

# 排除路由器上的WAN MACSEC故障

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[拓扑](#)

[MACSEC故障排除概述](#)

[MACsec数据包格式](#)

[WAN-MACSEC](#)

[WAN MACSEC数据包格式](#)

[WAN MACSEC术语](#)

[MACSEC密钥协议\(MKA\)和加密概述](#)

[预共享密钥](#)

[802.1x/EAP](#)

[排除WAN MACSEC故障](#)

[配置](#)

[运营问题](#)

[相关信息](#)

---

## 简介

本文档介绍用于了解Cisco IOS® XE路由器的操作和故障排除的基本WAN MACSEC协议。

## 先决条件

### 要求

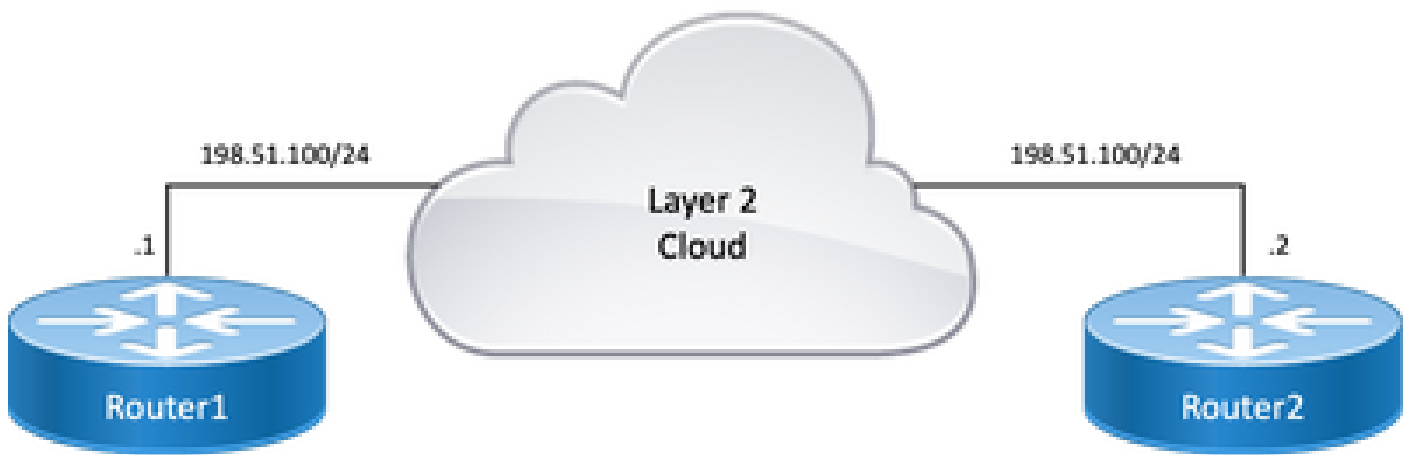
本文档没有任何特定的前提条件。

### 使用的组件

本文档中的信息特定于Cisco IOS XE路由器，如ASR 1000、ISR 4000和Catalyst 8000系列。寻找特定硬件和软件MACSEC支持。

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。

## 拓扑



拓扑图

## MACSEC故障排除概述

MACsec是基于IEEE 802.1AE标准的第2层逐跳加密，为具有AES-128加密的媒体访问控制协议提供数据机密性、数据完整性和数据来源验证，使用MACsec只能保护面向主机的链路(网络访问设备与终端设备 (例如PC或IP电话) 之间的链路)。

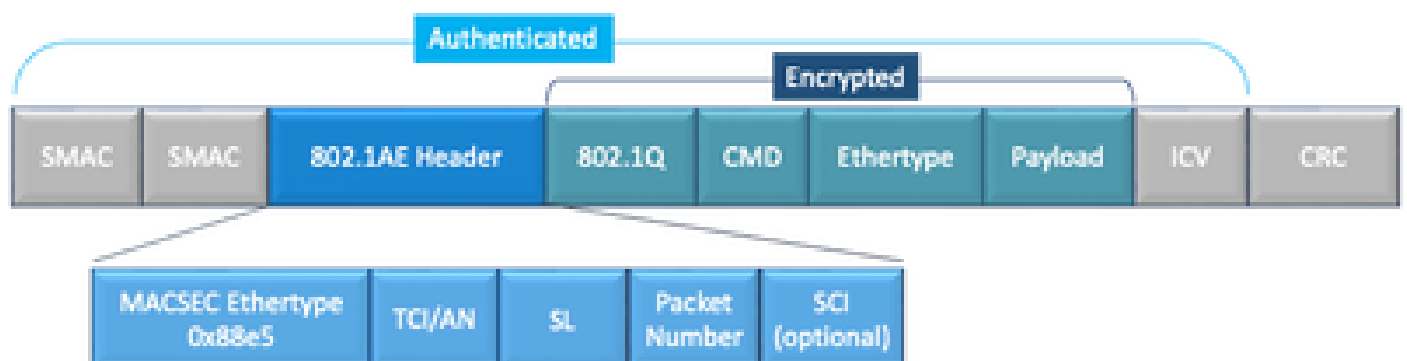
- 数据包在入口端口上解密。
- 数据包在设备中是透明的。
- 数据包在出口端口上进行加密。

