级映射到本地优先级 0。

```
[SwitchA] qos map-table dot1p-1p
[SwitchA-maptbl-dot1p-1p] import 3 export 1
[SwitchA-maptbl-dot1p-1p] import 0 export 0
[SwitchA-maptbl-dot1p-1p] import 1 export 0
[SwitchA-maptbl-dot1p-1p] import 2 export 0
[SwitchA-maptbl-dot1p-1p] import 4 export 0
[SwitchA-maptbl-dot1p-1p] import 5 export 0
[SwitchA-maptbl-dot1p-1p] import 6 export 0
[SwitchA-maptbl-dot1p-1p] import 7 export 0
[SwitchA-maptbl-dot1p-1p] quit
```

在以太网接口 Ten-GigabitEthernet1/0/1 上配置 WRR 队列,使 FCoE 流量和普通 LAN 流量各占 50%带宽。

[SwitchA] interface ten-gigabitethernet 1/0/1 [SwitchA-Ten-GigabitEthernet1/0/1] qos wrr byte-count [SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 1 group 1 byte-count 1 [SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 0 group 1 byte-count 1 # 在以太网接口 Ten-GigabitEthernet1/0/1 上配置其它的队列为 SP 调度方式。

```
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 2 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 3 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 4 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 5 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 6 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 7 group sp
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

(6) FCoE 部署

配置 FCoE 模式为 FCF 模式,进入 VSAN 100 的视图,开启 Fabric 配置功能(本步骤可选, Fabric 配置功能缺省开启)。

[SwitchA] fcoe-mode fcf

[SwitchA] vsan 100

[SwitchA-vsan100] domain configure enable

配置域 ID 为 2。

[SwitchA-vsan100] domain-id 2 preferred

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[\rm Y/N]:y$

全局开启 FSPF 功能。

[SwitchA-vsan100] fspf enable

[SwitchA-vsan100] quit

创建 VFC1 接口, 配置 VFC1 接口工作在 F 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 100,即允许 VSAN 100 的报文通过 VFC1 接口。

[SwitchA] interface vfc 1 [SwitchA-Vfc1] fc mode f [SwitchA-Vfc1] bind interface ten-gigabitethernet 1/0/1 [SwitchA-Vfc1] port trunk vsan 100 [SwitchA-Vfc1] quit

创建 VFC10 接口, 配置 VFC10 接口工作在 E 模式,将 VFC10 接口绑定到二层聚合接口 Bridge-Aggregation1 上,并将 VFC10 接口以 Trunk 方式加入 VSAN 100,即允许 VSAN 100 的报 文通过 VFC10 接口。

[SwitchA] interface vfc 10

[SwitchA-Vfc10] fc mode e

[SwitchA-Vfc10] bind interface bridge-aggregation 1

[SwitchA-Vfc10] port trunk vsan 100

开启 VFC10 接口的 FSPF 功能。

[SwitchA-Vfc10] undo fspf silent vsan 100

[SwitchA-Vfc10] quit

开启 VLAN 4001 的 FCoE 功能,并将其与 VSAN 100 进行映射。

[SwitchA] vlan 4001

[SwitchA-vlan4001] fcoe enable vsan 100

[SwitchA-vlan4001] quit

#进入 VSAN 100 的视图,配置允许默认 Zone 内的成员互相访问。

[SwitchA] vsan 100

[SwitchA-vsan100] zone default-zone permit [SwitchA-vsan100] quit

2. 配置 Switch B

Switch B 上的配置与 Switch A 类似,差异处为 Switch B 上配置的二层聚合接口是 Bridge-Aggregation2, Switch A 上配置的二层聚合接口是 Bridge-Aggregation1,配置步骤略。

3. 配置 Switch C

(1) 开启高级模式

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchC> system-view [SwitchC] system-working-mode advance Do you want to change the system working mode? [Y/N]:y The system working mode is changed, please save the configuration and reboot the system to make it effective. [SwitchC] save The current configuration will be written to the device. Are you sure? [Y/N]:y Please input the file name(*.cfg)[flash:/startup.cfg] (To leave the existing filename unchanged, press the enter key): Validating file. Please wait ... Saved the current configuration to mainboard device successfully. Slot 1: Save next configuration file successfully. [SwitchC] quit <SwitchC> reboot Start to check configuration with next startup configuration file, please wait.....DONE! Current configuration will be lost after the reboot, save current configuration? [Y/N]:y Please input the file name(*.cfg)[flash:/startup.cfg] (To leave the existing filename unchanged, press the enter key): flash:/startup.cfg exists, overwrite? [Y/N]:y Validating file. Please wait... Configuration is saved to flash successfully. This command will reboot the device. Continue? [Y/N]:y Now rebooting, please wait... (2) VLAN 和接口部署 # 创建 VLAN 4001,用来传输存储数据流量。 <SwitchC> system-view [SwitchC] vlan 4001 [SwitchC-vlan4001] description ToSAN [SwitchC-vlan4001] quit # 配置以太网接口 Ten-GigabitEthernet1/0/1 为 Hybrid 接口, 允许 VLAN 4001 的存储数据报文通过,

设置接口的 PVID 为 VLAN 4001。

[SwitchC] interface ten-gigabitethernet 1/0/1 [SwitchC-Ten-GigabitEthernet1/0/1] port link-type hybrid [SwitchC-Ten-GigabitEthernet1/0/1] port hybrid vlan 4001 tagged [SwitchC-Ten-GigabitEthernet1/0/1] port hybrid pvid vlan 4001 [SwitchC-Ten-GigabitEthernet1/0/1] quit # 创建二层聚合接口 1, 配置其对应的聚合组工作在动态聚合模式下。

[SwitchC] interface bridge-aggregation 1

[SwitchC-Bridge-Aggregation1] link-aggregation mode dynamic

[SwitchC-Bridge-Aggregation1] quit

#将以太网接口Ten-GigabitEthernet1/0/5~Ten-GigabitEthernet1/0/8共4个接口加入二层聚合组1。

[SwitchC] interface ten-gigabitethernet 1/0/5

[SwitchC-Ten-GigabitEthernet1/0/5] port link-aggregation group 1

[SwitchC-Ten-GigabitEthernet1/0/5] quit

[SwitchC] interface ten-gigabitethernet 1/0/6

[SwitchC-Ten-GigabitEthernet1/0/6] port link-aggregation group 1

[SwitchC-Ten-GigabitEthernet1/0/6] quit

[SwitchC] interface ten-gigabitethernet 1/0/7

[SwitchC-Ten-GigabitEthernet1/0/7] port link-aggregation group 1

[SwitchC-Ten-GigabitEthernet1/0/7] quit

[SwitchC] interface ten-gigabitethernet 1/0/8

[SwitchC-Ten-GigabitEthernet1/0/8] port link-aggregation group 1

[SwitchC-Ten-GigabitEthernet1/0/8] quit

配置二层聚合接口 1 为 Trunk 接口, 允许 VLAN 4001 的存储数据报文通过。

[SwitchC] interface bridge-aggregation 1

[SwitchC-Bridge-Aggregation1] port link-type trunk

[SwitchC-Bridge-Aggregation1] port trunk permit vlan 4001

[SwitchC-Bridge-Aggregation1] quit

(3) DCBX 部署

全局开启 LLDP 功能。

[SwitchC] lldp global enable

创建编号为 4000 的二层 ACL,并为其创建规则来匹配 FCoE 报文(协议号为 0x8906)和 FIP 报 文(协议号为 0x8914)。

[SwitchC] acl mac 4000

[SwitchC-acl-mac-4000] rule 0 permit type 8906 ffff

[SwitchC-acl-mac-4000] rule 5 permit type 8914 ffff

[SwitchC-acl-mac-4000] quit

定义名为 DCBX 的类,其下各规则间的关系为逻辑或,并定义其匹配 ACL 4000。

[SwitchC] traffic classifier DCBX operator or

[SwitchC-classifier-DCBX] if-match acl 4000

[SwitchC-classifier-DCBX] quit

定义名为 DCBX 的流行为,并配置标记报文的 802.1p 优先级为 3。

[SwitchC] traffic behavior DCBX

[SwitchC-behavior-DCBX] remark dot1p 3

[SwitchC-behavior-DCBX] quit

定义名为 DCBX 的 QoS 策略,为类 DCBX 指定采用的流行为是 DCBX,并指定该策略为 DCBX 模式。

[SwitchC] qos policy DCBX

[SwitchC-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx

[SwitchC-qospolicy-DCBX] quit
在以太网接口 Ten-GigabitEthernet1/0/1 上开启 LLDP 功能,并允许该接口发送 LLDP 报文时携带 DCBX TLV 字段。

[SwitchC] interface ten-gigabitethernet 1/0/1

[SwitchC-Ten-GigabitEthernet1/0/1] lldp enable

[SwitchC-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx

在以太网接口 Ten-GigabitEthernet1/0/1 的出方向上应用 QoS 策略。

[SwitchC-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound

(4) PFC 部署

在以太网接口 Ten-GigabitEthernet1/0/1 上配置与磁盘设备自动协商是否开启 PFC 功能,且设置 对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

[SwitchC-Ten-GigabitEthernet1/0/1] priority-flow-control auto

[SwitchC-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3

[SwitchC-Ten-GigabitEthernet1/0/1] qos trust dot1p

[SwitchC-Ten-GigabitEthernet1/0/1] quit

在以太网接口 Ten-GigabitEthernet1/0/5~Ten-GigabitEthernet1/0/8 上配置强制开启 PFC 功能, 且设置对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

且改直对 602.1P 化九级 5 万石 FIC 为能,开配直信任服义目带的 602.1P 化

[SwitchC] interface ten-gigabitethernet 1/0/5

[SwitchC-Ten-GigabitEthernet1/0/5] priority-flow-control enable

[SwitchC-Ten-GigabitEthernet1/0/5] priority-flow-control no-drop dot1p 3

[SwitchC-Ten-GigabitEthernet1/0/5] qos trust dot1p

[SwitchC-Ten-GigabitEthernet1/0/5] quit

[SwitchC] interface ten-gigabitethernet 1/0/6

[SwitchC-Ten-GigabitEthernet1/0/6] priority-flow-control enable

[SwitchC-Ten-GigabitEthernet1/0/6] priority-flow-control no-drop dot1p 3

[SwitchC-Ten-GigabitEthernet1/0/6] qos trust dot1p

[SwitchC-Ten-GigabitEthernet1/0/6] quit

[SwitchC] interface ten-gigabitethernet 1/0/7

[SwitchC-Ten-GigabitEthernet1/0/7] priority-flow-control enable

[SwitchC-Ten-GigabitEthernet1/0/7] priority-flow-control no-drop dot1p 3

[SwitchC-Ten-GigabitEthernet1/0/7] qos trust dot1p

[SwitchC-Ten-GigabitEthernet1/0/7] quit

[SwitchC] interface ten-gigabitethernet 1/0/8

[SwitchC-Ten-GigabitEthernet1/0/8] priority-flow-control enable

