

MACsec

This chapter contains the following sections:

- About MACsec, on page 1
- Guidelines and Limitations for MACsec on switches, on page 2
- Configuring MACsec for Fabric Links Using the GUI, on page 6
- Configuring MACsec for Access Links Using the GUI, on page 6
- Configuring MACsec Parameters Using the APIC GUI, on page 7
- Configuring MACsec Keychain Policy Using the GUI, on page 7
- Configuring MACsec Using the NX-OS Style CLI, on page 8

About MACsec

MACsec is an IEEE 802.1AE standards based Layer 2 hop-by-hop encryption that provides data confidentiality and integrity for media access independent protocols.

MACsec, provides MAC-layer encryption over wired networks by using out-of-band methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys.

The 802.1AE encryption with MKA is supported on all types of links, that is, host facing links (links between network access devices and endpoint devices such as a PC or IP phone), or links connected to other switches or routers.

MACsec encrypts the entire data except for the Source and Destination MAC addresses of an Ethernet packet. The user also has the option to skip encryption up to 50 bytes after the source and destination MAC address.

To provide MACsec services over the WAN or Metro Ethernet, service providers offer Layer 2 transparent services such as E-Line or E-LAN using various transport layer protocols such as Ethernet over Multiprotocol Label Switching (EoMPLS) and L2TPv3.

The packet body in an EAP-over-LAN (EAPOL) Protocol Data Unit (PDU) is referred to as a MACsec Key Agreement PDU (MKPDU). When no MKPDU is received from a participants after 3 hearbeats (each hearbeat is of 2 seconds), peers are deleted from the live peer list. For example, if a client disconnects, the participant on the switch continues to operate MKA until 3 heartbeats have elapsed after the last MKPDU is received from the client.

APIC Fabric MACsec

The APIC will be responsible for the MACsec keychain distribution to all the nodes in a Pod or to particular ports on a node. Below are the supported MACsec keychain and MACsec policy distribution supported by the APIC.

- A single user provided keychain and policy per Pod
- User provided keychain and user provided policy per fabric interface
- Auto generated keychain and user provided policy per Pod

A node can have multiple policies deployed for more than one fabric link. When this happens, the per fabric interface keychain and policy are given preference on the affected interface. The auto generated keychain and associated MACsec policy are then given the least preference.

APIC MACsec supports two security modes. The MACsec **must secure** only allows encrypted traffic on the link while the **should secure** allows both clear and encrypted traffic on the link. Before deploying MACsec in **must secure** mode, the keychain must be deployed on the affected links or the links will go down. For example, a port can turn on MACsec in **must secure** mode before its peer has received its keychain resulting in the link going down. To address this issue the recommendation is to deploy MACsec in **should secure** mode and once all the links are up then change the security mode to **must secure**.

Note Any MACsec interface configuration change will result in packet drops.

MACsec policy definition consists of configuration specific to keychain definition and configuration related to feature functionality. The keychain definition and feature functionality definitions are placed in separate policies. Enabling MACsec per Pod or per interface involves deploying a combination of a keychain policy and MACsec functionality policy.

Note Using internal generated keychains do not require the user to specify a keychain.

APIC Access MACsec

MACsec encryption is configured under fabric policies for fabric ports and access policies for access ports and can be applied to physical interfaces, port-channels, or vPCs (virtual port-channels). Interfaces with MACsec enabled can operate as either Layer 2 interfaces (such as EPGs or L3Out SVIs) or Layer 3 interfaces (including L3Out routed interfaces or routed sub-interfaces). Enabling MACsec on an interface enables MACsec encryption on the entire interface and applies to all VLANs or sub-interfaces configured on the interface.

