在Catalyst 8500上配置带子接口的WAN MACsec

目录

简介

本文档介绍在具有子接口的Cisco Catalyst 8500平台上配置WAN媒体访问控制安全(MACsec)的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 高级网络概念，包括WAN、VLAN和加密
- 了解MACsec (IEEE 802.1AE)和密钥管理(IEEE 802.1X-2010)
- 熟悉Cisco IOS® XE命令行界面(CLI)

使用的组件

本文档中的信息基于以下软件和硬件版本：

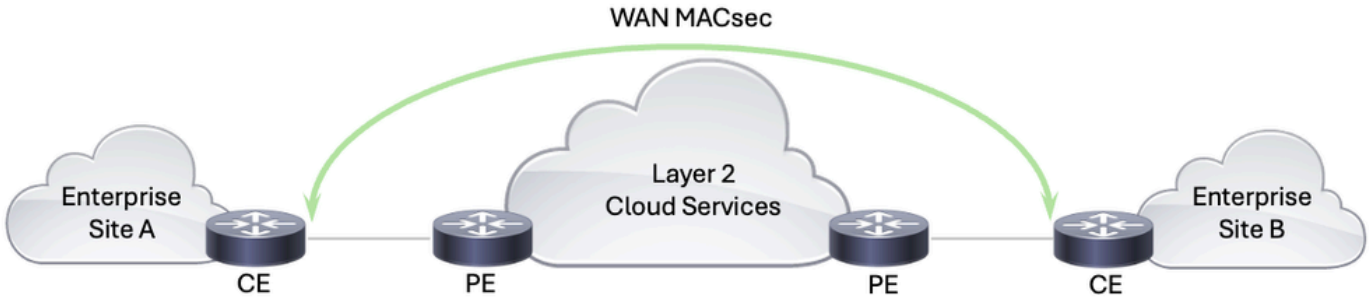
- Cisco Catalyst 8500系列边缘平台
- 思科IOS XE版本17.14.01a

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

WAN MACsec是一种安全解决方案，旨在利用MACsec的功能保护整个WAN网络中的网络流量。在使用服务提供商网络交换数据时，必须对传输中的数据加密以防止数据被篡改。WAN MACsec易于部署和管理，是需要保护其网络流量免受数据操纵（例如窃听和中间人攻击）的组织的理想之选。它提供无缝线速加密，确保数据在穿越各种网络基础设施（包括运营商网络、云环境和企业网络）时保持安全且不受影响。



WAN MACsec解决方案

为了共享一些历史记录，IEEE 802.1AE标准定义的MACsec通过确保以太网帧的数据保密性、完整性和源真实性来提供以太网网络上的安全通信。MACsec工作在开放式系统互联(OSI)模型的数据链路层（第2层），对以太网帧进行加密和身份验证，以确保节点之间的通信安全。MACsec最初是针对LAN而设计的，现在也发展为支持广域网部署。它提供线速加密，确保最低延迟和开销，这对于高速网络至关重要。

IEEE 802.1X-2010是对原始IEEE 802.1X标准的修订，该标准定义了基于端口的网络访问控制。2010年修订版引入了MACsec密钥协议(MKA)协议，该协议对MACsec实施中管理加密密钥至关重要。MKA处理MACsec用于加密和解密数据的加密密钥的分配和管理。MKA标准可促进MACsec部署的多供应商互操作性，支持安全密钥交换和密钥更新机制，这对于在动态广域网环境中保持持续的安全至关重要。

在WAN MACsec部署中，IEEE 802.1AE (MACsec)在数据链路层提供基本的加密和安全机制，确保所有以太网帧在流经网络时都受到保护。采用MKA协议的IEEE 802.1X-2010负责分发和管理MACsec正常运行所需的加密密钥。这些标准共同确保WAN MACsec能够在广域网中提供强大的高速加密，为传输中的数据提供全面保护，同时保持互操作性和易管理性。

