在帶有子介面的Catalyst 8500上配置WAN MACsec

目錄

簡介

本文檔介紹在具有子介面的Cisco Catalyst 8500平台上配置WAN介質訪問控制安全(MACsec)的過程。

必要條件

需求

思科建議您瞭解以下主題：

- 高級網路概念，包括WAN、VLAN和加密
- 瞭解MACsec (IEEE 802.1AE)和金鑰管理(IEEE 802.1X-2010)
- 熟悉Cisco IOS® XE命令列介面(CLI)

採用元件

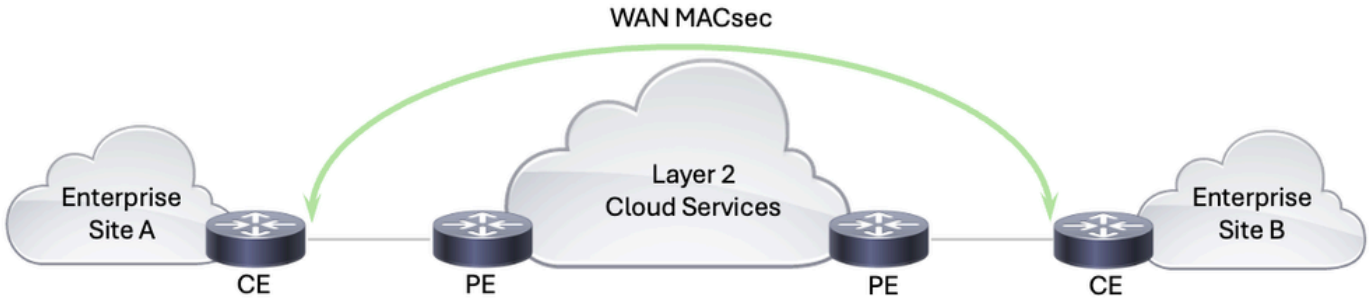
本文中的資訊係根據以下軟體和硬體版本：

- Cisco Catalyst 8500系列邊緣平台
- Cisco IOS XE版本17.14.01a

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

WAN MACsec是一種安全解決方案，旨在利用MACsec的功能來保護跨WAN網路的網路流量。使用服務提供商網路交換資料時，必須對傳輸中的資料進行加密，以防止資料被篡改。WAN MACsec易於部署和管理，非常適合需要保護其網路流量免受資料操縱（如竊聽和中間人攻擊）的組織。它提供無縫的線速加密，確保資料在穿越各種網路基礎設施（包括服務提供商網路、雲環境和企業網路）時保持安全和不受影響。



WAN MACsec解決方案

為了共用一點歷史記錄，IEEE 802.1AE標準定義的MACsec透過確保乙太網幀的資料保密性、完整性和源真實性來提供乙太網路上的安全通訊。MACsec在開放式系統互連(OSI)模型的資料鏈路層（第2層）運行，對乙太網幀進行加密和身份驗證，以保護節點之間的通訊。MACsec最初是為LAN而設計的，現在也發展為支援WAN部署。它提供線速加密，確保最小的延遲和開銷，這對於高速網路至關重要。

IEEE 802.1X-2010是對原始IEEE 802.1X標準的修訂，其中定義了基於埠的網路訪問控制。2010年修訂版引入了MACsec金鑰協定(MKA)協定，該協定對於管理MACsec實施中的加密金鑰至關重要。MKA處理MACsec用於加密和解密資料的加密金鑰的分配和管理。MKA是一種標準，它有助於實現MACsec部署的多供應商互操作性，支援安全金鑰交換和金鑰重建機制，對於在動態廣域網環境中保持持續的安全至關重要。

在WAN MACsec部署中，IEEE 802.1AE (MACsec)在資料鏈路層提供基本的加密和安全機制，確保所有乙太網幀在網路中傳輸時都受到保護。採用MKA協定的IEEE 802.1X-2010負責分發和管理MACsec正常運行所需的加密金鑰。總之，這些標準可以確保WAN MACsec跨廣域網提供穩健的高速加密，為傳輸中的資料提供全面的保護，同時保持互操作性和易管理性。

