
cisco Live!
Let's go
#CiscoLive

The bridge to possible

The deployment and principle of MACsec on NXOS

Selina Sun
@facebook.com/Xinsun888

BRKDCN-2007

cisco Live!

#CiscoLive

Cisco Webex App

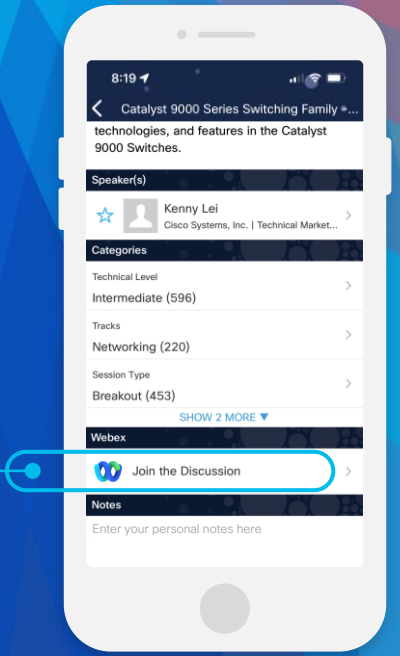
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.

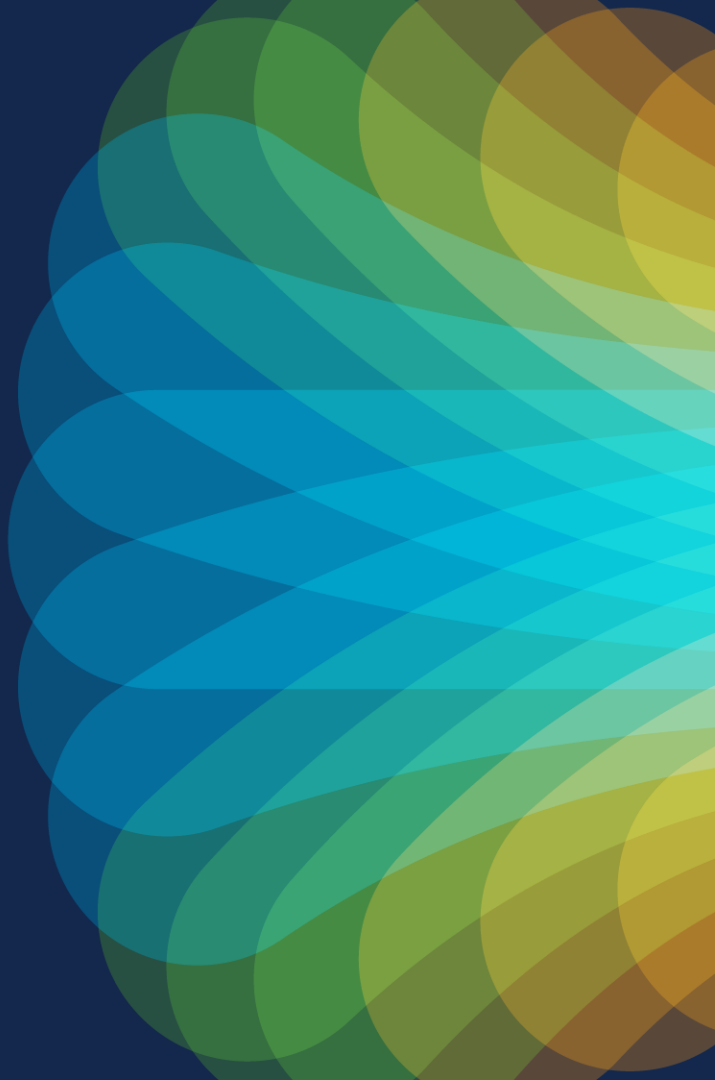


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKXXX-xxxx

Agenda

- Introduction
- HW support under NXOS
- Operating principle of MACsec
- Deployment case of MACsec
- Advantages