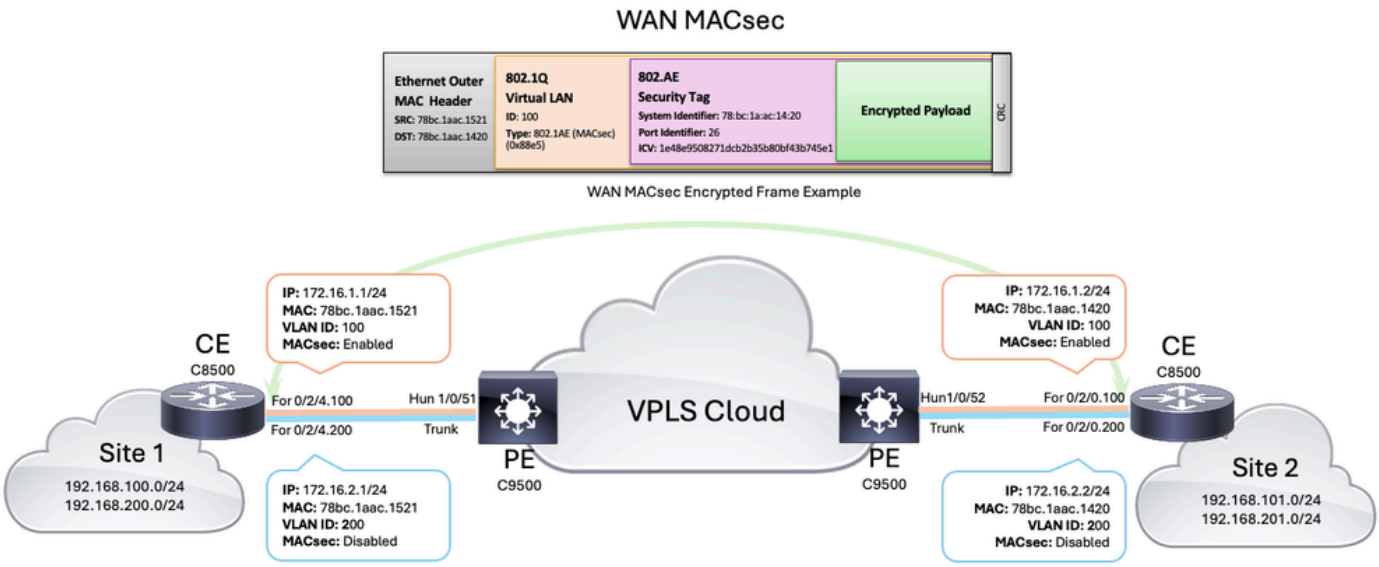
为了应对广域网环境的独特挑战，对传统MACsec部署进行了一些增强：

- 明文形式的802.1Q标记：此功能允许802.1Q VLAN标记暴露在加密MACsec报头之外，从而有助于更灵活的网络设计，尤其是在公共以太网传输环境中。此功能对于将MACsec与运营商级以太网服务集成至关重要，因为它允许在同一网络上同时存在加密流量和未加密流量，从而简化网络架构并降低成本。
- 在公共运营商以太网上的适应性：现代WAN MACsec实施可以适应公共运营商以太网服务。这种适应性包括修改LAN以太网身份验证协议(EAPoL)目标地址和EtherType，从而允许MACsec在运营商级以太网网络上无缝运行，否则这些帧可能会消耗或阻塞。

WAN MACsec代表着以太网加密技术的重大进步，它能够满足高速、安全的广域网连接不断增长的需求。它能够提供线速加密、支持灵活的网络设计，并能适应公共运营商服务，因此是现代网络安全架构的关键组成部分。通过利用WAN MACsec，组织可以实现高速广域网链路的强大安全性，同时简化网络架构并降低运营复杂性。

配置

网络图



WAN MACsec拓扑

配置

第1步：基本设备配置

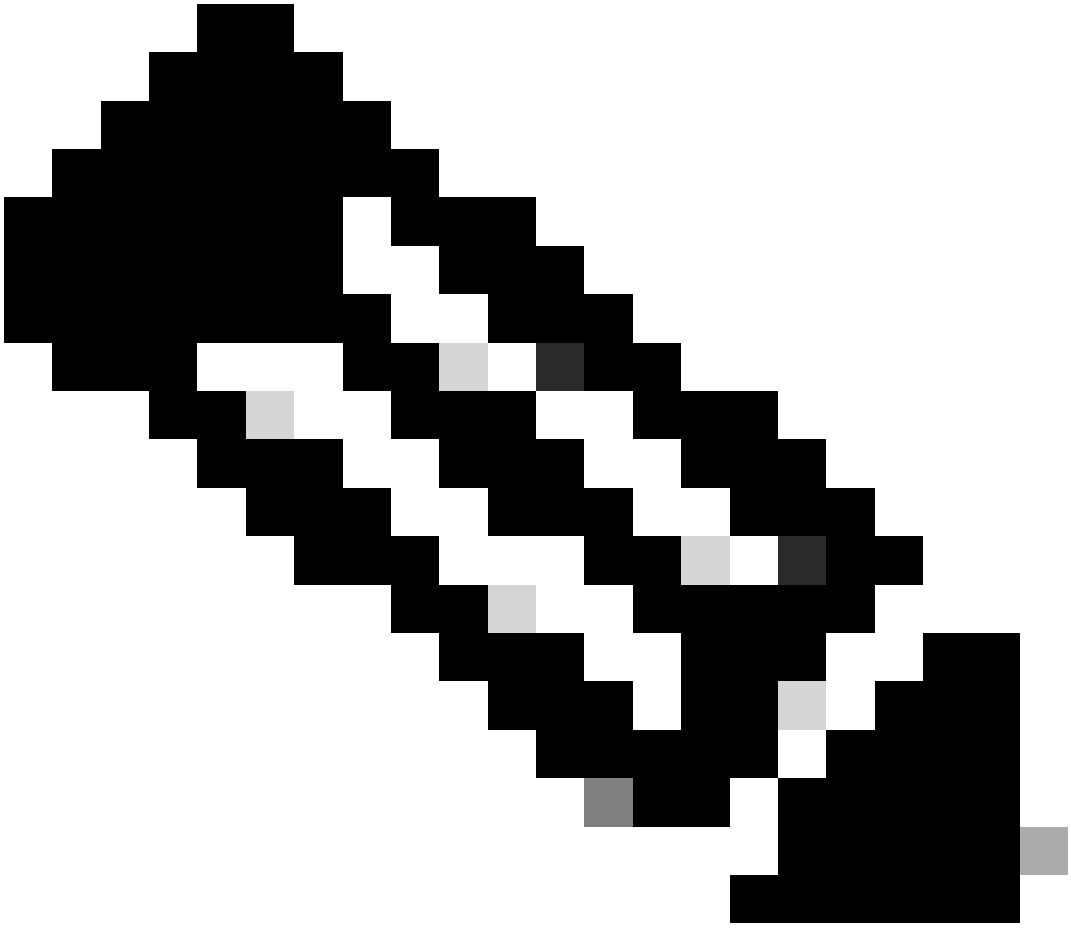
要启动配置，首先需要定义将用于流量分段和服务提供商连接的子接口。在本场景中，为关联到子网172.16.1.0/24的VLAN 100和关联到子网172.16.2.0/24的VLAN 200定义了两个子接口（稍后仅在一个子接口上配置了MACsec）。

CE 8500-1	CE 8500-2
<#root> interface FortyGigabitEthernet0/2/4.100 **encapsulation dot1Q 100 ip address 172.16.1.1 255.255.255.0** ! interface FortyGigabitEthernet0/2/4.200 **encapsulation dot1Q 200 ip address 172.16.2.1 255.255.255.0**	<#root> interface FortyGigabitEthernet0/2/0.100 **encapsulation dot1Q 100 ip address 172.16.** ! interface FortyGigabitEthernet0/2/0.200 **encapsulation dot1Q 200 ip address 172.16.**

