# Solucionar problemas de WAN MACSEC en routers

## Contenido



## Introducción

Este documento describe el protocolo MACSEC de WAN básico para comprender el funcionamiento y la resolución de problemas de los routers Cisco IOS® XE.

## Prerequisites

### Requirements

No hay requisitos previos específicos para este documento.

### Componentes Utilizados

La información de este documento es específica para los routers Cisco IOS XE, como las familias ASR 1000, ISR 4000 y Catalyst 8000. Busque compatibilidad específica con MACSEC de hardware y software.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Topología

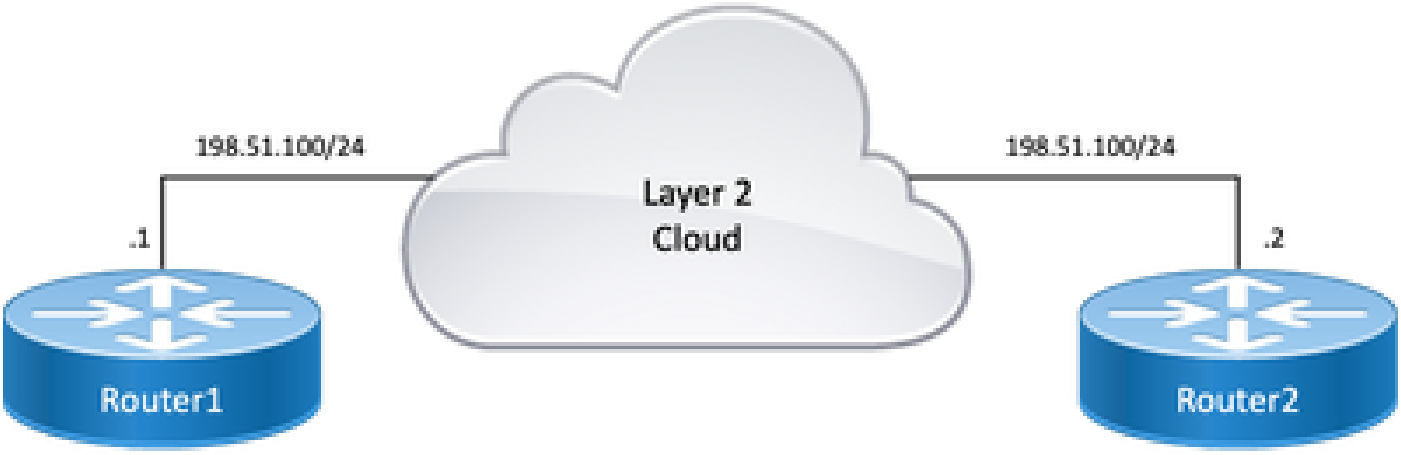



Diagrama de topología

# Descripción general de MACSEC para solucionar problemas

MACsec es un cifrado salto a salto de nivel 2 basado en el estándar IEEE 802.1AE que proporciona confidencialidad de datos, integridad de datos y autenticación de origen de datos para protocolos independientes de acceso a medios con cifrado AES-128. Solo los enlaces orientados al host (enlaces entre dispositivos de acceso a la red y dispositivos terminales como un PC o un teléfono IP) se pueden proteger mediante MACsec.

- Los paquetes se descifran en el puerto de ingreso.
- Los paquetes están claros en el dispositivo.
- Los paquetes se cifran en el puerto de salida.