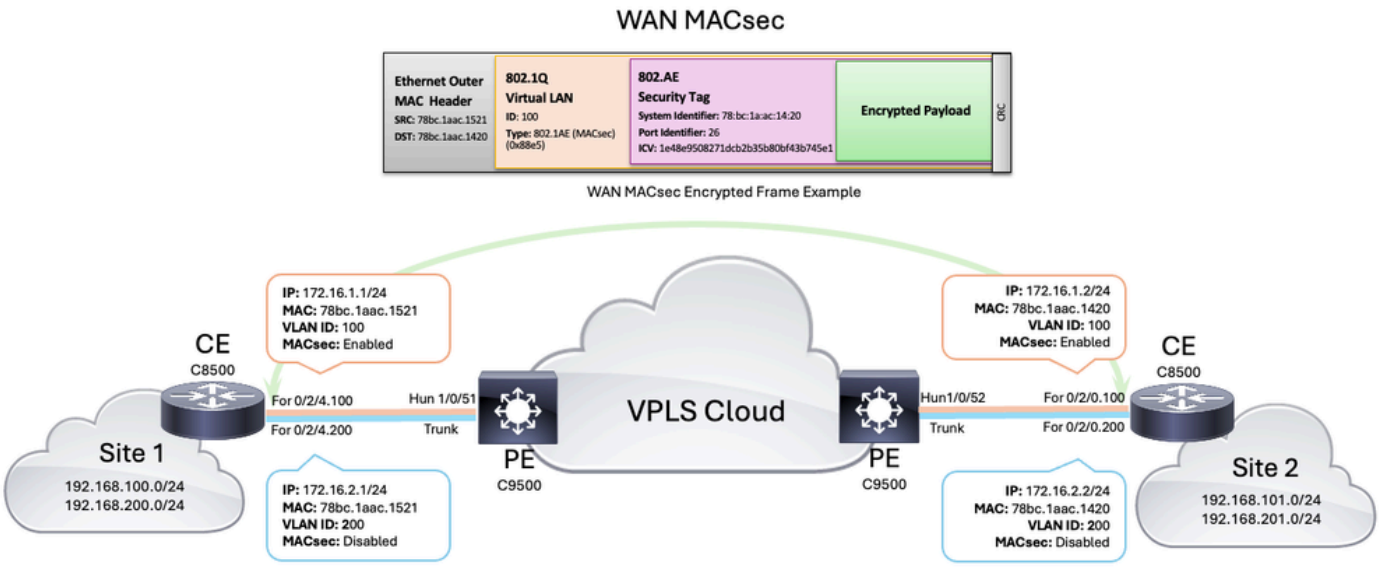
為了應對廣域網環境的獨特挑戰，對傳統MACsec部署進行了一些增強：

- Clear：此功能允許802.1Q VLAN標籤暴露在加密MACsec報頭之外，從而促進更靈活的網路設計，特別是在公共乙太網傳輸環境中。此功能對於將MACsec與業者級乙太網服務整合至關重要，因為它允許在同一網路上同時存在加密流量和未加密流量，從而簡化了網路架構並降低了成本。
- 公共業者級乙太網的適應性：現代WAN MACsec實施可以適應公共業者級乙太網服務。這種適應性包括修改LAN乙太網身份驗證協定(EAPoL)目標地址和EtherType，允許MACsec在業者級乙太網路上無縫運行，否則業者級乙太網會消耗或阻止這些幀。

WAN MACsec代表了乙太網加密的顯著進步，可滿足對高速、安全的廣域網連線的日益成長的需求。它能夠提供線速加密、支援靈活的網路設計，並能適應公共業者服務，因此是現代網路安全架構的關鍵組成部分。透過利用WAN MACsec，組織可以為其高速廣域網鏈路實現強大的安全性，同時簡化網路架構並降低運營複雜性。

