

라우터에서 WAN MACSEC 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[토폴로지](#)

[문제 해결을 위한 MACSEC 개요](#)

[MACsec 패킷 형식](#)

[WAN-MACSEC](#)

[WAN MACSEC 패킷 형식](#)

[WAN MACSEC 용어](#)

[MACSEC MKA\(Key Agreement Protocol\) 및 암호화 개요](#)

[사전 공유 키](#)

[802.1x/EAP](#)

[WAN MACSEC 문제 해결](#)

[설정](#)

[운영 문제](#)

[관련 정보](#)

소개

이 문서에서는 Cisco IOS® XE 라우터의 작동 및 문제 해결을 파악하기 위한 기본 WAN MACSEC 프로토콜에 대해 설명합니다.

사전 요구 사항

요구 사항

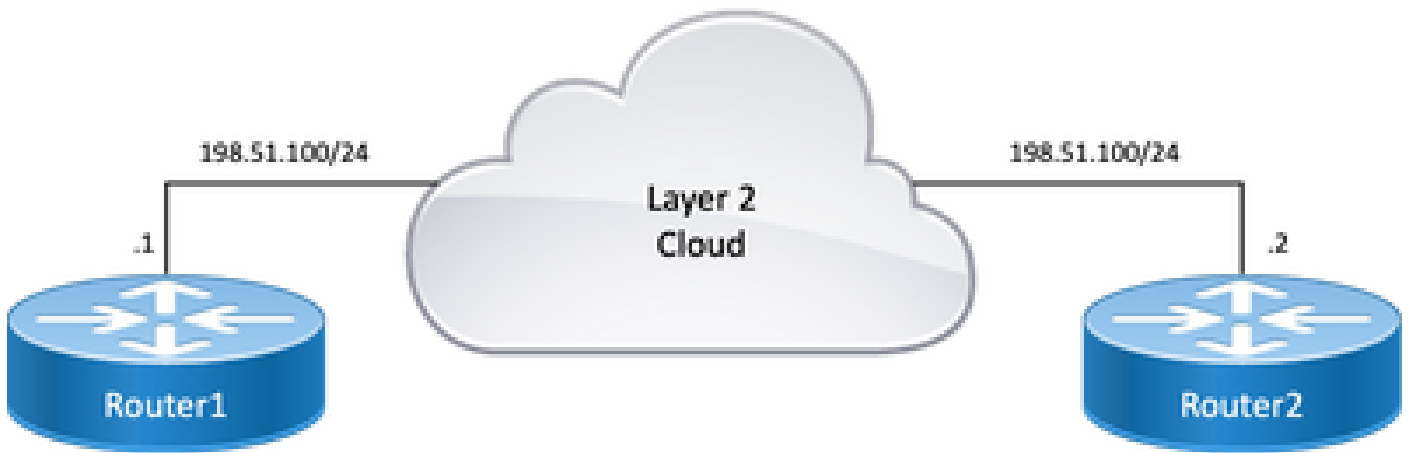
이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 ASR 1000, ISR 4000 및 Catalyst 8000 제품군과 같은 Cisco IOS XE 라우터에 대한 것입니다. 특정 하드웨어 및 소프트웨어 MACSEC 지원을 찾습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

토폴로지



토폴로지 다이어그램

문제 해결을 위한 MACSEC 개요

MACsec은 AES-128 암호화로 미디어 액세스 독립 프로토콜에 대한 데이터 기밀성, 데이터 무결성 및 데이터 출처 인증을 제공하는 IEEE 802.1AE 표준 기반 Layer 2 hop-by-hop 암호화이며, MACsec을 사용하여 호스트 연결 링크(네트워크 액세스 디바이스와 PC 또는 IP 전화와 같은 엔드 포인트 디바이스 간의 링크)만 보호할 수 있습니다.