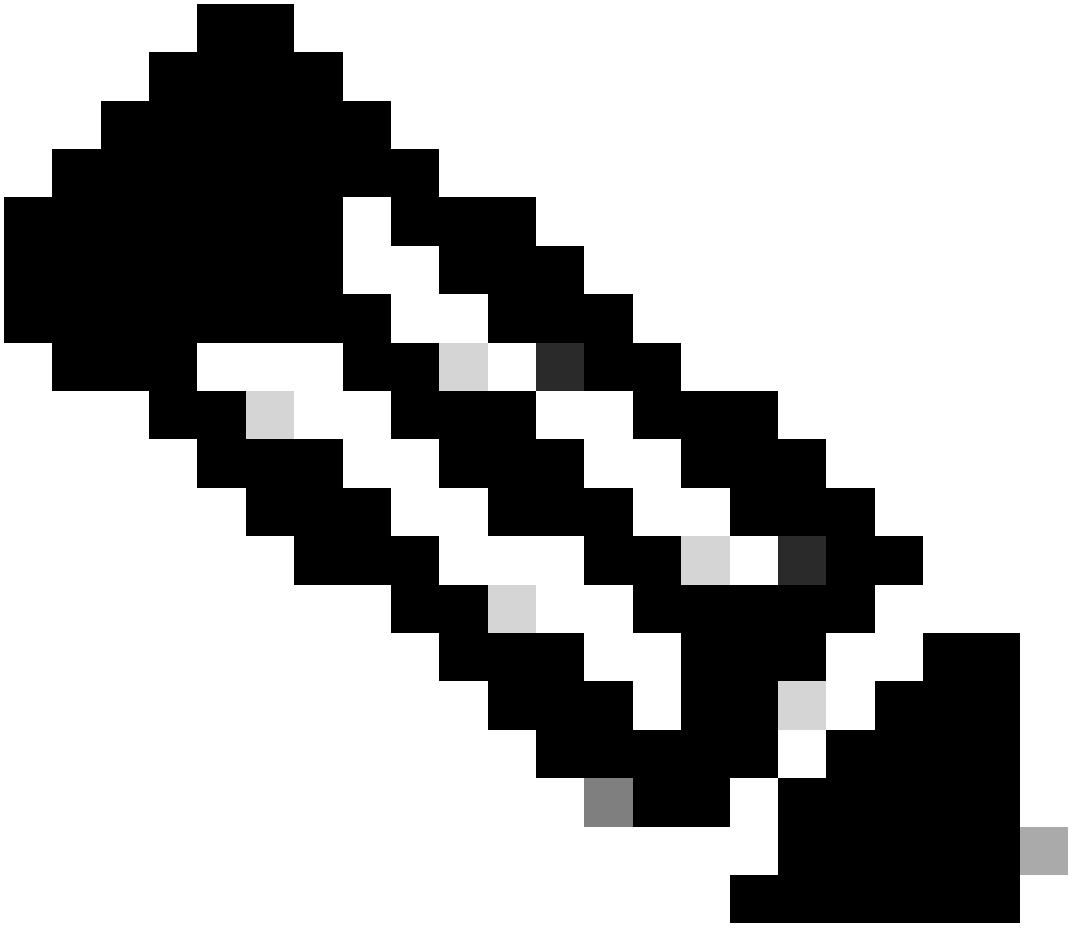
第2步：配置MACsec密钥链

请记住，IEEE 802.1X-2010标准规定，MACsec加密密钥可以通过802.1X可扩展身份验证协议(EAP)从预共享密钥(PSK)中获得，也可以通过MKA密钥服务器选择和分配。在本示例中，PSK通过MACsec密钥链使用和手动配置，这些密钥等于连接关联密钥(CAK)，后者是用于派生MACsec中使用的所有其他加密密钥的主密钥。

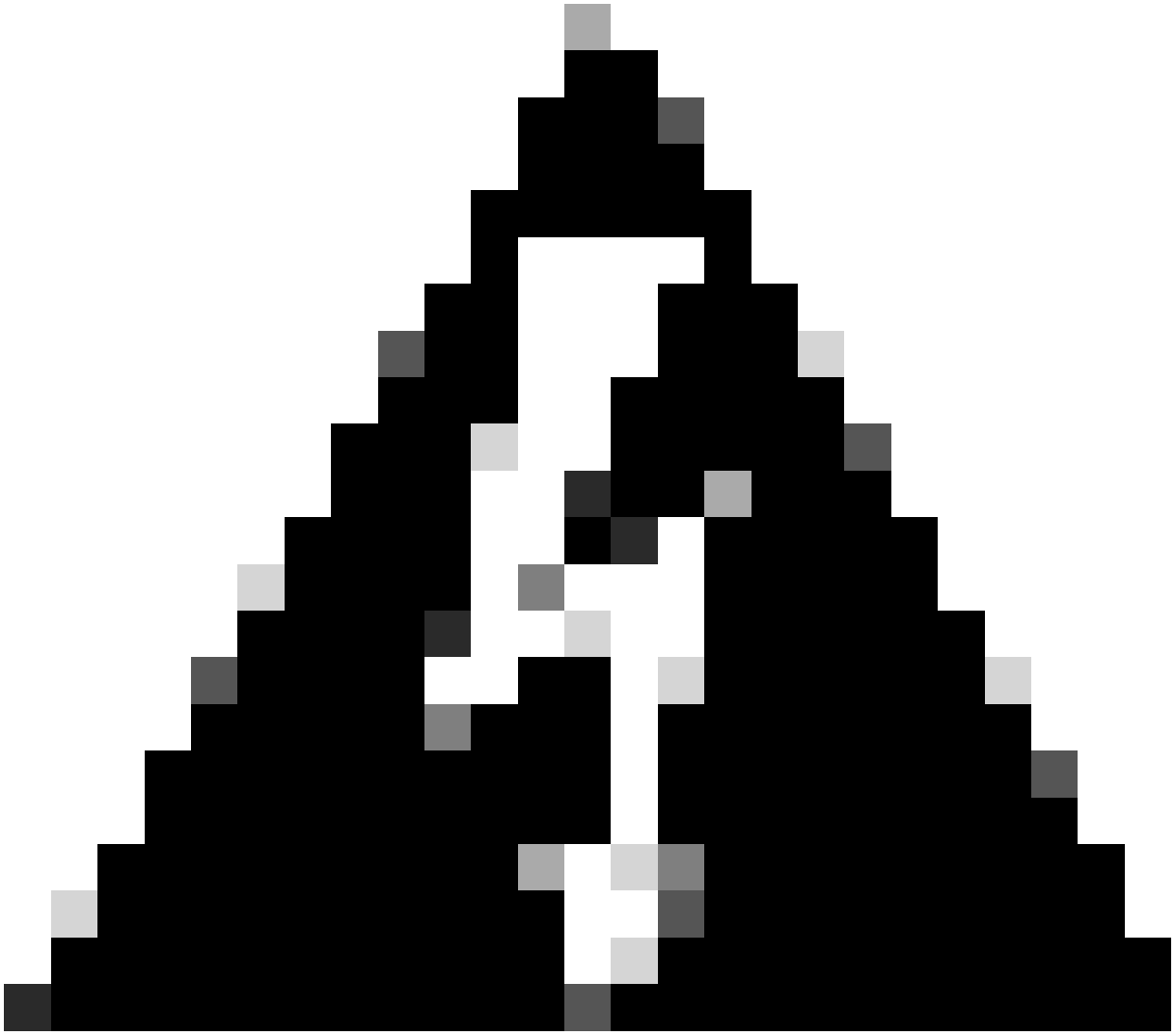
CE 8500-1	
<#root> 8500-1# **configure terminal** **8500-1(config)#** **key chain keychain_vlan100 macsec** **8500-1(config-keychain-macsec)#** **key 01** **8500-1(config-keychain-macsec-key)#** **cryptographic-algorithm aes-256-cmac** **8500-1(config-keychain-macsec-key)#** **key-string a5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e1** **8500-1(config-keychain-macsec-key)#** **lifetime 00:00:00 Jun 1 2024 duration 864000** **8500-1(config-keychain-macsec-key)#** **key 02** **8500-1(config-keychain-macsec-key)#** **cryptographic-algorithm aes-256-cmac** **8500-1(config-keychain-macsec-key)#** **key-string b5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e2** **8500-1(config-keychain-macsec-key)#** **lifetime 23:00:00 Jun 1 2024 infinite** **8500-1(config-keychain-macsec-key)#** **exit** **8500-1(config-keychain-macsec)#** **exit**	<#root> 8500-2# **configure terminal** **8500-2(config)#** **key chain keychain_vlan100** **8500-2(config-keychain-macs** **key 01** **8500-2(config-keychain-macs** **cryptographic-algorithm aes** **8500-2(config-keychain-macs** **key-string a5b2df4657bd8c02** **8500-2(config-keychain-macs** **lifetime 00:00:00 Jun 1 202** **8500-2(config-keychain-macs** **key 02** **8500-2(config-keychain-macs** **cryptographic-algorithm aes** **8500-2(config-keychain-macs** **key-string b5b2df4657bd8c02** **8500-2(config-keychain-macs** **lifetime 23:00:00 Jun 1 202** **8500-2(config-keychain-macs** **exit** **8500-2(config-keychain-macs** **exit**