設定

網路圖表



WAN MACsec拓撲

組態

第1步：基本裝置配置

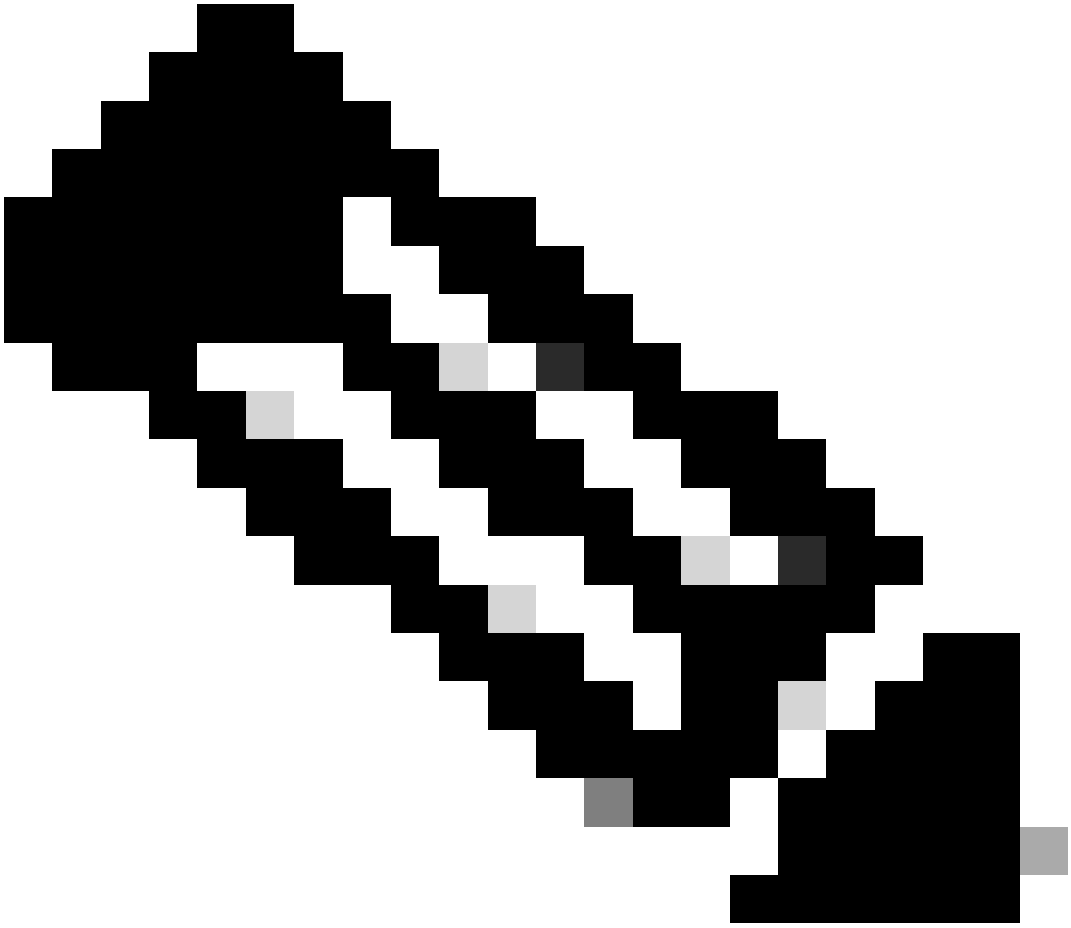
要啟動配置，首先需要定義將用於流量分段和連線到服務提供商的子介面。對於此方案，為與子網172.16.1.0/24關聯的VLAN 100和與子網172.16.2.0/24關聯的VLAN 200定義了兩個子介面（稍後僅在一個子介面上配置了MACsec）。