```
[SwitchC-Ten-GigabitEthernet1/0/8] priority-flow-control no-drop dotlp 3
```

[SwitchC-Ten-GigabitEthernet1/0/8] qos trust dot1p

[SwitchC-Ten-GigabitEthernet1/0/8] quit

(5) FCoE 部署

配置 FCoE 模式为 FCF 模式,进入 VSAN 100 的视图,开启 Fabric 配置功能(本步骤可选, Fabric 配置功能缺省开启)。

[SwitchC] fcoe-mode fcf [SwitchC] vsan 100 [SwitchC-vsan100] domain configure enable # 配置交换机的优先级为1,使 Switch C 成为主交换机。

[SwitchC-vsan100] priority 1

配置域 ID 为 1。

[SwitchC-vsan100] domain-id 1 preferred

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[Y/N]\!:\!y$

全局开启 FSPF 功能。

[SwitchC-vsan100] fspf enable [SwitchC-vsan100] quit

创建 VFC1 接口, 配置 VFC1 接口工作在 F 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 100,即允许 VSAN 100 的报文通过 VFC1 接口。

[SwitchC] interface vfc 1

[SwitchC-Vfc1] fc mode f

[SwitchC-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchC-Vfc1] port trunk vsan 100

[SwitchC-Vfc1] quit

创建 VFC10 接口, 配置 VFC10 接口工作在 E 模式,将 VFC10 接口绑定到二层聚合接口 Bridge-Aggregation1上,并将 VFC10 接口以 Trunk 方式加入 VSAN 100, 即允许 VSAN 100 的报 文通过 VFC10 接口。

[SwitchC] interface vfc 10

[SwitchC-Vfc10] fc mode e

[SwitchC-Vfc10] bind interface bridge-aggregation 1

[SwitchC-Vfc10] port trunk vsan 100

开启 VFC10 接口的 FSPF 功能。

[SwitchC-Vfc10] undo fspf silent vsan 100

[SwitchC-Vfc10] quit

开启 VLAN 4001 的 FCoE 功能,并将其与 VSAN 100 进行映射。

[SwitchC] vlan 4001

[SwitchC-vlan4001] fcoe enable vsan 100

[SwitchC-vlan4001] quit

#进入 VSAN 100 的视图,配置允许默认 Zone 内的成员互相访问。

[SwitchC] vsan 100 [SwitchC-vsan100] zone default-zone permit [SwitchC-vsan100] quit

4. 配置 Switch D

Switch D 上的配置与 Switch C 类似,差异处为 Switch D 上配置的二层聚合接口是 Bridge-Aggregation2, Switch C 上配置的二层聚合接口是 Bridge-Aggregation1,配置步骤略。

15.1.5 验证配置

1. 在 Switch A 上进行验证

#显示 VSAN 100 内的域信息。

[SwitchA] display fc domain vsan 100 Domain Information of VSAN 100:

> Running time information: State: Stable

```
Switch WWN: 48:33:43:2d:46:43:1A:1A
Fabric name: 48:33:43:2d:46:43:1C:1C
Priority: 128
Domain ID: 2
Configuration information:
Domain configure: Enabled
Domain auto-reconfigure: Disabled
Fabric name: 48:33:43:2d:46:43:1A:1A
Priority: 128
Domain ID: 2 (preferred)
Principal switch running time information:
Priority: 1
```

Path Interface Upstream Vfc10

从上述信息可以看出,Switch A 的配置已经结束,主交换机为 Switch A 分配的域 ID 为 2。

#显示 VSAN 100 内的域列表。

[SwitchA] display fc domain-list vsan 100

Domain list of VSAN 100:

Number of domains: 2

Domain ID WWN

0x01(1) 48:33:43:2d:46:43:1C:1C [Principal]

0x02(2) 48:33:43:2d:46:43:1A:1A [Local]

从上述信息可以看出,Switch C 成为主交换机,主交换机给自己分配了配置的想要获取的域 ID 1。

#显示 Switch A 路由表相关信息。

[SwitchA] display fc routing-table vsan 100

Routing Table: VSAN 100

Destinations : 5	Rou	tes : 5		
Destination/mask	Protocol	Preference	Cost	Interface
0x010000/8	FSPF	20	100	Vfc10
0xfffc01/24	DIRECT	0	0	InLoop0
0xfffffa/24	DIRECT	0	0	InLoop0
0xffffc/24	DIRECT	0	0	InLoop0
0xfffffd/24	DIRECT	0	0	InLoop0

从上述信息可以看出,Switch A 上存在了一条到 Switch C 的 FSPF 路由,出接口为 VFC10 接口。

