

排除路由器上的WAN MACSEC故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[拓撲](#)

[要排除故障的MACSEC概述](#)

[MACsec資料包格式](#)

[WAN-MACSEC](#)

[WAN MACSEC封包格式](#)

[WAN MACSEC術語](#)

[MACSEC金鑰協定\(MKA\)和加密概述](#)

[預共用金鑰](#)

[802.1x/EAP](#)

[排除WAN MACSEC故障](#)

[組態](#)

[操作問題](#)

[相關資訊](#)

簡介

本文檔介紹用於瞭解Cisco IOS® XE路由器的操作和故障排除的基本WAN MACSEC協定。

必要條件

需求

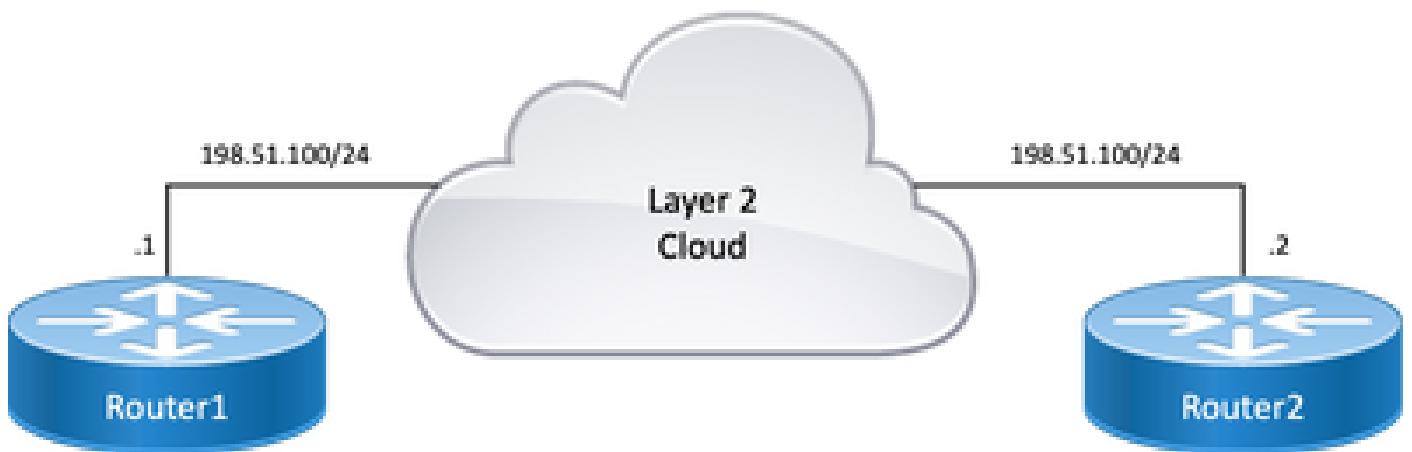
本文件沒有特定先決條件。

採用元件

本文檔中的資訊特定於Cisco IOS XE路由器，如ASR 1000、ISR 4000和Catalyst 8000系列。尋找特定的硬體和軟體MACSEC支援。

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。

拓撲



拓撲圖

要排除故障的MACSEC概述

MACsec是基於IEEE 802.1AE標準的第2層逐跳加密，為具有AES-128加密的媒體訪問獨立協定提供資料機密性、資料完整性和資料來源驗證，只有面向主機的鏈路(網路訪問裝置與終端裝置 (如PC或IP電話) 之間的鏈路)可以使用MACsec進行保護。