注意：在配置MACsec密钥链时，请记住，key-string必须仅包含十六进制数字，aes-128-cmac加密算法需要32个十六进制数字的密钥，aes-256-cmac加密算法需要64个十六进制数字的密钥。



注意：请记住，使用多个密钥时，在指定的密钥有效期到期后，它们之间需要重叠的时间才能实现无中断密钥滚动。



警告：必须确保两台路由器的时钟同步；因此，强烈建议使用网络时间协议(NTP)。如果不这样做，可能会阻止建立MKA会话，或导致这些会话在将来失败。

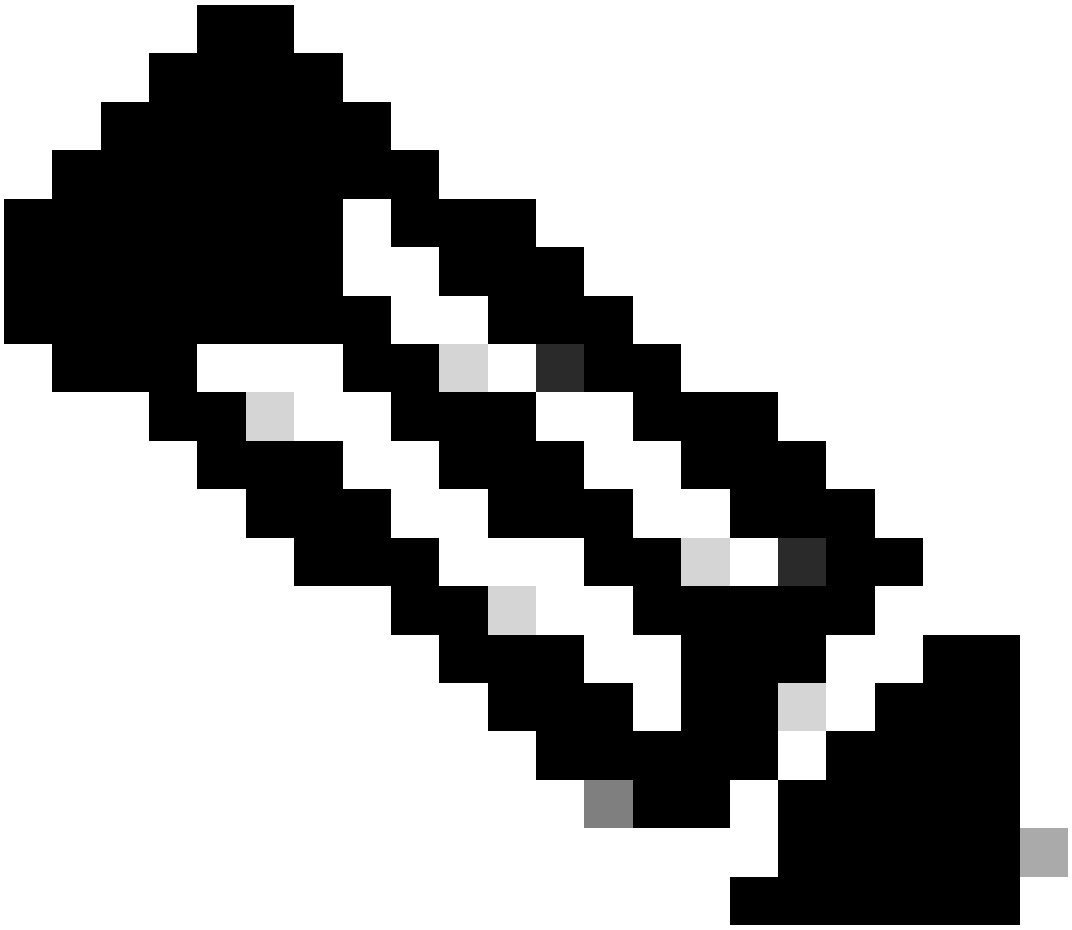
第3步：配置MKA策略

虽然默认MKA策略可用于初始设置和简单网络，但通常建议为WAN MACsec配置自定义MKA策略，以满足特定的安全、合规和性能要求。自定义策略提供更强的灵活性和控制力，确保您的网络安全功能强大且符合您的需求。