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.**

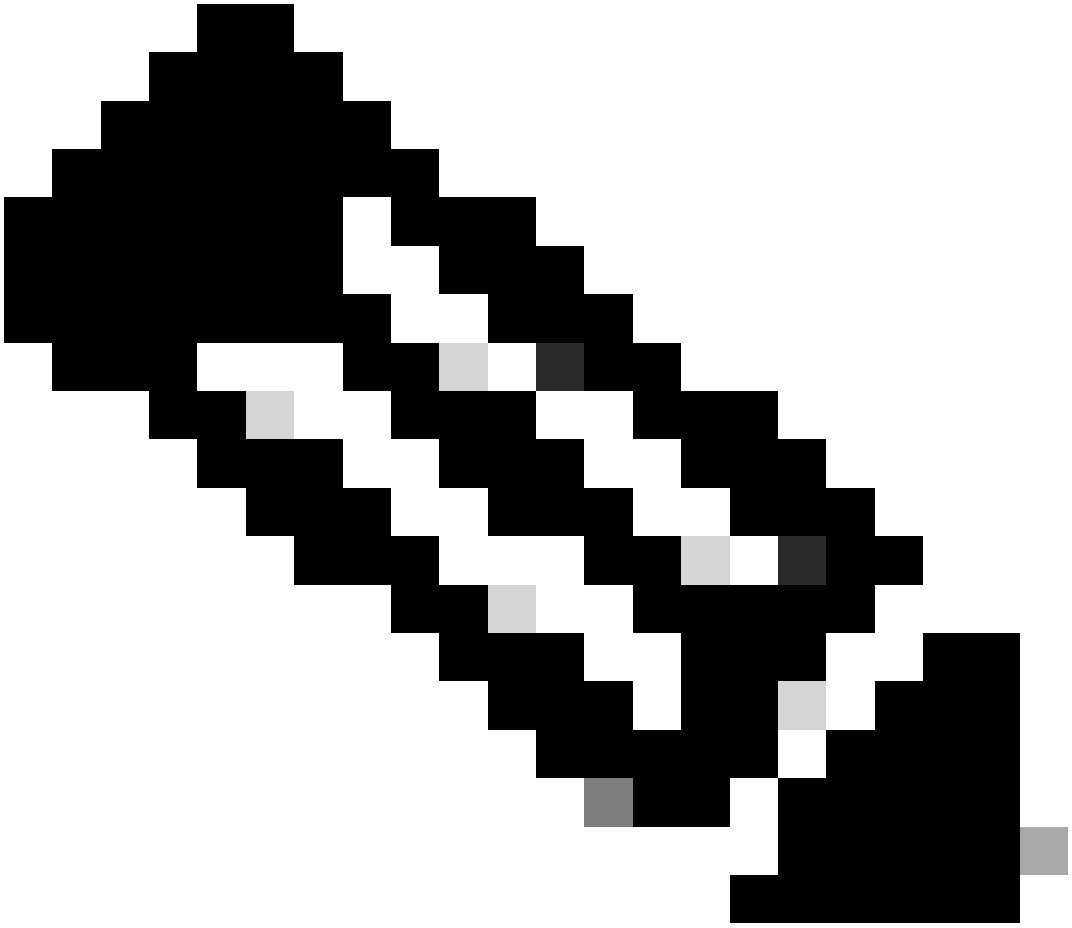
第2步：配置MACsec金鑰鏈

請記住，IEEE 802.1X-2010標準規定MACsec加密金鑰可以從預共用金鑰(PSK)、802.1X可擴展身份驗證協定(EAP)或由MKA金鑰伺服器選擇和分配。在本示例中，PSK是透過MACsec金鑰鏈使用和手動配置的，並且這些金鑰等於連線關聯金鑰(CAK)，CAK是用於衍生MACsec中使用的所有其他加密金鑰的主金鑰。

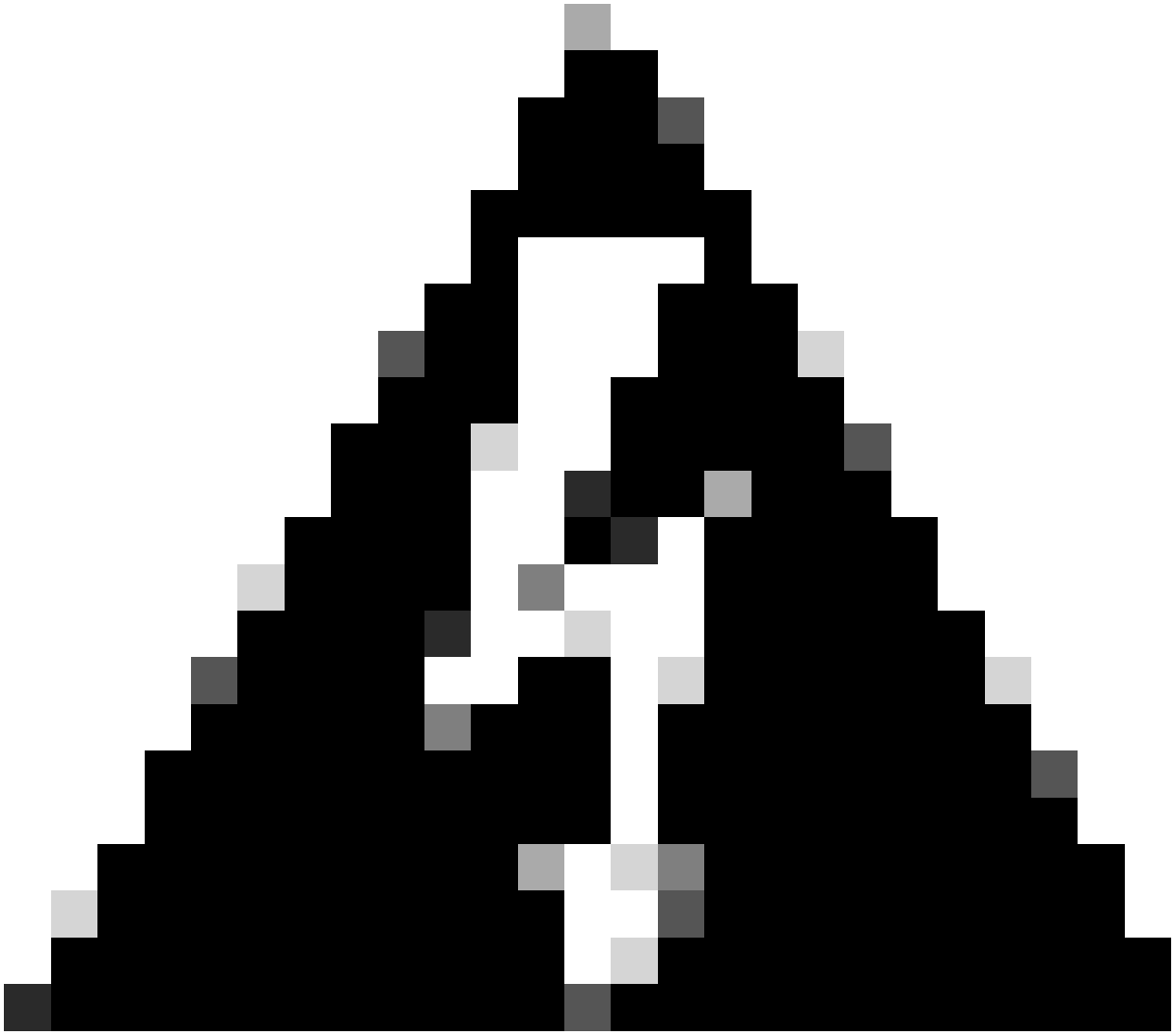
CE 8500-1	
<#root> 8500-1# **configure terminal** **8500-1(config)#** **key chain keychain_vlan100 macsec** **8500-1(config-keychain-macsec)#** **key 01** **8500-1(config-keychain-macsec-key)#** **cryptographic-algorithm aes-256-cmac** **8500-1(config-keychain-macsec-key)#** **key-string a5b2df4657bd8c02fcdaaf1212fe27ccc54626ad12d7c3b64c7a93e0113011e1** **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：配置MACsec金鑰鏈時，請記住，key-string必須僅包含十六進位制數字，aes-128-cmac加密演算法需要32個十六進位制數字的金鑰，aes-256-cmac加密演算法需要64個十六進位制數字的金鑰。



