# 目 录

# 1 MACsec

## 1.1 MACsec简介

MACsec（Media Access Control Security，MAC 安全）定义了基于 IEEE 802 局域网络的数据安全通信的方法。MACsec 可为用户提供安全的 MAC 层数据发送和接收服务，包括用户数据加密、数据帧完整性检查及数据源真实性校验。

MACsec 通常与 802.1X 认证框架配合使用，工作在 802.1X 认证过程成功之后，通过识别出已认证设备发送的报文，并使用 MKA（MACsec Key Agreement，MACsec 密钥协商）协议协商生成的密钥对已认证的用户数据进行加密和完整性检查，避免端口处理未认证设备的报文或者未认证设备篡改的报文。

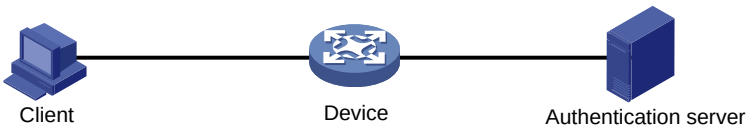
### 1.1.1 MACsec 典型组网模式

MACsec 包括两种典型组网模式：面向主机模式和面向设备模式。

#### 1. 面向主机模式

如图 1-1 所示，面向主机模式用于保护客户端和设备之间的数据帧。

**图1-1 面向主机模式组网图**




该模式包括以下三个组成元素：

- 客户端

客户端可以是请求接入局域网的用户终端，也可以是支持 802.1X Client 功能的设备，由局域网中的接入设备对其进行认证，并执行 MACsec 密钥协商和报文加密功能。

- 接入设备

接入设备控制客户端的接入，通过与认证服务器的交互，对所连接的客户端进行 802.1X 认证，并执行 MACsec 密钥协商和报文加密功能。

- 认证服务器

认证服务器用于对客户端进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。客户端通过认证后，认证服务器为客户端和接入设备分发密钥。

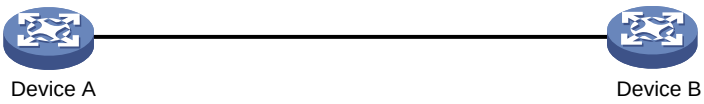
说明

面向主机模式中，接入设备上使能 MKA 协议的端口必须采用基于端口的 802.1X 认证方式，且必须配置 802.1X 认证方法为 EAP 中继方式。

#### 2. 面向设备模式

如图 1-2 所示，面向设备模式用于保护设备之间的数据帧。

图1-2 面向设备模式组网图




该模式下，互连的两台设备直接使用通过命令行配置的预共享密钥进行 MACsec 密钥协商和报文加密功能。

### 1.1.2 MACsec 基本概念

#### 1. CA

CA（Connectivity Association，安全连通集）是两个或两个以上使用相同密钥和密钥算法套件的成员的集合。CA 成员称为 CA 的参与者。CA 参与者使用的密钥称为 CAK。CAK 分为两种类型，一种是成对 CAK（Pairwise CAK），另一种是成组 CAK（Group CAK）。由两个成员组成 CA，它们所拥有的 CAK 称为成对 CAK。由三个或三个以上成员组成 CA，它们所拥有的 CAK 称为成组 CAK。目前，MACsec 主要应用在点对点组网的环境中，所以主要使用成对 CAK。成对 CAK 可以是 802.1X 认证过程中生成的 CAK，也可以是用户配置的预共享密钥（PSK，Pre-Shared Key）。如两者同时存在，优先使用用户配置的预共享密钥。

#### 2. SA

SA（Security Association，安全联盟）是 CA 参与者之间用于建立安全通道的安全参数集合，包括对数据进行加密算法套件、进行完整性检查的密钥等。一个安全通道中可包含多个 SA，每一个 SA 拥有一个不同的密钥，这个密钥称为 SAK。SAK 由 CAK 根据算法推导产生，用于加密安全通道间传输的数据。MKA 对每一个 SAK 可加密的报文数有所限制。当使用某 SAK 加密的报文超过限定的数目后，该 SAK 会被刷新。例如，在 10Gbps 的链路上，SAK 最快 300 秒刷新一次。

### 1.1.3 MACsec 协议机制

#### 1. 数据加密

使能了 MACsec 功能且启动了 MACsec 保护的端口发送数据帧时，需要对它进行加密；使能了 MACsec 功能的端口收到经过 MACsec 封装的数据帧时，需要对它进行解密。加解密所使用的密钥是通过 MKA 协议协商而来的。

### 2. 完整性检查

MACsec 封装的数据帧会使用 CAK 推导出的密钥进行 ICV（完整性校验值，Integrity Check Value）计算，并附加在 MACsec 报文的尾部。设备收到 MACsec 报文时，同样使用 MKA 协商出的密钥进行完整性检验值计算，然后将计算结果与报文中携带的 ICV 进行比较。如果比较结果相同，则表示报文合法；如果比较结果不相同，将依据配置的校验模式，决定是否丢弃报文。

