Fehlerbehebung bei WAN MACSEC auf Routern

Inhalt

Einleitung

In diesem Dokument wird das grundlegende WAN-MACSEC-Protokoll beschrieben, um die Funktionsweise und die Fehlerbehebung für Cisco IOS® XE-Router zu verstehen.

Voraussetzungen

Anforderungen

Es sind keine besonderen Voraussetzungen erforderlich, um den Inhalt dieses Dokuments nachzuvollziehen.

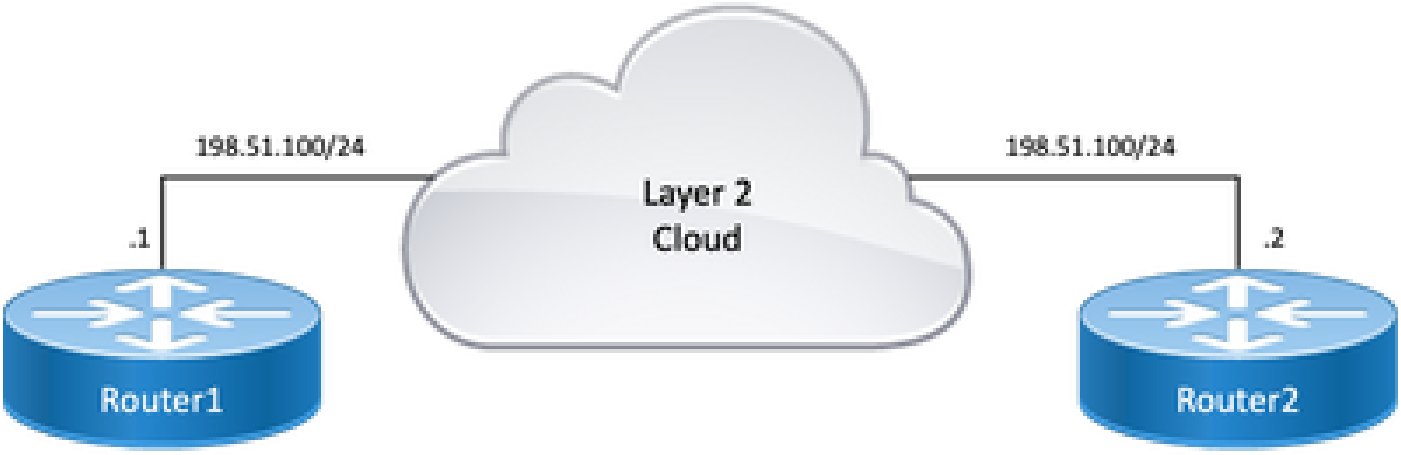
Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich speziell auf Cisco IOS XE-Router wie die Produktreihen ASR 1000, ISR 4000 und Catalyst 8000. Achten Sie auf speziellen MACSEC-Support für Hardware und Software.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher,

dass Sie die möglichen Auswirkungen aller Befehle kennen.

Topologie



Topologiediagramm

MACSEC-Übersicht zur Fehlerbehebung

MACsec ist eine standardbasierte Layer-2-Hop-by-Hop-Verschlüsselung nach IEEE 802.1AE, die Datenvertraulichkeit, Datenintegrität und Datenursprungsauthentifizierung für medienzugriffsunabhängige Protokolle mit AES-128-Verschlüsselung bietet. Nur hostseitige Verbindungen (Verbindungen zwischen Netzwerkzugriffsgeräten und Endgeräten wie einem PC oder IP-Telefon) können mit MACsec gesichert werden.

- Pakete werden am Eingangsport entschlüsselt.
- Die Pakete sind auf dem Gerät eindeutig.
- Pakete werden am Ausgangsport verschlüsselt.

