Configuring MACsec

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.

MACsec encrypts the entire data except for the Source and Destination MAC addresses of an Ethernet packet. It offers the following capabilities:

- Provides line rate encryption.
- Ensures data confidentiality by providing strong encryption at Layer 2.
- Provides integrity checking to help ensure that data cannot be modified in transit.
- Key Lifetime and Hitless Key Rollover, on page 2
- Fallback Key, on page 2

Key Lifetime and Hitless Key Rollover

A MACsec keychain can have multiple pre-shared keys (PSKs), each configured with a key ID and an optional lifetime. A key lifetime specifies at which time the key activates and expires. In the absence of a lifetime configuration, the default lifetime is unlimited. When a lifetime is configured, MKA rolls over to the next configured pre-shared key in the keychain after the lifetime is expired. The time zone of the key can be local or UTC. The default time zone is UTC.

To configure a MACsec keychain, see Creating a MACsec Keychain, on page 8

A key can roll over to a second key within the same keychain by configuring the second key (in the keychain) and configuring a lifetime for the first key. When the lifetime of the first key expires, it automatically rolls over to the next key in the list. If the same key is configured on both sides of the link at the same time, then the key rollover is hitless (that is, the key rolls over without traffic interruption).

Note The lifetime of the keys are overlapped to achieve hitless key rollover.

Fallback Key

A MACsec session can fail due to a key/key ID (CKN) mismatch or a finite key duration between the Fabric Interconnect and the peer. If a MACsec session fails, a fallback session can take over if a fallback key is configured. A fallback session prevents downtime due to primary session failure and allows a user time to fix the key issue causing the failure. A fallback key also provides a backup session if the primary session fails to start. This feature is optional.

For more information, see Creating a MACsec Keychain .

Guidelines and Limitations for MACsec

MACsec functionality supports the following:

- Ethernet Uplink interfaces
- Ethernet Port-channel member link interfaces

- MKA is the only supported key exchange protocol for MACsec.

Note The Security Association Protocol (SAP) is not supported.

MACsec functionality does not support the following:

- Unified uplink
- FCoE uplinks
- Server, Storage, and Appliance ports
- QSA
- Link-level flow control (LLFC) and priority flow control (PFC)
- Multiple MACsec peers (different SCI values) for the same interface
- 1G port or any port on a MAC block that has 1G ports on it.

Note MACsec configuration is supported on end host mode only.

Cisco UCS Fabric Interconnect Limitations

Cisco UCS Manager 4.3(4a) release supports MACsec functionality from Cisco UCS 6454, Cisco UCS 64108, and Cisco UCS 6536 series fabric interconnects onwards.

Keychain Limitations

- You cannot overwrite the Key Hex String when the MACsec Keychain is applied on the interface. Instead, you must delete the old key and create the new key or a new keychain.
- For a given keychain, key activation time must overlap to avoid any period of time when no key is activated. If a time period occurs during which no key is activated, session negotiation fails and traffic drops can occur. The key with the latest start time among the currently active keys takes precedence for a MACsec key rollover.

Fallback Limitations

- If a MACsec session is secured on an old primary key, it does not go to a fallback session in case of mismatched latest active primary key. So the session remains secured on the old primary key and shows as rekeying on the old CA (Connectivity Association) under status. And the MACsec session on the new key on primary PSK will be in the Init state.
- Use only one key with infinite lifetime in the fallback key chain. Multiple keys are not supported.
- The key ID (CKN) used in the fallback key chain must not match with any of the key IDs (CKNs) used in the primary key chain of the same switch interface and peer upstream switch interface.
- Once configured, fallback configuration on an interface cannot be removed, unless the complete MACsec configuration on the interface is removed.

MACsec Policy Limitations

- BPDU packets can be transmitted before a MACsec session becomes secure.
- We recommend you to apply the same security policy **Should Secure-Should Secure** or **Must Secure-Must Secure** on the fabric interconnect and the peer switch interface.

Note Configuring MACsec with security-policy as **must-secure** on an Uplink Interface brings down the port, and the traffic drops until the MACsec session is secured.

Layer 2 Tunneling Protocol (L2TP) Restrictions

MACsec is not supported on ports that are configured for dot1q tunneling or L2TP.

MACsec EAPOL Limitations

- For enabling EAPOL (Extensible Authentication Protocol over LAN) configuration, the range of Ethernet type between 0 to 0x599 is invalid.
- While configuring EAPOL packets, the following combinations must not be used:
  - MAC Address 0100.0ccd.cdd0 with any ethertype
  - Any MAC Address with Ether types: 0xfff0, 0x800, 0x86dd
  - The default destination MAC address, 0180.c200.0003 with the default Ethernet type, 0x888e
  - Different EAPOL DMAC addresses and Ethertype on both MACsec peers. The MACsec session works only if the MACsec peer is sending MKAPDUs with the DMAC and Ethertype configured locally.
  - Within the same slice of the forwarding engine, EAPOL ethertype and dot1q ethertype cannot have the same value.
  - More than one custom EAPOL is not supported.
  - You cannot modify a custom EAPOL configuration if applied on any interface.