### 3. 重播保护机制

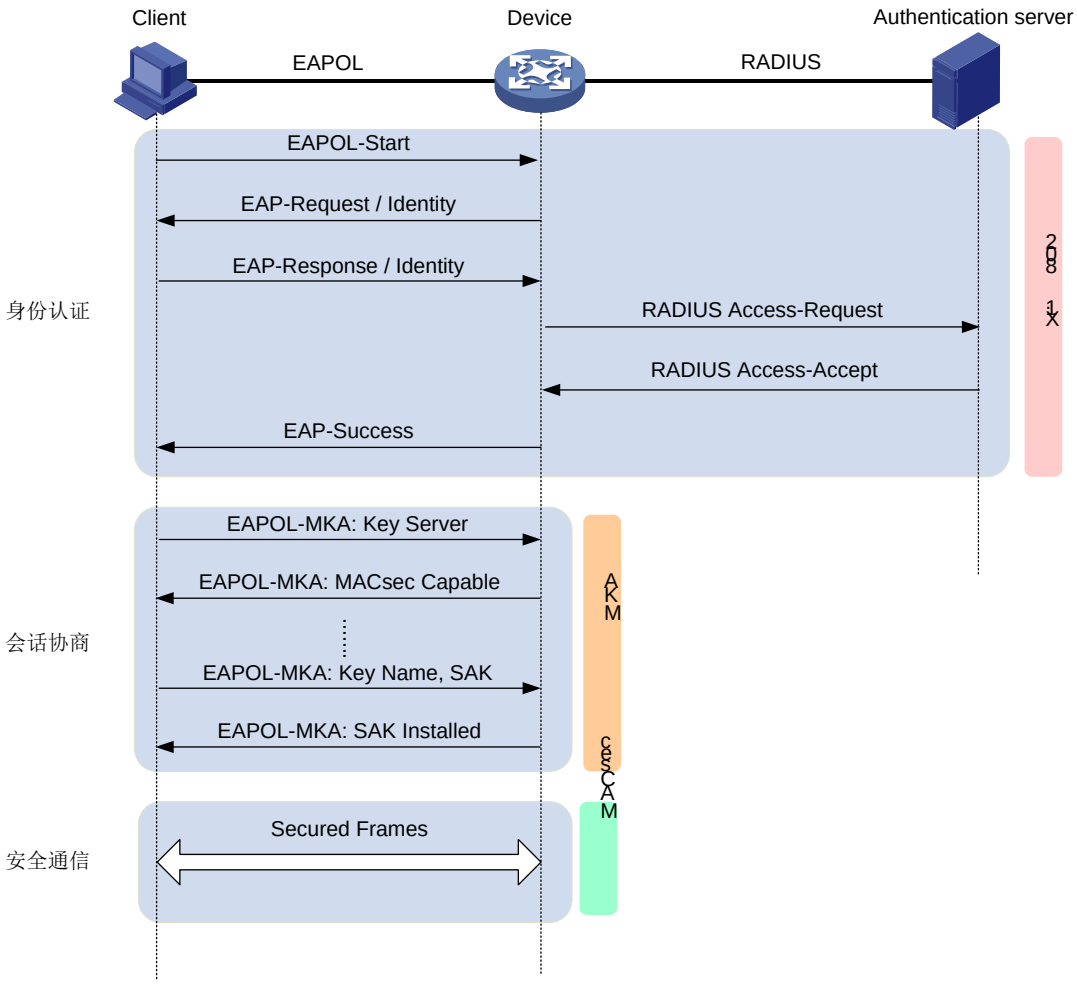
MACsec 封装的数据帧在网络中传输时，可能出现报文顺序的重排。MACsec 重播保护机制允许数据帧有一定的乱序，这些乱序的报文序号在用户指定的窗口范围内可以被合法接收，超出窗口的报文会被丢弃。

## 1.1.4 MACsec 运行机制

### 1. 面向主机模式的 MACsec 运行机制

如图 1-3 所示，在客户端和接入设备之间建立安全会话前，客户端首先需要在接入设备的端口上进行 802.1X 认证。通过认证之后，客户端将开始与接入设备进行会话协商、会话的建立和维护过程。MACsec 协议的交互过程主要分为四个阶段：身份认证、会话协商、安全通信和会话终止。

图1-3 面向主机模式的 MACsec 协议交互过程



(1)　身份认证

在客户端和接入设备之间建立安全会话前，客户端首先需要在接入设备的端口上进行802.1X认证。客户端通过认证后，RADIUS 服务器会把生成的 CAK 分发给客户端和接入设备。

(2)　会话协商

客户端和接入设备有了可用的 CAK，使用 EAPOL-MKA 报文开始协商会话。在协商会话的过程中，客户端和接入设备使用 MKA 协议向对方通告自身能力和建立会话所需的各种参数（如优先级、是否期望加密会话等）。会话协商时，接入设备会被自动选举为密钥服务器（Key Server）。密钥服务器使用 CAK 派生出用于加密数据报文的 SAK，并把 SAK 分发给客户端。

(3)　安全通信

会话协商完成后，客户端和接入设备有了可用的 SAK，并使用 SAK 加密数据报文，开始加密通信。

(4)　会话终止

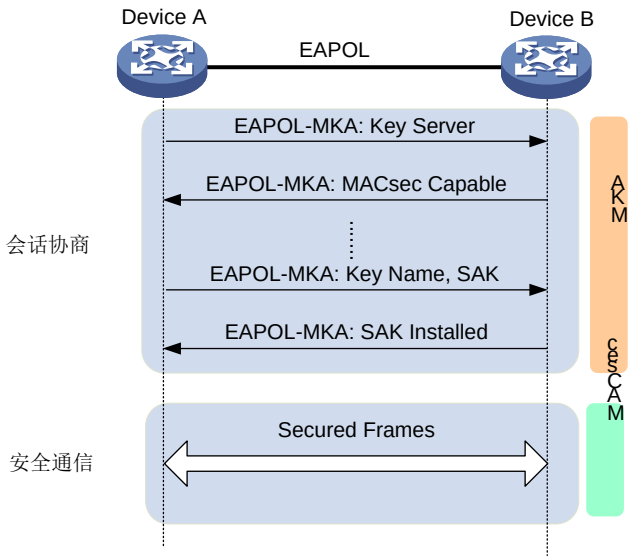
当接入设备收到 802.1X 客户端的下线请求消息后，立即清除该用户对应的安全会话，避免一个未认证的客户端使用端口上前一个已认证客户端建立的安全会话接入网络。

此外，MKA 协议里定义了一个会话保活定时器，如果在超时时间内（6 秒），本端没有收到对端的 MKA 协议报文，则在定时器超时后，本端将清除建立的安全会话。

### 2. 面向设备模式的 MACsec 运行机制

如图 1-4 所示，设备之间使用配置的预共享密钥开始协商会话，会话协商结束后开始安全通信。MACsec 协议的交互过程主要分为三个阶段：会话协商、安全通信和会话终止。

图1-4 面向设备模式的 MACsec 协议交互过程




(1)　会话协商

设备之间使用配置的预共享密钥（PSK，Pre-Shared Key）作为 CAK，通过 EAPOL-MKA 报文开始协商会话。设备间优先级较高的端口将被选举为密钥服务器（Key Server），负责生成和分发 SAK，设备之间通过 MKA 协议向对方通告自身能力和建立会话所需的各种参数（如优先级、是否期望加密会话等）。