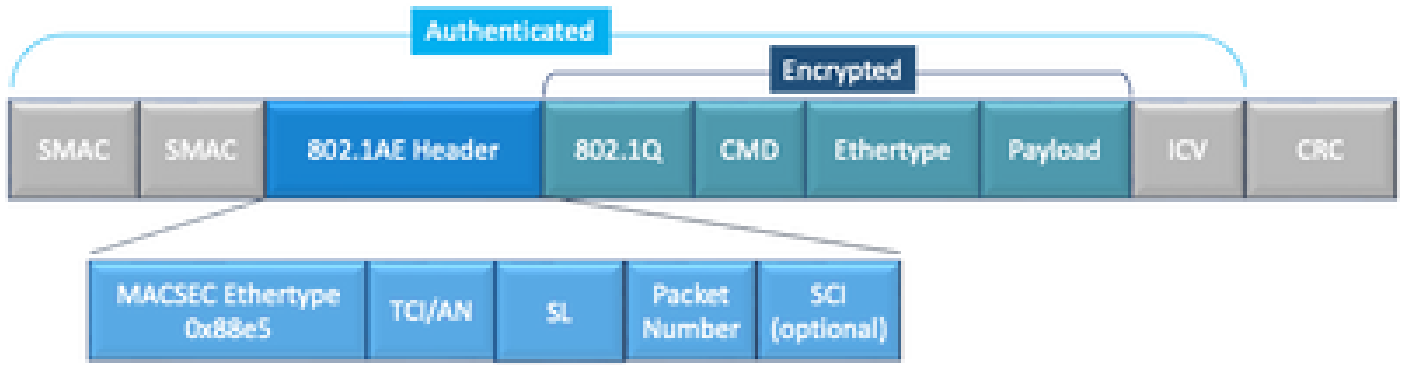
- 패킷은 인그레스 포트에서 해독됩니다.
- 디바이스에서 패킷이 지워집니다.
- 패킷은 이그레스 포트에서 암호화됩니다.

MACsec은 유선 LAN에서 보안 통신을 제공합니다. MACsec을 사용하여 LAN의 엔드포인트 간 통신을 보호하는 경우, 유선의 각 패킷은 대칭 키 암호화를 사용하여 암호화되므로 유선에서 통신을 모니터링하거나 변경할 수 없습니다. MACsec을 SGT(Security Group Tag)와 함께 사용하면 프레임의 페이로드에 포함된 데이터와 함께 태그에 대한 보호를 제공합니다.

MACsec은 대역 외 암호화 방식을 사용하여 유선 네트워크에서 MAC 계층 암호화를 제공합니다.

MACsec 패킷 형식

802.1AE(MACsec)를 사용하면 IP MTU 또는 단편화에 영향을 주지 않고 최소 L2 MTU에 영향을 주는 ~40바이트(Baby Giant Frame보다 작음)의 무결성 검사 값(ICV)으로 프레임이 암호화 및 보호됩니다.



MACSEC 패킷 형식 예

- MACsec EtherType: 0x88e5 - 프레임이 MACsec 프레임임을 지정합니다.
- TCI/AN: 태그 제어 정보/연결 번호 기밀성 또는 무결성이 단독으로 사용되는 경우 MACsec 버전 번호입니다.
- SL: 암호화된 데이터의 길이입니다.
- PN: 재생 보호에 사용되는 패킷 번호입니다.
- SCI: 보안 채널 식별자. 각 CA(Connectivity Association)는 가상 포트(물리적 인터페이스의 MAC 주소와 16비트 포트 ID)입니다.
- ICV: 무결성 검사 값