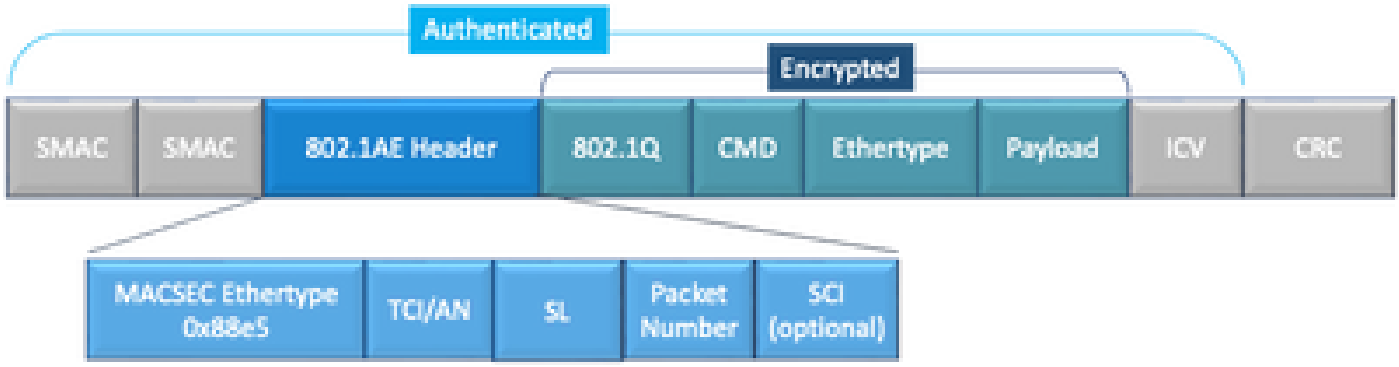
MACsec bietet sichere Kommunikation in kabelgebundenen LANs. Wenn MACsec verwendet wird, um die Kommunikation zwischen Endpunkten in einem LAN zu sichern, wird jedes Paket in der Leitung mithilfe einer Verschlüsselung mit symmetrischem Schlüssel verschlüsselt, sodass die Kommunikation in der Leitung nicht überwacht oder geändert werden kann. Wenn MACsec in Verbindung mit Security Group Tags (SGTs) verwendet wird, bietet es Schutz für das Tag zusammen mit den Daten, die in der Nutzlast des Frames enthalten sind.

MACsec ermöglicht die Verschlüsselung auf MAC-Ebene über kabelgebundene Netzwerke mithilfe von Out-of-Band-Methoden für die Verschlüsselung.

MACsec-Paketformat

Mit 802.1AE (MACsec) werden Frames verschlüsselt und mit einem Integritätsprüfwert (ICV) ohne Auswirkungen auf die IP-MTU oder Fragmentierung und minimalen L2-MTU-Auswirkungen

geschützt: ca. 40 Byte (weniger als bei Baby-Riesen-Frames).



Beispiel für das MACSEC-Paketformat

- MACsec-EtherType: 0x88e5: gibt an, dass es sich bei dem Frame um einen MACsec-Frame handelt.
- TCI/AN: TAG Control Information/Association Number (TAG-Steuerinformationen/Zuordnungsnummer) Ist die MACsec-Versionsnummer, wenn Vertraulichkeit oder Integrität allein verwendet werden.
- SL: Länge der verschlüsselten Daten.
- PN: Paketnummer für den Wiedergabeschutz.
- SCI: Secure Channel Identifier Jede CA ist ein virtueller Port (MAC-Adresse der physischen Schnittstelle plus 16-Bit-Port-ID).
- ICV: Integritätsprüfungswert.