(2)　安全通信

会话协商完成后，各设备有了可用的 SAK，并使用 SAK 加密数据报文，开始加密通信。

(3) 会话终止

当设备收到对方的下线请求消息后，立即清除该用户对应的安全会话。

### 1.1.5 协议规范

与 MACsec 相关的协议规范有：

- IEEE 802.1X-2010：Port-Based Network Access Control
- IEEE 802.1AE-2006：Media Access Control (MAC) Security

## 1.2 MACsec配置限制和指导

需要注意的是：

- 仅以下单板支持 MACsec 功能：
  - 下列 SA 系列接口板上编号为 1～8 的端口：LSQM2GP24TSSA0、LSQM2GT48SA0、；
  - 下列 SC 系列接口板上编号为 1～8 的端口：LSQM2GP44TSSC0、LSQM2GP24TSSC0、LSQM2GT24PTSSC0、LSQM2GT48SC0。
- 采用面向主机模式的 MACsec 会话连接时，使能 MACsec 的接口上不能开启生成树协议，关于 STP 配置命令的详细介绍，请参见“二层技术-以太网交换命令参考”中的“生成树”。
- 聚合接口上不支持配置 MACsec 功能，但聚合组内成员端口上支持配置 MACsec 功能。
- 如果要使用 MACsec 功能，规划业务流量时请预留 MACsec 报文头所占用的 38 个字节。

## 1.3 MACsec配置任务简介

MACsec 的配置包括两大部分：

- 接口上的 MACsec 配置：用于控制接口的 MACsec 属性参数，以及用于协商会话的 MKA 协议参数，包括使能接口上的 MKA 协议、配置预共享密钥、MKA 密钥服务器的优先级等。其中，预共享密钥和 MKA 密钥服务器的优先级的配置主要用于面向设备模式，在面向主机模式下不需要。在面向设备模式下，这些属性可以在二层以太网接口和三层以太网接口上配置；在面向主机模式下，只能在配置 802.1X 的接口上配合生效，且该接口上不能开启生成树协议。
- MKA 策略配置：用于配置一套 MACsec 属性参数，通过应用在接口上，实现接口上的 MACsec 属性参数个性化定制，同时也便于多个接口通过应用统一 MKA 策略来共享相同的 MACsec 属性参数。该配置属于可选配置。

由于 MACsec 属性参数既可以在接口上直接配置，又可以使用 MKA 策略配置，因此由配置顺序决定它们最终的生效情况。如果既在接口上直接配置 MACsec 属性参数，又在接口上应用了 MKA 策略，则后执行的配置参数生效。

**表1-1 接口上的 MACsec 配置任务简介**

| 配置任务 | 说明 | 详细配置 |
|---|---|---|
| 使能MKA协议 | 必选 | 1.4.1 |
| 配置MACsec保护 | 可选 | 1.4.2 |

| 配置任务 | | 说明 | 详细配置 |
| --- | --- | --- | --- |
| 配置预共享密钥 | | 面向设备模式下必选<br>面向主机模式下不建议配置 | 1.4.3 |
| 配置MKA密钥服务器的优先级 | | 可选 | 1.4.4 |
| 配置MACsec加密偏移量 | | 可选 | 1.4.5 |
| 配置MACsec重播保护功能 | 开启MACsec重播保护功能 | 可选 | 1.4.6 |
| | 配置MACsec重播保护窗口大小 | 可选 | |
| 配置MACsec校验 | | 可选 | 1.4.7 |

表1-2 MKA 策略配置任务简介

| 配置任务 | | | 说明 | 详细配置 |
| --- | --- | --- | --- | --- |
| 创建MKA策略 | | | 必选 | 1.5.1 |
| 配置MKA策略 | 配置MACsec加密偏移量 | | 可选 | 1.5.2 |
| | 配置MACsec重播保护功能 | 开启MACsec重播保护功能 | 可选 | |
| | | 配置MACsec重播保护窗口大小 | 可选 | |
| | 配置MACsec校验 | | 可选 | |
| 应用MKA策略 | 应用配置策略 | | 必选 | 1.5.3 |
| 配置MKA会话的日志信息功能 | | | 可选 | 1.6 |

# 1.4 在接口上配置MACsec

## 1.4.1 使能 MKA 协议

说明

无 MACsec 能力的接口上，不支持使能 MKA 协议。

- MKA 协议负责接口上 MACsec 安全通道的建立和管理，以及 MACsec 所使用密钥的协商。

表1-3 使能 MKA 协议

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 使能MKA协议 | **mka enable** | 缺省情况下，接口上的MKA协议处于 |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| | | 关闭状态 |

### 1.4.2 配置 MACsec 保护

设备期望进行 MACsec 保护表达了本端对发送的数据帧进行 MACsec 保护的意愿，但最终本端发送的数据帧是否启用 MACsec 保护，要由密钥服务器来决策。决策策略是：密钥服务器和它的对端都支持 MACsec 特性，且至少有一端期望进行 MACsec 保护。

表1-4 配置 MACsec 保护

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 启用MACsec保护 | **macsec desire** | 缺省情况下，接口上不需要对发送的数据帧进行MACsec保护 |

### 1.4.3 配置预共享密钥

在配置预共享密钥时，MACsec 应用模式的不同，需要注意：

- 在面向设备模式中，两端设备协商 MKA 会话使用的 CAK 通过预共享密钥直接配置。为了保证设备间的 MKA 会话可以正常建立，必须保证两端设备的接口上配置的预共享密钥一致。
- 在面向主机模式中，客户端和接入设备的端口使用的 CAK 由 802.1X 认证过程中生成，不需要配置预共享密钥。如果在接入设备的端口配置了预共享密钥，由于 802.1X 认证过程生成的 CAK 的优先级低于预共享密钥，该 CAK 将会被弃用，并导致 MKA 会话建立失败，因此不建议该模式下配置预共享密钥。
- 本端设备和对端设备建立 MACsec 连接时，请保证只有建立连接的两个端口上配置相同的 CKN，两端设备的其它端口上都不能配置与此相同的 CKN，以免一个端口学习到多个邻居而导致 MACsec 功能不能正常建立。

GCM-AES-128 加密套件要求所使用的 CKN、CAK 的长度都必须为 32 个字符。在运行 GCM-AES-128 加密套件时，对于长度不足 32 个字符的 CKN、CAK，系统会自动在其后补零，使其满足 32 个字符；对于长度大于 32 个字符的 CKN、CAK，系统只获取其前 32 个字符。