注意：請記住，使用多個金鑰時，需要在指定金鑰有效期到期後使用重疊的時間段來實現無中斷金鑰滾動更新。



警告：必須確保兩台路由器的時鐘同步；因此，強烈建議使用網路時間協定(NTP)。如果不這樣做，可能會阻止建立MKA會話，或導致它們在未來失敗。

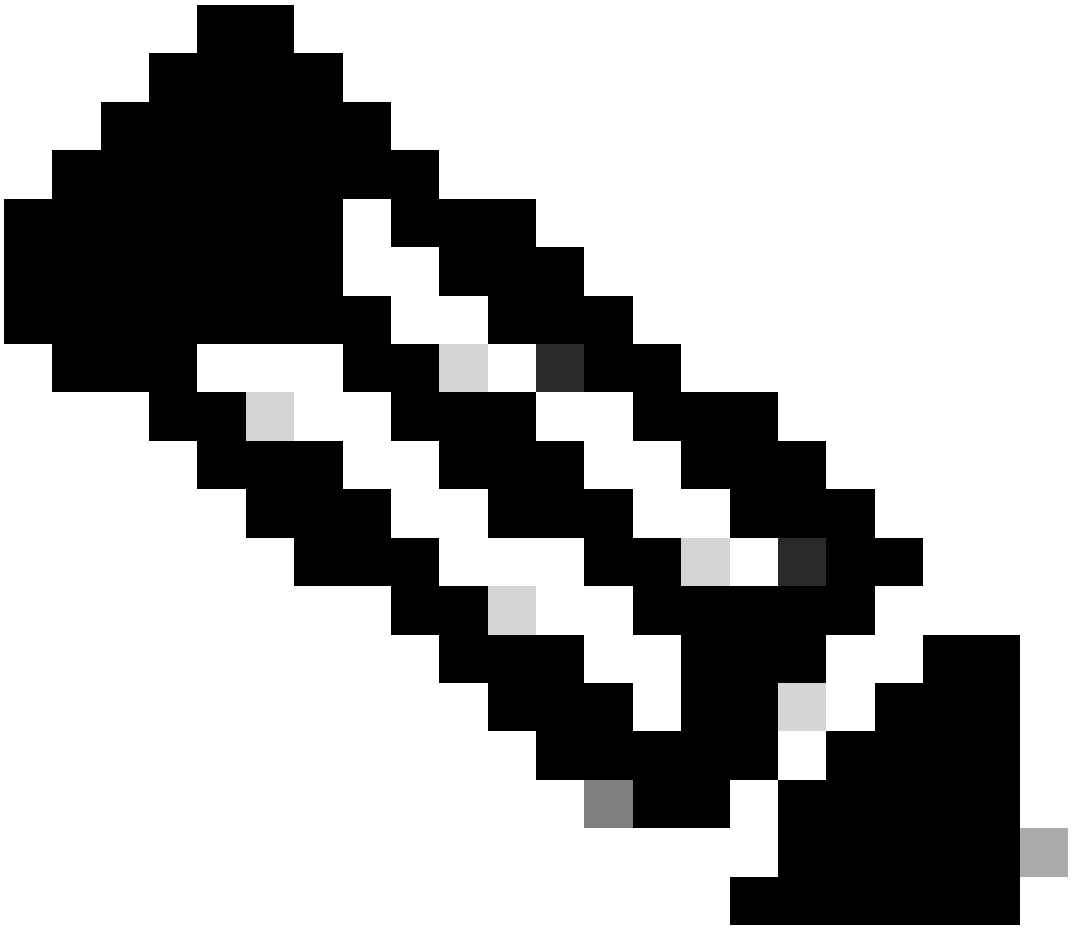
第3步：配置MKA策略

雖然預設MKA策略對於初始設定和簡單網路非常有用，但通常建議為WAN MACsec配置自定義MKA策略，以滿足特定的安全性、合規性和效能要求。自定義策略提供更高的靈活性和控制能力，確保您的網路安全功能強大且可根據您的需求定製。

配置MKA策略時，可以選擇不同的元素，例如金鑰伺服器優先順序、MACsec金鑰協定資料包資料單元(MKPDU)的延遲保護、密碼套件等。在此平台和軟體版本中，可以使用以下密碼：

MACsec密碼	說明
gcm-aes-128	使用128位元金鑰的進階加密標準(AES)的伽羅華/計數器模式(GCM)
gcm-aes-256	使用256位元金鑰的AES伽羅華/計數器模式(GCM)（加密強度較高）

gcm-aes-xpn-128	使用128位元金鑰和擴充封包編號(XPN)的AES伽羅華/計數器模式(GCM)
gcm-aes-xpn-256	使用256位元金鑰搭配XPN（較高加密強度）的AES伽羅華/計數器模式(GCM)



注意：XPN透過支援更長的資料包編號來增強GCM-AES密碼，從而改善長時間會話或高吞吐量環境的安全性。使用高速鏈路（例如40 Gb/s或100 Gb/s）會導致非常短的金鑰變換時間，因為MACsec幀內的資料包編號(PN)（通常基於傳送的資料包數量）可能會在這些速度下快速耗盡。XPN可擴充封包編號順序，並消除大容量連結中經常發生的安全關聯金鑰(SAK)重新金鑰的需求。

在本示例中，為MKA策略選擇的密碼是gcm-aes-xpn-256，其他元素將具有預設值：

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：在介面和子介面級別配置MACsec

在此方案中，即使沒有使用IP地址配置物理介面，也要在此級別應用某些macsec命令才能使解決方案正常工作。MACsec策略和金鑰鏈在子介面級別應用（請參閱配置示例）：

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**

在物理介面級別應用的命令

a. MTU設定為9216，因為拓撲中使用的服務提供商允許巨型幀，但這不是要求

b.命令macsec dot1q-in-clear允許選項將VLAN (dot1q)標籤放在透明（未加密）中

c.命令macsec access-control should-secure允許從物理介面或子介面傳送或接收未加密的資料包（如果某些子介面需要加密，而另一些子介面不需要，則使用此命令，這是由於預設的MACsec行為不允許從啟用了MACsec的同一物理介面傳送或接收任何未加密的資料包）