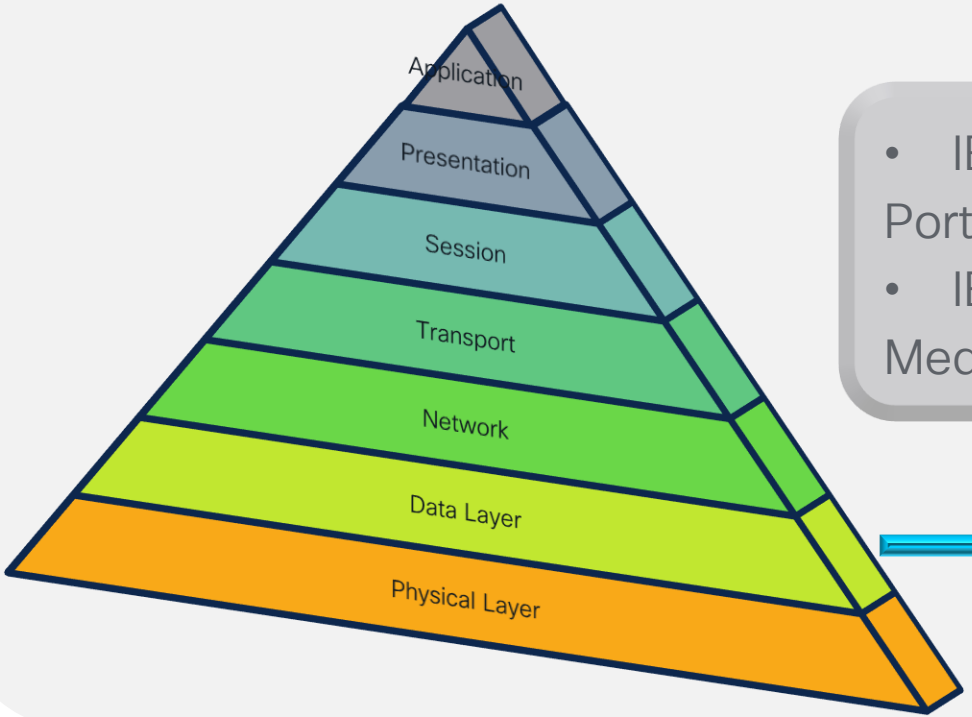
Introduction



What can you get from this section？

- The basic support of MACSEC in the data center, including software and hardware
- The operating principle of MACsec on the data center switch.
- Deployment case of MACsec on data center switch.

Introduction to MACSEC



- IEEE 802.1X-2010:

Port-Based Network Access Control

- IEEE 802.1AE-2006:

Media Access Control (MAC) Security

Media Access Control Security

HW Support under NXOS

HW support under NXOS

	N9K	N7K	N3K
Support	N9K-C93108TC-FX N9K-C93180YC-FX Nexus 9300-FX3(1G/10G) Nexus 9300-FX2	M1;M2;M3;F4 N7K-F248XP-25E N7K-F248XT-25E N77-F248XP-23E N7K-F348XP-25 N77-F348XP-23	Nexus 3264C-E
	N9K-X9736C-FX N9K-X9732C-EXM		

Limitation about MACsec under Nexus-9000 serious

- MKA is the only supported key exchange protocol for MACsec
- ONLY support P2P
- Cisco Nexus 9000 Series switches do not support MACsec on any of the MACsec capable ports when QSA is being used.
- Selectively enabling MACsec on a subset of sub-interfaces of the same Layer 3 routed interface is not supported.
- When the Cisco Nexus TOR switches are downgraded from Cisco NX-OS Release 9.x to Cisco NX-OS Release 7.x, MACsec is not supported.
- Link-level flow control (LLFC) and priority flow control (PFC) are not supported with MACsec.

Limitation about MACsec under Nexus-9000 serious

The following ports do not support MACsec when running at 1G:

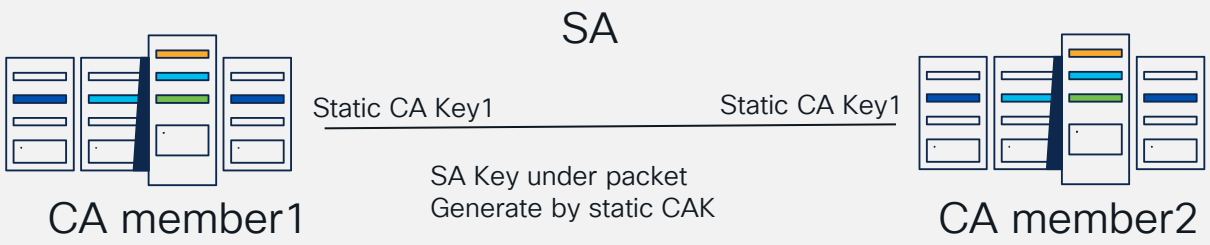
N9K-X9788TC-FX
N9K-C9336C-FX2
N9K-C93240YC-FX2
N9K-C93240YC-FX2-Z
N9K-X9736C-FX
N9K-C9364C
N9K-C9332C
N9K-C93360YC-FX3

N9K-C93216TC-FX2
N9K-C93360YC-FX3
N9K-C93360YC-FX2
N9K-C93180YC2-FX
N9K-C9336C-FX2
N9K-X96136YC-R

Operating principle of MACsec

Key exchange Protocol(MKA)

MKA: MACsec Key Agreement
CA: Secure Connectivity Association
SA: Secure Association
CAK: Secure Connectivity Association Key
SAK: Secure Association Key



Key exchange Protocol(MKA)

PSK: pre-shared key

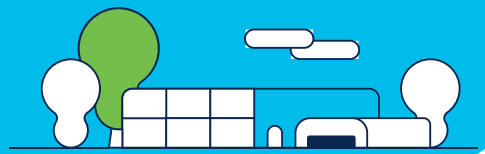
PN: packet number

GCM-AES-128/GCM-AES-256: Upon PN exhaustion (after reaching 75% of 2^{32} - 1), SAK rekey takes place automatically to refresh the data plane keys and the PN will wrap around.

GCM-AES-XPN-128/GCM-AES-XPN-256: Upon PN exhaustion (after reaching 75% of 2^{64} - 1), SAK rekey takes place automatically to refresh the data plane keys and the PN will wrap around.