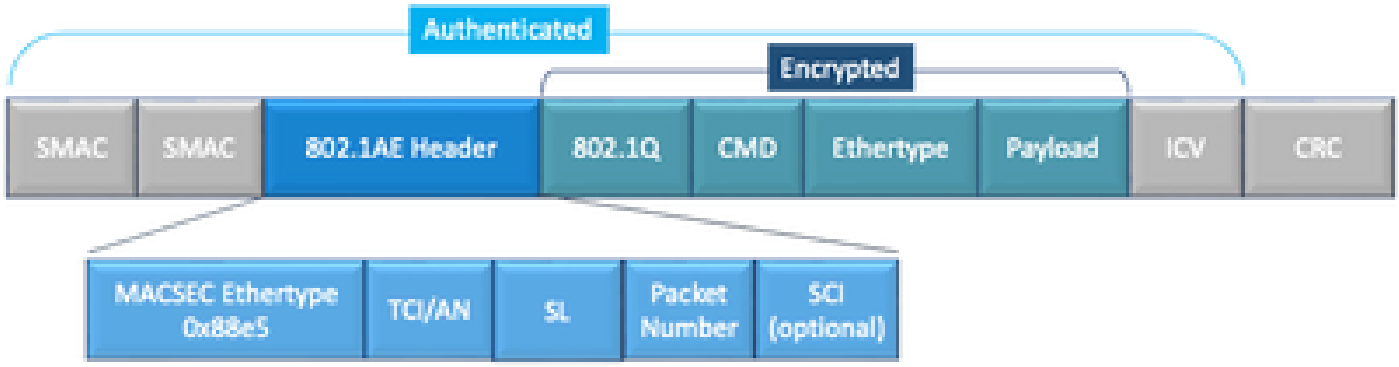
MACsec proporciona una comunicación segura en LAN por cable; cuando MACsec se utiliza para proteger la comunicación entre los terminales de una LAN, cada paquete del cable se cifra mediante criptografía de clave simétrica, de modo que la comunicación no se puede supervisar ni modificar en el cable. Cuando MACsec se utiliza junto con etiquetas de grupos de seguridad (SGT), proporciona protección para la etiqueta junto con los datos contenidos en la carga útil de la trama.

MACsec proporciona cifrado de capa MAC en redes con cables mediante el uso de métodos fuera de banda para la clave de cifrado.

## Formato de paquete MACsec

Con 802.1AE (MACsec), las tramas se cifran y protegen con un valor de comprobación de

integridad (ICV) sin impacto en la MTU de IP ni en la fragmentación, y con un impacto mínimo en la MTU de L2: ~40 bytes (menos que la trama Baby Giant).




Ejemplo de Formato de Paquete MACSEC

- MACsec EtherType: 0x88e5, designa que la trama es una trama MACsec.
- TCI/AN: Información de control de ETIQUETAS/Número de asociación. Es el número de versión de MACsec si la confidencialidad o la integridad se utilizan de forma independiente.
- SL: longitud de los datos cifrados.
- PN: número de paquete utilizado para la protección de reproducción.
- SCI: identificador de canal seguro. Cada asociación de conectividad (CA) es un puerto virtual (dirección MAC de la interfaz física más un ID de puerto de 16 bits).
- ICV: Valor de comprobación de integridad.

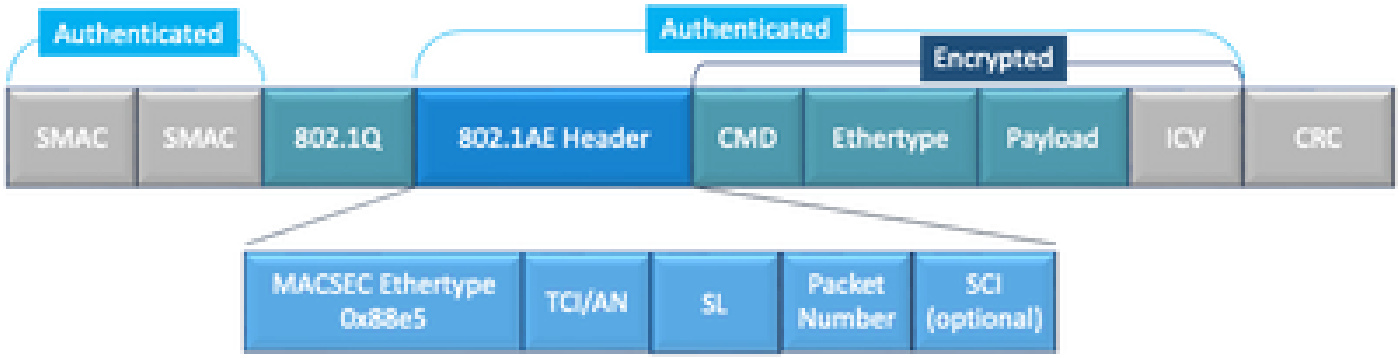
# WAN-MACSEC

Ethernet ha evolucionado más allá del transporte de LAN privada para incluir diversas opciones de transporte WAN o MAN. WAN MACSEC proporciona cifrado de extremo a extremo en el servicio WAN Ethernet de capa 2, ya sea punto a punto o punto a multipunto mediante AES de 128 o 256 bits.