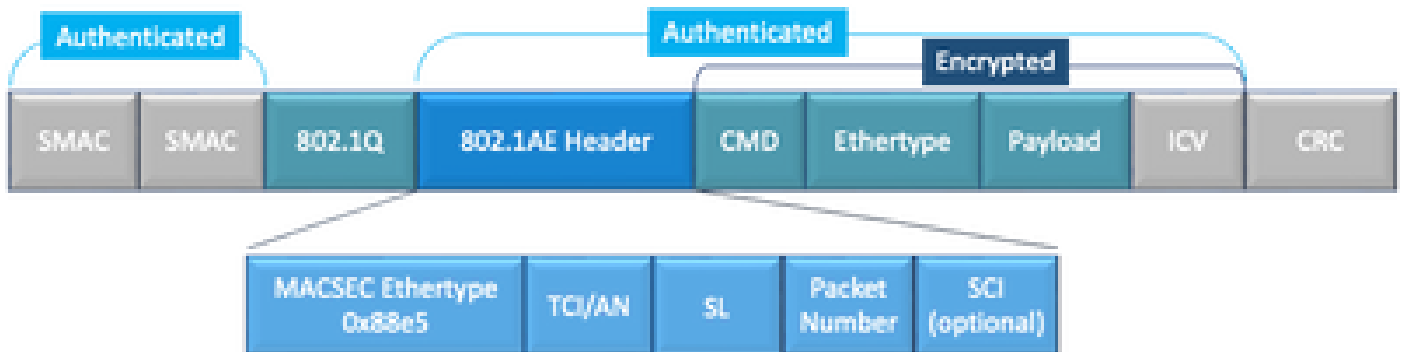
WAN-MACSEC

이더넷은 사실 LAN 전송을 넘어 다양한 WAN 또는 MAN 전송 옵션을 포함하도록 진화했습니다. WAN MACSEC은 AES 128 또는 256비트를 사용하여 포인트투포인트(point-to-point) 또는 포인트 투멀티포인트(point-to-multipoint) 중 하나의 레이어 2 이더넷 WAN 서비스를 통해 엔드 투 엔드 암호화를 제공합니다.

WAN MACsec은 (LAN) MACsec을 기반으로 하므로 (그리고 IPsec과는 별도로) 이름을 사용하지만, 이전에 사용할 수 없었던 몇 가지 추가 기능을 제공합니다.

WAN MACSEC 패킷 형식

WAN MACSEC이 802.1Q 헤더 이후의 모든 프레임을 암호화하도록 태그가 암호화된 경우 서비스 공급자가 MACsec 이더 타입을 지원하지 않고 L2 서비스를 차별화할 수 없을 수 있습니다.



Clear Packet Format 예제의 WAN MACSEC 802.1Q Tag

새로운 개선 사항 중 하나는 Clear(ClearTag라고도 함)에 802.1Q 태그를 포함합니다. 이러한 개선

을 통해 802.1Q 태그를 암호화된 MACsec 헤더의 외부에 표시할 수 있습니다. 이 필드를 공개하면 MACsec의 여러 설계 옵션이 제공되며, PMC(Public Carrier Ethernet) 전송 사업자의 경우 특정 전송 서비스를 활용해야 합니다.

MKA 기능 지원에서는 서비스 공급자가 서비스 멀티플렉싱을 제공할 수 있도록 VLAN 태그(802.1Q 태그)와 같은 터널링 정보를 제공하므로 단일 물리적 인터페이스에서 여러 지점 간 또는 다중 지점 서비스가 공존할 수 있으며 현재 보이는 VLAN ID를 기준으로 차별화될 수 있습니다.

서비스 멀티플렉싱 외에도 VLAN 태그를 사용하면 통신 사업자는 이제 802.1Q 태그의 일부로 표시되는 802.1P(CoS) 필드를 기반으로 SP 네트워크의 암호화된 이더넷 패킷에 QoS(Quality of Service)를 제공할 수 있습니다.

WAN MACSEC 용어

MKA	IEEE 802.1XREV-2010에 정의된 MACSec 키 계약 - MACSec 피어 검색 및 키 협상을 위한 키 계약 프로토콜.
MSK	EAP 교환 중에 생성되는 마스터 세션 키. 신청자 및 인증 서버는 MSK를 사용하여 CAK를 생성합니다
CAK	연결 연결 키는 MSK에서 파생됩니다. MACSec에 사용되는 다른 모든 키를 생성하는 데 사용되는 장기 마스터 키입니다.
CKN	Connectivity Association Key Name(연결 연결 키 이름) - CAK를 식별합니다.
삭크	Secure Association Key(보안 연결 키) - CAK에서 파생되며, 지정된 세션에 대한 트래픽을 암호화하는 신청자 및 스위치에서 사용되는 키입니다.
KS	주요 서버 담당자: <ul style="list-style-type: none"> • 암호 그룹 선택 및 광고 • CAK에서 SAK 생성
작은 나 무통	키 암호화 키 - MACsec 키(SAK)를 보호하는 데 사용됨