KN: Key number

AN: Association number

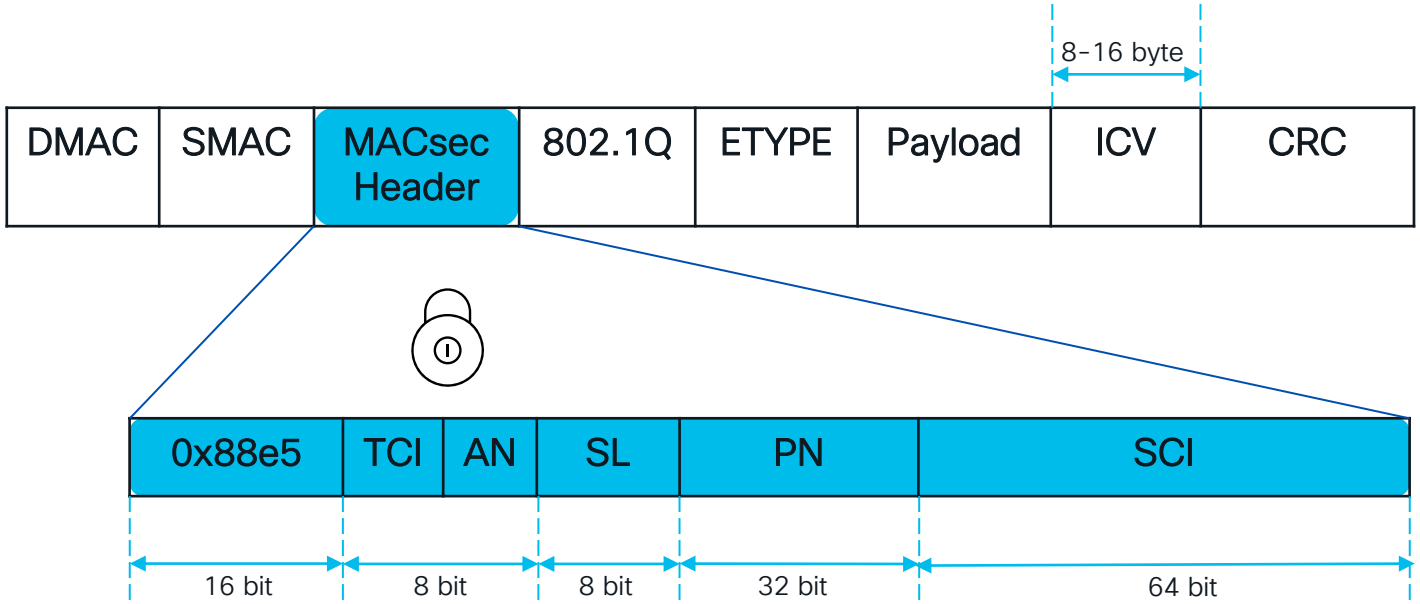


Key server

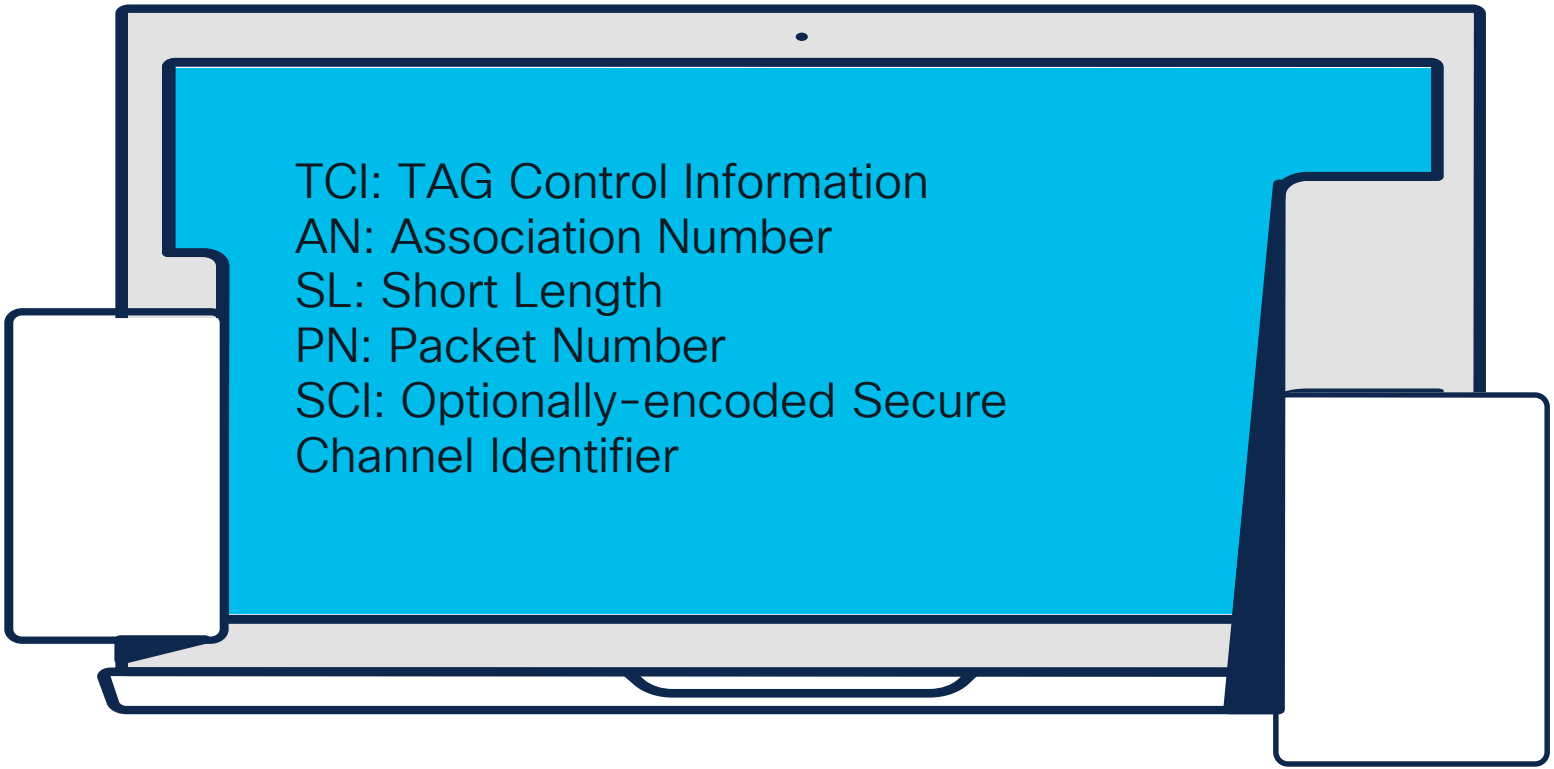
The user can configure the priority value of the interface. The smaller the value, the higher the priority, and the device interface with higher priority will be elected as the key server. When both parties have the same priority, compare the SCI value of the interface, and the interface with the smaller SCI value will be elected as the key server