MACsec可在有线LAN上提供安全通信，当MACsec用于保护LAN上终端之间的通信时，线上的每个数据包都使用对称密钥加密进行加密，这样便无法监控或更改线上的通信。当MACsec与安全组标记(SGT)配合使用时，它会为标记以及帧负载中包含的数据提供保护。

MACsec通过使用带外加密密钥方法提供有线网络上的MAC层加密。

## MACsec数据包格式

使用802.1AE(MACsec)时，使用完整性检查值(ICV)对帧进行加密和保护，不会影响IP MTU或分段，并且最小的L2 MTU影响：约40字节 (小于小巨型帧)。



MACSEC数据包格式示例

- MACsec EtherType: 0x88e5，表示该帧为MACsec帧。
- TCI/AN:标记控制信息/关联编号。如果单独使用机密性或完整性，则为MACsec版本号。
- SL：加密数据的长度。
- PN:用于重放保护的数据包编号。
- SCI:安全通道标识符。每个连接关联(CA)都是一个虚拟端口（物理接口的MAC地址加上16位端口ID）。
- ICV:完整性检查值。

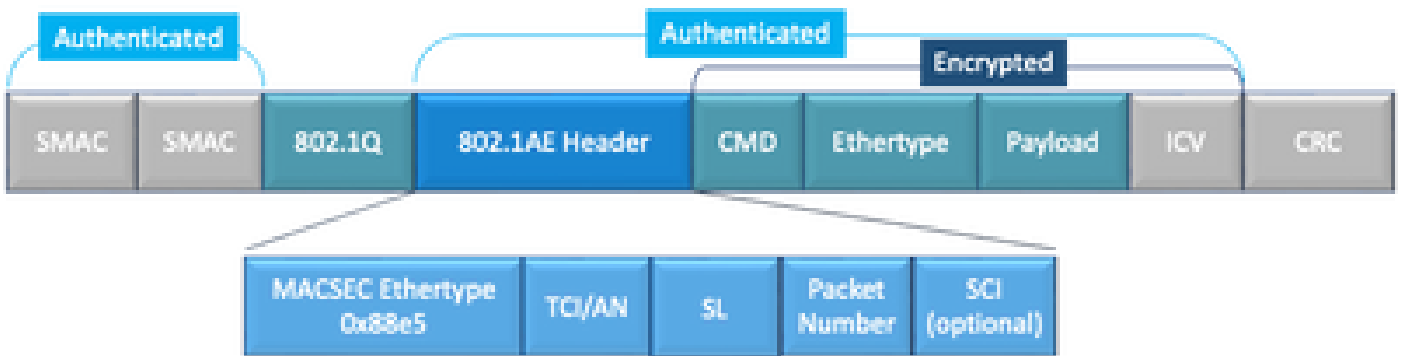
## WAN-MACSEC

以太网已经超越了私有LAN传输，包括各种WAN或MAN传输选项。WAN MACSEC使用AES 128或256位跨第2层以太网WAN服务提供点对点或点对多点端到端加密。

WAN MACsec基于(LAN)MACsec，因此使用名称（并与IPsec分离），但提供了一些之前无法提供的附加功能。

### WAN MACSEC数据包格式

如果标记已加密，则服务提供商可能不支持MACsec以太网类型且无法区分L2服务，因此WAN MACSEC会对802.1Q报头之后的帧的所有内容进行加密：



明文数据包格式中的WAN MACSEC 802.1Q标记示例

其中一个新的增强功能包括Clear中的802.1Q Tags（也称为ClearTag）。通过此增强功能，可以在加密MACsec报头外显示802.1Q标记。如果显示此字段，则会为MACsec提供多个设计选项；对于公共运营商机以太网传输提供商，则必须使用某些传输服务。