MACSEC MKA(Key Agreement Protocol) 및 암호화 개요

MKA는 WAN MACsec에서 사용하는 컨트롤 플레인 메커니즘으로, IEEE Std 802.1X에 지정되어 있으며 상호 인증된 MACsec 피어와 다음 작업을 검색합니다.

- CA(Connectivity Association)를 설정하고 관리합니다.
- 라이브/잠재적 피어 목록을 관리합니다.
- 암호 그룹 협상입니다.
- CA의 구성원 중에서 KS(Key Server)를 선택합니다.
- SAK(Secure Association Key) 파생 및 관리
- 보안 키 배포.
- 키 설치.

- 키 다시 입력.

구성된 키-서버 우선 순위(가장 낮음)에 따라 한 멤버가 키 서버로 선택됩니다. KS 우선 순위가 피어 간에 동일한 경우 가장 낮은 SCI가 승리합니다.

KS는 모든 잠재적 피어가 라이브가 되고 적어도 하나의 라이브 피어가 존재하는 경우에만 SAK를 생성한다. MKA PDU 또는 MKPDU를 사용하여 암호화된 형식으로 SAK와 사용된 암호를 다른 참가자에게 배포합니다.

참가자는 SAK에서 전송한 암호를 확인하고 지원되는 경우 모든 MKPDU에서 이를 사용하여 최신 키를 표시하며 그렇지 않으면 SAK를 거부합니다

3번의 하트비트(각 하트비트는 기본적으로 2초임) 이후 참가자로부터 MKPDU가 수신되지 않을 경우, 피어는 라이브 피어 목록에서 삭제됩니다. 예를 들어, 클라이언트의 연결이 끊어진 경우, 스위치의 참가자는 마지막 MKPDU가 클라이언트로부터 수신된 후 3번의 하트비트가 경과될 때까지 MKA를 계속 작동하게 됩니다.

이 프로세스에는 암호화 키를 구동하는 두 가지 방법이 있습니다.

- 사전 공유 키
- 802.1x/EAP

사전 공유 키

사전 공유 키를 사용하는 경우 CAK=PSK 및 CKN을 수동으로 입력해야 합니다. 키 수명의 경우 키 롤오버가 있고 키 재입력 시 겹쳐서 다음을 수행할 수 있습니다.

- 새 SAK 키를 교환 및 설치하고 유효 SA에 바인딩합니다.
- 기존 SAK 키를 제거하고 새 유효 SA를 할당합니다.

컨피그레이션 예시:

```
<#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
```

여기서 굵은 단어는 다음을 의미합니다.

M_Key: 키 체인 이름

키 01: 연결 연결 키 이름(CKN과 동일).

aes-128-cmac: MKA 인증 암호.


12345678901234567890123456789012: CAK(연결 연결 키).

정책 정의:

<#root>


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

위치 **gcm-aes-256**은 SAK(secure association key) 파생용 암호 그룹을 나타냅니다.

 참고: 기본 정책 컨피그레이션이며, 구현에 따라 기밀성 오프셋, sak-rekey, include-icv-indicator 등과 같은 추가 옵션을 사용할 수 있습니다.


인터페이스:

```
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
```

 참고: mka 정책을 구성하거나 적용하지 않으면 기본 정책이 활성화되고, show mka default-policy detail을 통해 검토할 수 있습니다.

802.1x/EAP

EAP 방법을 사용하는 경우 모든 키가 MSK(Master Session Key)에서 생성됩니다. IEEE 802.1X EAP(Extensible Authentication Protocol) 프레임워크에서 MKA는 디바이스 간에 EAPoL-MKA 프레임을 교환하며, EAPoL 프레임의 이더 유형은 0x888E이며 EAPOL PDU(Protocol Data Unit)의 패킷 본문은 MACsec MKPDU(Key Agreement PDU)라고 합니다. 이러한 EAPoL 프레임에는 발신자의 CKN, 키 서버 우선순위 및 MACsec 기능이 포함됩니다.