配置MKA策略时，可以选择不同的元素，例如密钥服务器优先级、MACsec密钥协议数据包数据单元(MKPDU)的延迟保护、密码套件等。在此平台和软件版本中，可以使用以下密码：

MACsec密码	描述
gcm-aes-128	使用128位密钥的高级加密标准(AES)的伽罗瓦/计数器模式(GCM)
gcm-aes-256	使用256位密钥的AES的伽罗瓦/计数器模式(GCM)（加密强度更高）

gcm-aes-xpn-128	使用128位密钥和扩展数据包编号(XPN)的AES的伽罗瓦/计数器模式(GCM)
gcm-aes-xpn-256	使用256位密钥和XPN（更高的加密强度）的AES的伽罗瓦/计数器模式(GCM)



注意：XPN通过支持更长的数据包编号来增强GCM-AES加密功能，从而提高超长寿命会话或高吞吐量环境的安全性。使用高速链路（例如40 Gb/s或100 Gb/s）可能会导致非常短的密钥翻转时间，因为MACsec帧中的数据包编号(PN)（通常基于发送的数据包数量）可能会在这些速度下快速耗尽。XPN扩展了数据包编号顺序，消除了高容量链路中可能发生的频繁的安全关联密钥(SAK)重新生成密钥的需要。

在本示例中，为MKA策略选择的密码是gcm-aes-xpn-256，其他元素将具有默认值：

CE 8500-1	CE 8500-2
<#root> 8500-1#	<#root> 8500-2#

configure terminal Enter configuration commands, one per line. End with CNTL/Z. 8500-1(config)# **mka policy subint100** 8500-1(config-mka-policy)# **macsec-cipher-suite gcm-aes-xpn-256** 8500-1(config-mka-policy)# **end**	**configure terminal** Enter configuration commands, one per line 8500-2(config)# **mka policy subint100** 8500-2(config-mka-policy)# **macsec-cipher-suite gcm-aes-xpn-256** 8500-2(config-mka-policy)# **end**

第4步：在接口和子接口级别配置MACsec

在此方案中，即使没有为物理接口配置IP地址，也要在此级别应用一些macsec命令以使解决方案起作用。MACsec策略和密钥链应用于子接口级别（请参阅配置示例）：

CE 8500-1	CE 8500-2
<#root> 8500-1# **configure terminal** 8500-1(config)# **interface FortyGigabitEthernet0/2/4** 8500-1(config-if)# **mtu 9216** 8500-1(config-if)# **cdp enable** 8500-1(config-if)# **macsec dot1q-in-clear 1** 8500-1(config-if)# **macsec access-control should-secure** 8500-1(config-if)# **exit** 8500-1(config)# **interface FortyGigabitEthernet0/2/4.100** 8500-1(config-if)# **eapol destination-address broadcast-address**	<#root> 8500-2# **configure terminal** 8500-2(config)# **interface FortyGigabitEthernet0/2/0** 8500-2(config-if)# **mtu 9216** 8500-2(config-if)# **cdp enable** 8500-2(config-if)# **macsec dot1q-in-clear 1** 8500-2(config-if)# **macsec access-control should-secure** 8500-2(config-if)# **exit** 8500-1(config)# **interface FortyGigabitEthernet0/2/0.100** 8500-2(config-if)# **eapol destination-address broadcast-address**

8500-1(config-if)#	8500-2(config-if)#
eapol eth-type 876F	**eapol eth-type 876F**
8500-1(config-if)#	8500-2(config-if)#
mka policy subint100	**mka policy subint100**
8500-1(config-if)#	8500-2(config-if)#
mka pre-shared-key key-chain keychain_vlan100	**mka pre-shared-key key-chain keychain_vlan100**
8500-1(config-if)#	8500-2(config-if)#
macsec	**macsec**
8500-2(config-if)#	8500-2(config-if)#
end	**end**

在物理接口级别应用的命令

a. MTU设置为9216，因为拓扑中使用的服务提供商允许巨型帧，但这不是要求

b.命令macsec dot1q-in-clear允许选项将VLAN (dot1q)标记明文显示（未加密）

c.命令macsec access-control should-secure允许从物理接口或子接口发送或接收未加密的数据包（如果一些子接口要求加密，而另一些要求不加密，则需要此命令，这是因为默认MACsec行为，它不允许从启用MACsec的同一物理接口发送或接收任何未加密的数据包）