MKA功能支持以明文形式提供隧道信息，例如VLAN标记（802.1Q标记），因此服务提供商可以提供服务多路复用，以便多个点对点或多点服务可以在单个物理接口上共存，并根据现在可见的VLAN ID进行区分。

除了服务多路复用，清除中的VLAN标记还使服务提供商能够根据802.1P(CoS)字段（现在作为802.1Q标记的一部分可见）通过SP网络为加密的以太网数据包提供服务质量(QoS)。

### WAN MACSEC术语

MKA	IEEE 802.1XREV-2010中定义的MACSec密钥协议 — 用于发现MACSec对等体和协商密钥的密钥协议协议。
-----	--

MSK	主会话密钥，在EAP交换期间生成。请求方和身份验证服务器使用MSK生成CAK
CAK	连接关联密钥源自MSK。是长期主密钥，用于生成用于MACSec的所有其他密钥。
CKN	连接关联密钥名称 — 标识CAK。
SAK	安全关联密钥 — 从CAK派生，是请求方和交换机用于加密给定会话流量的密钥。
KS	密钥服务器负责： <ul style="list-style-type: none"> <li>• 选择和通告密码套件</li> <li>• 从CAK生成SAK。</li> </ul>
KEK	密钥加密密钥 — 用于保护MACsec密钥(SAK)

## MACSEC密钥协议(MKA)和加密概述

MKA是WAN MACsec使用的控制平面机制；在IEEE标准802.1X中指定，用于发现相互验证的MACsec对等体以及后续操作：

- 建立和管理CA ( 连接关联 )。
- 管理实时/潜在对等体列表。
- 密码套件协商。
- 在CA成员中选择密钥服务器(KS)。
- 安全关联密钥(SAK)派生和管理。
- 安全密钥分发。
- 密钥安装。
- 重新生成密钥。

一个成员根据配置的密钥服务器优先级 ( 最低 ) 被选为密钥服务器，如果对等体中的KS优先级相同，则最低SCI优先。

KS仅在所有潜在对等体都成为活动对等体且至少有一个活动对等体之后生成SAK。它使用MKA PDU或MKPDU以加密格式将使用的SAK和密码分发给其他参与者。

参与者检查SAK发送的密码，如果支持，则安装该密码，在每个MKPDU上使用它来表示他们拥有的最新密钥；否则，他们应拒绝SAK

如果参与者在3个心跳后没有收到MKPDU ( 每个心跳默认为2秒 )，则从实时对等体列表中删除对等体；例如，如果客户端断开，交换机上的参与者继续运行MKA，直到从客户端收到最后一个MKPDU后发生3个心跳为止。

对于此过程，有两种方法可驱动加密密钥：

- 预共享密钥
- 802.1x/EAP

## 预共享密钥

如果使用预共享密钥，必须手动输入CAK=PSK和CKN。对于密钥使用时间，请确保在重新生成密钥期间进行密钥滚动和重叠，以便：

- Exchange并安装新的SAK密钥并将其绑定到空闲SA。
- 清除旧的SAK密钥并分配新的空闲SA。

配置示例：

```
<#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
```

其中粗体字是指：

**M\_Key**：密钥链名称。

**密钥01**：连接关联密钥名称（与CKN相同）。

**aes-128-cmac**:MKA身份验证密码。

**12345678901234567890123456789012**：连接关联密钥(CAK)。


定义策略：

```
<#root>
```

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

其中 gcm-aes-256是指用于安全关联密钥(SAK)衍生的密码套件。

---


 注：这是基本策略配置，根据实施情况，有更多可用选项(如confidentiality-offset、sak-rekey、include-icv-indicator等)和更多选项。

---

接口:

```
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：如果未配置或应用mka策略，则启用默认策略，并可通过show mka default-policy detail查看。

---

## 802.1x/EAP

如果使用EAP方法，则所有密钥均从主会话密钥(MSK)生成。借助IEEE 802.1X可扩展身份验证协议(EAP)框架，MKA在设备之间交换EAPoL-MKA帧，EAPoL帧的以太网类型为0x888E，而EAPoL协议数据单元(PDU)中的数据主体称为MACsec密钥协议PDU(MKPDU)。这些EAPoL帧包含发送方的CKN、密钥服务器优先级和MACsec功能。

---

 注：默认情况下，交换机处理EAPoL-MKA帧，但不转发这些帧。

---

基于证书的MACsec加密配置示例：

注册证书（需要证书颁发机构）：

```
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身份验证和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配置文件和802.1X凭证：