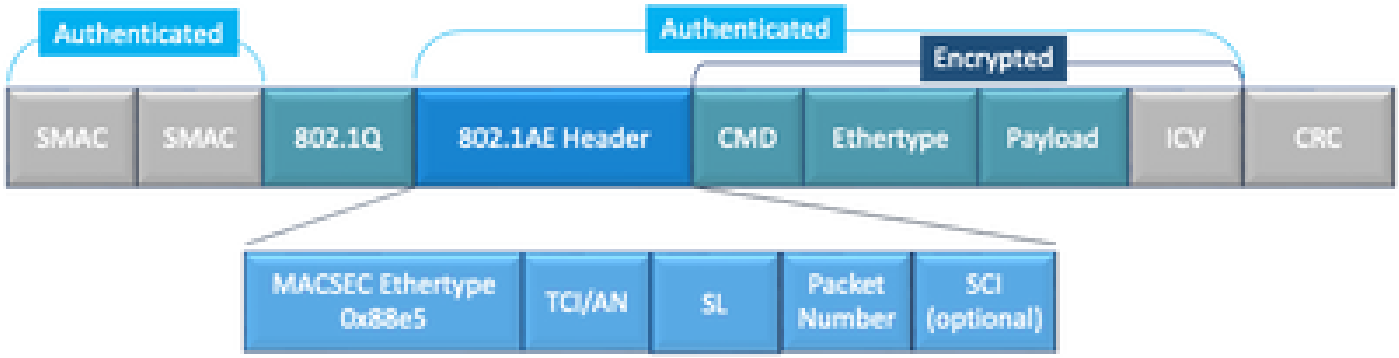
WAN-MACSEC

Ethernet hat sich über einen privaten LAN-Transport hinaus weiterentwickelt und umfasst nun eine Reihe von WAN- oder MAN-Transportoptionen. WAN MACSEC bietet eine End-to-End-Verschlüsselung für den Layer-2-Ethernet-WAN-Service, entweder Point-to-Point oder Point-to-Multipoint, unter Verwendung von AES 128 oder 256 Bit.

WAN MACsec basiert auf (LAN-)MACsec, daher der Name (und getrennt von IPsec), bietet jedoch einige zusätzliche Funktionen, die zuvor nicht verfügbar waren.

WAN MACSEC-Paketformat

Es besteht die Möglichkeit, dass der Service Provider keinen MACsec-Ethertype unterstützt und keinen L2-Service differenzieren kann, wenn das Tag verschlüsselt ist, sodass WAN MACSEC den gesamten Frame nach 802.1Q-Headern verschlüsselt:



WAN MACSEC 802.1Q-Tag im Beispiel für ein klares Paketformat

Eine der Neuerungen umfasst 802.1Q-Tags im Clear-Tag (auch ClearTag genannt). Diese Erweiterung ermöglicht die Offenlegung des 802.1Q-Tags außerhalb des verschlüsselten MACsec-Headers. Die Angabe dieses Felds bietet verschiedene Designoptionen für MACsec, und für öffentliche Carrier Ethernet-Transportanbieter ist dies für die Nutzung bestimmter Transportdienste erforderlich.

Die MKA-Funktionsunterstützung stellt Tunneling-Informationen wie den VLAN-Tag (802.1Q-Tag) klar zur Verfügung, sodass der Service Provider Service-Multiplexing bereitstellen kann, sodass mehrere Point-to-Point- oder Multipoint-Services auf einer einzigen physischen Schnittstelle koexistieren können und basierend auf der jetzt sichtbaren VLAN-ID differenziert werden.

Neben dem Service-Multiplexing können Service Provider mit dem VLAN-Tag im Klartext auch Quality of Service (QoS) für das verschlüsselte Ethernet-Paket im SP-Netzwerk auf Basis des 802.1P-Felds (CoS) bereitstellen, das jetzt als Teil des 802.1Q-Tags sichtbar ist.

WAN-MACSEC-Terminologie

MKA	MACSec Key Agreement, definiert in IEEE 802.1XREV-2010 - Key Agreement Protocol for discovering MACSec peers and negotiation keys.
MSK	Hauptsitzungsschlüssel, der beim EAP-Austausch generiert wird. Supplicant- und Authentifizierungsserver verwenden MSK, um CAK zu generieren.
KUCHEN	Der Verbindungszuordnungsschlüssel wird von MSK abgeleitet. Ist ein langlebiger Hauptschlüssel, der verwendet wird, um alle anderen Schlüssel zu generieren, die für MACSec verwendet werden.
CKN	Connectivity Association Key Name (Verbindungszuordnungsschlüsselname): identifiziert die CAK.
SAK	Sicherer Zuordnungsschlüssel - Wird vom CAK abgeleitet und ist der Schlüssel, der von Supplicant und Switch zum Verschlüsseln des Datenverkehrs für eine bestimmte Sitzung verwendet wird.
KS	Schlüsselserver, der verantwortlich ist für: • Auswählen und Anzeigen einer Verschlüsselungssuite • Generieren des SAK aus dem CAK.
TASK	Schlüsselverschlüsselungsschlüssel - zum Schutz von MACsec-Schlüsseln (SAK)

MACSEC Key Agreement Protocol (MKA) und Kryptografie - Überblick

MKA ist der von WAN MACsec verwendete Steuerungsebenenmechanismus. Dieser wird im IEEE-Standard 802.1X spezifiziert, der gegenseitig authentifizierte MACsec-Peers sowie die folgenden Aktionen erkennt:

- Erstellt und verwaltet eine CA (Connectivity Association).
- Verwaltet Live-/potenzielle Peer-Liste.
- Verhandlung über die Verschlüsselungssuite.
- Wählt Key Server (KS) unter den Mitgliedern einer Zertifizierungsstelle aus.
- Ableitung und Verwaltung von Secure Association Key (SAK).
- Sichere Schlüsselverteilung
- Schlüsselinstallation.
- Erneute Eingabe.