SCI(Secure Channel Identifier)=interface mac + interface index

Packet structure



Packet structure



Advanced Encryption Standard(AES)

AES encryption

Encryption is mainly divided into two categories: symmetric encryption and asymmetric encryption. AES encryption is a kind of symmetric encryption, that is, encryption and decryption use the same key

GCM-AES-128

Packet LEN: 128 bits Key LEN: 128 bits

GCM-AES-256

Packet LEN: 128 bits Key LEN: 256 bits

GCM-AES-XPN-128

With extended packet number

GCM-AES-XPN-256

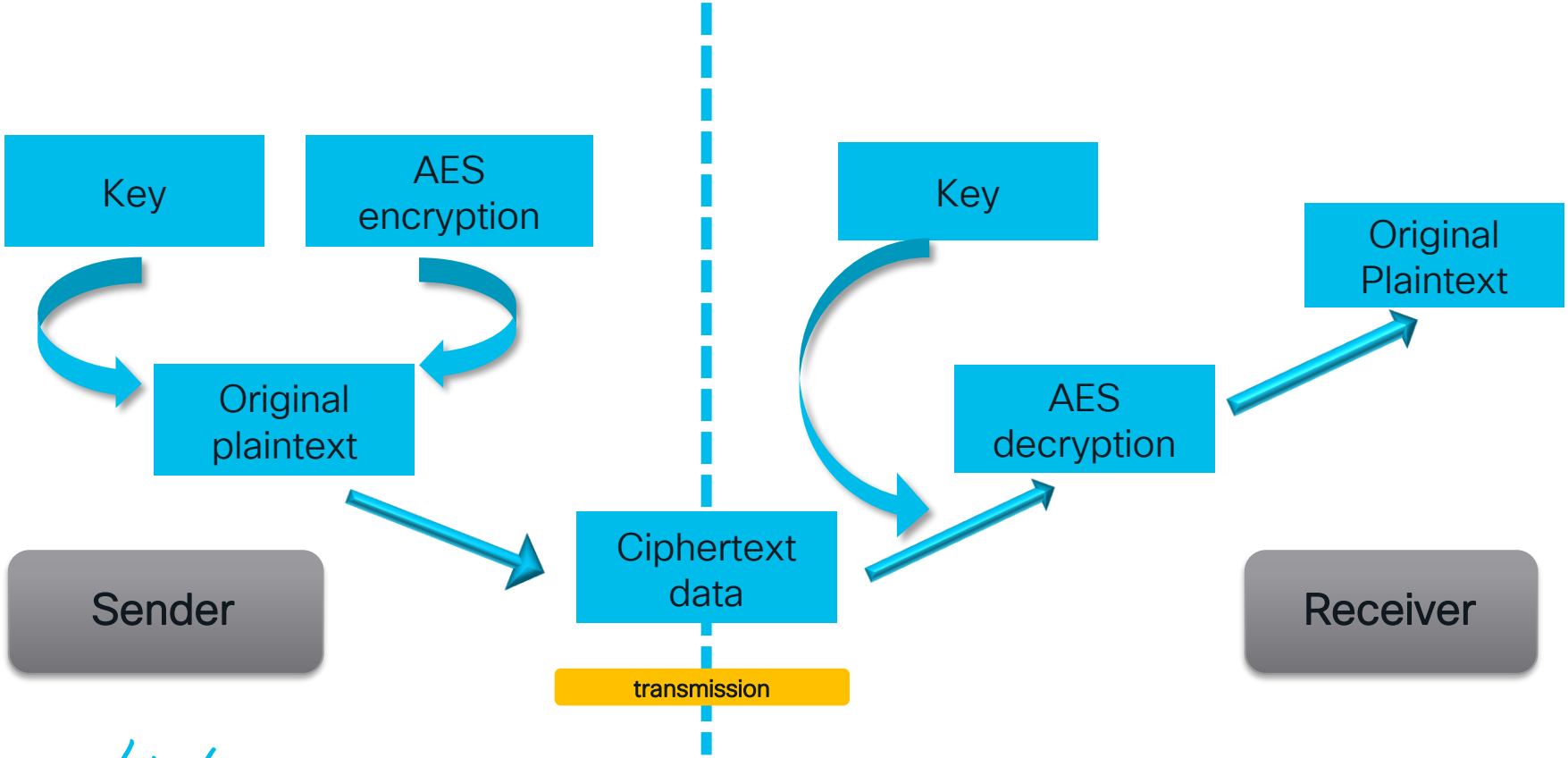
With extended packet number

Session keep alive

Session keepalive timeout

If within six seconds of the timeout period, the local switch does not receive the MKA protocol message from the peer device, the device in this segment will restart the timer and consider the connection to be unsafe. The next step is to delete the session and renegotiate.

Encryption process



The specific interaction process of the session

Election key server

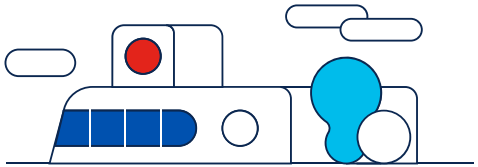
The key server generates and distributes the SAK to the key client

Generate and install SAK

The sender calculates ICV1 and appends it to the packet. After receiving the packet, the receiver calculates ICV2 in the same way and compares it with ICV1 in the packet. If they are the same, the packet is considered complete, otherwise the packet is discarded.

Data encryption and decryption

Secure Communication



Deployment case of MACSEC

Basic configuration

```
Feature Macsec
Key chain 1 Macsec
Key 1000