表1-5 配置预共享密钥

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置预共享密钥 | **mka psk ckn** *name* **cak { cipher \| simple }** *string* | 缺省情况下，接口不存在MKA预共享密钥 |

### 1.4.4 配置 MKA 密钥服务器的优先级

MACsec 加密数据报文使用的 SAK 由密钥服务器生成。在配置 MKA 密钥服务器的优先级时，根据 MACsec 应用模式的不同，需要注意：

- 在面向主机模式中，接入设备的端口被自动选举为密钥服务器，不需要配置 MKA 密钥服务器的优先级。
- 在面向设备模式中，MKA 密钥服务器优先级较高（值较小）的设备端口将被选举为密钥服务器。如果设备端口的优先级相同，则比较设备端口的 SCI（MAC 地址+端口的 ID），SCI 值较小的端口将被选举为密钥服务器。
- 优先级为 255 的设备端口不能被选举为密钥服务器。相互连接的端口不能都配置优先级为 255，否则 MKA 会话选举不出密钥服务器。

表1-6 配置 MKA 密钥服务器的优先级

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置MKA密钥服务器的优先级 | **mka priority** *priority-value* | 缺省情况下，MKA密钥服务器的优先级为0 |

### 1.4.5 配置 MACsec 加密偏移量

MACsec 加密偏移量表示从用户数据帧帧头开始偏移多少字节后开始加密，协议提供 0、30、50 三个偏移量供用户使用。

需要注意的是，MACsec 加密偏移量最终以密钥服务器发布的加密偏移量为准。如果本端不是密钥服务器，则应用密钥服务器发布的加密偏移量；如果本端是密钥服务器，则应用本端配置的加密偏移量。

表1-7 配置 MACsec 加密偏移量

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置接口上的MACsec加密偏移量 | **macsec confidentiality-offset** *offset-value* | 缺省情况下，接口上的MACsec加密偏移量为0，表示整个数据帧都要加密 |

### 1.4.6 配置 MACsec 重播保护功能

MACsec 重播保护功能可以防止本端收到乱序或重复的数据帧。MACsec 重播保护功能可以单独开启，且仅针对接收到的数据帧。配置的重播保护窗口大小仅在重播保护功能开启的情况下有效。

表1-8 配置重播保护功能

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 开启接口上的MACsec重播保护功能 | **macsec replay-protection enable** | 缺省情况下，接口上的MACsec重播保护功能处于开启状态 |
| 配置接口上的MACsec重播保护窗口大小 | **macsec replay-protection window-size** *size-value* | 缺省情况下，接口上的MACsec重播保护窗口大小为0个数据帧，表示不允许接收乱序或重复的数据帧 |

### 1.4.7 配置 MACsec 校验

如果接口开启 MACsec 校验功能，接口收到报文后，计算报文的 ICV，与报文尾部的 ICV 比较，并根据校验模式，决定报文是否丢弃。MACsec 校验模式分以下方式：

- **check**：检查模式，表示只作校验，但不丢弃非法数据帧。
- **strict**：严格校验模式，表示校验接收数据帧，并丢弃非法数据帧。

在网络中部署支持 MACsec 的设备时，为避免两端因密钥协商不一致而造成流量丢失，建议两端均先配置为 **check** 模式，在密钥协商成功后，再配置为 **strict** 模式。

表1-9 配置 MACsec 校验模式

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置接口上的MACsec校验模式 | **macsec validation mode** { **check** \| **strict** } | 缺省情况下，接口上的MACsec校验模式是**check** |

## 1.5 配置及应用MKA策略

### 1.5.1 创建 MKA 策略

系统中可配置多个 MKA 策略。其中，缺省 MKA 策略 default-policy 不能被删除和修改，它的参数取值均为接口上对应配置的缺省值。

表1-10 创建 MKA 策略

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 创建一个MKA策略，并进入MKA策略视图 | **mka policy** *policy-name* | 缺省情况下，存在一个缺省的MKA策略，名称为default-policy |

### 1.5.2 配置 MKA 策略

MKA 策略中包括以下配置项：

- 加密偏移量：指定用户数据从多少字节后开始加密。
- 开启重播保护功能和配置重播保护窗口大小：用于防止收到乱序或重复的数据帧。
- 接收数据帧的校验模式：用于控制是否校验数据帧以及是否丢弃非法数据帧。

表1-11 配置 MKA 策略

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入MKA策略视图 | **mka policy** *policy-name* | - |
| 配置MACsec加密偏移量 | **confidentiality-offset** *offset-value* | 缺省情况下，加密偏移为0 |
| 配置MACsec重播保护功能 | • 开启 MACsec 重播保护功能：**replay-protection enable** | 缺省情况下，接口上的MACsec重播保护功能处于使能状态 |
| | • 配置 MACsec 重播保护窗口大小：**replay-protection window-size** *size-value* | 缺省情况下，接口上的MACsec重播保护窗口大小为0个数据帧，表示不允许接收乱序或重复的数据帧 |
| 配置MACsec校验模式 | **validation mode** { **check** \| **strict** } | 缺省情况下，MACsec校验模式是**check** |

### 1.5.3 应用 MKA 策略

一个 MKA 策略可应用于一个或多个接口。在接口上应用了 MKA 策略时，需要注意的是：

- 接口上应用的 MKA 策略中配置的 MACsec 属性参数（加密偏移、校验模式、重播保护功能和重播保护窗口大小）会覆盖接口上配置的对应的 MACsec 属性参数。
- 当修改应用到接口上的 MKA 策略配置时，接口上的相应的配置也会改变。
- 取消接口上应用的指定 MKA 策略时，接口上的加密偏移、校验模式、重播保护功能和重播保护窗口大小都恢复为缺省情况。
- 当接口应用了一个不存在的 MKA 策略时，该接口会自动应用缺省 MKA 策略 default-policy。之后，如果该策略被创建，则接口会自动使用配置的 MKA 策略。

表1-12 应用 MKA 策略

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入进口视图 | **interface** *interface-type interface-number* | - |
| 应用MKA策略 | **mka apply policy** *policy-name* | 缺省情况下，接口上没有应用MKA策略 |

## 1.6 配置MKA会话的日志信息功能

### 1. 功能简介

MKA 会话的日志信息是为了满足网络管理员维护的需要，对用户的接入信息（如对端老化、SAK 更新）进行记录。设备生成的 MKA 会话的日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