WAN MACsec se basa en (LAN) MACsec, de ahí el nombre (e independiente de IPsec), pero ofrece varias funciones adicionales que no estaban disponibles anteriormente.

## Formato de paquete WAN MACSEC

Existe la posibilidad de que el proveedor de servicios no admita MACsec ethertype y no pueda diferenciar el servicio L2 si la etiqueta está cifrada de modo que WAN MACSEC cifra toda la trama después de los encabezados 802.1Q:




Ejemplo de Etiqueta WAN MACSEC 802.1Q en el Formato Clear Packet

Una de las nuevas mejoras incluye las etiquetas 802.1Q en Clear (también denominado ClearTag). Esta mejora habilita la capacidad de exponer la etiqueta 802.1Q fuera del encabezado MACsec cifrado. La exposición de este campo proporciona varias opciones de diseño con MACsec, y en el caso de los proveedores de transporte de Ethernet de operadores públicos, es necesario para aprovechar determinados servicios de transporte.

La compatibilidad con la función MKA proporciona información de tunelización, como la etiqueta VLAN (etiqueta 802.1Q) en la nube, de modo que el proveedor de servicios puede proporcionar multiplexación de servicios de modo que varios servicios punto a punto o multipunto puedan coexistir en una única interfaz física y diferenciarse en función del ID de VLAN ahora visible.

Además de la multiplexación de servicios, la etiqueta de VLAN en el modo sin cifrar también permite a los proveedores de servicios proporcionar calidad de servicio (QoS) al paquete Ethernet cifrado a través de la red SP en función del campo 802.1P (CoS) que ahora es visible como parte de la etiqueta 802.1Q.

## Terminología MACSEC de WAN

| | |
|---|---|
| MKA | Acuerdo de clave MACSec, definido en IEEE 802.1XREV-2010: protocolo de acuerdo de clave para descubrir pares MACSec y negociar claves. |
| MSK | Clave de sesión maestra, generada durante el intercambio EAP. El suplicante y el servidor de autenticación utilizan el MSK para generar el CAK |
| PASTEL | La clave de asociación de conectividad deriva de MSK. Es una clave maestra de larga duración que se utiliza para generar todas las demás claves utilizadas para MACSec. |
| CKN | Nombre de clave de asociación de conectividad: identifica el CAK. |
| PREGUNTAR | Secure Association Key (Clave de asociación segura): Derivada del CAK y es la clave que utilizan el solicitante y el switch para cifrar el tráfico de una sesión determinada. |
| KS | Servidor de claves responsable de:<br>• Selección y publicidad de un conjunto de cifrado<br>• Generando el SAK del CAK. |

| | |
|---|---|
| KEK | Clave de cifrado de clave: se utiliza para proteger las claves MACsec (SAK) |

## Descripción general del protocolo MACSEC Key Agreement Protocol (MKA) y la criptografía

MKA es el mecanismo del plano de control que utiliza WAN MACsec; se especifica en la norma IEEE 802.1X, que detecta los pares MACsec autenticados mutuamente, además de las siguientes acciones:

- Establece y gestiona una CA (asociación de conectividad).
- Gestiona la lista de pares activos/potenciales.
- Negociación de conjunto de cifrado.
- Selecciona el servidor de claves (KS) entre los miembros de una CA.
- Derivación y gestión de la clave de asociación segura (SAK).
- Distribución de clave segura.
- Instalación de claves.
- Rekey.

Un miembro se elige como servidor de claves según la prioridad de servidor de claves configurada (más baja); si la prioridad KS es la misma entre los pares, el SCI más bajo gana.

KS genera un SAK solo después de que todos los peers potenciales se hayan convertido en live y haya, al menos, un peer vivo. Distribuye el SAK y el código usado a otros participantes usando la PDU o MKPDU de MKA en un formato cifrado.

Los participantes comprueban el código enviado por el SAK y lo instalan si es compatible, utilizándolo en cada MKPDU para indicar la última clave que tienen; de lo contrario, rechazarán el SAK

Cuando no se recibe ninguna MKPDU de un participante después de 3 latidos (cada latido es de 2 segundos de forma predeterminada), los peers se eliminan de la lista de peers activos; por ejemplo, si un cliente se desconecta, el participante en el switch continúa operando MKA hasta que han transcurrido 3 latidos después de que se reciba la última MKPDU del cliente.