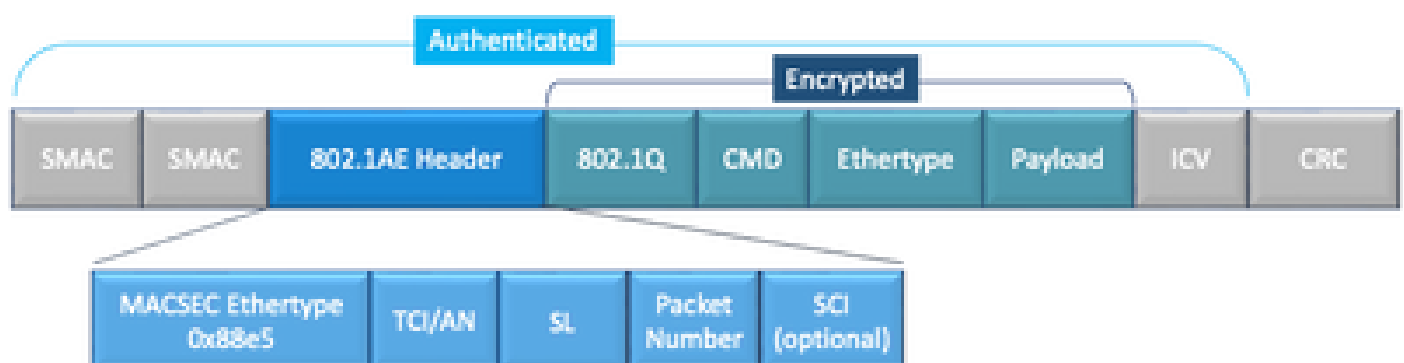
- 封包會在輸入連線埠上解密。
- 裝置中的資料包已清除。
- 封包在輸出連線埠上已加密。

MACsec在有線LAN上提供安全通訊，當MACsec用於保護LAN上終端之間的通訊時，線上的每個封包都會使用對稱金鑰加密法加密，因此線上的通訊無法受到監控或更改。當MACsec與安全組標籤(SGT)結合使用時，它會為標籤以及幀有效負載中包含的資料提供保護。

MACsec通過使用帶外加密金鑰加密方法，在有線網路上提供MAC層加密。

MACsec資料包格式

使用802.1AE(MACsec)時，訊框會進行加密並使用完整性檢查值(ICV)加以保護，不會影響IP MTU或分段，且最小第2層MTU影響：約40位元組 (小於小型巨型訊框)。



MACSEC封包格式範例

- MACsec EtherType: 0x88e5，指定該幀為MACsec幀。
- TCI/AN:標籤控制資訊/關聯編號。如果單獨使用機密性或完整性，則為MACsec版本號。
- SL：加密資料的長度。
- PN:用於重放保護的資料包編號。
- SCI:安全通道識別符號。每個連線關聯(CA)都是虛擬埠（物理介面的MAC地址加上16位埠ID）。
- ICV:完整性檢查值。

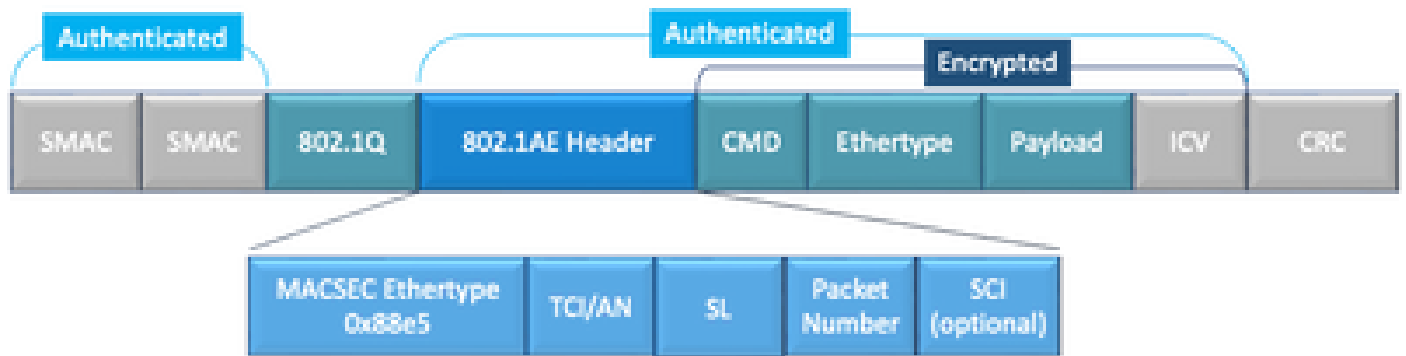
WAN-MACSEC

乙太網已經超越了私有LAN傳輸，已發展為包括各種WAN或MAN傳輸選項。WAN MACSEC使用AES 128或256位提供跨第2層乙太網WAN服務的端到端加密（點對點或點對多點）。