```
#显示 Switch A 上的节点注册的相关信息。
```

[SwitchA] display fc login vsan 100

Interface VSAN FCID Node WWN

Port WWN

Vfc1 100 0x020000 21:01:00:1b:32:a0:fa:12 21:01:00:1b:32:a0:fa:11

#显示 VSAN 100 内的名称服务数据库的简要信息。

[SwitchA] display fc name-service database vsan 100

VSAN 100:

FCID	Туре	PWWN(vendor)	FC4-type:feature
0x010000	0x01(N)	10:00:00:05:30:00:25:a3	SCSI-FCP:Target
0x020000	0x01(N)	21:01:00:1b:32:a0:fa:11	SCSI-FCP:Initiator

2. 在 Switch B 上进行验证

Switch B上的验证方法与 Switch A 的完全相同,验证信息略。

3. 在 Switch C 上进行验证

#显示 Switch C 上的节点注册的相关信息。

[SwitchC] display fc login vsan 100 Interface VSAN FCID Node WWN Port WWN Vfcl 100 0x010000 10:00:05:30:00:25:a4 10:00:00:05:30:00:25:a3

4. 在 Switch D 上进行验证

Switch D 上的验证方法与 Switch C 的完全相同,验证信息略。

15.2 IRF模式的FCoE配置举例

15.2.1 组网需求

如<u>图 15-2</u>所示, Switch A 和 Switch B 与以太网交换机连接,作为 LAN 网络的接入层; Switch A 和 Switch B 分别与 Switch C 和 Switch D 连接,作为 SAN 网络的 FCF 交换机。 要求实现:

- Switch A 和 Switch B 与以太网交换机所组成的传输网络能够使服务器为 LAN 网络提供业务服务; Switch A~Switch D 所组成的传输网络能够使服务器访问磁盘设备内的存储资源。
- 满足用户对服务器、磁盘设备等设备收发报文的高可靠性要求,需要实现链路备份功能。
- 提高 Switch A 和 Switch C 之间、Switch B 和 Switch D 之间链路的带宽,并实现链路备份和 负载分担。
- 实现对 Switch A 和 Switch B 的统一管理,集合多台设备的硬件资源和软件处理能力,一旦其中一台设备发生故障,另一台设备能够迅速起到备份作用,以保证业务不中断。

15.2.2 组网图

图15-2 配置 IRF 模式的 FCoE 组网图



15.2.3 配置思路

- 为了实现对 Switch A 和 Switch B 的统一管理和设备间的备份作用,将 Switch A 和 Switch B 通过部署 IRF 功能虚拟化成一台 IRF 设备(Switch A 为主用设备),作为 LAN 网络的接入层和 SAN 网络的 FCF 交换机。
- 将 Switch A 和 Switch B 相连接的 4 条物理链路配置为一条 IRF 链路, 链路两端的端口分别为 IRF 端口 1/1 和 IRF 端口 2/2。Switch A 和 Switch B 与以太网交换机之间的以太网链路形成跨 设备聚合, 即以太网聚合链路 3。
- 为了实现 SAN 网络中的存储数据流量能够在无损以太网链路上传输,建议用户在交换机上与服务器连接的以太网接口上配置 DCBX、自动协商模式的 PFC、ETS 功能;在交换机上与磁盘设备连接的以太网接口上配置 DCBX、自动协商模式的 PFC 功能;在交换机之间连接的以太网接口上要强制开启 PFC 功能。
- 为了实现服务器到磁盘设备间的链路备份,使用互相隔离的两个 SAN 网络(服务器、IRF 设备、Switch C 和磁盘设备所组成的 SAN 网络与服务器、IRF 设备、Switch D 和磁盘设备所组成的 SAN 网络是两个不同的物理 SAN 网络)为服务器提供到存储设备的连接,但由于服务

器连接的不再是两台独立的设备,而是连接了一台 IRF 设备,所以两个 SAN 网络需要使用不同的 VSAN (例如 VSAN 100 和 VSAN 200), IRF 设备连接这两个 VSAN。

- LAN 网络的以太网数量流量在 VLAN 1001 中传输, IRF 设备与 LAN 网络/服务器所连接的以太网接口上需要允许 VLAN 1001 中的报文通过。
- SAN 网络的存储数据流量在 VSAN 100、VSAN 200 中传输,Switch A 和 Switch C 上接入 SAN 网络的接口上需要允许 VSAN 100 中的报文通过,Switch B 和 Switch D 上接入 SAN 网络的接口上需要允许 VSAN 200 中的报文通过。配置 VLAN 4001 与 VSAN 100 进行映射,使得 VSAN 100 内的存储数据流量在 VLAN 4001 中传输;配置 VLAN 4002 与 VSAN 200 进行映射,使得 VSAN 200 内的存储数据流量在 VLAN 4002 中传输。
- 为了防止 LAN 网络存在物理环路,需要在 IRF 设备与 LAN 网络/服务器所连接的以太网接口 开启 STP 功能。为了避免 STP 功能阻塞 IRF 设备负责转发存储数据流量的接口,需要保证 IRF 设备与 Switch C 和 Switch D 连接的接口上没有开启 STP 功能。
- 由于 SAN 网络结构比较复杂,建议用户采用动态方式建立 Fabric 网络,使用 FSPF 协议建立 FC 路由。
- 为了实现服务器能够访问磁盘设备内的存储资源,需要配置允许默认 Zone 内的成员互相访问。
- 为了提高 IRF 设备和 Switch C 之间、IRF 设备和 Switch D 之间链路的带宽,并实现链路备份 和负载分担,分别配置以太网聚合链路 1 和以太网聚合链路 2。

15.2.4 配置步骤

🕑 说明

- 本例中只列出 FCoE 的相关配置。
- 本例中 IRF 的相关配置略,具体配置请参考 "IRF 配置指导"中的 "IRF 配置"。
- IRF 端口是一种专用于 IRF 成员设备之间进行连接的逻辑接口,它需要和物理端口绑定之后才能 生效。IRF 端口所在的链路即为 IRF 链路。
- Switch A 和 Switch B 通过部署 IRF 功能虚拟化成一台 IRF 设备后, IRF 设备的所有配置均可在 其中一台设备上完成配置过程。

1. 配置 Switch A (IRF 形成后)

(1) 开启高级模式

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchA> system-view [SwitchA] system-working-mode advance Do you want to change the system working mode? [Y/N]:y The system working mode is changed, please save the configuration and reboot the system to make it effective. [SwitchA] save The current configuration will be written to the device. Are you sure? [Y/N]:y Please input the file name(*.cfg)[flash:/startup.cfg] (To leave the existing filename unchanged, press the enter key): Validating file. Please wait... Saved the current configuration to mainboard device successfully. Slot 1: Save next configuration file successfully. [SwitchA] quit <SwitchA> reboot Start to check configuration with next startup configuration file, please wait.....DONE! Current configuration will be lost after the reboot, save current configuration? [Y/N]:y Please input the file name(*.cfg)[flash:/startup.cfg] (To leave the existing filename unchanged, press the enter key): flash:/startup.cfg exists, overwrite? [Y/N]:y Validating file. Please wait ... Configuration is saved to flash successfully. This command will reboot the device. Continue? [Y/N]:y Now rebooting, please wait... (2) VLAN 和接口部署 # 创建 VLAN 1001、4001、4002,分别用来传输以太网数据流量和存储数据流量。 <SwitchA> system-view [SwitchA] vlan 1001 [SwitchA-vlan1001] description ToLAN [SwitchA-vlan1001] guit [SwitchA] vlan 4001 [SwitchA-vlan4001] description ToSAN_A [SwitchA-vlan4001] quit [SwitchA] vlan 4002 [SwitchA-vlan4002] description ToSAN_B [SwitchA-vlan4002] quit #开启全局 STP 功能。 [SwitchA] stp global enable # 配置以太网接口 Ten-GigabitEthernet1/1/0/1 为 Hybrid 接口, 允许 VLAN 1001 的以太网数据报文 不带 Tag 标签通过, 允许 VLAN 4001 的存储数据报文带 Tag 标签通过, 设置接口的 PVID 为 VLAN 1001,并开启 STP 功能。 [SwitchA] interface ten-gigabitethernet 1/1/0/1 [SwitchA-Ten-GigabitEthernet1/1/0/1] port link-type hybrid [SwitchA-Ten-GigabitEthernet1/1/0/1] port hybrid vlan 1001 untagged [SwitchA-Ten-GigabitEthernet1/1/0/1] port hybrid vlan 4001 tagged [SwitchA-Ten-GigabitEthernet1/1/0/1] port hybrid pvid vlan 1001 [SwitchA-Ten-GigabitEthernet1/1/0/1] stp enable [SwitchA-Ten-GigabitEthernet1/1/0/1] quit # 配置以太网接口 Ten-GigabitEthernet2/1/0/1 为 Hybrid 接口, 允许 VLAN 1001 的以太网数据报文 不带 Tag 标签通过, 允许 VLAN 4002 的存储数据报文带 Tag 标签通过, 设置接口的 PVID 为 VLAN 1001,并开启 STP 功能。 [SwitchA] interface ten-gigabitethernet 2/1/0/1 [SwitchA-Ten-GigabitEthernet2/1/0/1] port link-type hybrid