 참고: 기본적으로 스위치는 EAPoL-MKA 프레임을 처리하지만 전달하지는 않습니다.

인증서 기반 MACsec 암호화 컨피그레이션 예:

인증서 등록(인증 기관 필요):

```
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 인증 및 AAA 구성 필요:

```
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 프로파일 및 802.1X 자격 증명:

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

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

인터페이스:

```
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
```

WAN MACSEC 문제 해결

설정

플랫폼에 따라 적절한 컨피그레이션 및 구현 지원을 확인합니다. 키와 매개변수가 일치해야 합니다. 컨피그레이션에 문제가 있는지 확인하기 위한 일반적인 로그 중 일부는 다음과 같습니다.

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

피어 하드웨어의 MACsec 기능을 확인하거나 인터페이스에 대한 MACsec 컨피그레이션을 변경하여 MACsec 기능의 요구 사항을 낮춥니다.

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

라우터가 컨피그레이션 및 플랫폼의 서로 다른 기본 설정에 따라 예상하거나 예상하지 못하는 몇 가지 선택적 매개변수가 있습니다. 컨피그레이션에 포함되거나 무시해야 합니다.

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


정책 암호 그룹에 컨피그레이션 불일치가 있습니다. 올바르게 일치하는지 확인하십시오.

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

MKPDU가 다음 유효성 검사 중 하나 이상에 실패했습니다.

- 유효한 MAC 주소 및 EAPOL 헤더: 두 인터페이스 컨피그레이션을 모두 확인하고 인그레스 인터페이스의 패킷 캡처를 통해 현재 값을 확인할 수 있습니다.
- 유효한 CKN 및 알고리즘 민첩성: 유효한 키 및 알고리즘 모음을 확인합니다.
- ICV 확인: ICV 확인은 선택적 매개 변수이며 컨피그레이션 양끝이 일치해야 합니다.
- MKA 페이로드의 올바른 순서 존재: 상호 운용성 문제.
- 피어가 있는 경우 MI 확인: 각 참가자에 대해 고유한 구성원 식별자 확인
- 피어가 존재하는 경우 MN 확인: 전송된 모든 MKPDU에서 고유한 메시지 번호 확인 및 모든 전송에서 증분

운영 문제

구성이 설정되면 %MKA-5-SESSION_START 메시지가 표시되지만 세션이 시작되는지 확인해야 합니다. 다음으로 시작하는 좋은 명령은 show mka sessions [interface interface_name]입니다.

<#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

Status(상태)는 컨트롤 플레인 세션을 나타냅니다. Secured(보안)는 Rx 및 Tx SAK가 설치되어 있음을 의미합니다. 설치되어 있지 않으면 Not Secured(보안되지 않음)로 표시됩니다.

- 상태가 Init를 유지하는 경우 물리적 인터페이스 상태, 피어에 대한 ping을 통한 연결 및 컨피그레이션 일치 여부를 확인합니다. 이 시점에서는 수신된 MKPDU와 라이브 피어가 없고, 일부 플랫폼은 패딩을 수행하지만 다른 플랫폼은 패딩을 수행하지 않습니다. 최대 32바이트의 헤더 오버헤드를 고려하고 적절한 작동을 위해 더 큰 MTU를 보장합니다.
- 상태가 Pending(보류 중)에 있는 경우 MKPDU가 제어 평면에서 인그레스 또는 이그레스 또는 인터페이스 오류/삭제로 삭제되었는지 확인합니다.
- 상태가 Not Secured(보안 없음)로 유지되면 MKA 인터페이스가 가동 중이고 MKPDU가 통과하지만 SAK가 설치되지 않은 경우 다음 로그가 표시됩니다.