Guidelines and Limitations for MACsec on switches

MACsec is supported on the following switches:

- N9K-C93108TC-FX3P
- N9K-C93108TC-FX3 (beginning with the 6.0(5) release)

- N9K-C93108TC-FX
- N9K-C93180YC-FX3
- N9K-C93180YC-FX
- N9K-C93216TC-FX2
- N9K-C93240YC-FX2
- N9K-C9332C
- N9K-C93360YC-FX2
- N9K-C9336C-FX2
- N9K-C9348GC-FXP, only with 10G+
- N9K-C9364C
- N9K-C9364D-GX2A
- N9K-C9348D-GX2A
- N9K-C9332D-GX2B
- N9K-C9408 (beginning with the 6.0(2) release)

MACsec is supported on the following line cards:

- N9K-X9716D-GX
- N9K-X9736C-FX

Configure MACsec on switches according to the following guidelines and limitations:

- MACsec encryption is configured under fabric policies for fabric ports and access policies for access ports and can be applied to physical interfaces, port-channels, or vPCs (virtual port-channels). Interfaces with MACsec enabled can operate as either Layer 2 interfaces (such as EPGs or L3Out SVIs) or Layer 3 interfaces (including L3Out routed interfaces or routed sub-interfaces). Enabling MACsec on an interface enables MACsec encryption on the entire interface and applies to all VLANs or sub-interfaces configured on the interface.
- MACsec is not supported on 10G QSA modules.
- MACsec is not supported with 1G speed on a Cisco ACI leaf switch.
- MACsec between a Cisco ACI leaf switch and a computer host has not been validated by Cisco. Switch-to-switch mode has been validated and is supported.
- MACsec is supported on breakout ports.
- MACsec is supported on remote leaf switches.
- When using copper ports, the copper cables must be connected directly the peer device (standalone N9k) in 10G mode.
- A 10G copper SFP module on the peer is not supported.
- FEX ports are not supported for MACsec.

- The **must-secure** mode is not supported at the pod level.
- A MACsec policy with the name "default" is not supported.
- Auto-key generation is only supported at the pod level for fabric ports.
- Do not clean reboot a node if the fabric ports of that node is running MACsec in **must-secure** mode.
- Adding a new node to a pod or stateless reboot of a node in a pod that is running MACsec, **must-secure** mode requires changing the mode to **should-secure** for the node to join the pod.
- Only initiate an upgrade or downgrade if the fabric links are in the **should-secure** mode. After the upgrade or downgrade has completed, you can change the mode to **must-secure**. Upgrading or downgrading in the **must-secure** mode results in nodes losing connectivity to the fabric. Recovering from connectivity loss requires you to configure in **should-secure** mode the fabric links of the nodes that are visible to the Cisco Application Policy Infrastructure Controller (APIC). If the fabric was downgraded to a version which does not support MACsec, then nodes which are out of fabric will need to be clean rebooted.
- For a PC or vPC interface, MACsec can be deployed using policy groups per PC or vPC interface. Port selectors are used to deploy the policies to a particular set of ports.
- We recommend that you configure MACsec polices with the **should-secure** mode before you export a configuration.
- All of the links on a spine switch are considered to be fabric links. However, if a spine switch link is used for IPN connectivity, then this link will be treated as an access link. This means that a MACsec access policy must be used to deploy MACsec on these links.
- The 5.2(3) release added support for Multi-Pod Spines Back-to-Back. The following guidelines and limitations apply to MACsec with Multi-Pod Spines Back-to-Back:
  - The back-to-back links are treated as fabric links. You must create a MACsec fabric policy when enabling MACsec on the spine back-to-back links.

    For information about creating a MACsec fabric policy, see the "Configuring MACsec for Fabric Links Using the GUI" procedure in the *Cisco APIC Layer 2 Networking Configuration Guide*.
  - Both back-to-back links must use the same MACsec policy. If you used pod polices, then both pods should deploy the same MACsec policy.
- If a remote leaf fabric link is used for IPN connectivity, then this link will be treated as an access link. A MACsec access policy needs to be used to deploy MACsec on these links.
- Improper deployment of **must-secure** mode on remote leaf switch fabric links can result in loss of connectivity to the fabric. Follow the instructions provided in Deploying must-secure mode, on page 5 to prevent such issues.
- MACsec sessions can take up to a minute to form or tear down when a new key is added to an empty keychain or an active key is deleted from a keychain.
- Before reloading a line card or fabric module on a spine switch, all **must-secure** links should be changed to the **should-secure** mode. After the reload completes and the session comes up in the **should-secure** mode, change the mode to **must-secure**.
- When selecting the cipher suite AES 128 or AES 256 without Extended Packet Numbering (XPN), you must explicitly specify the Security Association Key (SAK) expiry time. Leaving the SAK expiry time value at the default ("disabled") can cause interfaces to go out of service randomly.