key-octet-string 7 104f0b<skip>272 cryptographic-algorithm AES_256_CMAC

Macsec policy 1
  cipher-suite GCM-AES-256
  key-server-priority 0
  window-size 512
  sak-expiry-time 100
  conf-offset CON-OFFSET-0

interface Ethernet1/1
  macsec keychain 1 policy 1
```

Basic policy

Window-size

Configures the replay protection window: Out-of-sequence packet sequence numbers can be legally received within the window range specified by the user, and packets beyond the window will be discarded

SAK-expiry-time

Force a SAK key update timer

conf-offset

Start encryption after offset X bytes

Cipher-suite

GCM-AES-128 GCM-AES-256
GCM-AES-XPN-128
GCM-AES-XPN-256

Basic check

```
N9K-C9508-1# show MACSEC MKA session
Interface         Local-TxSCI                # Peers      Status         Key-Server      Auth Mode
------------------ ------------------------------ ------------------ ------------------ ----------
Ethernet1/1       00a3.8eff.f5cc/0001        1          Secured        Yes             PRIMARY-PSK
------------------ ------------------------------ ------------------ ------------------ ----------
Total Number of Sessions : 1
      Secured Sessions : 1
      Pending Sessions : 0
```

```
N9K-C9508-1# show MACSEC MKA summary
Interface         Status   Cipher (Operational)   Key-Server   MACSEC-policy     Keychain          Fallback-keychain
------------------ -------- ---------------------- ------------ ----------------- ------------------------------
Ethernet1/1       Secured  GCM-AES-256            Yes          1                 1                 no keychain
```