```
[SwitchA-Ten-GigabitEthernet2/1/0/1] port hybrid vlan 1001 untagged
```

```
[SwitchA-Ten-GigabitEthernet2/1/0/1] port hybrid vlan 4002 tagged
```

```
[SwitchA-Ten-GigabitEthernet2/1/0/1] port hybrid pvid vlan 1001
```

```
[SwitchA-Ten-GigabitEthernet2/1/0/1] stp enable
```

[SwitchA-Ten-GigabitEthernet2/1/0/1] quit

配置以太网接口 Ten-GigabitEthernet1/1/0/10 和 Ten-GigabitEthernet2/1/0/10 为 Trunk 接口,允许 VLAN 1001 的以太网数据报文通过,并开启 STP 功能。

[SwitchA] interface ten-gigabitethernet 1/1/0/10

[SwitchA-Ten-GigabitEthernet1/1/0/10] port link-type trunk

[SwitchA-Ten-GigabitEthernet1/1/0/10] port trunk permit vlan 1001

[SwitchA-Ten-GigabitEthernet1/1/0/10] stp enable

[SwitchA-Ten-GigabitEthernet1/1/0/10] quit

[SwitchA] interface ten-gigabitethernet 2/1/0/10

[SwitchA-Ten-GigabitEthernet2/1/0/10] port link-type trunk

[SwitchA-Ten-GigabitEthernet2/1/0/10] port trunk permit vlan 1001

[SwitchA-Ten-GigabitEthernet2/1/0/10] stp enable

[SwitchA-Ten-GigabitEthernet2/1/0/10] quit

创建二层聚合接口 1, 配置其对应的聚合组工作在动态聚合模式下, 并关闭 STP 功能。

[SwitchA] interface bridge-aggregation 1

[SwitchA-Bridge-Aggregation1] link-aggregation mode dynamic

[SwitchA-Bridge-Aggregation1] undo stp enable

[SwitchA-Bridge-Aggregation1] quit

将以太网接口 Ten-GigabitEthernet1/1/0/5~Ten-GigabitEthernet1/1/0/8 共4个接口加入二层聚合 组 1。

[SwitchA] interface ten-gigabitethernet 1/1/0/5

```
[SwitchA-Ten-GigabitEthernet1/1/0/5] port link-aggregation group 1
```

[SwitchA-Ten-GigabitEthernet1/1/0/5] quit

[SwitchA] interface ten-gigabitethernet 1/1/0/6

[SwitchA-Ten-GigabitEthernet1/1/0/6] port link-aggregation group 1

[SwitchA-Ten-GigabitEthernet1/1/0/6] quit

[SwitchA] interface ten-gigabitethernet 1/1/0/7

[SwitchA-Ten-GigabitEthernet1/1/0/7] port link-aggregation group 1

[SwitchA-Ten-GigabitEthernet1/1/0/7] quit

[SwitchA] interface ten-gigabitethernet 1/1/0/8

[SwitchA-Ten-GigabitEthernet1/1/0/8] port link-aggregation group 1

[SwitchA-Ten-GigabitEthernet1/1/0/8] quit

配置二层聚合接口 1 为 Trunk 接口, 允许 VLAN 4001 的存储数据报文通过。

[SwitchA] interface bridge-aggregation 1

[SwitchA-Bridge-Aggregation1] port link-type trunk

[SwitchA-Bridge-Aggregation1] port trunk permit vlan 4001

[SwitchA-Bridge-Aggregation1] quit

创建二层聚合接口 2, 配置其对应的聚合组工作在动态聚合模式下,并关闭 STP 功能。

[SwitchA] interface bridge-aggregation 2

[SwitchA-Bridge-Aggregation2] link-aggregation mode dynamic

[SwitchA-Bridge-Aggregation2] undo stp enable

[SwitchA-Bridge-Aggregation2] quit

```
# 将以太网接口 Ten-GigabitEthernet2/1/0/5~Ten-GigabitEthernet2/1/0/8 共4个接口加入二层聚合组2。
```

[SwitchA] interface ten-gigabitethernet 2/1/0/5

[SwitchA-Ten-GigabitEthernet2/1/0/5] port link-aggregation group 2

[SwitchA-Ten-GigabitEthernet2/1/0/5] guit [SwitchA] interface ten-gigabitethernet 2/1/0/6 [SwitchA-Ten-GigabitEthernet2/1/0/6] port link-aggregation group 2 [SwitchA-Ten-GigabitEthernet2/1/0/6] quit [SwitchA] interface ten-gigabitethernet 2/1/0/7 [SwitchA-Ten-GigabitEthernet2/1/0/7] port link-aggregation group 2 [SwitchA-Ten-GigabitEthernet2/1/0/7] quit [SwitchA] interface ten-gigabitethernet 2/1/0/8 [SwitchA-Ten-GigabitEthernet2/1/0/8] port link-aggregation group 2 [SwitchA-Ten-GigabitEthernet2/1/0/8] quit # 配置二层聚合接口 2 为 Trunk 接口, 允许 VLAN 4002 的存储数据报文通过。 [SwitchA] interface bridge-aggregation 2 [SwitchA-Bridge-Aggregation2] port link-type trunk [SwitchA-Bridge-Aggregation2] port trunk permit vlan 4002 [SwitchA-Bridge-Aggregation2] guit # 创建二层聚合接口 3, 配置其对应的聚合组工作在动态聚合模式下, 并开启 STP 功能。 [SwitchA] interface bridge-aggregation 3 [SwitchA-Bridge-Aggregation3] link-aggregation mode dynamic [SwitchA-Bridge-Aggregation3] stp enable #开启二层聚合接口3的LACP MAD 检测功能。 [SwitchA-Bridge-Aggregation3] mad enable You need to assign a domain ID (range: 0-4294967295) [Current domain is: 1]: The assigned domain ID is: 1 Info: MAD LACP only enable on dynamic aggregation interface. [SwitchA-Bridge-Aggregation3] quit # 将以太网接口 Ten-GigabitEthernet1/1/0/10、Ten-GigabitEthernet2/1/0/10 加入二层聚合组 3。 [SwitchA] interface ten-gigabitethernet 1/1/0/10 [SwitchA-Ten-GigabitEthernet1/1/0/10] port link-aggregation group 3 [SwitchA-Ten-GigabitEthernet1/1/0/10] quit [SwitchA] interface ten-gigabitethernet 2/1/0/10 [SwitchA-Ten-GigabitEthernet2/1/0/10] port link-aggregation group 3 [SwitchA-Ten-GigabitEthernet2/1/0/10] quit # 配置二层聚合接口 3 为 Trunk 接口, 允许 VLAN 1001 的存储数据报文通过。 [SwitchA] interface bridge-aggregation 3 [SwitchA-Bridge-Aggregation3] port link-type trunk [SwitchA-Bridge-Aggregation3] port trunk permit vlan 1001 [SwitchA-Bridge-Aggregation3] quit (3) DCBX 部署 # 全局开启 LLDP 功能。 [SwitchA] lldp global enable # 创建编号为 4000 的二层 ACL,并为其创建规则来匹配 FCoE 报文(协议号为 0x8906)和 FIP 报 文(协议号为0x8914)。 [SwitchA] acl mac 4000 [SwitchA-acl-mac-4000] rule 0 permit type 8906 ffff [SwitchA-acl-mac-4000] rule 5 permit type 8914 ffff

[SwitchA-acl-mac-4000] quit

定义名为 DCBX 的类,其下各规则间的关系为逻辑或,并定义其匹配 ACL 4000。

[SwitchA] traffic classifier DCBX operator or

[SwitchA-classifier-DCBX] if-match acl 4000

[SwitchA-classifier-DCBX] quit

定义名为 DCBX 的流行为,并配置标记报文的 802.1p 优先级为 3。

[SwitchA] traffic behavior DCBX

[SwitchA-behavior-DCBX] remark dot1p 3

[SwitchA-behavior-DCBX] quit

定义名为 DCBX 的 QoS 策略,为类 DCBX 指定采用的流行为是 DCBX,并指定该策略为 DCBX 模式。

[SwitchA] qos policy DCBX

[SwitchA-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx

[SwitchA-qospolicy-DCBX] quit

在以太网接口 Ten-GigabitEthernet1/1/0/1 上开启 LLDP 功能,并允许该接口发送 LLDP 报文时携带 DCBX TLV 字段。

[SwitchA] interface ten-gigabitethernet 1/1/0/1

[SwitchA-Ten-GigabitEthernet1/1/0/1] lldp enable

[SwitchA-Ten-GigabitEthernet1/1/0/1] lldp tlv-enable dot1-tlv dcbx

在以太网接口 Ten-GigabitEthernet1/1/0/1 的出方向上应用 QoS 策略。

[SwitchA-Ten-GigabitEthernet1/1/0/1] qos apply policy DCBX outbound

[SwitchA-Ten-GigabitEthernet1/1/0/1] quit

在以太网接口 Ten-GigabitEthernet2/1/0/1 上开启 LLDP 功能,并允许该接口发送 LLDP 报文时携带 DCBX TLV 字段。

[SwitchA] interface ten-gigabitethernet 2/1/0/1

[SwitchA-Ten-GigabitEthernet2/1/0/1] lldp enable

[SwitchA-Ten-GigabitEthernet2/1/0/1] lldp tlv-enable dot1-tlv dcbx

在以太网接口 Ten-GigabitEthernet2/1/0/1 的出方向上应用 QoS 策略。

 $[SwitchA-Ten-GigabitEthernet2/1/0/1]\ qos\ apply\ policy\ DCBX\ outbound$

[SwitchA-Ten-GigabitEthernet2/1/0/1] quit

(4) PFC 部署

在以太网接口 Ten-GigabitEthernet1/1/0/1 和 Ten-GigabitEthernet2/1/0/1 上配置与服务器自动协商是否开启 PFC 功能,且设置对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