在子接口级别应用的命令

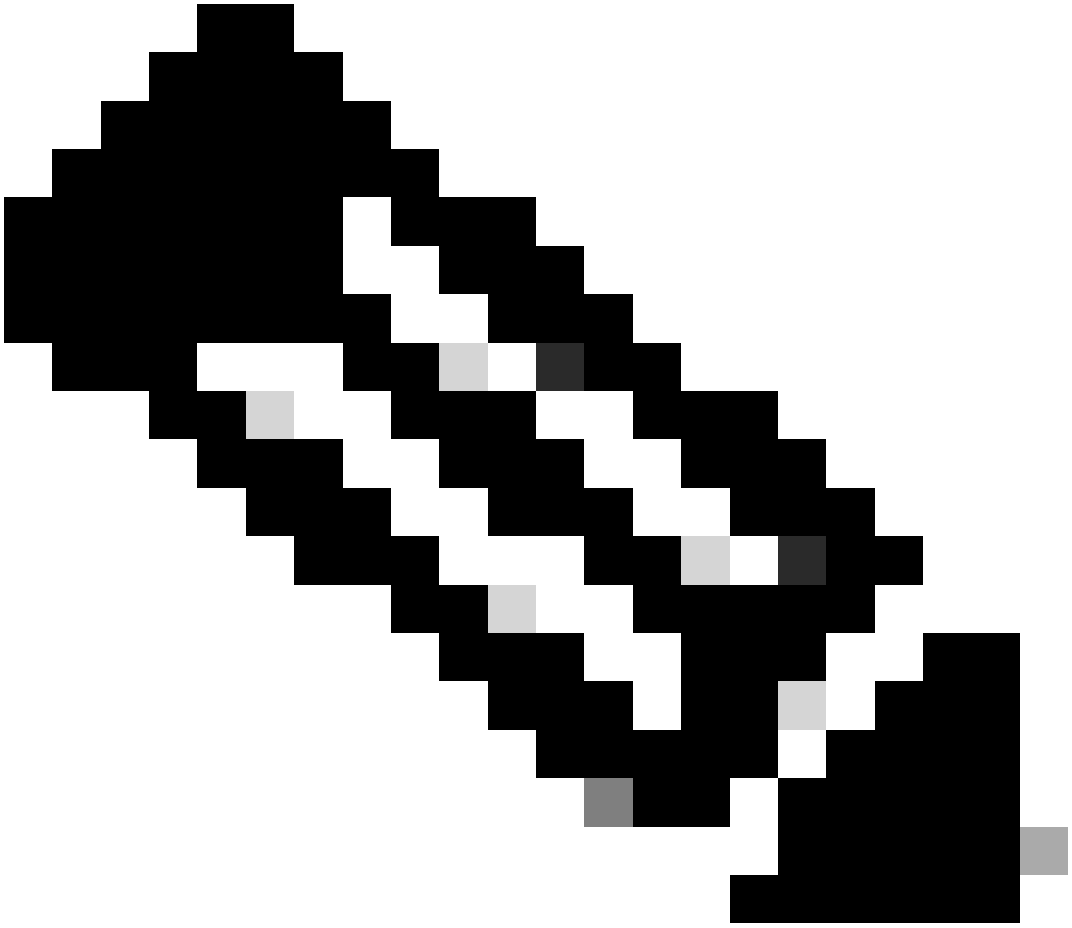
a.现在，需要使用eapol destination-address broadcast-address命令将EAPoL帧(默认情况下为组播MAC地址01:80：C2:00:00:03)的目标MAC地址更改为广播MAC地址，以确保服务提供商泛洪这些帧，并且不丢弃或使用它们。

b.也可使用eapol eth-type 876F命令将EAPoL帧的默认以太网类型（默认情况下为0x888E）更改为0x876F。为了防止服务提供商丢弃或使用这些帧，需要再次执行上述操作。

c.命令mka policy <policy name>和mka pre-shared-key key-chain <key chain name>用于向子接口应用自定义策略和密钥链。

d.最后但并非最不重要的是，macsec命令会在子接口级别启用MACsec。

在当前设置中，如果之前未更改EAPoL，则服务提供商端的9500交换机不会转发EAPoL帧。



注意：诸如dot1q-in-clear和should-secure等MACsec命令由子接口继承。 此外，可以在物理接口级别设置EAPoL命令，在这种情况下，子接口也会继承这些命令。 但是，在子接口上显式配置EAPoL命令会覆盖该子接口继承的值或策略。