### 2. 配置限制和指导

为了防止设备输出过多的 MKA 会话的日志信息，一般情况下建议关闭此功能。

### 3. 配置步骤

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 开启MKA会话的日志信息功能 | **macsec mka-session log enable** | MKA会话的日志信息功能处于关闭状态 |

## 1.7 MACsec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 MACsec 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** 命令可以重建会话和清除统计信息。

表1-13 MACsec 显示和维护

| 操作 | 命令 |
| --- | --- |
| 显示接口上的MACsec运行信息 | **display macsec** [ **interface** *interface-type interface-number* ] [ **verbose** ] |
| 显示MKA会话信息 | **display mka session** [ **interface** *interface-type interface-number* \| **local-sci** *sci-id* ] [ **verbose** ] |
| 显示MKA策略相关信息 | **display mka** { **default-policy** \| **policy** [ **name** *policy-name* ] } |
| 显示接口上的MKA统计信息 | **display mka statistics** [ **interface** *interface-type interface-number* ] |
| 重建接口上的MKA会话 | **reset mka session** [ **interface** *interface-type interface-number* ] |
| 清除接口上的MKA统计信息 | **reset mka statistics** [ **interface** *interface-type interface-number* ] |

# 1.8 MACsec典型配置举例

## 1.8.1 面向主机模式配置举例（主机作为客户端）

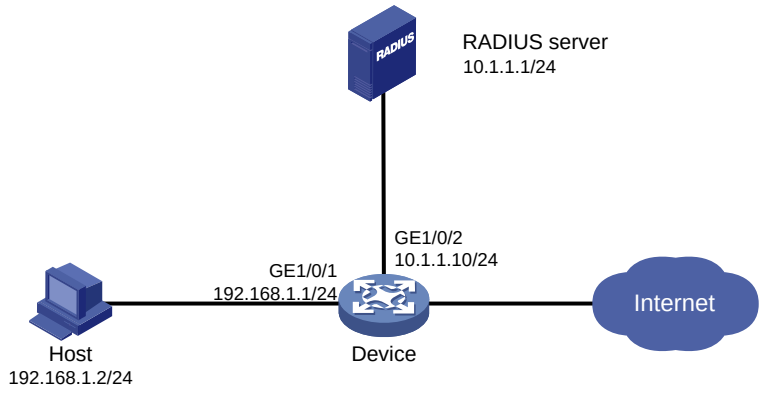
### 1. 组网需求

用户通过 Device 的端口 GigabitEthernet1/0/1 接入网络，认证服务器为 RADIUS 服务器。设备对该端口接入的用户进行 802.1X 认证以控制其访问外网，为保证数据帧传输的安全性，有以下具体要求：

- 要求用户和 Device 之间的数据通信进行 MACsec 保护，且加密报文的密钥通过 MKA 协议协商获得。
- MACsec 加密偏移量为 30 字节。
- 开启 MACsec 重播保护功能，配置重播保护窗口大小为 100。
- 配置严格的 MACsec 校验。

### 2. 组网图

图1-5 面向主机模式 MACsec 配置组网图（主机作为客户端）




### 3. 配置步骤

说明

- 下述配置步骤中包含了若干 AAA/RADIUS 协议的配置命令，关于这些命令的详细介绍请参见“安全命令参考”中的“AAA”。
- 完成 RADIUS 服务器的配置，添加用户账户，保证用户的认证/授权/计费功能正常运行。

(1) 配置各接口的 IP 地址（略）

(2) 配置 AAA

```
<Device> system-view
```

# 配置 RADIUS 方案 radius1。具体参数取值请以服务器上的实际情况为准，此处仅为示例。

```
[Device] radius scheme radius1
[Device-radius-radius1] primary authentication 10.1.1.1
[Device-radius-radius1] primary accounting 10.1.1.1
```

```
[Device-radius-radius1] key authentication simple name
[Device-radius-radius1] key accounting simple money
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

# 配置 802.1X 用户使用认证域 bbb。

```
[Device] domain bbb
[Device-isp-bbb] authentication lan-access radius-scheme radius1
[Device-isp-bbb] authorization lan-access radius-scheme radius1
[Device-isp-bbb] accounting lan-access radius-scheme radius1
[Device-isp-bbb] quit
```

(3) 配置 802.1X

# 开启端口 GigabitEthernet1/0/1 的 802.1X。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

# 配置端口的 802.1X 接入控制方式为 **portbased**。

```
[Device-GigabitEthernet1/0/1] dot1x port-method portbased
```

# 指定端口上接入的 802.1X 用户使用强制认证域 bbb。

```
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
[Device-GigabitEthernet1/0/1] quit
```

# 开启全局 802.1X，启用 EAP 中继的认证方法。

```
[Device] dot1x
[Device] dot1x authentication-method eap
```

(4) 配置 MACsec

# 创建一个名称为 pls 的 MKA 策略。

```
[Device] mka policy pls
```

# 配置 MACsec 加密偏移量为 30。

```
[Device-mka-policy-pls] confidentiality-offset 30
```

# 开启 MACsec 重播保护功能。

```
[Device-mka-policy-pls] replay-protection enable
```

# 配置 MACsec 重播保护窗口大小为 100。

```
[Device-mka-policy-pls] replay-protection window-size 100
```

# 配置严格的 MACsec 校验模式。

```
[Device-mka-policy-pls] validation mode strict
[Device-mka-policy-pls] quit
[Device] interface gigabitethernet 1/0/1
```

# 在端口 GigabitEthernet1/0/1 上应用 MKA 策略。

```
[Device-GigabitEthernet1/0/1] mka apply policy pls
```

# 在端口 GigabitEthernet1/0/1 上配置期望进行 MACsec 保护及使能 MKA 协议。

```
[Device-GigabitEthernet1/0/1] macsec desire
[Device-GigabitEthernet1/0/1] mka enable
[Device-GigabitEthernet1/0/1] quit
```

### 4. 验证配置

配置完成后，用户可以使用 **display** 命令查看设备上 MACsec 的运行情况。

# 查看 Device 上的 MACsec 运行信息。