Detail check

```
N9K# show MACSEC MKA statistics inter ethernet 1/1
Per-CA MKA Statistics for Session on interface
(Ethernet1/1) with CKN 1000
=======================================
CA Statistics
   Pairwise CAK Rekeys..... 0

SA Statistics
   SAKs Generated..... 1
   SAKs Rekeyed..... 0
   SAKs Received..... 0
   SAK Responses Received.. 1

MKPDU Statistics
   MKPDUs Transmitted..... 2432
      "Distributed SAK".. 1

   MKPDUs Validated & Rx... 2425
      "Distributed SAK".. 0
```

```
MKA Statistics for Session on interface
(Ethernet1/1)
=================================
CA Statistics
   Pairwise CAK Rekeys..... 0

SA Statistics
   SAKs Generated..... 1
   SAKs Rekeyed..... 0
   SAKs Received..... 0
   SAK Responses Received.. 1

MKPDU Statistics
   MKPDUs Transmitted..... 2432
      "Distributed SAK".. 1
   MKPDUs Validated & Rx... 2425
      "Distributed SAK".. 0

MKA IDB Statistics
   MKPDUs Tx Success..... 2432
   MKPDUs Tx Fail..... 0
   MKPDUS Tx Pkt build fail... 0
   MKPDUS No Tx on intf down.. 0
   MKPDUS No Rx on intf down.. 0
   MKPDUs Rx CA Not found..... 0
   MKPDUs Rx Error..... 0
   MKPDUs Rx Success..... 2425
```

```
MKPDU Failures
   MKPDU Rx Validation ..... 0
   MKPDU Rx Bad Peer MN..... 0
   MKPDU Rx Non-recent Peerlist MN..... 0
   MKPDU Rx Drop SAKUSE, KN mismatch..... 0
   MKPDU Rx Drop SAKUSE, Rx Not Set..... 0
   MKPDU Rx Drop SAKUSE, Key MI mismatch.... 0
   MKPDU Rx Drop SAKUSE, AN Not in Use..... 0
   MKPDU Rx Drop SAKUSE, KS Rx/Tx Not Set... 0
   MKPDU Rx Drop Packet, Ethertype Mismatch. 0
   MKPDU Rx Drop Packet, DestMAC Mismatch... 0

SAK Failures
   SAK Generation..... 0
   Hash Key Generation..... 0
   SAK Encryption/Wrap..... 0
   SAK Decryption/Unwrap..... 0

CA Failures
   ICK Derivation..... 0
   KEK Derivation..... 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SA Installation..... 0
   Tx SA Installation..... 0
```

Detail check

```
N9K# show MACSEC secy statistics interface ethernet 1/1
Interface Ethernet1/1 MACSEC SecY Statistics:
-------------------------------------------
Interface Rx Statistics:
   Unicast Uncontrolled Pkts: 22551
   Multicast Uncontrolled Pkts: 329691
   Broadcast Uncontrolled Pkts: 6
   Uncontrolled Pkts - Rx Drop: 0
   Uncontrolled Pkts - Rx Error: 0
   Unicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Multicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Broadcast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Controlled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
   Controlled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
   In-Octets Uncontrolled: 34265643 bytes
   In-Octets Controlled: 624950 bytes
   Input rate for Uncontrolled Pkts: 0 pps
   Input rate for Uncontrolled Pkts: 733 bps
   Input rate for Controlled Pkts: 0 pps
   Input rate for Controlled Pkts: 114 bps
-------------------------------------------
Interface Tx Statistics:
   Unicast Uncontrolled Pkts: 22548
   Multicast Uncontrolled Pkts: 318092
   Broadcast Uncontrolled Pkts: 7
   Uncontrolled Pkts - Rx Drop: 0
   Uncontrolled Pkts - Rx Error: 0
   Unicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Multicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Broadcast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
   Controlled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
   Controlled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
   Out-Octets Uncontrolled: 33963450 bytes
   Out-Octets Controlled: 611860 bytes
   Out-Octets Common: 33963450 bytes
   Output rate for Uncontrolled Pkts: 0 pps
   Output rate for Uncontrolled Pkts: 743 bps
   Output rate for Controlled Pkts: 0 pps
   Output rate for Controlled Pkts: 111 bps
```

Advantages

Advantages

- Works at Layer 2 of the seven-layer OSI model, Provide secure MAC layer data transmission and reception services.
- Can protect protocol messages above the second layer, such as arp, lldp
- It does not need to be passed to the upper layer of the protocol, Can be implemented based on hardware and has the characteristics of low latency.
- Data communication can be secured between every two devices.

The bridge to possible

Thank you

cisco Live!


cisco Live!
Let's go
#CiscoLive