Para este proceso, hay dos métodos para controlar las claves de cifrado:

- Claves previamente compartidas
- 802.1x/EAP

Claves previamente compartidas

Si utiliza claves previamente compartidas, CAK=PSK y CKN deben introducirse manualmente. Para el tiempo de vida de la clave, asegúrese de que tiene una sustitución y superposición de claves durante el tiempo de actualización de claves para:

- Intercambie e instale la nueva clave SAK y enlácela a SA inactiva.
- Purgue la clave SAK antigua y asigne una nueva SA inactiva.

Ejemplo de configuración:

<#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
```

Donde las palabras en negrita se refieren a:
M_Key: Nombre de la cadena de claves.

key 01: nombre de la clave de asociación de conectividad (igual que CKN).

aes-128-cmac: cifrado de autenticación MKA.

12345678901234567890123456789012: Clave de asociación de conectividad (CAK).

Definir política:

<#root>

```
mka policy example
 macsec-cipher-suite
```

**gcm-aes-256**

Where gcm-aes-256 hace referencia a conjuntos de cifrado para derivación de clave de asociación segura (SAK).

Nota: Se trata de una configuración de política básica; hay más opciones, como confidencialidad-offset, sak-rekey, include-icv-indicator y más disponibles para su uso, según la implementación.

Interfaz:

```
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
```

Nota: Si no se configura o aplica ninguna política mka, la política predeterminada se habilita y se puede revisar mediante show mka default-policy detail.

802.1x/EAP

Si utiliza el método EAP, todas las claves se generan a partir de la clave de sesión maestra (MSK). Con el marco de protocolo de autenticación ampliable (EAP) IEEE 802.1X, MKA intercambia tramas EAPoL-MKA entre dispositivos; el tipo Ether de tramas EAPoL es 0x888E, mientras que el cuerpo del paquete en una unidad de datos de protocolo (PDU) EAPOL se denomina PDU de acuerdo de clave MACsec (MKPDU). Esas tramas EAPoL contienen el CKN del remitente, la prioridad del servidor de claves y las capacidades MACsec.

Nota: De forma predeterminada, los switches procesan tramas EAPoL-MKA pero no las reenvían.

Ejemplo de configuración de cifrado MACsec basado en certificados:

Inscripción del certificado (requiere autoridad de certificación):

```
  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
```

Autenticación 802.1x y configuración AAA necesarias:

```
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
```

Perfil EAP-TLS y credenciales 802.1X:

```
eap profile EAPTLS-PROF-IOSCA
 method tls
 pki-trustpoint EXAMPLE-CA
!

dot1x credentials EAPTLSCRED-IOSCA
 username asr1000@user.example
 pki-trustpoint EXAMPLE-CA
!
```

Interfaz:

```
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
```

## Solucionar problemas de WAN MACSEC

Configuración

Verifique la configuración adecuada y el soporte de implementación según la plataforma; las claves y los parámetros deben coincidir. Algunos de los registros comunes para identificar si hay un problema en la configuración son los siguientes:

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

Verifique la capacidad MACsec del hardware de los pares o reduzca los requisitos para la capacidad MACsec cambiando la configuración MACsec para la interfaz.

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

Hay algunos parámetros opcionales que el router puede esperar o no en función de la configuración y de los diferentes valores predeterminados de la plataforma; asegúrese de incluir o descartar la configuración.

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

Hay una discordancia de configuración en el conjunto de cifrado de políticas, asegúrese de que la coincidencia sea correcta.

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

MKPDU no pasó una o más de las siguientes comprobaciones de validación:

- Dirección MAC y encabezado EAPOL válidos: verifique la configuración de ambas interfaces, la captura de paquetes en la interfaz de ingreso puede corroborar los valores actuales.
- CKN y agilidad de algoritmo válidos: garantice claves y conjuntos de algoritmos válidos.
- Verificación ICV: la verificación ICV es un parámetro opcional, la configuración de ambos extremos debe coincidir.
- Existencia de orden correcto de cargas útiles MKA: posible problema de interoperabilidad.
- Verificación de IM si existen pares: verificación del identificador de miembro, único para cada participante.
- Verificación de MN si existen peers: Verificación de número de mensaje, único en cada MKPDU transmitido e incrementa en cada transmisión.

Problemas operativos

Una vez establecida la configuración, puede ver el mensaje %MKA-5-SESSION_START pero necesita verificar si la sesión aparece, un buen comando para comenzar es 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**

El estado se refiere a la sesión del plano de control; Seguro significa que Rx y Tx SAK están instalados; si no lo están, se muestran como No protegido.

- Si el estado permanece en Init, verifique el estado de la interfaz física, la conectividad a través de ping para los pares y la coincidencia de la configuración. En este punto no hay pares MKPDU recibidos y activos, algunas plataformas no rellenan mientras que otras no; considere hasta 32 bytes de sobrecarga de encabezado y asegúrese de una MTU más grande para un funcionamiento correcto.
- Si el estado permanece en Pendiente, verifique si MKPDU se descarta en el plano de control de ingreso o egreso o si se descartan errores/descartes de interfaces.
- Si el estado permanece en No protegido, la interfaz MKA está activa y las MKPDU fluyen a través pero SAK no está instalado, en este caso se ve el siguiente registro:

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

Esto se debe a que no hay compatibilidad con MACsec, a que la configuración MACsec no es válida o a que se ha producido un error de MKA en el lado local o del mismo nivel antes de establecer un canal seguro (SC) y de instalar asociaciones seguras (SA) en MACsec. Puede utilizar el comando detail para obtener más información 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:
  MI                       MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                            Priority  Installed
  ------------------------------------------------------------------------------------
  272DA12A009CD0A3D313FADF  14712       40b5.c133.020a/0012  1         YES            0


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

Busque información SAK sobre pares y datos relevantes resaltados para entender mejor la situación, si hay diferentes SAK en su lugar, examine la clave utilizada y las opciones de rekey de duración o SAK configuradas, si se utilizan claves previamente compartidas puede utilizar show mka keychains:

<#root>

```
Router1#
show mka keychains


MKA PSK Keychain(s) Summary...

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

Master_Key


01

                                                          Te0/1/2
                 <HIDDEN>
```

Nunca se muestra CAK, pero puede corroborar el nombre del llavero y CKN.

Si se ha establecido la sesión pero tiene inestabilidades o flujo de tráfico intermitente, debe verificar si las MKPDU fluyen correctamente entre los pares; si hay un tiempo de espera, puede ver el siguiente mensaje:

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

Si hay un peer, la sesión MKA se termina, en caso de que tenga múltiples peers y MKA no haya recibido una MKPDU de uno de sus peers por más de 6 segundos, el Peer vivo se elimina de la lista de peers activos, puede comenzar con show mka statistics [interface interface_name]:

<#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
```

Las MKPDU transmitidas y recibidas deben tener números similares para un par, asegúrese de que aumenten en Rx y Tx ambos extremos, para determinar o guiar la dirección problemática, si hay diferencias puede habilitar debug mka linksec-interface frames ambos extremos:

```
*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
```

En caso de que no se reciba ninguna MKPDU, busque errores o caídas de la interfaz entrante, el estado de las interfaces de peers y la sesión mka; en caso de que ambos routers envíen pero no reciban, las MKPDU se pierden en los medios y deben verificar los dispositivos intermedios para un reenvío correcto.

Si no envía MKPDU, verifique el estado de la interfaz física (línea y errores/caídas) y la configuración; examine si está generando esos paquetes en el nivel del plano de control, el seguimiento FIA y la captura de paquetes incrustada (EPC) son herramientas confiables para este propósito. Consulte Solución de Problemas con la Función Cisco IOS XE Datapath Packet Trace

Puede utilizar debug mka events y buscar razones para guiar los siguientes pasos.

---

Nota: Utilice con precaución debug mka y debug mka diagnostics ya que muestran la máquina de estado e información muy detallada que puede causar problemas de plano de control en el router.

---

Si la sesión es segura y estable pero el tráfico no fluye, verifique si el tráfico cifrado envía a ambos peers:

<#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
```

Los contadores SecY son paquetes actuales en la interfaz física, mientras que los otros están relacionados con el Tx Secure Channel significa que los paquetes se están cifrando y transmitiendo y Rx Secured Association significa paquetes válidos recibidos en la interfaz.

Más depuraciones como debug mka errors y debug mka packets ayudan en la identificación de problemas, por favor utilice esta última con precaución ya que puede inducir un registro pesado.

## Información Relacionada

- Guía de configuración de MACsec y MKA
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).