```
[SwitchA] interface ten-gigabitethernet 1/1/0/1
[SwitchA-Ten-GigabitEthernet1/1/0/1] priority-flow-control auto
[SwitchA-Ten-GigabitEthernet1/1/0/1] priority-flow-control no-drop dot1p 3
[SwitchA-Ten-GigabitEthernet1/1/0/1] quit
[SwitchA] interface ten-gigabitethernet 2/1/0/1
[SwitchA-Ten-GigabitEthernet2/1/0/1] priority-flow-control auto
[SwitchA-Ten-GigabitEthernet2/1/0/1] priority-flow-control no-drop dot1p 3
[SwitchA-Ten-GigabitEthernet2/1/0/1] qos trust dot1p
[SwitchA-Ten-GigabitEthernet2/1/0/1] qos trust dot1p
```

在以太网接口 Ten-GigabitEthernet1/1/0/5 ~ Ten-GigabitEthernet1/1/0/8 和以太网接口 Ten-GigabitEthernet2/1/0/5~Ten-GigabitEthernet2/1/0/8 上配置 PFC 功能的开启模式为强制模式, 且设置对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

```
[SwitchA] interface ten-gigabitethernet 1/1/0/5
[SwitchA-Ten-GigabitEthernet1/1/0/5] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet1/1/0/5] priority-flow-control no-drop dot1p 3
[SwitchA-Ten-GigabitEthernet1/1/0/5] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/1/0/5] guit
[SwitchA] interface ten-gigabitethernet 1/1/0/6
[SwitchA-Ten-GigabitEthernet1/1/0/6] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet1/1/0/6] priority-flow-control no-drop dotlp 3
[SwitchA-Ten-GigabitEthernet1/1/0/6] gos trust dot1p
[SwitchA-Ten-GigabitEthernet1/1/0/6] quit
[SwitchA] interface ten-gigabitethernet 1/1/0/7
[SwitchA-Ten-GigabitEthernet1/1/0/7] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet1/1/0/7] priority-flow-control no-drop dot1p 3
[SwitchA-Ten-GigabitEthernet1/1/0/7] gos trust dot1p
[SwitchA-Ten-GigabitEthernet1/1/0/7] guit
[SwitchA] interface ten-gigabitethernet 1/1/0/8
[SwitchA-Ten-GigabitEthernet1/1/0/8] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet1/1/0/8] priority-flow-control no-drop dotlp 3
[SwitchA-Ten-GigabitEthernet1/1/0/8] qos trust dot1p
[SwitchA-Ten-GigabitEthernet1/1/0/8] quit
[SwitchA] interface ten-gigabitethernet 2/1/0/5
[SwitchA-Ten-GigabitEthernet2/1/0/5] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet2/1/0/5] priority-flow-control no-drop dot1p 3
[SwitchA-Ten-GigabitEthernet2/1/0/5] gos trust dot1p
[SwitchA-Ten-GigabitEthernet2/1/0/5] quit
[SwitchA] interface ten-gigabitethernet 2/1/0/6
[SwitchA-Ten-GigabitEthernet2/1/0/6] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet2/1/0/6] priority-flow-control no-drop dotlp 3
[SwitchA-Ten-GigabitEthernet2/1/0/6] qos trust dot1p
[SwitchA-Ten-GigabitEthernet2/1/0/6] quit
[SwitchA] interface ten-gigabitethernet 2/1/0/7
[SwitchA-Ten-GigabitEthernet2/1/0/7] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet2/1/0/7] priority-flow-control no-drop dot1p 3
[SwitchA-Ten-GigabitEthernet2/1/0/7] qos trust dot1p
[SwitchA-Ten-GigabitEthernet2/1/0/7] quit
[SwitchA] interface ten-gigabitethernet 2/1/0/8
[SwitchA-Ten-GigabitEthernet2/1/0/8] priority-flow-control enable
[SwitchA-Ten-GigabitEthernet2/1/0/8] priority-flow-control no-drop dotlp 3
[SwitchA-Ten-GigabitEthernet2/1/0/8] qos trust dot1p
[SwitchA-Ten-GigabitEthernet2/1/0/8] quit
(5) ETS 部署
```

配置 802.1p 优先级到本地优先级的映射,将 802.1p 优先级 3 映射到本地优先级 1,配置其它的 802.1p 优先级映射到本地优先级 0。

[SwitchA] qos map-table dot1p-1p

