

MACSec Using EAP-TLS Authentication

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
MACsec Using EAP-TLS Authentication	Release 7.3.1	IEEE 802.1X authentication mechanism for Port-Based Network Access Control is the first line of defense against outside attack. It is also one of the most commonly targeted attack vectors, which makes it a security priority. In this release, EAP-TLS, a certificate-based authentication method is used to send client information through IEEE 802.1X, thereby resulting in a secured network connection.

Note MACsec Using EAP-TLS Authentication is supported only on the following variants of Cisco NCS 540 routers:

- N540-24Z8Q2C-SYS
- N540-24Z8Q2C-M

This chapter describes how to achieve MACSec encryption between two Routers using the 802.1X port-based authentication with Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). EAP-TLS allows mutual authentication using certificates, between the authentication server and the client, and generates the Master Session Key (MSK). This MSK is used to derive the Connectivity Association Key (CAK), and the corresponding Connectivity Association Key Name (CKN) is derived from the EAP session ID.

The enable-tls1.3-legacy-kdf must be configured when using EAP based MACsec with Local EAP Authentication to ensure interoperability with XR releases earlier than Release 25.4.1.

- Configure MACSec Encryption Using EAP-TLS Authentication, on page 2

Configure MACSec Encryption Using EAP-TLS Authentication

The system supports certificate-based MACsec encryption using both local and remote EAP-TLS authentications.

Restrictions for MACSec Using EAP-TLS Authentication

- The system does not support certificate-based (EAP-TLS) MACsec encryption on sub-interfaces.
- The system does not support MACSec using EAP-TLS authentication in **multi-auth** host mode.

You must also follow the guidelines and restrictions applicable to EAP-TLS session. For details, see the #unique_237 section in the *802.1X Port-Based Authentication* chapter.

Prerequisites

For MACSec using EAP-TLS authentication, you must first configure a EAP-TLS session. For more information on configuring EAP-TLS session, see the following topics in the *802.1X Port-Based Authentication* chapter:

- 802.1X with Remote RADIUS Authentication
- 802.1X with Local EAP Authentication
- Router as 802.1X Supplicant

The MKA participant with 802.1X PAE role as **authenticator** acts as the key server and the **supplicant** acts as the non-key server.

Configure MACSec EAP on an Interface

The following section describes the steps to configure MACSec EAP on an interface.

Configuration Example

```
Router#configure
Router(config)#interface HundredGigE 0/1/1/2
Router(config-if)#macsec eap
Router(config-if)#commit
```

Running Configuration

```
Router#show run interface HundredGigE 0/1/1/2
interface HundredGigE 0/1/1/2
    macsec eap
!
```

You can also configure MACSec EAP on an interface by specifying the configured MACSec policy name.

Configuration Example

```
Router(config-if)#macsec eap policy test-macsec-policy
```

Running Configuration

```
Router#show run interface HundredGigE 0/1/1/2
interface HundredGigE 0/1/1/2
    macsec eap policy test-macsec-policy
!
```

Verify MACSec EAP Configuration on an Interface

You can use these commands to verify the MACSec EAP configuration:

- **show macsec mka session interface**

  Sample output:

```
Router# show macsec mka session interface HundredGigE 0/1/1/2
================================================================================
Interface-Name    Local-TxSCI     #Peers Status  Key-Server PSK/EAP CKN
================================================================================
Hu0/1/12      0201.9ab0.85af/0001    1   Secured YES        EAP     A94399 ...
```

- **show macsec mka session interface detail**

  Sample output:

```
Router# show macsec mka session interface HundredGigE 0/1/1/2 detail

MKA Detailed Status for MKA Session
===================================
Status                                : SECURED - Secured MKA Session with MACsec

Local Tx-SCI                          : 0201.9ab0.85af/0001
Local Tx-SSCI                         : 2
Interface MAC Address                 : 0201.9ab0.85af
MKA Port Identifier                   : 1
Interface Name                        : Hu0/1/1/2
CAK Name (CKN)                        : A94399EE68B2A455F85527A4309485DA
CA Authentication Mode                : EAP
Keychain                              : NA (EAP mode)
Member Identifier (MI)                : 3222A4A7678A6BDA553FDB54
Message Number (MN)                   : 114
Authenticator                         : YES
Key Server                            : YES
MKA Cipher Suite                      : AES-128-CMAC
Configured MACSec Cipher Suite        : GCM-AES-XPN-256
Latest SAK Status                     : Rx & Tx
Latest SAK AN                         : 1
Latest SAK KI (KN)                    : 3222A4A7678A6BDA553FDB5400000001 (1)
Old SAK Status                        : No Rx, No Tx
Old SAK AN                            : 0
Old SAK KI (KN)                       : RETIRED (0)
SAK Transmit Wait Time                : 0s (Not waiting for any peers to respond)
SAK Retire Time                       : 0s (No Old SAK to retire)
Time to SAK Rekey                     : NA
MKA Policy Name                       : *DEFAULT POLICY*
Key Server Priority                   : 16
Delay Protection                      : FALSE
Replay Window Size                    : 64
Include ICV Indicator                 : FALSE
Confidentiality Offset                : 0
Algorithm Agility                     : 80C201
```

```
SAK Cipher Suite                          : 0080C20001000004 (GCM-AES-XPN-256)
MACsec Capability                         : 3 (MACsec Integrity, Confidentiality, &
Offset)
MACsec Desired                            : YES

# of MACsec Capable Live Peers            : 1
# of MACsec Capable Live Peers Responded : 1

Live Peer List:
MI                        MN     Rx-SCI (Peer)      SSCI    KS-Priority
-----------------------------------------------------------------------------
86B47DE76B42D9D7AB6805F7  113   0257.3fae.5cda/0001   1        16

Potential Peer List:
MI      MN         Rx-SCI (Peer)             SSCI         KS-Priority
-----------------------------------------------------------------------------

Peers Status:
Last Tx MKPDU   : 2018 Mar 01 13:36:56.450
Peer Count      : 1
RxSCI           : 02573FAE5CDA0001
MI              : 86B47DE76B42D9D7AB6805F7
Peer CAK        : Match
Latest Rx MKPDU : 2018 Mar 01 13:36:56.450
```

- **show macsec mka summary**

  Sample output:

```
Router#show macsec mka summary
================================================================================
Interface-Name Status   Cipher-Suite    KeyChain      PSK/EAP   CKN
================================================================================
Hu0/1/12       Secured  GCM-AES-XPN-256 NA(EAP mode)  EAP       A94399 ...

Total MACSec Sessions : 1
Secured Sessions : 1
Pending Sessions : 0
```