Ein Mitglied wird als Key-Server basierend auf der konfigurierten Key-Server-Priorität (niedrigste) ausgewählt, wenn die KS-Priorität unter den Peers gleich ist, dann gewinnt der niedrigste SCI.

KS generiert ein SAK erst, nachdem alle potenziellen Peers live geworden sind und mindestens ein Live-Peer vorhanden ist. Er verteilt das SAK und die verwendete Verschlüsselung an andere Teilnehmer und verwendet dazu die MKA PDU oder MKPDU in verschlüsselter Form.

Die Teilnehmer überprüfen die vom SAK gesendete Verschlüsselung und installieren sie, falls sie unterstützt wird, und verwenden sie auf jeder MKPDU, um den aktuellen Schlüssel anzugeben. Andernfalls lehnen sie das SAK ab.

Wenn nach dem dritten Heartbeat keine MKPDU von einem Teilnehmer empfangen wird (standardmäßig ist jeder Heartbeat 2 Sekunden), werden Peers aus der Live-Peer-Liste gelöscht. Wenn beispielsweise ein Client die Verbindung trennt, arbeitet der Teilnehmer am Switch so lange mit MKA, bis nach dem Empfang der letzten MKPDU vom Client drei Heartbeats verstrichen sind.

Für diesen Prozess gibt es zwei Methoden zum Steuern von Verschlüsselungsschlüsseln:

- Vorinstallierte Schlüssel
- 802.1x/EAP

Vorinstallierte Schlüssel

Wenn Sie Pre-Shared Keys verwenden, müssen Sie CAK=PSK und CKN manuell eingeben. Achten Sie auf einen wichtigen Rollover und Überschneidungen während der erneuten Schlüsselerstellung, um:

- Tauschen Sie einen neuen SAK-Schlüssel aus, installieren Sie ihn, und binden Sie ihn an die SA im Leerlauf.
- Löschen des alten SAK-Schlüssels und Zuweisen eines neuen freien SAs

Konfigurationsbeispiel:

<#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
```

Wobei sich fette Wörter auf Folgendes beziehen:
M_Key: Schlüsselbundname.

key 01: Connectivity Association Key Name (identisch mit CKN).

aes-128-cmac: MKA-Authentifizierungs-Verschlüsselung.

12345678901234567890123456789012: Connectivity Association Key (CAK).

Definieren der Richtlinie:

<#root>

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

gcm-aes-256

Dabei gilt gcm-aes-256 bezieht sich auf Verschlüsselungssuite(en) zur Ableitung eines sicheren Zuordnungsschlüssels (SAK).

Hinweis: Hierbei handelt es sich um eine grundlegende Richtlinienkonfiguration. Je nach Implementierung stehen weitere Optionen wie Vertraulichkeits-Offset, sak-rekey, include-icv-indicator und mehr zur Verfügung.

Schnittstelle:

```
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
```

Hinweis: Wenn keine mka-Richtlinie konfiguriert oder angewendet wird, ist die Standardrichtlinie aktiviert und kann über show mka default-policy detail überprüft werden.

802.1x/EAP

Wenn Sie die EAP-Methode verwenden, werden alle Schlüssel über den Master Session Key (MSK) generiert. Mit dem IEEE 802.1X Extensible Authentication Protocol (EAP) Framework tauscht MKA EAPoL-MKA-Frames zwischen Geräten aus, der Ether-Typ von EAPoL-Frames ist 0x888E, während der Paketkörper in einer EAPOL Protocol Data Unit (PDU) als MACsec Key Agreement PDU (MKPDU) bezeichnet wird. Diese EAPoL-Frames enthalten die CKN des Absenders, die Schlüsselserverpriorität und die MACsec-Funktionen.

Hinweis: Standardmäßig verarbeiten die Switches EAPoL-MKA-Frames, leiten sie aber nicht weiter.

Konfigurationsbeispiel für die zertifikatbasierte MACsec-Verschlüsselung:

Registrieren des Zertifikats (erfordert Zertifizierungsstelle):