- A replay window is necessary to support the use of MACsec over provider networks that reorder frames. Frames within the window can be received out of order, but are not replay protected. The default window size is 64. The replay window size can be configured in the range of 0 to 2^{32}-1 if you use the Cisco APIC GUI or CLI. If you use a XPN cipher suite, the maximum replay window size is 2^{30}-1, and if you configure a higher window size, the window size gets restricted to 2^{30}-1. If you change the cipher suite to a non-XPN cipher suite, then there is no restriction and the configured window size is used.
- In the 5.2(2) release and later, if you are using MACsec on Cisco N9K-X9716D-GX line card fabric ports and then downgrade to a release prior to 5.2(2), the earlier releases do not support MACsec on this line card. However, no fault is raised to indicate that MACsec is not supported. In this scenario, if the peer leaf switch supports MACsec, the session comes up as secure. But, on the spine side, the session shows as pending.
- Link-level flow control (LLFC) and priority flow control (PFC) are not supported with MACsec.
- Cisco APIC does not support passing MACsec through its infrastrucutre for clients.

Deploying must-secure mode

Incorrectly deploying a policy that is configured for **must-secure** mode can result in a loss of connectivity. The procedure below should be followed in order to prevent such issues:

- You must ensure that each link pair has their keychains before enabling MACsec **must-secure** mode. To ensure this, we recommend that you deploy the policy in **should-secure** mode, and once MACsec sessions are active on the expected links, change the mode to **must-secure**.
- Attempting to replace the keychain on a MACsec policy that is configured to **must-secure** can cause links to go down. In this case, use the following procedure:
  1. Change MACsec policy that is using the new keychain to **should-secure** mode.
  2. Verify that the affected interfaces are using **should-secure** mode.
  3. Update MACsec policy to use new keychain.
  4. Verify that relevant interfaces with active MACsec sessions are using the new keychain.
  5. Change MACsec policy to **must-secure** mode.
- Use the following procedure to disable/remove a MACsec policy deployed in **must-secure** mode:
  1. Change the MACsec policy to **should-secure**.
  2. Verify that the affected interfaces are using **should-secure** mode.
  3. Disable/remove the MACsec policy.

Keychain Definition

- There should be one key in the keychain with a start time of **now**. If **must-secure** is deployed with a keychain that does not have a key that is immediately active then traffic will be blocked on that link until the key becomes current and a MACsec session is started. If **should-secure** mode is being used then traffic will be unencrypted until the key becomes current and a MACsec session has started.

- There should be one key in the keychain with an end time of **infinite**. When a keychain expires, then traffic is blocked on affected interfaces which are configured for **must-secure** mode. Interfaces configured for **should-secure** mode transmit unencrypted traffic.
- There should be overlaps in the end time and start time of keys that are used sequentially to ensure the MACsec session stays up when there is a transition between keys.

Configuring MACsec for Fabric Links Using the GUI

Procedure

Step 1 On the menu bar, click **Fabric** > **Fabric Policies** > **Policies** > **MACsec** > **Interfaces**. In the **Navigation** pane, right click on **Interfaces** to open **Create MACsec Fabric Interface Policy** and perform the following actions:

a) In the **Name** field, enter a name for the MACsec Fabric Interface policy.
b) In the **MACsec Parameters** field, either select a previously configured MACsec Parameters policy or create a new one.
c) In the **MACsec Keychain Policy** field, either select a previously configured MACsec Parameters policy or create a new one and click **Submit**.

To create a **MACsec Keychain Policy**, see Configuring MACsec Keychain Policy Using the GUI, on page 7.

Step 2 To apply the **MACsec Fabric Interface Policy** to a Fabric Leaf or Spine Port Policy Group, in the Navigation pane, click **Interfaces** > ***Leaf/Spine*** **Interfaces** > **Policy Groups** > ***Spine/Leaf*** **Port Policy Group_*name***. In the **Work** pane, select the **MACsec Fabric Interface Policy** just created.

Step 3 To apply the **MACsec Fabric Interface Policy** to a Pod Policy Group, in the Navigation pane, click **Pods** > **Policy Groups** > **Pod Policy Group_*name***. In the **Work** pane, select the **MACsec Fabric Interface Policy** just created.