WAN MACsec基於(LAN)MACsec，因此使用名稱（並與IPsec分離），但提供了一些之前無法提供的附加功能。

WAN MACSEC封包格式

如果標籤已加密，則服務提供商可能不支援MACsec ethertype且無法區分第2層服務，因此WAN MACSEC會對802.1Q報頭之後的所有幀進行加密：



清除資料包格式中的WAN MACSEC 802.1Q標籤示例

其中一個新的增強功能包括Clear（也稱為ClearTag）中的802.1Q標籤。此增強功能允許將802.1Q標籤暴露在加密MACsec報頭之外。公開此欄位提供了幾個使用MACsec的設計選項，而在公共運營商乙太網傳輸提供商中，必須使用某些傳輸服務。

MKA功能支援以明文形式提供隧道資訊，例如VLAN標籤（802.1Q標籤），以便服務提供商可以提供服務多路複用，以便多個點對點或多點服務可以共存於單個物理介面上，並根據現在可見的VLAN ID進行區分。

除了服務多路複用之外，清除中的VLAN標籤還使服務提供商能夠根據802.1P(CoS)欄位（現在作為802.1Q標籤的一部分可見）通過SP網路為加密的乙太網資料包提供服務品質(QoS)。

WAN MACSEC術語

MKA	MACSec金鑰協定，在IEEE 802.1XREV-2010中定義 — 用於發現MACSec對等體和協商金鑰的金鑰協定協定。
-----	---

MSK	主會話金鑰，在EAP交換期間生成。請求方和身份驗證伺服器使用MSK生成CAK
CAK	連線關聯金鑰是從MSK派生的。是持久的主金鑰，用於生成用於MACSec的所有其他金鑰。
CKN	連線關聯金鑰名稱 — 標識CAK。
SAK	安全關聯金鑰 — 從CAK派生，是請求方和交換機用於加密給定會話流量的金鑰。
KS	主要伺服器負責： <ul style="list-style-type: none"> • 選擇和通告密碼套件 • 從CAK生成SAK。
KEK	金鑰加密金鑰 — 用於保護MACsec金鑰(SAK)

MACSEC金鑰協定協定(MKA)和加密概述

MKA是WAN MACsec使用的控制平面機制；在IEEE Std 802.1X中指定，用於發現相互驗證的MACsec對等體以及後續操作：

- 建立和管理CA (連線關聯)。
- 管理即時/潛在對等體清單。
- 密碼套件協商。
- 在CA的成員中選擇金鑰伺服器(KS)。
- 安全關聯金鑰(SAK)派生和管理。
- 安全金鑰分發。
- 金鑰安裝。
- 重新生成金鑰。

一個成員根據配置的金鑰伺服器優先順序 (最低) 被選為金鑰伺服器，如果對等體中的KS優先順序相同，則最低的SCI將獲選。

KS僅在所有潛在對等體都變為活動狀態且至少有一個活動對等體時生成SAK。它使用MKA PDU或MKPDU以加密格式將使用的SAK和密碼分發給其他參與者。

參與者檢查SAK傳送的密碼，並在受支援的情況下安裝該密碼，在每個MKPDU上使用它來指示他們擁有的最新金鑰；否則，他們應拒絕SAK

如果參與者在3個心跳後未收到MKPDU (每個心跳預設為2秒)，則從活動對等體清單中刪除對等體；例如，如果客戶端斷開，交換機上的參與者繼續運行MKA，直到從客戶端收到最後一個MKPDU後經過3個心跳為止。

對於此過程，有兩種方法可驅動加密金鑰：

- 預共用金鑰
- 802.1x/EAP

預共用金鑰

如果使用預共用金鑰，則必須手動輸入CAK=PSK和CKN。對於金鑰使用時間，請確保在重新生成金鑰期間有一個金鑰滾動更新並重疊，以便：

- Exchange並安裝新的SAK金鑰，並將其繫結到空閒SA。
- 清除舊的SAK金鑰並分配新的空閒SA。

組態範例:

```
<#root>
key chain
M_Key
  macsec
    key 01
      cryptographic-algorithm
        aes-128-cmac
      key-string
        12345678901234567890123456789001
      lifetime 12:59:59 Oct 1 2023 duration 5000
    key 02
      cryptographic-algorithm aes-128-cmac
      key-string 12345678901234567890123456789002
      lifetime 14:00:00 Oct 1 2023 16:15:00 Oct 1 2023
    key 03
      cryptographic-algorithm aes-128-cmac
      key-string 12345678901234567890123456789003
      lifetime 16:15:00 Oct 1 2023 17:15:00 Oct 1 2023
    key 04
      cryptographic-algorithm aes-128-cmac
      key-string 12345678901234567890123456789012
      lifetime 17:00:00 Oct 1 2023 infinite
```