```
  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
```

802.1x-Authentifizierung und AAA-Konfiguration erforderlich:

```
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-Profil und 802.1X-Anmeldedaten:

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

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

Schnittstelle:

```
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
```

Fehlerbehebung bei WAN MACSEC

Konfiguration

Prüfen Sie, ob die Konfiguration und die Implementierung plattformabhängig sind. Schlüssel und Parameter müssen übereinstimmen. Die folgenden Protokolle dienen zur Identifizierung von Konfigurationsproblemen:

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

Überprüfen Sie die MACsec-Funktion der Peer-Hardware, oder senken Sie die Anforderungen an die MACsec-Funktion, indem Sie die MACsec-Konfiguration für die Schnittstelle ändern.

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

Es gibt einige optionale Parameter, die der Router aufgrund der Konfiguration und verschiedener Standardeinstellungen der Plattform erwarten kann. Sie müssen diese bei der Konfiguration berücksichtigen oder verwerfen.

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

Die Richtlinienchiffrierungs-Suite weist eine Konfigurationsabweichung auf. Stellen Sie sicher, dass die Übereinstimmung richtig ist.

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

Mindestens eine der nächsten Validierungsprüfungen für MKPDU fehlgeschlagen:

- Gültige MAC-Adresse und EAPOL-Header: Überprüfen Sie die Konfiguration beider Schnittstellen, da die Paketerfassung an der Eingangsschnittstelle die aktuellen Werte bestätigen kann.
- Gültige CKN- und Algorithmusflexibilität: Stellen Sie gültige Schlüssel und Algorithmussuiten sicher.
- ICV-Verifizierung: Die ICV-Verifizierung ist ein optionaler Parameter. Die Konfiguration muss auf beiden Seiten übereinstimmen.
- Korrekte Reihenfolge der MKA-Payloads: Mögliche Interoperabilitätsprobleme.
- MI-Verifizierung, falls Peers vorhanden sind: Verifizierung der Mitglieds-ID, eindeutig für jeden Teilnehmer.
- MN-Verifizierung, falls Peers vorhanden sind: Verifizierung der Meldungsnummer, die für jede übertragene MKPDU eindeutig ist und bei jeder Übertragung erhöht wird.

Betriebliche Probleme

Sobald die Konfiguration festgelegt ist, wird die Meldung %MKA-5-SESSION_START angezeigt. Sie müssen jedoch überprüfen, ob die Sitzung gestartet wird. Ein guter Befehl zum Starten ist show mka sessions [interface interface_name]:

<#root>

```
Router1#
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
=============================================================================================
Te0/1/2         40b5.c133.0e8a/0012
Example
           NO
NO


18              40b5.c133.020a/0012  1
Secured


01
```

Status bezieht sich auf die Sitzung der Kontrollebene. Gesichert bedeutet, dass Rx und Tx SAK installiert sind. Ist dies nicht der Fall, wird sie als Nicht Gesichert angezeigt.

- Wenn der Status auf Init beibehalten wird, überprüfen Sie den Zustand der physischen Schnittstelle und die Verbindung über Ping auf Peers und die Übereinstimmung der Konfiguration. An diesem Punkt gibt es keine MKPDU empfangen und Live-Peers, einige Plattformen tun Padding, während andere nicht; berücksichtigen Sie bis zu 32 Byte Header-Overhead und stellen Sie größere MTU für den ordnungsgemäßen Betrieb.
- Wenn der Status auf Ausstehend bleibt, überprüfen Sie, ob MKPDU entweder in der Kontrollebene ein- oder ausgehend verworfen wird oder ob Fehler/Verwerfungen an der Schnittstelle vorliegen.
- Wenn der Status auf "Nicht gesichert" bleibt, ist die MKA-Schnittstelle aktiv und MKPDUs werden durchlaufen, aber SAK ist nicht installiert. In diesem Fall wird das nächste Protokoll

angezeigt:

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

Dies liegt daran, dass vor der Einrichtung eines Secure Channel (SC) und der Installation von Secure Associations (SA) in MACsec keine MACsec-Unterstützung, eine ungültige MACsec-Konfiguration oder ein anderer MKA-Fehler auf lokaler oder Peer-Seite aufgetreten ist. Sie können den Befehl detail für weitere Informationen show mka session [interface interface_name] detail verwenden:

<#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
  ------------------------------------------------------------------------------------
```

Suchen Sie nach SAK-Informationen zu Peers und markierten relevanten Daten, um die Situation besser zu verstehen. Wenn ein anderes SAK vorhanden ist, prüfen Sie den verwendeten Schlüssel und die konfigurierten Optionen für die Lebensdauer bzw. den SAK-Schlüssel. Wenn vorinstallierte Schlüssel verwendet werden, können Sie show mka keychains verwenden:

<#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>
```

CAK wird nie angezeigt, aber Sie können den Schlüsselbundnamen und CKN bestätigen.

Wenn eine Sitzung eingerichtet wurde, Sie jedoch Flaps oder einen unregelmäßigen

Datenverkehrsfluss haben, müssen Sie überprüfen, ob MKPDUs ordnungsgemäß zwischen Peers übertragen werden. Wenn eine Zeitüberschreitung vorliegt, wird die nächste Meldung angezeigt:

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

Wenn es einen Peer gibt, wird die MKA-Sitzung beendet. Wenn Sie mehrere Peers haben und MKA für mehr als 6 Sekunden keine MKPDU von einem Peer erhalten hat, wird der Live-Peer aus der Live-Peers-Liste entfernt. Sie können mit show mka statistics [interface interface_name] beginnen:

<#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
```

Die gesendeten und empfangenen MKPDUs müssen ähnliche Nummern für einen Peer haben. Stellen Sie sicher, dass sie an beiden Enden von Rx und Tx zunehmen, um die problematische Richtung zu bestimmen oder zu steuern. Wenn Unterschiede bestehen, können Sie mka linksec-interface frames both ends aktivieren:

```
*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
```

Wenn keine MKPDU empfangen wurde, suchen Sie nach eingehenden Schnittstellenfehlern oder -abbrüchen, dem Status der Peers-Schnittstellen und der MKU-Sitzung. Wenn beide Router senden, aber nicht empfangen, gehen MKPDUs auf den Medien verloren und müssen zwischengeschaltete Geräte auf eine korrekte Weiterleitung überprüfen.

Wenn Sie keine MKPDUs senden, überprüfen Sie den physischen Schnittstellenstatus (Leitung und Fehler/Löschungen) und die Konfiguration. Überprüfen Sie, ob Sie diese Pakete auf Kontrollebene generieren. FIA-Ablaufverfolgung und Embedded Packet Capture (EPC) sind hierfür zuverlässige Tools. Weitere Informationen finden Sie unter Fehlerbehebung mit der Paketverfolgungsfunktion von Cisco IOS XE Datapath

Sie können mka-Ereignisse debug verwenden und nach Gründen suchen, die die nächsten Schritte leiten können.

Hinweis: Verwenden Sie mka mit Vorsicht und debug mka diagnostics, da diese Statuscomputer und sehr detaillierte Informationen zeigen, die Probleme auf der Steuerungsebene auf dem Router verursachen können.

Wenn die Sitzung gesichert und stabil ist, der Datenverkehr jedoch nicht fließt, überprüfen Sie, ob verschlüsselter Datenverkehr an beide Peers gesendet wird:

<#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
```

Die Sicherheitszähler sind aktuelle Pakete an einer physischen Schnittstelle, während die anderen mit dem sicheren Tx-Kanal zusammenhängen. Dies bedeutet, dass Pakete verschlüsselt und übertragen werden, und Rx-gesicherte Zuordnung bedeutet, dass gültige Pakete an der Schnittstelle empfangen werden.

Mehr Debug-Programme wie debug mka-Fehler und debug mka-Pakete hilft bei der Identifizierung von Problemen, verwenden Sie bitte diese letzte mit Vorsicht, da kann zu schweren Protokollierung.

Zugehörige Informationen

- MACsec- und MKA-Konfigurationsleitfaden
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.