Configuring MACsec for Access Links Using the GUI

Procedure

Step 1 On the menu bar, click **Fabric** > **External Access Policies**. In the **Navigation** pane, click on **Policies** > **Interface** > **MACsec** > **Interfaces** and right click on **Interfaces** to open **Create MACsec Fabric Interface Policy** and perform the following actions:

a) In the **Name** field, enter a name for the MACsec Access Interface policy.
b) In the **MACsec Parameters** field, either select a previously configured MACsec Parameters policy or create a new one.
c) In the **MACsec Keychain Policy** field, either select a previously configured MACsec Parameters policy or create a new one and click **Submit**.

To create a **MACsec Keychain Policy**, see Configuring MACsec Keychain Policy Using the GUI, on page 7.

Step 2 To apply the **MACsec Access Interface Policy** to a Fabric Leaf or Spine Port Policy Group, in the Navigation pane, click **Interfaces** > ***Leaf/Spine*** **Interfaces** > **Policy Groups** > ***Spine/Leaf*** **Policy Group_*name***. In the **Work** pane, select the **MACsec Fabric Interface Policy** just created.

Configuring MACsec Parameters Using the APIC GUI

Procedure

Step 1 On the menu bar, click **Fabric** > **Access Policies**. In the **Navigation** pane, click on **Interface Policies** > **Policies** and right click on **MACsec Policies** to open **Create MACsec Access Parameters Policy** and perform the following actions:

a) In the **Name** field, enter a name for the MACsec Access Parameters policy.

b) In the **Security Policy** field, select a mode for encrypted traffic and click **Submit**.

Note
Before deploying MACsec in **Must Secure Mode**, the keychain must be deployed on the affected interface or the interface will go down.

Step 2 To apply the **MACsec Access Parameters Policy** to a Leaf or Spine Port Policy Group, in the Navigation pane, click **Interface Policies** > **Policy Groups** > **Spine/Leaf Policy Group_*name***. In the **Work** pane, select the **MACsec Access Interface Policy** just created.

Configuring MACsec Keychain Policy Using the GUI

Procedure

Step 1 On the menu bar, click **Fabric** > **Fabric Policies** > **Policies** > **MACsec** > **KeyChains**. In the **Navigation** pane, right click on **KeyChains** to open **Create MACsec Keychain Policy** and perform the following actions:

a) In the **Name** field, enter a name for the MACsec Fabric Interface policy.

b) Expand the **MACsec Key Policy** table to create the Key policy.

Step 2 In the **MACsec Key Policy** dialog box perform the following actions:

a) In the **Name** field, enter a name for the MACsec Key policy.

b) In the **Key Name** field, enter a key name (up to 64 hexadecimal characters).

Note
A maximum of 64 keys are supported per keychain.

c) In the **Pre-shared Key** field, enter the pre-shared key information.

Note
- For 128-bit cipher suites only 32 character PSKs are permitted.

- For 256-bit cipher suites only 64 Character PSKs are permitted.

d) In the **Start Time** field, select a date for the key to become valid.
e) In the **End Time** field, select a date for the key to expire. Click **Ok** and **Submit**.

Note
When defining multiple keys in a keychain, the keys must be defined with overlapping times in order to assure a smooth transition from the old key to the new key. The endTime of the old key should overlap with the startTime of the new key.

For configuring the Keychain policy through Access Policies, on the menu bar click **Fabric** > **External Access Policies**. In the **Navigation** pane, click on **Policies** > **Interface** > **MACsec** > **MACsec KeyChain Policies** and right click on to open **Create MACsec Keychain Policy** and perform the steps above.

Configuring MACsec Using the NX-OS Style CLI

Procedure

Step 1 Configure MACsec Security Policy for access interfaces

Example:

```
apic1# configure
apic1(config)#   template macsec access security-policy accmacsecpol1
apic1(config-macsec-param)#     cipher-suite gcm-aes-128
apic1(config-macsec-param)#     conf-offset offset-30
apic1(config-macsec-param)#     description 'description for mac sec parameters'
apic1(config-macsec-param)#     key-server-priority 1
apic1(config-macsec-param)#     sak-expiry-time 110
apic1(config-macsec-param)#     security-mode must-secure
aapic1(config-macsec-param)#     window-size 1
apic1(config-macsec-param)#     exit
apic1(config)#
```

Step 2 Configure MACsec key chain for access interface:

PSK can be configured in 2 ways:

Note
- Inline with the **psk-string** command as illustrated in key 12ab below. The PSK is not secure because it is logged and exposed.
- Entered separately in a new command **Enter PSK string** after the **psk-string** command as illustrated in key ab12. The PSK is secured because it is only echoed locally and is not logged.