```
[SwitchA-maptbl-dot1p-lp] import 3 export 1
[SwitchA-maptbl-dot1p-lp] import 0 export 0
[SwitchA-maptbl-dot1p-1p] import 1 export 0
[SwitchA-maptbl-dot1p-lp] import 2 export 0
[SwitchA-maptbl-dot1p-lp] import 4 export 0
[SwitchA-maptbl-dot1p-lp] import 5 export 0
[SwitchA-maptbl-dot1p-1p] import 6 export 0
[SwitchA-maptbl-dot1p-1p] import 7 export 0
[SwitchA-maptbl-dot1p-lp] quit
# 在以太网接口 Ten-GigabitEthernet1/1/0/1 上配置 WRR 队列,使 FCoE 流量和普通 LAN 流量各
占50%带宽。
[SwitchA] interface ten-gigabitethernet 1/1/0/1
[SwitchA-Ten-GigabitEthernet1/1/0/1] gos wrr byte-count
[SwitchA-Ten-GigabitEthernet1/1/0/1] qos wrr afl group 1 byte-count 1
[SwitchA-Ten-GigabitEthernet1/1/0/1] gos wrr be group 1 byte-count 1
# 在以太网接口 Ten-GigabitEthernet1/1/0/1 上配置其它的队列为 SP 调度方式。
[SwitchA-Ten-GigabitEthernet1/1/0/1] qos wrr af2 group sp
[SwitchA-Ten-GigabitEthernet1/1/0/1] qos wrr af3 group sp
[SwitchA-Ten-GigabitEthernet1/1/0/1] qos wrr af4 group sp
[SwitchA-Ten-GigabitEthernet1/1/0/1] gos wrr ef group sp
[SwitchA-Ten-GigabitEthernet1/1/0/1] qos wrr cs6 group sp
[SwitchA-Ten-GigabitEthernet1/1/0/1] qos wrr cs7 group sp
[SwitchA-Ten-GigabitEthernet1/1/0/1] guit
# 在以太网接口 Ten-GigabitEthernet2/1/0/1 上配置 WRR 队列,使 FCoE 流量和普通 LAN 流量各
占50%带宽。
[SwitchA] interface ten-gigabitethernet 2/1/0/1
[SwitchA-Ten-GigabitEthernet2/1/0/1] qos wrr af1 group 1 byte-count 1
[SwitchA-Ten-GigabitEthernet2/1/0/1] qos wrr be group 1 byte-count 1
# 在以太网接口 Ten-GigabitEthernet2/1/0/1 上配置其它的队列为 SP 调度方式。
[SwitchA-Ten-GigabitEthernet2/1/0/1] qos wrr af2 group sp
[SwitchA-Ten-GigabitEthernet2/1/0/1] qos wrr af3 group sp
[SwitchA-Ten-GigabitEthernet2/1/0/1] qos wrr af4 group sp
[SwitchA-Ten-GigabitEthernet2/1/0/1] qos wrr ef group sp
[SwitchA-Ten-GigabitEthernet2/1/0/1] qos wrr cs6 group sp
[SwitchA-Ten-GigabitEthernet2/1/0/1] qos wrr cs7 group sp
[SwitchA-Ten-GigabitEthernet2/1/0/1] quit
(6) FCoE 部署
# 配置 FCoE 模式为 FCF 模式。
[SwitchA] fcoe-mode fcf
# 创建 VSAN 100,开启 Fabric 配置功能(本步骤可选,Fabric 配置功能缺省开启)。
[SwitchA] vsan 100
[SwitchA-vsan100] domain configure enable
# 配置域 ID 为 2。
[SwitchA-vsan100] domain-id 2 preferred
```

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[\texttt{Y}/\texttt{N}]:_{\texttt{Y}}$

全局开启 VSAN 100 的 FSPF 功能。

[SwitchA-vsan100] fspf enable

[SwitchA-vsan100] quit

创建 VSAN 200, 开启 Fabric 配置功能(本步骤可选, Fabric 配置功能缺省开启)。

[SwitchA] vsan 200

[SwitchA-vsan200] domain configure enable

配置域 ID 为 3。

[SwitchA-vsan200] domain-id 3 preferred Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? $[Y/N]\!:_Y$

全局开启 VSAN 200 的 FSPF 功能。

[SwitchA-vsan200] fspf enable

[SwitchA-vsan200] quit

创建 VFC1 接口, 配置 VFC1 接口工作在 F 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 100, 即允许 VSAN 100 的报文通过 VFC1 接口。

[SwitchA] interface vfc 1

