

Support for MACsec and IPsec Encryption

- Support for MACsec and IPsec Encryption, on page 1
- Software Supported MACsec, on page 1

Support for MACsec and IPsec Encryption

You can configure MACsec on the LAN port and IPsec on the WAN port to secure sensitive traffic. This traffic moves from DA assets. The router connects to the DA assets, allowing them to use MACsec encryption at Layer 2 and create IPsec tunnels through the LTE or WAN port.

Note Cisco supports only the **should secure** MACsec mode, which allows unencrypted traffic even in a secured state.

Limitation:

The router does not support the **must secure** mode.

For more information about IPsec and MACsec configuration, see the following guides:

- Security and VPN Configuration Guide, Cisco IOS XE 17.X

Software Supported MACsec

Overview

All existing Cisco IOS XE based router/switch use special transceiver to do MACsec encryption/decryption. This software MACsec uses CDAL infrastructure in QFP to do crypto operation. Comparing to the hardware choice, the way configuration/status/datapath is done is different thus creating some limitation on the functionality.

The MACsec port must be put into access mode. As the encryption happens on the egress SVI interface, the vlan used for the port should be unique, meaning no other interface can use that vlan. This limitation is because the QFP does not have MAC table information.

Note Since MACsec is being done through software, performances are not line rate on L2 interfaces.

Note Cisco supports only the should secure MACsec mode, which allows unencrypted traffic even in a secured state.

Limitation:

The router does not support the must secure mode.

For an egress packet, SVI only know the packet needs to go out on a vlan without info about any specific interface. It is up to the switch chip to decide which port to go. All the packets without MACsec tag can come in as usual. Outgoing L2 packet will also egress without encryption or modification.

Both the NE and NA license support GCM-AES-128. From Cisco IOS XE 26.2.1, GCM-AES-256 is also supported. This feature is not available running the NPE image.

The MACsec protocol is defined in IEEE802.1AE.

Feature Limitations

- MACsec is not supported in controller mode in this release.
- There must be a unique vlan id for a MACsec interface.
- Releases earlier than Cisco IOS XE Release 26.2.1 support only the gcm-aes-128 cipher suite.
- Cisco IOS XE Release 26.2.1 and later releases support the gcm-aes-128 and gcm-aes-256 cipher suites.
- Both explicit and non-explicit SCI are supported on ingress side. The router sends out only explicit SCI packets as it is not an end system.
- The router does not support confidentiality offset.
- Integrity only is not supported in this first release.
- For gcm-aes-128, up to 32 bytes are added to an encrypted packet compared to a plain packet. So the MTU setup should add 32 for it to work properly.
- The MACsec key is managed by the MKA module. For that device, it requires a static key for MKA to negotiate MACsec key.
- There is no MIB support.
- IP Device Tracking (IPDT) is not supported in the host-to-switch MACsec configurations.

Related Documentation

Further information can be found at the following:

- MACsec and the MACsec Key Agreement (MKA) Protocol
- MACSEC and MKA Configuration Guide, Cisco IOS XE 17

Sample MKA Configuration

See the following example:

```
conf t
   aaa new-model
   mka policy p1
       key-server priority 1
       macsec-cipher-suite gcm-aes-128
       sak-rekey interval 3600
end
conf t
   key chain cak1 macsec
      key 414243
         cryptographic-algorithm aes-128-cmac
         key-string 0 12345678901234567890123456789012
         lifetime local 00:00:00 29 November 2021 infinite
end
conf t
   int fa 0/0/2
      switchport mode access
      switchport access vlan 77
      mtu 1532
      mka policy p1
      mka pre-shared-key key-chain cak1
      macsec network-link
      macsec replay-protection window-size 128
end
```

Show Commands

Show cpp_cp internal info:

```
show platform hardware cpp active feature soft-macsec server tx [dp] [item]
show platform hardware cpp active feature soft-macsec server rx [dp] [item]
show platform hardware cpp active feature soft-macsec server control [dp] [item]
```

Other show commands:

```
show macsec summary
show macsec status int fa 0/0/2
show macsec statistics int fa 0/0/2A
```

Clear Statistics

```
Clear macsec statis int fa 0/0/2
```

Test Command

Print 10 MKA packet for debug:

```
test platform software smacsec mka-ingress
```