Example:

```
apic1# configure
apic1(config)#   template macsec access keychain acckeychainpol1
apic1(config-macsec-keychain)#     description 'macsec key chain kc1'
apic1(config-macsec-keychain)#     key 12ab
```

```
apic1(config-macsec-keychain-key)#       life-time start 2017-09-19T12:03:15 end 2017-12-19T12:03:15
apic1(config-macsec-keychain-key)#       psk-string 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)#       exit
apic1(config-macsec-keychain)#     key ab12
apic1(config-macsec-keychain-key)#       life-time start now end infinite
apic1(config-macsec-keychain-key)#       life-time start now end infinite
apic1(config-macsec-keychain-key)# psk-string
Enter PSK string: 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)# exit
apic1(config-macsec-keychain)# exit
apic1(config)#
```

Step 3 Configure MACsec interface policy for access interface:

Example:

```
apic1# configure
apic1(config)#   template macsec access interface-policy accmacsecifpol1
apic1(config-macsec-if-policy)#     inherit macsec security-policy accmacsecpol1 keychain
acckeychainpol1
apic1(config-macsec-if-policy)#     exit
apic1(config)#
```

Step 4 Associate MACsec interface policy to access interfaces on leaf (or spine):

Example:

```
apic1# configure
apic1(config)#   template macsec access interface-policy accmacsecifpol1
apic1(config-macsec-if-policy)#     inherit macsec security-policy accmacsecpol1 keychain
acckeychainpol1
apic1(config-macsec-if-policy)#     exit
apic1(config)
```

Step 5 Configure MACsec Security Policy for fabric interfaces:

Example:

```
apic1# configure
apic1(config)#   template macsec fabric security-policy fabmacsecpol1
apic1(config-macsec-param)#     cipher-suite gcm-aes-xpn-128
apic1(config-macsec-param)#     description 'description for mac sec parameters'
apic1(config-macsec-param)#     window-size 1
apic1(config-macsec-param)#     sak-expiry-time 100
apic1(config-macsec-param)#     security-mode must-secure
apic1(config-macsec-param)#     exit
apic1(config)#
```

Step 6 Configure MACsec key chain for fabric interface:

PSK can be configured in 2 ways:

Note

- Inline with the **psk-string** command as illustrated in key 12ab below. The PSK is not secure because it is logged and exposed.
- Entered separately in a new command **Enter PSK string** after the **psk-string** command as illustrated in key ab12. The PSK is secured because it is only echoed locally and is not logged.

Example:

```
apic1# configure
apic1(config)#   template macsec fabric security-policy fabmacsecpol1
apic1(config-macsec-param)#     cipher-suite gcm-aes-xpn-128
apic1(config-macsec-param)#     description 'description for mac sec parameters'
```

```
apic1(config-macsec-param)#     window-size 1
apic1(config-macsec-param)#     sak-expiry-time 100
apic1(config-macsec-param)#     security-mode must-secure
apic1(config-macsec-param)#     exit
apic1(config)#   template macsec fabric keychain fabkeychainpol1
apic1(config-macsec-keychain)#     description 'macsec key chain kc1'
apic1(config-macsec-keychain)#     key 12ab
apic1(config-macsec-keychain-key)#       psk-string 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)#       life-time start 2016-09-19T12:03:15 end 2017-09-19T12:03:15
apic1(config-macsec-keychain-key)#       exit
apic1(config-macsec-keychain)#     key cd78
apic1(config-macsec-keychain-key)# psk-string
Enter PSK string: 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)# life-time start now end infinite
apic1(config-macsec-keychain-key)# exit
apic1(config-macsec-keychain)# exit
apic1(config)#
```

Step 7 Associate MACsec interface policy to fabric interfaces on leaf (or spine):

Example:

```
apic1# configure
apic1(config)#   leaf 101
apic1(config-leaf)#     fabric-interface ethernet 1/52-53
apic1(config-leaf-if)#       inherit macsec interface-policy fabmacsecifpol2
apic1(config-leaf-if)#       exit
apic1(config-leaf)#
```