其中粗體字是指：

M_Key：金鑰鏈名稱。

金鑰01：連線關聯金鑰名稱（與CKN相同）。

aes-128-cmac:MKA身份驗證密碼。


12345678901234567890123456789012：連線關聯金鑰(CAK)。

定義策略：

```
<#root>
```


```
mka policy example
  macsec-cipher-suite
gcm-aes-256
```

其中 gcm-aes-256是指用於安全關聯金鑰(SAK)匯出的密碼套件。

 注意：這是基本策略配置，根據實施情況，有更多可用選項(如confidentiality-offset、sak-rekey、include-icv-indicator)等。

Interface:

```
interface TenGigabitEthernet0/1/2
  mtu 2000
  ip address 198.51.100.1 255.255.255.0
  ip mtu 1468
  eapol destination-address broadcast-address
  mka policy example
  mka pre-shared-key key-chain M_Key
  macsec
end
```

 注意：如果未配置或應用mka策略，則預設策略處於啟用狀態，可以通過show mka default-policy detail進行檢視。

802.1x/EAP

如果使用EAP方法，則所有金鑰均從主會話金鑰(MSK)生成。在IEEE 802.1X可擴展身份驗證協定(EAP)框架下，MKA在裝置之間交換EAPoL-MKA幀，EAPoL幀的乙太網型別為0x888E，而EAPoL協定資料單元(PDU)中的資料包主體稱為MACsec金鑰協定PDU(MKPDU)。這些EAPoL幀包含傳送方的CKN、關鍵伺服器優先順序和MACsec功能。

 注意：預設情況下，交換機會處理EAPoL-MKA幀，但不會轉發這些幀。

基於證書的MACsec加密配置示例：

註冊證書 (需要證書頒發機構)：

```
crypto pki trustpoint EXAMPLE-CA
  enrollment terminal
  subject-name CN=ASR1000@user.example, C=IN, ST=KA, OU=ENG,O=Example
  revocation-check none
  rsakeypair mkaioscarsa
```

storage nvram:

```
crypto pki authenticate EXAMPLE-CA
```

需要802.1x身份驗證和AAA配置：

```
aaa new-model
dot1x system-auth-control
radius server ISE
  address ipv4 auth-port 1645 acct-port 1646
  automate-tester username dummy
  key dummy123
  radius-server deadtime 2
!
aaa group server radius ISEGRP
  server name ISE
!
aaa authentication dot1x default group ISEGRP
aaa authorization network default group ISEGRP
```

EAP-TLS配置檔案和802.1X憑證：

```
eap profile EAPTLS-PROF-IOSCA
  method tls
  pki-trustpoint EXAMPLE-CA
!
dot1x credentials EAPTLSCRED-IOSCA
  username asr1000@user.example
  pki-trustpoint EXAMPLE-CA
!
```

Interface:

```
interface TenGigabitEthernet0/1/2
  macsec network-link
  authentication periodic
  authentication timer reauthenticate
  access-session host-mode multi-host
  access-session closed
  access-session port-control auto
  dot1x pae both
  dot1x credentials EAPTLSCRED-IOSCA
  dot1x supplicant eap profile EAPTLS-PROF-IOSCA
  service-policy type control subscriber DOT1X_POLICY_RADIUS
```

排除WAN MACSEC故障

組態

根據平台檢查正確的配置和實施支援；金鑰和引數必須匹配。以下是一些用於識別配置是否存在問題的常見日誌：

```
%MKA-3-INVALID_MACSEC_CAPABILITY : Terminating MKA Session because no peers had the required MACsec Cap
```

檢查對等體硬體的MACsec功能，或通過更改介面的MACsec配置來降低MACsec功能要求。

```
%MKA-3-INVALID_PARAM_SET : %s, Local-TxSCI %s, Peer-RxSCI %s, Audit-SessionID %s
```

有些可選引數是路由器根據配置和平台的不同預設設定所期望或不期望的，請確保在配置中包括或放棄這些引數。

```
%MKA-4-MKA_MACSEC_CIPHER_MISMATCH: Lower/Higher strength MKA-cipher than macsec-cipher for RxSCI %s, Au
```

策略密碼套件上的配置不匹配，請確保正確匹配。

```
%MKA-3-MKPDU_VALIDATE_FAILURE : MKPDU validation failed for Local-TxSCI %s, Peer-RxSCI %s, Audit-Session
```