```
[Device] display macsec interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
  Protect frames         : Yes
  Active MKA policy      : pls
  Replay protection      : Enabled
  Replay window size     : 100 frames
  Confidentiality offset : 30 bytes
  Validation mode        : Strict
  Included SCI           : No
  SCI conflict           : No
  Cipher suite           : GCM-AES-128
  Transmit secure channel:
    SCI           : 00E00100000A0006
      Elapsed time: 00h:02m:07s
      Current SA  : AN 0        PN 1
  Receive secure channels:
    SCI           : 00E0020000000106
      Elapsed time: 00h:02m:03s
      Current SA  : AN 0        LPN 1
      Previous SA : AN N/A      LPN N/A
```

# 用户上线之后，查看 Device 上的 MKA 会话信息。

```
[Device] display mka session interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
Tx-SCI    : 00E00100000A0006
Priority  : 0
Capability: 3
 CKN for participant: 1234
   Key server            : Yes
   MI (MN)               : A1E0D2897596817209CD2307 (2509)
   Live peers            : 1
   Potential peers       : 0
   Principal actor       : Yes
   MKA session status    : Secured
   Confidentiality offset: 30 bytes
   Current SAK status    : Rx & Tx
   Current SAK AN        : 0
   Current SAK KI (KN)   : A1E0D2897596817209CD230700000002 (2)
   Previous SAK status   : N/A
   Previous SAK AN       : N/A
   Previous SAK KI (KN)  : N/A
   Live peer list:
   MI                        MN         Priority  Capability  Rx-SCI
   B2CAF896C9BFE2ABFB135E63  2512       0         3           00E0020000000106
```

### 1.8.2 面向主机模式配置举例（设备作为客户端）

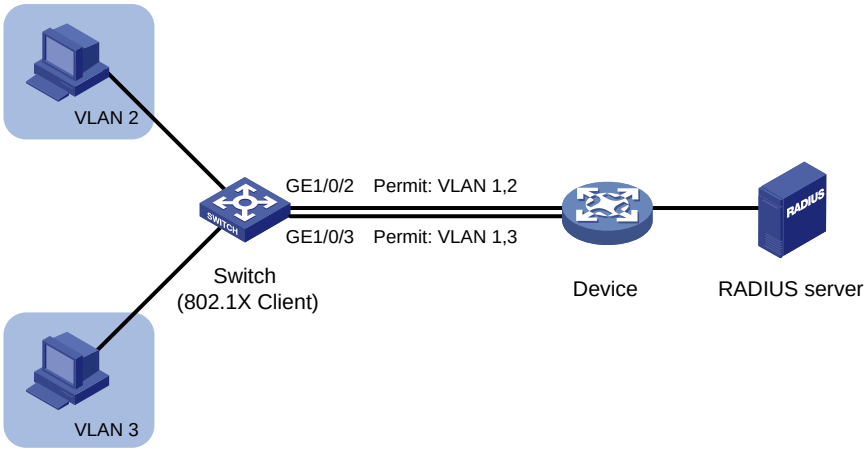
#### 1. 组网需求

Switch 的下行口与终端设备相连，上行通过 Trunk 端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 与 Device 的对应端口相连；认证服务器为 RADIUS 服务器。

Device 为无法通过命令行配置预共享密钥进行 MACsec 密钥协商和报文加密的设备。需要开启 Switch 的 802.1X Client 功能，将其作为 802.1X 客户端，Device 作为接入设备，采用面向主机模式的 MACsec 机制，在 802.1X 认证过程中生成 CAK，从而实现 Switch 上不同端口与 Device 之间的数据通信均可以进行 MACsec 保护，且加密报文的密钥通过 MKA 协议协商获得。

#### 2. 组网图

图1-6 面向主机模式 MACsec 配置组网图（设备作为客户端）




#### 3. 配置步骤

说明

- 完成设备各接口的 IP 地址配置，保证 Switch、Device 和服务器之间的路由可达。
- 完成 RADIUS 服务器的配置，添加用户账户，保证用户的认证/授权/计费功能正常运行。
- 不同厂商 Device 上的配置有所差异，具体请参见对应的产品手册。下述配置步骤中仅包括 Switch 上的配置，其中关于 802.1X Client 的配置命令的详细介绍请参见“安全命令参考”中的“802.1X Client”。

# 创建 VLAN 2。

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
```

# 将 GigabitEthernet1/0/2 的链路类型配置为 Trunk，并允许 VLAN 2 的报文通过。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-Gigabitethernet1/0/2] port link-type trunk
[Switch-Gigabitethernet1/0/2] port trunk permit vlan 2
```

# 在端口 GigabitEthernet1/0/2 上配置 802.1X 认证用户名为 aaaa，认证密码为明文 123456。

```
[Switch-Gigabitethernet1/0/2] dot1x supplicant username aaaa
[Switch-Gigabitethernet1/0/2] dot1x supplicant password simple 123456
```
# 配置 802.1X Client 采用的认证方法为 TTLS-GTC。
```
[Switch-Gigabitethernet1/0/2] dot1x supplicant eap-method ttls-gtc
```
# 配置 802.1X Client 认证使用的 MAC 地址为 1-1-1。

[Switch-GigabitEthernet1/0/2] dot1x supplicant mac 1-1-1

# 在端口 GigabitEthernet1/0/2 开启 802.1X Client 功能。
```
[Switch-Gigabitethernet1/0/2] dot1x supplicant enable
```
# 在端口 GigabitEthernet1/0/2 上配置期望进行 MACsec 保护及使能 MKA 协议。
```
[Switch-Gigabitethernet1/0/2] macsec desire
[Switch-Gigabitethernet1/0/2] mka enable
[Switch-Gigabitethernet1/0/2] quit
```
# 创建 VLAN 3。
```
[Switch] vlan 3
[Switch-vlan3] quit
```
# 将 GigabitEthernet1/0/3 的链路类型配置为 Trunk，并允许 VLAN 3 的报文通过。
```
[Switch] interface gigabitethernet 1/0/3
[Switch-Gigabitethernet1/0/3] port link-type trunk
[Switch-Gigabitethernet1/0/3] port trunk permit vlan 3
```
# 在端口 GigabitEthernet1/0/3 上配置 802.1X 认证用户名为 bbbb，认证密码为明文 654321。
```
[Switch-Gigabitethernet1/0/3] dot1x supplicant username bbbb
[Switch-Gigabitethernet1/0/3] dot1x supplicant password simple 654321
```
# 配置 802.1X Client 采用的认证方法为 TTLS-GTC。
```
[Switch-Gigabitethernet1/0/3] dot1x supplicant eap-method ttls-gtc
```
# 配置 802.1X Client 认证使用的 MAC 地址为 1-1-2。

[Switch-GigabitEthernet1/0/3] dot1x supplicant mac 1-1-2

# 在端口 GigabitEthernet1/0/2 开启 802.1X Client 功能。
```
[Switch-Gigabitethernet1/0/3] dot1x supplicant enable
```
# 在端口 GigabitEthernet1/0/3 上配置期望进行 MACsec 保护及使能 MKA 协议。
```
[Switch-Gigabitethernet1/0/3] macsec desire
[Switch-Gigabitethernet1/0/3] mka enable
```
### 4. 验证配置

配置完成后，用户可以使用 **display** 命令查看 Switch 上 MACsec 的运行情况。

# 显示接口 GigabitEthernet1/0/2 上的 MACsec 运行的详细信息。
```
[Switch] display macsec interface gigabitethernet 1/0/2 verbose
Interface GigabitEthernet1/0/2
  Protect frames         : Yes
  Active MKA policy      : pls
  Replay protection      : Enabled
  Replay window size     : 100 frames
  Confidentiality offset : 30 bytes
  Validation mode        : Strict
  Included SCI           : No
  SCI conflict           : No
```