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

接口：

```
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

### 配置

根据平台检查正确的配置和实施支持；密钥和参数必须匹配。确定配置是否有问题的一些常见日志是以下日志：

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

检查对等体硬件的MACsec功能或通过更改接口的MACsec配置来降低MACsec功能要求。

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

有些可选参数路由器可以根据配置和平台的不同默认设置来预测或不预测，请确保在配置中包括或丢弃这些参数。

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

策略密码套件上的配置不匹配，请确保正确匹配。

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

MKPDU未通过一个或多个后续验证检查：

- 有效的MAC地址和EAPOL报头：检查两个接口配置，入口接口上的数据包捕获可以证实当前值。
- 有效的CKN和算法灵活性：确保密钥和算法套件有效。
- ICV验证：ICV验证是一个可选参数，配置两端必须匹配。
- MKA有效负载的正确顺序：可能的互操作性问题。
- 如果存在对等体，则进行MI验证：成员标识符验证，对每个参与者是唯一的。
- 如果存在对等体则进行MN验证：消息编号验证，在传输的每个MKPDU上是唯一的，并在每次传输时递增。

### 运营问题

设置配置后，您可以看到%MKA-5-SESSION\_START消息，但需要检查会话是否启动，一个好的开



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

状态是指控制平面会话；“安全”表示已安装Rx和Tx SAK，如果没有，则显示为“未安全”。

- 如果状态保持在Init上，请检查物理接口状态，通过ping检查对等体的连接性和配置匹配。此时，没有收到和处于活动状态的MKPDU对等体，某些平台会进行填充，而另一些平台则不会；请考虑最多32字节的报头开销，并确保较大的MTU以进行正确操作。
- 如果状态保持为Pending，请检查是否在控制平面或接口错误/丢弃中丢弃了入口或出口MKPDU。
- 如果状态保持为Not Secured（未保护），则MKA接口为up（打开）状态，MKPDU流经，但SAK未安装，在这种情况下，将会显示下一个日志：

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

这是因为在MACsec中建立安全通道(SC)和安装安全关联(SA)之前，本地或对等端没有MACsec支持、无效的MACsec配置或其他MKA故障。您可以使用detail命令获取有关show mka session [interface interface\_name] detail的详细信息：

<#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:

MI	MN	Rx-SCI (Peer)	KS Priority	RxSA Installed	SSCI
272DA12A009CD0A3D313FADF	14712	40b5.c133.020a/0012	1	YES	0

Potential Peers List:

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

-----

查找有关对等体的SAK信息以及突出显示的相关数据，以便更好地了解情况。如果存在不同的SAK，请检查使用的密钥以及已配置的SAK密钥选项和生存期，如果使用预共享密钥，则可以使用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从未显示，但您可以证实密钥链名称和CKN。

如果会话已建立，但您有抖动或间歇性流量，则必须检查MKPDU是否在对等体之间正确流动，如果超时，您会看到下一条消息：

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

如果有一个对等体，则MKA会话终止，如果您有多个对等体，并且MKA从其中一个对等体接收了MKPDU超过6秒钟，则Live Peer会从Live Peers List中删除，您可以从show mka statistics [interface interface\_name]开始：

<#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
```

发送和接收的MKPDU必须有一个对等体的相似编号，确保它们在Rx和Tx两端增加，以确定或引导有问题的方向，如果存在差异，您可以启用debug mka linksec-interface frames:


```
*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
```

如果没有收到MKPDU，请查找传入接口错误或丢弃、对等体接口和mka会话的状态；如果两个路由器正在发送但未接收，则MKPDU在介质上丢失，需要检查中间设备是否正确转发。

如果您不发送MKPDU，请检查物理接口状态（线路和错误/丢弃）和配置；检查您是否在控制平面级别生成这些数据包，FIA跟踪和嵌入式数据包捕获(EPC)是达到此目的的可靠工具。请参阅[使用Cisco IOS XE数据路径数据包跟踪功能进行故障排除](#)

您可以使用debug mka events并查找原因以指导后续步骤。

---

 **注意：**请谨慎使用debug mka和debug mka diagnostics，因为它们显示可能导致路由器控制平面问题的状态机和非常详细的信息。

---

如果会话安全且稳定，但流量未流动，请检查发送两个对等体的加密流量：

<#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计数器是物理接口上的当前数据包，而其他计数器与Tx安全通道相关，表示数据包被加密和传输，而Rx安全关联表示接口上接收的有效数据包。

更多调试(例如debug mka errors 和debug mka packets 有助于识别问题)，请谨慎使用最后一个，因为这样会引起大量日志记录。

## 相关信息

- [MACsec和MKA配置指南](#)
- [思科技术支持和下载](#)

## 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）。