Statistics Limitations

- Statistics are cumulative.
- Few CRC errors may occur during the transition between MACsec and non-MACsec mode (regular port shut/no shut).
- The IEEE8021-SECY-MIB OIDs secyRxSAStatsOKPkts, secyTxSAStatsProtectedPkts, and secyTxSAStatsEncryptedPkts can carry only up to 32 bits of counter values, but the traffic may exceed 32 bits.

Enabling or Disabling MACsec Configuration

Note Disabling MACsec only deactivates this feature and does not remove the associated MACsec configurations.

Before you begin

Ensure that MACsec is enabled.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec**.

Step 3 Click the **General** tab.

Step 4 In the **Admin State** field, click the **Enabled** radio button to enable MACsec or the **Disabled** radio button to disable MACsec.

Table 1: Properties Area

Name	Description
Admin State radio button	Allows you to enable the MACsec feature. Disabling the MACsec feature removes the operational MACsec configuration from the interface, which causes the interface to go down.

Step 5 Click **Save Changes** to save the configuration change.

Creating a MACsec Policy

You can create multiple MACsec policies with different parameters. However, only one policy can be active on an interface.

Before you begin

Ensure that MACsec is enabled.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Policy**.

Step 3 Click **Add**.

Step 4 In the **Create MACsec Policy** dialog box, complete the following fields:

Name	Description
Name field	Name of the MACsec policy.
Description field	Enter a brief description for the policy.
Cipher Suite radio button	Allows you to select the cipher suite used for the encryption along with associated attributes of related to the encryption. This can be one of the following: • GCM AES XPN 256 • GCM AES XPN 128 • GCM AES 256 • GCM AES 128
Key Server Priority field	Allows you to enter the key server priority. You can enter a value between 0-255. Lower the value, higher the preference to be selected as the key server.
Security Policy radio button	Allows you to configure the security policy parameters. This can be one of the following: • **Must Secure**—Must-Secure imposes only MACsec encrypted traffic to flow. Hence, until the MKA session is not secured, traffic is dropped. • **Should Secure**— Allows unencrypted traffic to flow until the MKA session is secured. After the MKA session is secured, the **Should-Secure** policy imposes only encrypted traffic to flow. This is the default value.
Replay Window Size field	Allows you to configure the window size.
Sak Expiry Time field	Configures the time in seconds to force an SAK rekey.
Conf Offset radio button	Configures one of the following confidentiality offsets in the Layer 2 frame, where encryption begins: CONF-OFFSET-0, CONF-OFFSET-30, or CONF-OFFSET-50.
Include lcv Param radio button	Configure the ICV for the frame arriving on the port.

Step 5 Click **OK**.

Viewing or Modifying a MACsec Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Policy**.

Step 3 Select the MACsec policy, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view or modify the following:

Name	Description
Name field	Name of the MACsec policy.
Description field	Enter a brief description for the policy.
Cipher Suite radio button	Allows you to select the cipher suite used for the encryption along with associated attributes of related to the encryption. This can be one of the following: • GCM AES XPN 256 • GCM AES XPN 128 • GCM AES 256 • GCM AES 128
Key Server Priority field	Allows you to enter the key server priority. You can enter a value between 0-255. Lower the value, higher the preference to be selected as the key server.
Security Policy radio button	Allows you to configure the security policy parameters. This can be one of the following: • **Must Secure**—Must-Secure imposes only MACsec encrypted traffic to flow. Hence, until the MKA session is not secured, traffic is dropped. • **Should Secure**— Allows unencrypted traffic to flow until the MKA session is secured. After the MKA session is secured, the **Should-Secure** policy imposes only encrypted traffic to flow. This is the default value.
Replay Window Size field	Allows you to configure the window size.
Sak Expiry Time field	Configures the time in seconds to force an SAK rekey.

Name	Description
Conf Offset radio button	Configures one of the following confidentiality offsets in the Layer 2 frame, where encryption begins: CONF-OFFSET-0, CONF-OFFSET-30, or CONF-OFFSET-50.
Include lcv Param radio button	Configure the ICV for the frame arriving on the port.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec Policy

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Policy**.

Step 3 In the **Actions** area, click **Delete** to delete a MACsec policy configuration.

Step 4 Click **Yes** in the confirmation dialog box.

Creating a MACsec Keychain

Only MACsec keychains result in converged MKA sessions.

You can create a MACsec keychain and keys on the device.

Before you begin

Ensure that MACsec is enabled.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Click **Add** to create a MACsec Keychain.

Step 4 In the **Create MACsec Keychain** dialog box, complete the following fields:

Name	Description
Name field	Enter a suitable name for the keychain and click **OK** to save.

Step 5 Click **OK**.

Viewing or Modifying a MACsec Keychain

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Select the MACsec keychain, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify of the following:

Name	Description
Name field	Enter a suitable name for the keychain and click **OK** to save.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec Keychain

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 In the **Actions** area, click **Delete** to delete a MACsec keychain configuration.

Step 4 Click **Yes** in the confirmation dialog box .