MKPDU未通過一個或多個後續驗證檢查：

- 有效的MAC地址和EAPOL報頭：檢查兩個介面配置，入口介面上的資料包捕獲可以證實當前值。
- 有效的CKN和演算法靈活性：確保有效的金鑰和演算法套件。
- ICV驗證：ICV驗證是一個可選引數，配置兩端必須匹配。
- MKA有效負載的正確順序存在：可能的互操作性問題。
- 如果存在對等體，則進行MI驗證：成員識別符號驗證，對每個參與者是唯一的。
- 如果存在對等體則進行MN驗證：消息編號驗證，在傳輸的每個MKPDU上唯一，並在每次傳輸時遞增。

操作問題

設定配置後，您可以看到%MKA-5-SESSION_START消息，但需要檢查會話是否啟動，一個好的開

始命令是show mka sessions [interface interface_name]:

<#root>

Router1#

show mka sessions

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

Interface Port-ID	Local-TxSCI Peer-RxSCI	Policy-Name MACsec-Peers	Inherited Status	Key-Server CKN
Te0/1/2	40b5.c133.0e8a/0012			

Example

NO

NO

18 40b5.c133.020a/0012 1

Secured

01

狀態是指控制平面會話；「安全」表示已安裝Rx和Tx SAK，如果沒有，則顯示為「未安全」。

- 如果狀態保持為Init，請檢查物理介面狀態、通過ping連線對等體以及配置匹配。此時，沒有收到的MKPDU和活動對等體，某些平台會進行填充，而另一些平台則不會；請考慮最多32位元組的報頭開銷，並確保較大的MTU以進行正確操作。
- 如果狀態保持為Pending，請檢查控制平面或介面錯誤/丟棄中是否丟棄了MKPDU。
- 如果狀態處於Not Secured狀態，則MKA介面為up狀態，且MKPDU流經但未安裝SAK，此時將顯示下一個日誌：

%MKA-5-SESSION_UNSECURED : MKA Session was not secured for Local-TxSCI %s, Peer-RxSCI %s, Audit-Session

這是因為在MACsec中建立安全通道(SC)和安裝安全關聯(SA)之前，沒有MACsec支援、無效的MACsec配置或本地或對等端上的其他MKA故障。您可以使用detail命令獲取詳細資訊show mka session [interface interface_name] detail:

<#root>

Router1#

show mka sessions detail

MKA Detailed Status for MKA Session

=====

Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI..... 40b5.c133.0e8a/0012
Interface MAC Address.... 40b5.c133.0e8a
MKA Port Identifier..... 18
Interface Name..... TenGigabitEthernet0/1/2
Audit Session ID.....

CAK Name (CKN)..... 01

Member Identifier (MI)... DC5F7E3E38F4210925AAC8CA
Message Number (MN)..... 14462
EAP Role..... NA
Key Server..... NO

MKA Cipher Suite..... AES-128-CMAC

Latest SAK Status..... Rx & Tx
Latest SAK AN..... 0
Latest SAK KI (KN)..... 272DA12A009CD0A3D313FADF00000001 (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..... Example
Key Server Priority..... 2
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..... 0080C20001000002 (GCM-AES-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:

Table with 6 columns: MI, MN, Rx-SCI (Peer), KS Priority, RxSA Installed, SSCI. Row 1: 272DA12A009CD0A3D313FADF, 14712, 40b5.c133.020a/0012, 1, YES, 0

Potential Peers List:

MI	MN	Rx-SCI (Peer)	KS Priority	RxSA Installed	SSCI
----	----	---------------	----------------	-------------------	------

查詢有關對等體的SAK資訊以及突出顯示的相關資料，以便更好地瞭解情況。如果存在不同的SAK，請檢查使用的金鑰以及已配置的生存期或SAK金鑰選項；如果使用預共用金鑰，則可以使用show mka keychain:

<#root>

Router1#

show mka keychains

MKA PSK Keychain(s) Summary...