在子介面級別應用的命令

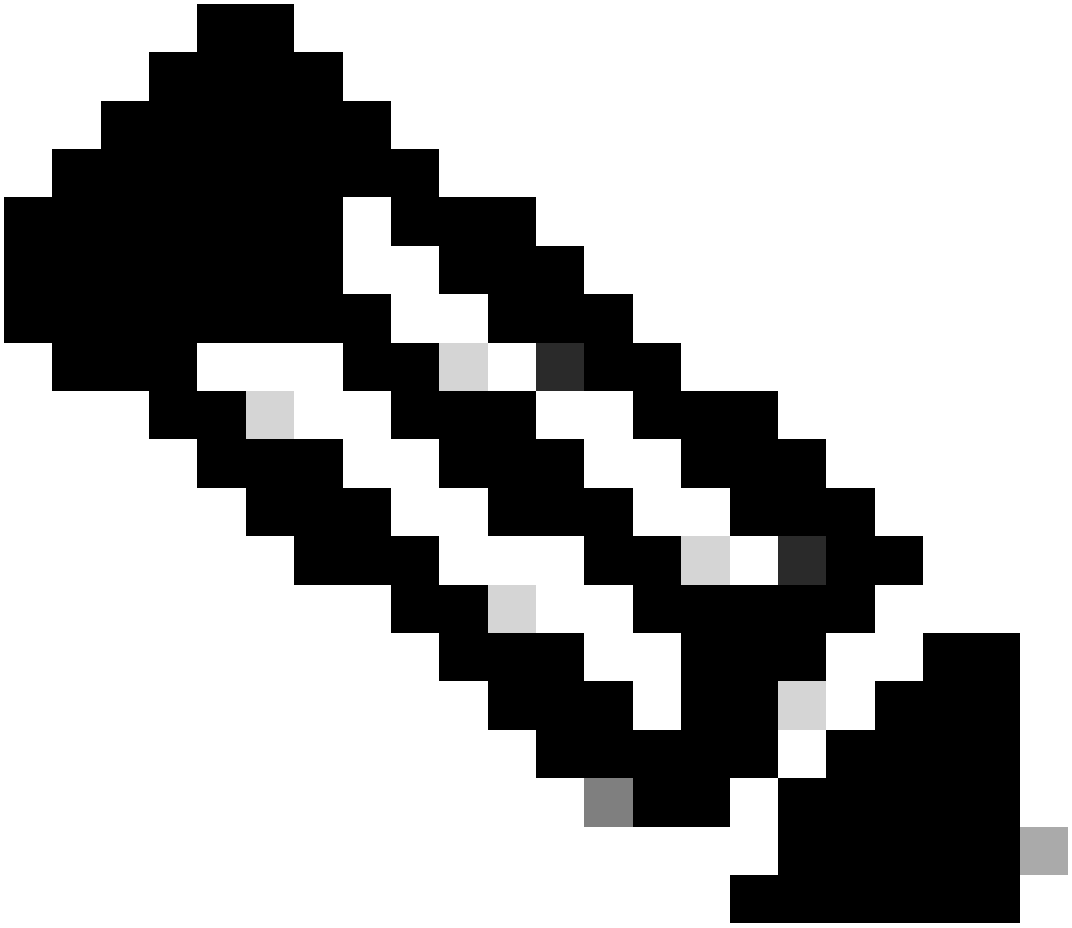
a.現在，需要使用eapol destination-address broadcast-address命令將EAPoL幀(預設情況下是組播MAC地址01:80：C2:00:00:03)的目標MAC地址更改為廣播MAC地址，以確保服務提供商泛洪廣播這些幀，而不會丟棄或使用它們。

b.命令eapol eth-type 876F還用於更改EAPoL幀的預設乙太網型別（預設值為0x888E），並將其更改為0x876F。這再次是防止服務提供商丟棄或使用這些幀所必需的。

c.命令mka policy <policy name>和mka pre-shared-key key-chain <key chain name>用於向子介面應用自定義策略和金鑰鏈。

d.最後但並非最不重要的一點是，macsec命令在子介面級別啟用MACsec。

在目前的設定中，若沒有之前的EAPoL變更，則服務提供者端的9500交換器不會轉送EAPoL訊框。



注意：子介面會繼承MACsec命令，例如dot1q-in-clear和should-secure。 此外，EAPoL命令可在物理介面級別進行設定，在這種情況下，子介面也會繼承這些命令。 但是，在子介面上顯式配置EAPoL命令會覆蓋該子介面繼承的值或策略。