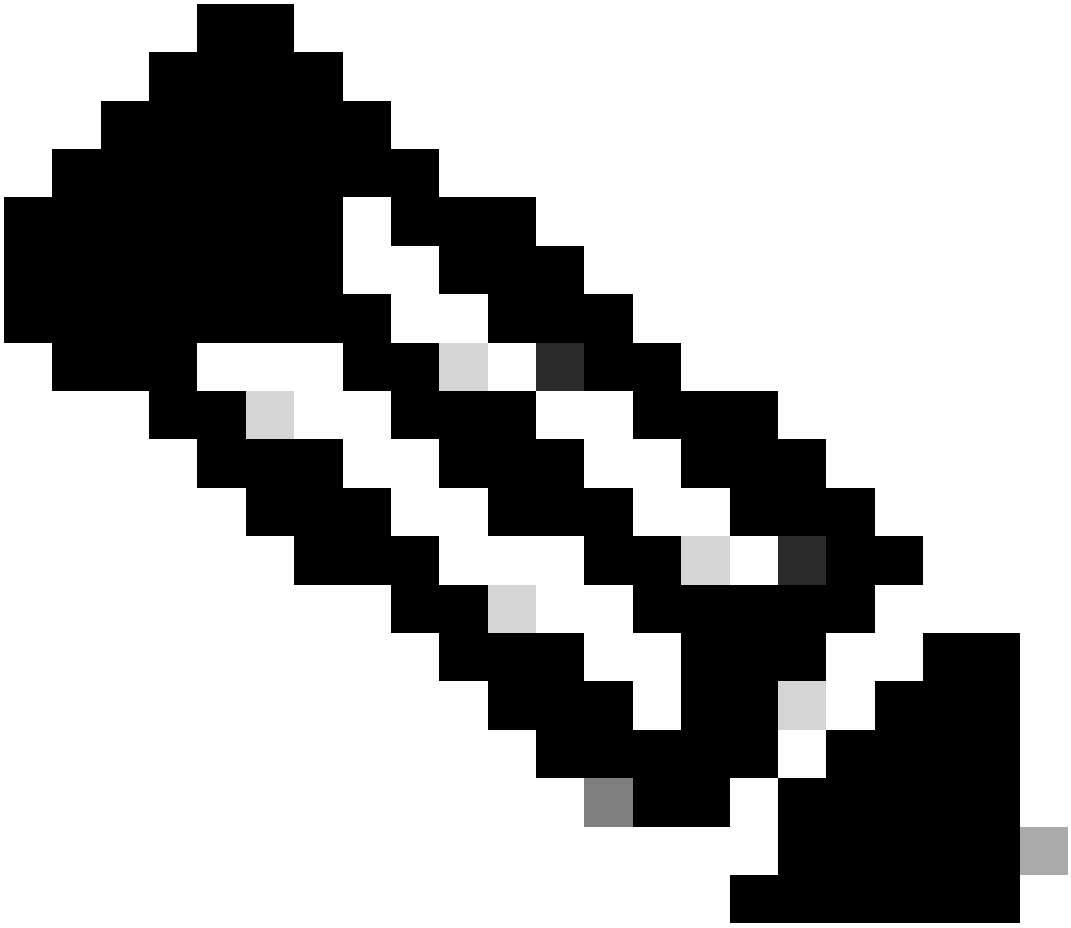
验证

应用配置后，下一个输出将显示每台客户边缘(CE) C8500路由器的相关运行配置（省略了某些配置）：

```
<#root>
8500-1#
show running-config

Building configuration...
```

```
Current configuration : 8792 bytes
!
!
version 17.14
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
!
hostname 8500-1
!
boot-start-marker
boot system flash bootflash:c8000aep-universalk9.17.14.01a.SPA.bin
boot-end-marker
!
!
no logging console
no aaa new-model
!
!

key chain keychain_vlan100 macsec key 01 cryptographic-algorithm aes-256-cmac key-string a5b2df4657bd8c

!
!
!
!
!
!
license boot level network-premier addon dna-premier
!
!
spanning-tree extend system-id
!

mka policy subint100 macsec-cipher-suite gcm-aes-xpn-256


!
!
!
!
!
!
cdp run
!
!
!
!
interface Loopback100
 ip address 192.168.100.10 255.255.255.0
!
interface Loopback200
 ip address 192.168.200.10 255.255.255.0
!
!

interface FortyGigabitEthernet0/2/4

 mtu 9216
 no ip address
 no negotiation auto
 cdp enable
```

```
 macsec dot1q-in-clear 1 macsec access-control should-secure
!
interface FortyGigabitEthernet0/2/4.100
 encapsulation dot1Q 100
 ip address 172.16.1.1 255.255.255.0

ip mtu 9184
 eapol destination-address broadcast-address eapol eth-type 876F mka policy subint100 mka pre-shared-key
!
interface FortyGigabitEthernet0/2/4.200
 encapsulation dot1Q 200
 ip address 172.16.2.1 255.255.255.0
!
!
router eigrp 100
 network 172.16.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
!
ip forward-protocol nd
!
!
!
control-plane
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 login
 transport input ssh
!
!
!
!
!
!
end

8500-1#
```



注意：请注意，启用MACsec之后，通过应用macsec命令，该接口上的MTU会自动调整并减少32个字节，以弥补MACsec开销。

接下来，您可以找到可用于检查并验证对等体之间MACsec状态的基本命令列表。这些命令为您提供有关当前MACsec会话、密钥链、策略和统计信息的详细信息：

show mka sessions -此命令显示当前MKA会话状态。

show mka sessions detail -此命令提供每个MKA会话的详细信息。

show mka keychains -此命令显示用于MACsec的密钥链和分配的接口。

show mka policy -此命令显示应用的策略、使用的接口和密码套件。

show mka summary -此命令提供MKA会话和统计信息的汇总。

show macsec statistics interface <interface name> -此命令显示指定接口的MACsec统计信息，并且有助于标识是否正在发送和接收加密流量。

```
<#root>

8500-1#

show mka sessions


Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=============================================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server
Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN
=============================================================================================================

Fo0/2/4.100

     78bc.1aac.1521/001a

subint100

         NO                 NO

26

              78bc.1aac.1420/001a  1

Secured

            02


8500-1#

show mka sessions detail


MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

TX-SSCI.................. 2
Local Tx-SCI............. 78bc.1aac.1521/001a

Interface MAC Address.... 78bc.1aac.1521

MKA Port Identifier...... 26
Interface Name........... FortyGigabitEthernet0/2/4.100
Audit Session ID.........
CAK Name (CKN)........... 02
Member Identifier (MI)... 8387013B6C4D6106D4443285
Message Number (MN)...... 439243
EAP Role................. NA
Key Server............... NO

MKA Cipher Suite......... AES-256-CMAC


Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... F5720CC2E83183F1E673DACD00000001 (1)
Old SAK Status........... FIRST-SAK
Old SAK AN............... 0
```

```
Old SAK KI (KN).......... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)


MKA Policy Name.......... subint100

Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO

SAK Cipher Suite......... 0080C20001000004 (GCM-AES-XPN-256)

MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------
  F5720CC2E83183F1E673DACD  439222      78bc.1aac.1420/001a  0         YES            1

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority

Installed

  ------------------------------------------------------------------------------------

8500-1#

show mka keychains


MKA PSK Keychain(s) Summary...

Keychain         Latest CKN                                                    Interface(s)
Name             Latest CAK                                                    Applied
=============================================================================================

keychain_vlan100 02 Fo0/2/4.100


                 <HIDDEN>

8500-1#

show mka policy


MKA Policy defaults :
         Send-Secure-Announcements: DISABLED
```

```
MKA Policy Summary...

Codes : CO - Confidentiality Offset, ICVIND - Include ICV-Indicator,
        SAKR OLPL - SAK-Rekey On-Live-Peer-Loss,
        DP - Delay Protect, KS Prio - Key Server Priority

Policy            KS   DP    CO SAKR  ICVIND Cipher          Interfaces
Name              Prio          OLPL         Suite(s)        Applied
================================================================================
*DEFAULT POLICY*  0    FALSE 0  FALSE TRUE   GCM-AES-128
                                             GCM-AES-256


subint100 0 FALSE 0 FALSE TRUE GCM-AES-XPN-256 Fo0/2/4.100




8500-1#

show mka summary


Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

================================================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server
Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN
================================================================================================================
Fo0/2/4.100     78bc.1aac.1521/001a  subint100         NO                 NO
26              78bc.1aac.1420/001a  1                 Secured            02



MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 14
   Fallback Secured............ 0
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 13
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated.............. 0
   SAKs Rekeyed................ 2
   SAKs Received............... 18
   SAK Responses Received...... 0
   SAK Rekeyed as KN Mismatch.. 0

MKPDU Statistics


MKPDUs Validated & Rx...... 737255
```

```
      "Distributed SAK"..... 18
      "Distributed CAK"..... 0


MKPDUs Transmitted......... 738485

      "Distributed SAK"..... 0
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Session Failures
   Bring-up Failures.............. 0
   Reauthentication Failures........ 0
   Duplicate Auth-Mgr Handle........ 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0
   SAK Cipher Mismatch.............. 0

CA Failures
   Group CAK Generation............. 0
   Group CAK Encryption/Wrap........ 0
   Group CAK Decryption/Unwrap...... 0
   Pairwise CAK Derivation.......... 0
   CKN Derivation................... 0
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SC Creation................... 0
   Tx SC Creation................... 0
   Rx SA Installation............... 0
   Tx SA Installation............... 0

MKPDU Failures
   MKPDU Tx............................... 0
   MKPDU Rx ICV Verification.............. 0
   MKPDU Rx Fallback ICV Verification..... 0
   MKPDU Rx Validation.................... 0
   MKPDU Rx Bad Peer MN................... 0
   MKPDU Rx Non-recent Peerlist MN........ 0
SAK USE Failures
   SAK USE Latest KN Mismatch............. 0
   SAK USE Latest AN not in USE........... 0

8500-1#

show macsec statistics interface Fo0/2/4.100

MACsec Statistics for FortyGigabitEthernet0/2/4.100
 SecY Counters
  Ingress Untag Pkts:       0
  Ingress No Tag Pkts:      0
  Ingress Bad Tag Pkts:     0
  Ingress Unknown SCI Pkts: 0
  Ingress No SCI Pkts:      0
  Ingress Overrun Pkts:     0
  Ingress Validated Octets: 0
```

```
Ingress Decrypted Octets: 11853398

  Egress Untag Pkts:        0
  Egress Too Long Pkts:     0
  Egress Protected Octets:  0


Egress Encrypted Octets: 11782598


 Controlled Port Counters
  IF In Octets:             14146226
  IF In Packets:            191065
  IF In Discard:            0
  IF In Errors:             0
  IF Out Octets:            14063174
  IF Out Packets:           190042
  IF Out Errors:            0

 Transmit SC Counters (SCI: 78BC1AAC1521001A)
  Out Pkts Protected:       0
  Out Pkts Encrypted:       190048
 Transmit SA Counters (AN 0)
  Out Pkts Protected:       0
  Out Pkts Encrypted:       190048

 Receive SA Counters (SCI: 78BC1AAC1420001A  AN 0)
  In Pkts Unchecked:        0
  In Pkts Delayed:          0
  In Pkts OK:               191069
  In Pkts Invalid:          0
  In Pkts Not Valid:        0
  In Pkts Not using SA:     0
  In Pkts Unused SA:        0
  In Pkts Late:             0
```