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

=====

Master_Key

01

Te0/1/2

<HIDDEN>

CAK從未顯示，但您可以驗證金鑰鏈名稱和CKN。

如果已建立作業階段，但您有擺動或間歇性流量傳輸，您必須檢查MKPDU是否在對等體之間正確傳輸；如果有逾時，您可以看到下一訊息：

%MKA-4-KEEPALIVE_TIMEOUT : Keepalive Timeout for Local-TxSCI %s, Peer-RxSCI %s, Audit-SessionID %s, CKN

如果有一個對等體，則MKA會話終止，如果您有多個對等體，並且MKA從其中一個對等體接收了MKPDU的時間超過6秒，則活動對等體將從「活動對等體清單」中刪除，您可以從show mka statistics [interface interface_name]開始：

<#root>

Router1#

show mka statistics interface TenGigabitEthernet0/1/2

```
MKA Statistics for Session
=====
Reauthentication Attempts.. 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..... 0
SAKs Received..... 1
SAK Responses Received.. 0
```

MKPDU Statistics

```
MKPDUs Validated & Rx... 11647
```

```
"Distributed SAK".. 1
"Distributed CAK".. 0
```

```
MKPDUs Transmitted..... 11648
```

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

傳送和接收的MKPDU必須有一個對等點的共同編號，確保在Rx和Tx兩端增加，以確定或引導有問題的方向，如果存在差異，您可以啟用debug mka linksec-interface frames兩端：

```
*Sep 20 21:14:10.803: MKA-LLI-MKPDU: Received CKN length (2 bytes) from Peer with CKN 01
*Sep 20 21:14:10.803: MKA-LLI-MKPDU: MKPDU Received: Interface: [Te0/1/2 : 18] Peer MAC: 40:B5:C1:33:02
*Sep 20 21:14:12.101: MKA-LLI-MKPDU: MKPDU transmitted: Interface [Te0/1/2: 18] with CKN 01
*Sep 20 21:14:12.803: MKA-LLI-MKPDU: Received CKN length (2 bytes) from Peer with CKN 01
*Sep 20 21:14:12.803: MKA-LLI-MKPDU: MKPDU Received: Interface: [Te0/1/2 : 18] Peer MAC: 40:B5:C1:33:02
```

如果沒有收到MKPDU，請查詢傳入介面錯誤或丟棄、對等體介面和mka會話的狀態；如果兩個路由器都傳送但未接收，則MKPDU在介質上丟失，需要檢查中間裝置是否正確轉發。

如果不傳送MKPDU，請檢查物理介面狀態（線路和錯誤/丟棄）和配置；檢查是否在控制平面級別生成這些資料包，FIA跟蹤和嵌入式資料包捕獲(EPC)是實現這一目的的可靠工具。請參閱[使用 Cisco IOS XE資料路徑資料包跟蹤功能進行故障排除](#)

您可以使用debug mka events並查詢原因以指導後續步驟。

 **注意：**請謹慎使用debug mka和debug mka診斷，因為它們顯示可能導致路由器上控制平面問題的狀態機和非常詳細的資訊。

如果作業階段已安全且穩定，但流量沒有流動，請檢查是否加密流量正在傳送兩個對等點：

<#root>

Router1#

show macsec statistics interface TenGigabitEthernet 0/1/2

MACsec Statistics for TenGigabitEthernet0/1/2

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: 98020

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

Egress Encrypted Octets: 98012

Controlled Port Counters

IF In Octets:	595380
IF In Packets:	5245
IF In Discard:	0
IF In Errors:	0
IF Out Octets:	596080
IF Out Packets:	5254
IF Out Errors:	0

Transmit SC Counters (SCI: 40B5C1330E8B0013)

Out Pkts Protected:	0
---------------------	---

Out Pkts Encrypted: 970

Transmit SA Counters (AN 0)

Out Pkts Protected:	0
---------------------	---

Out Pkts Encrypted: 970

Receive SA Counters (SCI: 40B5C133020B0013 AN 0)

In Pkts Unchecked:	0
In Pkts Delayed:	0

In Pkts OK: 967

In Pkts Invalid: 0

In Pkts Not Valid:	0
--------------------	---

In Pkts Not using SA:	0
In Pkts Unused SA:	0
In Pkts Late:	0

SecY計數器是物理介面上的當前資料包，而其它與Tx安全通道相關的計數器表示正在加密和傳輸的資料包，而Rx安全關聯表示介面上接收的有效資料包。

更多調試(如debug mka errors和debug mka packets)可幫助確定問題，請謹慎使用最後一個，因為這樣會引起大量日誌記錄。

相關資訊

- [MACsec和MKA配置指南](#)
- [思科技術支援與下載](#)

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）。