```
[SwitchA-Vfc1] fc mode f
```

[SwitchA-Vfc1] bind interface ten-gigabitethernet 1/1/0/1

[SwitchA-Vfc1] port trunk vsan 100

[SwitchA-Vfc1] quit

创建 VFC2 接口, 配置 VFC2 接口工作在 F 模式,将 VFC2 接口绑定到以太网接口 Ten-GigabitEthernet2/1/0/1 上,并将 VFC2 接口以 Trunk 方式加入 VSAN 200, 即允许 VSAN 200 的报文通过 VFC2 接口。

[SwitchA] interface vfc 2

[SwitchA-Vfc2] fc mode f

[SwitchA-Vfc2] bind interface ten-gigabitethernet 2/1/0/1

[SwitchA-Vfc2] port trunk vsan 200

[SwitchA-Vfc2] quit

创建 VFC10 接口, 配置 VFC10 接口工作在 E 模式,将 VFC10 接口绑定到二层聚合接口 Bridge-Aggregation1上,并将 VFC10 接口以 Trunk 方式加入 VSAN 100,即允许 VSAN 100 的报 文通过 VFC10 接口。

[SwitchA] interface vfc 10

[SwitchA-Vfc10] fc mode e

[SwitchA-Vfc10] bind interface bridge-aggregation 1

[SwitchA-Vfc10] port trunk vsan 100

开启 VFC10 接口的 FSPF 功能。

[SwitchA-Vfc10] undo fspf silent vsan 100

[SwitchA-Vfc10] quit

创建 VFC11 接口, 配置 VFC11 接口工作在 E 模式,将 VFC11 接口绑定到二层聚合接口 Bridge-Aggregation2上,并将 VFC11 接口以 Trunk 方式加入 VSAN 200,即允许 VSAN 200 的报 文通过 VFC11 接口。

[SwitchA] interface vfc 11

[SwitchA-Vfc11] fc mode e

[SwitchA-Vfc11] bind interface bridge-aggregation 2

[SwitchA-Vfc11] port trunk vsan 200 #开启 VFC11 接口的 FSPF 功能。

[SwitchA-Vfc11] undo fspf silent vsan 200

[SwitchA-Vfc11] quit

开启 VLAN 4001 的 FCoE 功能,并将其与 VSAN 100 进行映射。

[SwitchA] vlan 4001

[SwitchA-vlan4001] fcoe enable vsan 100

[SwitchA-vlan4001] quit

开启 VLAN 4002 的 FCoE 功能,并将其与 VSAN 200 进行映射。

[SwitchA] vlan 4002

[SwitchA-vlan4002] fcoe enable vsan 200

[SwitchA-vlan4002] quit

#进入 VSAN 100 的视图, 配置允许默认 Zone 内的成员互相访问。

[SwitchA] vsan 100

[SwitchA-vsan100] zone default-zone permit

[SwitchA-vsan100] quit

#进入 VSAN 200 的视图,配置允许默认 Zone 内的成员互相访问。

[SwitchA] vsan 200 [SwitchA-vsan200] zone default-zone permit

[SwitchA-vsan200] quit

2. 配置 Switch C

(1) 开启高级模式

配置设备工作模式为高级模式并保存配置重启设备(如果已经配置设备为高级模式此步骤可略)。

<SwitchC> system-view

[SwitchC] system-working-mode advance

Do you want to change the system working mode? [Y/N]:y

The system working mode is changed, please save the configuration and reboot the system to make it effective.

[SwitchC] save

The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(*.cfg)[flash:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

Slot 1:

Save next configuration file successfully.

[SwitchC] quit

<SwitchC> reboot

Start to check configuration with next startup configuration file, please wait.....DONE! Current configuration will be lost after the reboot, save current configuration? [Y/N]:y Please input the file name(*.cfg)[flash:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

flash:/startup.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait...

Configuration is saved to flash successfully.

This command will reboot the device. Continue? $[{\tt Y}/{\tt N}]:_{\tt Y}$

Now rebooting, please wait...

(2) VLAN 和接口部署

创建 VLAN 4001,用来传输存储数据流量。

<SwitchC> system-view

[SwitchC] vlan 4001

[SwitchC-vlan4001] description ToSAN_A

[SwitchC-vlan4001] quit

配置以太网接口 Ten-GigabitEthernet1/0/1 为 Hybrid 接口, 允许 VLAN 4001 的存储数据报文通过, 设置接口的 PVID 为 VLAN 4001。

[SwitchC] interface ten-gigabitethernet 1/0/1

[SwitchC-Ten-GigabitEthernet1/0/1] port link-type hybrid

[SwitchC-Ten-GigabitEthernet1/0/1] port hybrid vlan 4001 tagged

[SwitchC-Ten-GigabitEthernet1/0/1] port hybrid pvid vlan 4001

[SwitchC-Ten-GigabitEthernet1/0/1] quit

创建二层聚合接口 1, 配置其对应的聚合组工作在动态聚合模式下。

[SwitchC] interface bridge-aggregation 1

[SwitchC-Bridge-Aggregation1] link-aggregation mode dynamic

[SwitchC-Bridge-Aggregation1] quit

#将以太网接口Ten-GigabitEthernet1/0/5~Ten-GigabitEthernet1/0/8共4个接口加入二层聚合组1。

[SwitchC] interface ten-gigabitethernet 1/0/5

[SwitchC-Ten-GigabitEthernet1/0/5] port link-aggregation group 1

[SwitchC-Ten-GigabitEthernet1/0/5] quit

[SwitchC] interface ten-gigabitethernet 1/0/6

[SwitchC-Ten-GigabitEthernet1/0/6] port link-aggregation group 1

[SwitchC-Ten-GigabitEthernet1/0/6] quit

[SwitchC] interface ten-gigabitethernet 1/0/7

[SwitchC-Ten-GigabitEthernet1/0/7] port link-aggregation group 1

[SwitchC-Ten-GigabitEthernet1/0/7] quit

[SwitchC] interface ten-gigabitethernet 1/0/8

[SwitchC-Ten-GigabitEthernet1/0/8] port link-aggregation group 1

[SwitchC-Ten-GigabitEthernet1/0/8] quit

配置二层聚合接口 1 为 Trunk 接口, 允许 VLAN 4001 的存储数据报文通过。

[SwitchC] interface bridge-aggregation 1

[SwitchC-Bridge-Aggregation1] port link-type trunk

[SwitchC-Bridge-Aggregation1] port trunk permit vlan 4001

[SwitchC-Bridge-Aggregation1] quit

(3) DCBX 部署

全局开启 LLDP 功能。

[SwitchC] lldp global enable

创建编号为 4000 的二层 ACL,并为其创建规则来匹配 FCoE 报文(协议号为 0x8906)和 FIP 报 文(协议号为 0x8914)。

[SwitchC] acl mac 4000

[SwitchC-acl-mac-4000] rule 0 permit type 8906 ffff

[SwitchC-acl-mac-4000] rule 5 permit type 8914 ffff

[SwitchC-acl-mac-4000] quit

定义名为 DCBX 的类,其下各规则间的关系为逻辑或,并定义其匹配 ACL 4000。

[SwitchC] traffic classifier DCBX operator or

[SwitchC-classifier-DCBX] if-match acl 4000

[SwitchC-classifier-DCBX] quit

定义名为 DCBX 的流行为,并配置标记报文的 802.1p 优先级为 3。

[SwitchC] traffic behavior DCBX

[SwitchC-behavior-DCBX] remark dot1p 3

[SwitchC-behavior-DCBX] quit

定义名为 DCBX 的 QoS 策略,为类 DCBX 指定采用的流行为是 DCBX,并指定该策略为 DCBX 模式。

[SwitchC] qos policy DCBX

[SwitchC-qospolicy-DCBX] classifier DCBX behavior DCBX mode dcbx

[SwitchC-qospolicy-DCBX] quit

在以太网接口 Ten-GigabitEthernet1/0/1 上开启 LLDP 功能,并允许该接口发送 LLDP 报文时携带 DCBX TLV 字段。

[SwitchC] interface ten-gigabitethernet 1/0/1

[SwitchC-Ten-GigabitEthernet1/0/1] lldp enable

 $[SwitchC-Ten-GigabitEthernet1/0/1] \ lldp \ tlv-enable \ dot1-tlv \ dcbx$

在以太网接口 Ten-GigabitEthernet1/0/1 的出方向上应用 QoS 策略。

[SwitchC-Ten-GigabitEthernet1/0/1] qos apply policy DCBX outbound

(4) PFC 部署

在以太网接口 Ten-GigabitEthernet1/0/1 上配置与磁盘设备自动协商是否开启 PFC 功能,且设置 对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

[SwitchC-Ten-GigabitEthernet1/0/1] priority-flow-control auto

[SwitchC-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dotlp 3

[SwitchC-Ten-GigabitEthernet1/0/1] qos trust dotlp

[SwitchC-Ten-GigabitEthernet1/0/1] quit

在以太网接口 Ten-GigabitEthernet1/0/5~Ten-GigabitEthernet1/0/8 上配置强制开启 PFC 功能, 且设置对 802.1p 优先级 3 开启 PFC 功能,并配置信任报文自带的 802.1p 优先级。

[SwitchC] interface ten-gigabitethernet 1/0/5

[SwitchC-Ten-GigabitEthernet1/0/5] priority-flow-control enable

[SwitchC-Ten-GigabitEthernet1/0/5] priority-flow-control no-drop dot1p 3

[SwitchC-Ten-GigabitEthernet1/0/5] qos trust dotlp

[SwitchC-Ten-GigabitEthernet1/0/5] quit

[SwitchC] interface ten-gigabitethernet 1/0/6

[SwitchC-Ten-GigabitEthernet1/0/6] priority-flow-control enable

[SwitchC-Ten-GigabitEthernet1/0/6] priority-flow-control no-drop dot1p 3

[SwitchC-Ten-GigabitEthernet1/0/6] qos trust dot1p

[SwitchC-Ten-GigabitEthernet1/0/6] quit

[SwitchC] interface ten-gigabitethernet 1/0/7

[SwitchC-Ten-GigabitEthernet1/0/7] priority-flow-control enable

[SwitchC-Ten-GigabitEthernet1/0/7] priority-flow-control no-drop dot1p 3

[SwitchC-Ten-GigabitEthernet1/0/7] qos trust dot1p

[SwitchC-Ten-GigabitEthernet1/0/7] quit

[SwitchC] interface ten-gigabitethernet 1/0/8

[SwitchC-Ten-GigabitEthernet1/0/8] priority-flow-control enable

[SwitchC-Ten-GigabitEthernet1/0/8] priority-flow-control no-drop dot1p 3

[SwitchC-Ten-GigabitEthernet1/0/8] qos trust dot1p

[SwitchC-Ten-GigabitEthernet1/0/8] quit

(5) FCoE 部署

配置 FCoE 模式为 FCF 模式,进入 VSAN 100 的视图,开启 Fabric 配置功能(本步骤可选, Fabric 配置功能缺省开启)。

[SwitchC] fcoe-mode fcf

[SwitchC] vsan 100

[SwitchC-vsan100] domain configure enable

配置交换机的优先级为 1, 使 Switch C 成为主交换机。

[SwitchC-vsan100] priority 1

配置域 ID 为 1。

[SwitchC-vsan100] domain-id 1 preferred

Nondisruptive reconfiguration might be performed or the switch might be isolated. Continue? [Y/N]:y

全局开启 FSPF 功能。

[SwitchC-vsan100] fspf enable

[SwitchC-vsan100] quit

创建 VFC1 接口, 配置 VFC1 接口工作在 F 模式,将 VFC1 接口绑定到以太网接口 Ten-GigabitEthernet1/0/1 上,并将 VFC1 接口以 Trunk 方式加入 VSAN 100,即允许 VSAN 100 的报文通过 VFC1 接口。

[SwitchC] interface vfc 1

[SwitchC-Vfc1] fc mode f

[SwitchC-Vfc1] bind interface ten-gigabitethernet 1/0/1

[SwitchC-Vfc1] port trunk vsan 100

[SwitchC-Vfc1] quit

创建 VFC10 接口, 配置 VFC10 接口工作在 E 模式,将 VFC10 接口绑定到二层聚合接口 Bridge-Aggregation1上,并将 VFC10 接口以 Trunk 方式加入 VSAN 100,即允许 VSAN 100 的报 文通过 VFC10 接口。

[SwitchC] interface vfc 10

[SwitchC-Vfc10] fc mode e

[SwitchC-Vfc10] bind interface bridge-aggregation 1

[SwitchC-Vfc10] port trunk vsan 100

开启 VFC10 接口的 FSPF 功能。

[SwitchC-Vfc10] undo fspf silent vsan 100

[SwitchC-Vfc10] quit

开启 VLAN 4001 的 FCoE 功能,并将其与 VSAN 100 进行映射。

[SwitchC] vlan 4001

[SwitchC-vlan4001] fcoe enable vsan 100

[SwitchC-vlan4001] quit

#进入 VSAN 100 的视图, 配置允许默认 Zone 内的成员互相访问。

[SwitchC] vsan 100

[SwitchC-vsan100] zone default-zone permit

[SwitchC-vsan100] quit

3. 配置 Switch D

Switch D 上的配置与 Switch C 类似,差异处为 Switch D 上配置的 VLAN、VSAN 和二层聚合接口 为 VLAN 4002、VSAN 200 和 Bridge-Aggregation2, Switch C 上配置的 VLAN、VSAN 和二层聚 合接口为 VLAN 4001、VSAN 100 和 Bridge-Aggregation1,配置步骤略。

15.2.5 验证配置

1. 在 Switch A 上进行验证