来自不同子接口的可达性以及192.168.0.0/16子网之间的可达性都成功。下一ping测试显示了连接是否成功：

```
<#root>

8500-1#

ping 172.16.1.2


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
8500-1#

ping 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
8500-1#

ping 192.168.101.10 source 192.168.100.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.101.10, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
8500-1#
```

从提供商边缘(PE)设备上的ICMP测试捕获数据包后，可以比较加密帧和未加密帧。注意两个帧上的以太网外部MAC报头相同，并且dot1q标记可见。但是，加密帧显示0x88E5 (MACsec)的EtherType，而未加密帧显示0x0800 (IPv4)的EtherType以及ICMP协议信息：

加密帧VLAN 100

```
<#root>

F241.03.03-9500-1#

show monitor capture cap buffer detail | begin Frame 80


Frame 80: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface /tmp/epc_ws/wif_to
    Interface id: 0 (/tmp/epc_ws/wif_to_ts_pipe)
        Interface name: /tmp/epc_ws/wif_to_ts_pipe
    Encapsulation type: Ethernet (1)
    Arrival Time: Jul 29, 2024 23:50:16.528191000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1722297016.528191000 seconds
    [Time delta from previous captured frame: 0.224363000 seconds]
    [Time delta from previous displayed frame: 0.224363000 seconds]
    [Time since reference or first frame: 21.989269000 seconds]
    Frame Number: 80
    Frame Length: 150 bytes (1200 bits)
    Capture Length: 150 bytes (1200 bits)
    [Frame is marked: False]
    [Frame is ignored: False]


[Protocols in frame: eth:ethertype:vlan:ethertype:macsec:data]

Ethernet II, Src: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21), Dst: 78:bc:1a:ac:14:20 (78:bc:1a:ac:14:20)

    Destination: 78:bc:1a:ac:14:20 (78:bc:1a:ac:14:20)
        Address: 78:bc:1a:ac:14:20 (78:bc:1a:ac:14:20)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21)
        Address: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)

 Type: 802.1Q Virtual LAN (0x8100) 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100

    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0110 0100 = ID: 100

 Type: 802.1AE (MACsec) (0x88e5) 802.1AE Security tag
```

```
    0010 11.. = TCI: 0x0b, VER: 0x0, SC, E, C
        0... .... = VER: 0x0
        .0.. .... = ES: Not set
        ..1. .... = SC: Set
        ...0 .... = SCB: Not set
        .... 1... = E: Set
        .... .1.. = C: Set
    .... ..00 = AN: 0x0
    Short length: 0

 Packet number: 147 System Identifier: 78:bc:1a:ac:15:21 (78:bc:1a:ac:15:21) Port Identifier: 26 ICV: 2

Data (102 bytes)

0000  99 53 71 3e f6 c7 9b bb 00 21 68 48 d6 ca 26 af   .Sq>.....!hH..&.
0010  80 a5 76 40 19 c9 45 97 b3 5a 48 d3 2d 30 72 a6   ..v@..E..ZH.-0r.
0020  96 47 6e a7 4c 30 90 e5 70 10 80 e8 68 00 5f ad   .Gn.L0..p...h._.
0030  7f dd 4a 70 a8 46 00 ef 7d 56 fe e2 66 ba 6c 1b   ..Jp.F..}V..f.l.
0040  3a 07 44 4e 5e e7 04 cb cb f4 03 71 8d 40 da 55   :.DN^......q.@.U
0050  9f 1b ef a6 3a 1e 42 c7 05 e6 9e d0 39 6e b7 3f   ....:.B.....9n.?
0060  f2 82 cf 66 f2 5b                                 ...f.[
    Data: 9953713ef6c79bbb00216848d6ca26af80a5764019c94597b^@&
    [Length: 102]
```

相关信息

- WAN MACSEC和MKA支持增强功能
- 以太网加密的创新(802.1AE - MACsec)可保护高速(1-100GE)广域网部署
- 排除路由器上的WAN MACSEC故障

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。