```
  Cipher suite           : GCM-AES-128
  Transmit secure channel:
    SCI           : 00E00100000A0006
      Elapsed time: 00h:02m:07s
      Current SA  : AN 0        PN 1
  Receive secure channels:
    SCI           : 00E0020000000106
      Elapsed time: 00h:02m:03s
      Current SA  : AN 0        LPN 1
      Previous SA : AN N/A      LPN N/A
```

# 显示接口 GigabitEthernet1/0/3 上的 MACsec 运行的详细信息。

```
[Switch] display macsec interface gigabitethernet 1/0/3 verbose
Interface GigabitEthernet1/0/3
  Protect frames         : Yes
  Replay protection      : Enabled
  Replay window size     : 100 frames
  Confidentiality offset : 30 bytes
  Validation mode        : Check
  Included SCI           : No
  SCI conflict           : No
  Cipher suite           : GCM-AES-128
  Transmit secure channel:
    SCI           : A087100801000103
      Elapsed time: 00h:00m:55s
      Current SA  : AN 0        PN 1
  Receive secure channels:
    SCI           : A0872B3602000003
      Elapsed time: 00h:00m:52s
      Current SA  : AN 0        LPN 1
      Previous SA : AN N/A      LPN N/A
```

# 802.1X Client 上线之后，在 Switch 上可查看接口 GigabitEthernet1/0/2 上的 MKA 会话详细信息。

```
[Switch] display mka session interface gigabitethernet 1/0/2 verbose
Interface GigabitEthernet1/0/2
Tx-SCI    : 00E00100000A0006
Priority  : 0
Capability: 3
 CKN for participant: 1234
   Key server            : Yes
   MI (MN)               : A1E0D2897596817209CD2307 (2509)
   Live peers            : 1
   Potential peers       : 0
   Principal actor       : Yes
   MKA session status    : Secured
   Confidentiality offset: 30 bytes
   Current SAK status    : Rx & Tx
   Current SAK AN        : 0
   Current SAK KI (KN)   : A1E0D2897596817209CD230700000002 (2)
   Previous SAK status   : N/A
```

```
  Previous SAK AN       : N/A
  Previous SAK KI (KN)  : N/A
  Live peer list:
  MI                        MN         Priority  Capability  Rx-SCI
  B2CAF896C9BFE2ABFB135E63  2512       0         3           00E0020000000106
```

# 802.1X Client 上线之后，在 Switch 上可查看接口 GigabitEthernet1/0/3 上的 MKA 会话详细信息。

```
[Switch] display mka session interface gigabitethernet 1/0/3 verbose
Interface GigabitEthernet1/0/3
Tx-SCI    : A087100801000103
Priority  : 0
Capability: 3
  CKN for participant: 7B8784F16F85ED8F9D0130AA9B93D0F0
    Key server            : No
    MI (MN)               : D3F6D374598C8FD1F1819D6C (78)
    Live peers            : 1
    Potential peers       : 0
    Principal actor       : Yes
    MKA session status    : Secured
    Confidentiality offset: 0 bytes
    Current SAK status    : Rx & Tx
    Current SAK AN        : 0
    Current SAK KI (KN)   : FCA71854FCAE51398EC2DA7900000001 (1)
    Previous SAK status   : N/A
    Previous SAK AN       : N/A
    Previous SAK KI (KN)  : N/A
    Live peer list:
    MI                        MN         Priority  Capability  Rx-SCI
    FCA71854FCAE51398EC2DA79  71         0         3           A0872B3602000003
```

## 1.8.3 面向设备模式配置举例

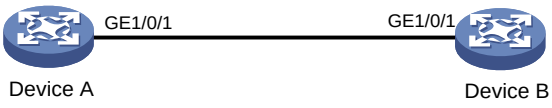
### 1. 组网需求

Device A 和 Device B 相连，要求两台设备之间的数据通信进行 MACsec 保护，具体要求如下：

- MACsec 加密偏移量为 30 字节。
- 开启 MACsec 重播保护功能，重播保护窗口大小为 100。
- 开启严格的 MACsec 校验。
- 两台设备使用的 CAK 均为静态配置，CKN 为 E9AC，CAK 为 09DB3EF1。
- 由 Device A 作为密钥服务器。

### 2. 组网图

图1-7 面向设备模式 MACsec 配置组网图



### 3. 配置步骤

(1) 配置 Device A

```
<DeviceA> system-view
```

# 在接口 GigabitEthernet1/0/1 上配置期望进行 MACsec 保护。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] macsec desire
```

# 配置 MKA 密钥服务器的优先级为 5。（本例中，Device A 作为密钥服务器，所以配置的 Device A 的优先级要比 Device B 的优先级高）

```
[DeviceA-GigabitEthernet1/0/1] mka priority 5
```