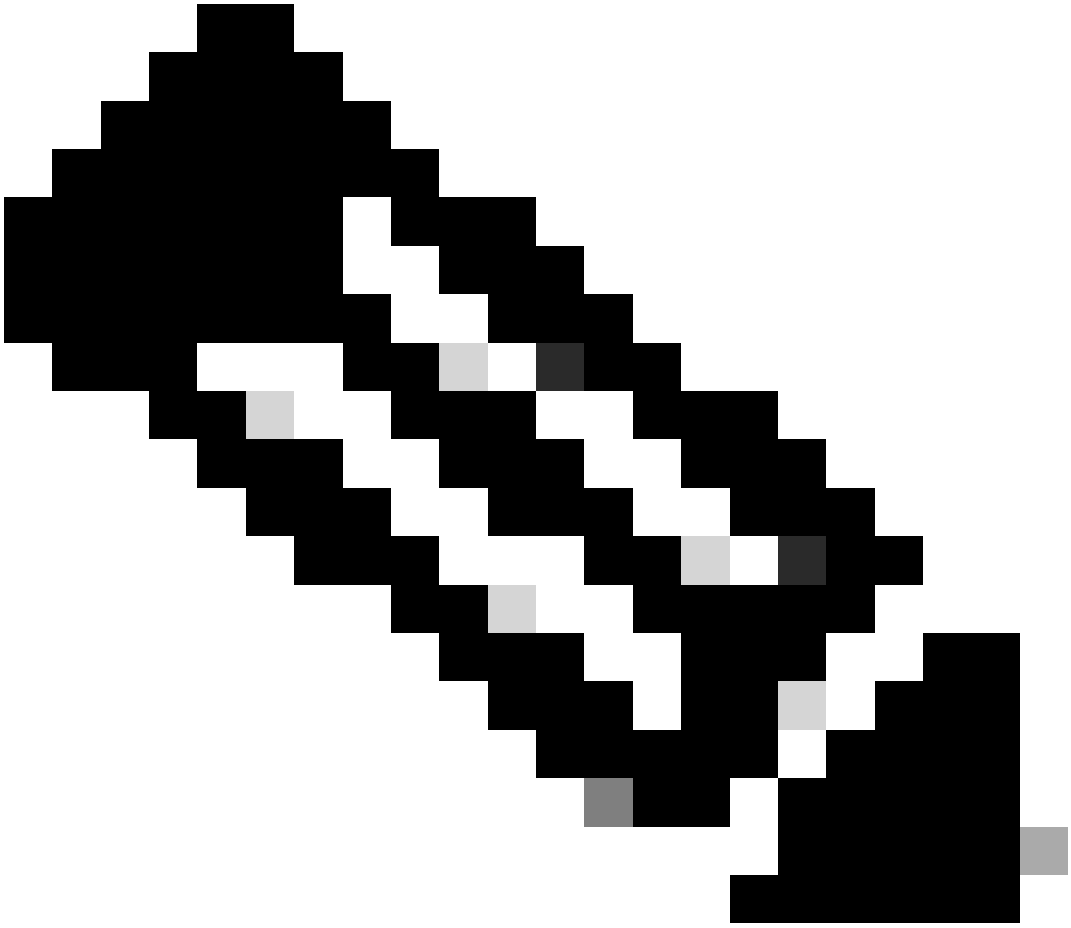
驗證

應用配置後，下一個輸出將顯示每台客戶邊緣(CE) C8500路由器的相關運行配置（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：請注意，啟用MACsec之後，透過應用macsec命令，該介面的MTU將自動調整並降低32位元組，以增加MACsec開銷。

接下來，您可以找到一系列可用來檢查對等體之間MACsec狀態的基本命令。這些命令為您提供有關當前MACsec會話、金鑰鏈、策略和統計資訊的詳細資訊：

show mka sessions - 此命令顯示當前MKA會話狀態。

show mka sessions detail -此命令提供每個MKA會話的詳細資訊。

show mka keychains -此命令顯示用於MACsec的金鑰鏈和分配的介面。

show mka policy -此命令顯示應用的策略、使用的介面和密碼套件。

show mka summary -此命令提供MKA會話和統計資訊的彙總。

show macsec statistics interface <interface name> - 此命令顯示指定介面的MACsec統計資訊，並可幫助標識是否正在傳送和接收加密流量。

```
<#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
```

來自不同子介面的可達性成功，192.168.0.0/16子網之間的可達性也成功。下一ping測試將演示連線是否成功：

```
<#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#
```

在提供商邊緣(PE)裝置上捕獲ICMP測試的資料包後，您可以比較加密幀和未加密幀。請注意，兩個幀上的乙太網外部MAC報頭相同，可以看到dot1q標籤。但是，加密的幀顯示的是0x88E5 (MACsec)的EtherType，而未加密的幀顯示的是0x0800 (IPv4)的EtherType以及ICMP協定資訊：

加密幀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]
```

相關資訊

- WAN MACSEC和MKA支援增強功能
- 乙太網路加密的創新(802.1AE - MACsec)可保護高速(1-100GE)WAN部署
- 排除路由器上的WAN MACSEC故障

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。