```
(1) 查看 VSAN 100 的信息
# 显示 Switch A 在 VSAN 100 内的域信息。
[SwitchA] display fc domain vsan 100
Domain Information of VSAN 100:
Running time information:
```

```
State: Stable
Switch WWN: 48:33:43:2d:46:43:1A:1A
Fabric name: 48:33:43:2d:46:43:1C:1C
Priority: 128
Domain ID: 2
Configuration information:
Domain configure: Enabled
Domain auto-reconfigure: Disabled
Fabric name: 48:33:43:2d:46:43:1A:1A
Priority: 128
Domain ID: 2 (preferred)
Principal switch running time information:
Priority: 1
```

Path Interface Upstream Vfc10

从上述信息可以看出,Switch A 的配置已经结束,主交换机为 Switch A 分配的域 ID 为 2。 # 显示 Switch A 在 VSAN 100 内的域列表。

```
[SwitchA] display fc domain-list vsan 100
```

```
Domain list of VSAN 100:
Number of domains: 2
```

Domain ID	WWN	
0x01(1)	48:33:43:2d:46:43:1C:1C	[Principal]
0x02(2)	48:33:43:2d:46:43:1A:1A	[Local]

从上述信息可以看出,Switch C 成为主交换机,主交换机给自己分配了配置的想要获取的域 ID 1。

#显示 Switch A 在 VSAN 100 内的路由表相关信息。

```
[SwitchA] display fc routing-table vsan 100
Routing Table: VSAN 100
Destinations : 5 Routes : 5
Destination/mask Protocol Preference Cost Interface
0x010000/8 FSPF 20 100 Vfc10
```

0xfffc01/24	DIRECT	0	0	InLoop0
0xfffffa/24	DIRECT	0	0	InLoop0
0xffffc/24	DIRECT	0	0	InLoop0
0xfffffd/24	DIRECT	0	0	InLoop0

从上述信息可以看出,Switch A 上存在了一条到 Switch C 的 FSPF 路由,出接口为 VFC10 接口。

#显示 Switch A 在 VSAN 100 内的节点注册的相关信息。

[SwitchA] display fc login vsan 100

Interface VSAN	I FCID	Node WWN	Port WWN
----------------	--------	----------	----------

Vfc1 100 0x020000 21:01:00:1b:32:a0:fa:12 21:01:00:1b:32:a0:fa:11

```
#显示 Switch A 在 VSAN 100 内的名称服务数据库的简要信息。
```

[SwitchA] display fc name-service database vsan 100 VSAN 100:

FCID	Туре	PWWN(vendor)	FC4-type:feature
0x010000	0x01(N)	10:00:00:05:30:00:25:a3	SCSI-FCP:Target
0x020000	0x01(N)	21:01:00:1b:32:a0:fa:11	SCSI-FCP:Initiator

(2) 查看 VSAN 200 的信息

#显示 Switch A 在 VSAN 200 内的域信息。

```
[SwitchA] display fc domain vsan 200
Domain Information of VSAN 200:
```

```
Running time information:
State: Stable
Switch WWN: 48:33:43:2d:46:43:1B:1B
Fabric name: 48:33:43:2d:46:43:1D:1D
Priority: 128
Domain ID: 2
Configuration information:
Domain configure: Enabled
Domain auto-reconfigure: Disabled
Fabric name: 48:33:43:2d:46:43:1B:1B
Priority: 128
Domain ID: 2 (preferred)
Principal switch running time information:
Priority: 1
```

Path Interface Upstream Vfc11

从上述信息可以看出,Switch A 的配置已经结束,主交换机为 Switch A 分配的域 ID 为 2。 # 显示 Switch A 在 VSAN 200 内的域列表。

[SwitchA] display fc domain-list vsan 200 Domain list of VSAN 200: Number of domains: 2

Domain ID	WWN	
0x01(1)	48:33:43:2d:46:43:1D:1D	[Principal]
0x02(2)	48:33:43:2d:46:43:1B:1B	[Local]

从上述信息可以看出,Switch D 成为主交换机,主交换机给自己分配了配置的想要获取的域 ID 1。 # 显示 Switch A 在 VSAN 200 内的路由表相关信息。

[SwitchA] display fc routing-table vsan 200 Routing Table: VSAN 200

Destinations : 5	Rou	ites : 5		
Destination/mask	Protocol	Preference	Cost	Interface
0x010000/8	FSPF	20	100	Vfc10
0xfffc01/24	DIRECT	0	0	InLoop0
0xfffffa/24	DIRECT	0	0	InLoop0
0xfffffc/24	DIRECT	0	0	InLoop0
0xffffd/24	DIRECT	0	0	InLoop0

从上述信息可以看出,Switch A 上存在了一条到 Switch C 的 FSPF 路由,出接口为 VFC10 接口。

#显示 VSAN 200 的节点注册的相关信息。

[SwitchA] display fc login vsan 200

Interface VSAN FCID Node WWN

Port WWN

Vfc1 200 0x020000 21:01:00:1b:32:a0:fa:12 21:01:00:1b:32:a0:fa:13

#显示 VSAN 200 内的名称服务数据库的简要信息。

[SwitchA] display fc name-service database vsan 200

VSAN 200:

FCID	Туре	PWWN(vendor)	FC4-type:feature
0x010000	0x01(N)	10:00:00:05:30:00:25:a5	SCSI-FCP:Target
0x020000	0x01(N)	21:01:00:1b:32:a0:fa:13	SCSI-FCP:Initiator

2. 在 Switch C 上进行验证

#显示 VSAN 100 的节点注册的相关信息。

[SwitchC] display fc login vsan 100 Interface VSAN FCID Node WWN Port WWN Vfc1 100 0x010000 10:00:00:05:30:00:25:a4 10:00:00:05:30:00:25:a3

3. 在 Switch D 上进行验证

Switch D 上的验证方法与 Switch C 的完全相同,验证信息略。

16 附录

16.1 附录A FC地址分配

表16-1 FC 地址分配

FC_ID	描述
0x000000	未定义(N_Port通过FLOGI请求地址时使用全0)
0x000001 – 0x00ffff	保留
0x010000 - 0xefffff	N_Port地址
0xf00000 – 0xfff9ff	保留
0xfffa00 – 0xfffa0f	保留给内部Loopback地址使用
0xfffa10 – 0xfffa1f	保留给外部Loopback地址使用
0xfffa20 – 0xfffaff	保留
0xfffb00 – 0xfffbff	保留给组播地址使用
0xfffc00	保留
0xfffc01 – 0xfffcef	域控制器地址
0xfffcf0 - 0xfffef	保留
0xfffff0 – 0xfffffc	知名地址
Oxffffd	Fabric控制器地址,代表所有的E_Port
Oxffffe	F_Port控制器地址,代表所有的F_Port
Oxffffff	广播地址

16.2 附录B Fabric知名地址

表16-2 Fabric 知名地址用途描述

FC_ID	描述
0xfffff0	N_Port控制器,代表所有的N_Port
0xfffff1 – 0xfffff3	保留
0xfffff4	事件服务
0xfffff5	组播服务器
0xfffff6	时钟同步服务
0xfffff7	安全密钥分发服务
0xffff8	别名服务

FC_ID	描述
0xfffff9	保留
Oxffffa	管理服务
Oxffffb	时间服务
Oxffffc	路径服务(名称服务)