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

이는 MACsec에서 SC(Secure Channel)를 설정하고 SA(Secure Associations)를 설치하기 전에 로컬 또는 피어 측에서 MACsec을 지원하지 않거나 MACsec 컨피그레이션이 잘못되었거나 기타 MKA 오류가 발생했기 때문입니다. show mka session [interface interface_name] detail에 대한 자세한 내용은 detail 명령을 사용할 수 있습니다.

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

상황을 더 잘 이해하기 위해 강조 표시된 피어 및 관련 데이터에 대한 SAK 정보를 찾습니다. 다른 SAK가 있는 경우 사용된 키와 수명 또는 구성된 SAK rekey 옵션을 검토합니다. 사전 공유 키가 사용되는 경우 show mka keychains를 사용할 수 있습니다.

```
<#root>
```

```
Router1#
```

```
show mka keychains
```

```
MKA PSK Keychain(s) Summary...
```

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

```
=====
Master_Key
```

<HIDDEN>

CAK는 표시되지 않지만 키체인 이름과 CKN을 확인할 수 있습니다.

세션이 설정되었지만 플랩 또는 간헐적 트래픽 흐름이 있는 경우 MKPDU가 피어 간에 올바르게 흐르고 있는지 확인해야 합니다. 시간 초과가 있는 경우 다음 메시지가 표시됩니다.

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

피어가 하나 있는 경우 MKA 세션이 종료되며, 여러 피어가 있고 MKA가 해당 피어 중 하나에서 6초 이상 MKPDU를 받지 못한 경우 라이브 피어가 라이브 피어 목록에서 제거되며, show mka statistics [interface_name]으로 시작할 수 있습니다.

<#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

MKPDU Transmitted..... 11648
"Distributed SAK".. 0
"Distributed CAK".. 0


전송 및 수신된 MKPDU는 한 피어에 대해 비슷한 숫자를 가져야 하며, Rx 및 Tx 양단에서 증가해야 문제의 방향을 결정하거나 안내합니다. 차이가 있는 경우 mka linksec 인터페이스 프레임 양단 디버그를 활성화할 수 있습니다.

```
*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
```

수신된 MKPDU가 없는 경우, 들어오는 인터페이스 오류 또는 삭제, 피어 인터페이스 및 mka 세션의 상태를 확인합니다. 두 라우터가 모두 전송되지만 수신되지 않는 경우, MKPDU는 미디어에서 손실되며 중간 디바이스에서 올바른 포워딩을 확인해야 합니다.

MKPDU를 전송하지 않는 경우 물리적 인터페이스 상태(라인 및 오류/삭제) 및 컨피그레이션을 확인합니다. 컨트롤 플레인 레벨에서 이러한 패킷을 생성하는지 확인합니다. FIA 추적 및 EPC(Embedded Packet Capture)는 이러한 목적을 위한 신뢰할 수 있는 도구입니다. [Cisco IOS XE Datapath 패킷 추적 기능을 사용한 문제 해결을 참조하십시오](#)

debug mka 이벤트를 사용하고 이유를 찾아 다음 단계를 안내할 수 있습니다.

 참고: 상태 시스템과 라우터에서 컨트롤 플레인 문제를 일으킬 수 있는 매우 자세한 정보가 표시되므로 debug mka 및 debug mka diagnostics를 신중하게 사용하십시오.

세션이 보안되고 안정적이지만 트래픽이 흐르지 않는 경우, 두 피어를 모두 전송하는 암호화된 트래픽을 확인합니다.

<#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 카운터는 물리적 인터페이스의 현재 패킷이며, 다른 카운터는 Tx 보안 채널과 관련이 있습니다. 즉, 패킷이 암호화되어 전송됨을 의미하며, Rx Secured Association은 인터페이스에서 수신된 유효한 패킷을 의미합니다.

디버그 mka 오류 및 디버그 mka 패킷과 같은 더 많은 디버그는 문제 식별에 도움이 됩니다. 이 마지막 디버그는 대량의 로깅을 유발할 수 있는 예방 조치와 함께 사용하십시오.

관련 정보

- [MACsec 및 MKA 컨피그레이션 가이드](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.