# 配置预共享密钥的名称为 E9AC，预共享密钥为明文 09DB3EF1。

```
[DeviceA-GigabitEthernet1/0/1] mka psk ckn E9AC cak simple 09DB3EF1
```

# 配置 MACsec 加密偏移量为 30。

```
[DeviceA-GigabitEthernet1/0/1] macsec confidentiality-offset 30
```

# 开启 MACsec 重播保护功能。

```
[DeviceA-GigabitEthernet1/0/1] macsec replay-protection enable
```

# 配置 MACsec 重播保护窗口大小为 100。

```
[DeviceA-GigabitEthernet1/0/1] macsec replay-protection window-size 100
```

# 配置严格的 MACsec 校验模式。

```
[DeviceA-GigabitEthernet1/0/1] macsec validation mode strict
```

# 使能 MKA 协议。

```
[DeviceA-GigabitEthernet1/0/1] mka enable
[DeviceA-GigabitEthernet1/0/1] quit
```

(2) 配置 Device B

```
<DeviceB> system-view
```

# 进入 GigabitEthernet1/0/1 接口视图。

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

# 配置期望进行 MACsec 保护。

```
[DeviceB-GigabitEthernet1/0/1] macsec desire
```

# 配置 MKA 密钥服务器的优先级为 10。

```
[DeviceB-GigabitEthernet1/0/1] mka priority 10
```

# 配置预共享密钥的名称为 E9AC，预共享密钥为明文 09DB3EF1。

```
[DeviceB-GigabitEthernet1/0/1] mka psk ckn E9AC cak simple 09DB3EF1
```

# 配置 MACsec 加密偏移量为 30。

```
[DeviceB-GigabitEthernet1/0/1] macsec confidentiality-offset 30
```

# 开启 MACsec 重播保护功能。

```
[DeviceB-GigabitEthernet1/0/1] macsec replay-protection enable
```

# 配置 MACsec 重播保护窗口大小为 100。

```
[DeviceB-GigabitEthernet1/0/1] macsec replay-protection window-size 100
```

# 配置严格的 MACsec 校验模式。

```
[DeviceB-GigabitEthernet1/0/1] macsec validation mode strict
```

# 使能 MKA 协议。

```
[DeviceB-GigabitEthernet1/0/1] mka enable
[DeviceB-GigabitEthernet1/0/1] quit
```

### 4. 验证配置

配置完成后，用户可以使用 **display** 命令查看设备上 MACsec 的运行情况。

# 查看 DeviceA 的 MACsec 运行信息。

```
[DeviceA] display macsec interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
Protect frames         : Yes
Replay protection      : Enabled
Replay window size     : 100 frames
Confidentiality offset : 30 bytes
Validation mode        : Strict
Included SCI           : No
SCI conflict           : No
Cipher suite           : GCM-AES-128
Transmit secure channel:
    SCI           : 00E00100000A0006
      Elapsed time: 00h:05m:00s
      Current SA  : AN 0        PN 1
Receive secure channels:
    SCI           : 00E0020000000106
      Elapsed time: 00h:03m:18s
      Current SA  : AN 0        LPN 1
      Previous SA : AN N/A      LPN N/A
```

# 查看 DeviceA 上的 MKA 会话信息。

```
[DeviceA] display mka session interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
Tx-SCI    : 00E00100000A0006
Priority  : 5
Capability: 3
  CKN for participant: E9AC
    Key server            : Yes
    MI (MN)               : 85E004AF49934720AC5131D3 (182)
    Live peers            : 1
    Potential peers       : 0
    Principal actor       : Yes
    MKA session status    : Secured
    Confidentiality offset: 30 bytes
    Current SAK status    : Rx & Tx
    Current SAK AN        : 0
    Current SAK KI (KN)   : 85E004AF49934720AC5131D300000003 (3)
    Previous SAK status   : N/A
    Previous SAK AN       : N/A
    Previous SAK KI (KN)  : N/A
    Live peer list:
    MI                        MN         Priority  Capability  Rx-SCI
    12A1677D59DD211AE86A0128  182        10        3           00E0020000000106
```

# 查看 DeviceB 上的 MACsec 运行信息。

```
[DeviceB]display macsec interface gigabitethernet 1/0/1 verbose
```

```
Interface GigabitEthernet1/0/1
Protect frames         : Yes
Replay protection      : Enabled
Replay window size     : 100 frames
Confidentiality offset : 30 bytes
Validation mode        : Strict
Included SCI           : No
SCI conflict           : No
Cipher suite           : GCM-AES-128
Transmit secure channel:
    SCI           : 00E0020000000106
      Elapsed time: 00h:05m:36s
      Current SA  : AN 0        PN 1
Receive secure channels:
    SCI           : 00E00100000A0006
      Elapsed time: 00h:03m:21s
      Current SA  : AN 0        LPN 1
      Previous SA : AN N/A      LPN N/A
```

# 查看 DeviceB 上的 MKA 会话信息。

```
[DeviceB] display mka session interface gigabitethernet 1/0/1 verbose
Interface GigabitEthernet1/0/1
Tx-SCI    : 00E0020000000106
Priority  : 10
Capability: 3
CKN for participant: E9AC
Key server            : No
MI (MN)               : 12A1677D59DD211AE86A0128 (1219)
Live peers            : 1
Potential peers       : 0
Principal actor       : Yes
MKA session status    : Secured
Confidentiality offset: 30 bytes
Current SAK status    : Rx & Tx
Current SAK AN        : 0
Current SAK KI (KN)   : 85E004AF49934720AC5131D300000003 (3)
Previous SAK status   : N/A
Previous SAK AN       : N/A
Previous SAK KI (KN)  : N/A
Live peer list:
MI                        MN         Priority  Capability  Rx-SCI
85E004AF49934720AC5131D3  1216       5         3           00E00100000A0006
```

## 1.9 常见配置错误举例

### 1. 故障现象

在链路状态正常且链路两端设备都支持 MACsec 功能，MACsec 安全会话未建立。

### 2. 故障分析

可能的原因有：

- 接口未使能 MKA 协议。
- 如果接口使用预共享密钥，接口的预共享密钥未配置或配置不一致。

### 3. 故障排除

- 进入接口视图下，使用 **display this** 命令查看 MKA 是否使能，如果未使能，请使用 **mka enable** 命令使能 MKA 协议。
- 进入接口视图下，使用 **display this** 命令查看是否配置预共享密钥，如果未配置，请使用 **mka psk** 命令配置；否则，请检查已有配置的密钥是否一致，不一致，则重新配置一致。