Creating a MACsec Key

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Choose a MACsec keychain.

Step 4 In the **Actions** area, click **Create MACsec Key**.

Step 5 In the **Create MACsec Key** dialog box, complete the following fields:

Name	Description
Key ID field	Allows you to enter the key ID (CKN) used in the primary key chain. **Note** Key IDs must be unique under a keychain configuration.
Key Hex String field	Consists of 32 to up to 144 hexadecimal characters. For a type-0 (un-encrypted key) the length of the key is 32 hexadecimal characters for an **AES_128_CMAC** cryptographic algorithm and 64 hexadecimal characters for an **AES_256_CMAC** cryptographic algorithm.
Encrypt Type radio button	Allows you to select the encrypt type. The encrypt type includes the following: • **Type 0**—When the configured key-hex-string is an unencrypted string, type-0 must be selected. • **Type 7**—When the configured key-hex-string is a Type-7 encrypted string, this option must be selected.
Cryptographic Algorithm radio button	Set cryptographic authentication algorithm with 128-bit or 256-bit encryption.

Step 6 Click **OK**.

Viewing or Modifying a MACsec Key

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Select the MACsec Key, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify of the following:

Name	Description
Key ID field	Allows you to enter the key ID (CKN) used in the primary key chain. **Note** Key IDs must be unique under a keychain configuration.

Name	Description
Key Hex String field	Consists of 32 to up to 144 hexadecimal characters. For a type-0 (un-encrypted key) the length of the key is 32 hexadecimal characters for an **AES_128_CMAC** cryptographic algorithm and 64 hexadecimal characters for an **AES_256_CMAC** cryptographic algorithm.
Encrypt Type radio button	Allows you to select the encrypt type. The encrypt type includes the following: • **Type 0**—When the configured key-hex-string is an unencrypted string, type-0 must be selected. • **Type 7**—When the configured key-hex-string is a Type-7 encrypted string, this option must be selected.
Cryptographic Algorithm radio button	Set cryptographic authentication algorithm with 128-bit or 256-bit encryption.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec Key

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Choose a MACsec key.

Step 4 In the **Actions** area, click **Delete** to delete a MACsec key.

Step 5 Click **Yes** in the confirmation dialog box.

Creating a LifeTime

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Choose a MACsec key.

Step 4 In the **Actions** area, click **Create LifeTime**.

Step 5 In the **Create LifeTime** dialog box, complete the following fields:

Name	Description
Start Date Time field	The start date time is the time of day and date that the key becomes active. Allows you to enter a start date in YYYY-MM-DD HH:MM:SS format.
End Date Time field	Allows you to enter an end date in YYYY-MM-DD HH:MM:SS format.
Duration field	Allows you to enter length of the LifeTime in seconds. The duration is the length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).
Time Zone radio button	Allows you to select a timezone.

Step 6 Click **OK**.

Viewing or Modifying a MACsec Key Lifetime

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Select the MACsec Key Lifetime, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify the following:

Name	Description
Start Date Time field	The start date time is the time of day and date that the key becomes active. Allows you to enter a start date in YYYY-MM-DD HH:MM:SS format.
End Date Time field	Allows you to enter an end date in YYYY-MM-DD HH:MM:SS format.
Duration field	Allows you to enter length of the LifeTime in seconds. The duration is the length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).
Time Zone radio button	Allows you to select a timezone.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec Key Lifetime

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Keychain**.

Step 3 Select the MACsec key, which you want to delete.

Step 4 In the **Actions** area, click **Delete LifeTime** to delete a MACsec Lifetime configuration.

Step 5 Click **Yes** in the confirmation dialog box.

Creating a MACsec Interface Configuration

Configure different keychain for primary and fallback PSKs.

We recommend that you first change the primary PSK and save the changes. Then, change the fallback PSK.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Interface Configuration**.

Step 3 In the **Properties** area, click **Add**.

Step 4 In the **Create MACsec Interface Configuration** dialog box, complete the following fields:

Name	Description
Name field	Enter a name for the MACsec interface configuration.
MACsec Keychain Name drop-down list	Allows you to select MACsec keychain from the drop-down list.
MACsec Fallback KeyChain Name drop-down list	Allows you to select MACsec backup keychain from the drop-down list.
MACsec Policy Name drop-down list	Allows you to select MACsec policy from the drop-down list.
MACsec EAPOL Name drop-down list	Allows you to select MACsec EAPOL from the drop-down list.

For more information on MACsec EAPOL, see Configurable EAPOL Destination and Ethernet Type.

Step 5 Click **OK**.

Viewing or Modifying a MACsec Interface Configuration

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Interface Configuration**.

Step 3 Select the MACsec interface configuration, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify the following:

Name	Description
Name field	Enter a name for the MACsec interface configuration.
MACsec Keychain Name drop-down list	Allows you to select MACsec keychain from the drop-down list.
MACsec Fallback KeyChain Name drop-down list	Allows you to select MACsec backup keychain from the drop-down list.
MACsec Policy Name drop-down list	Allows you to select MACsec policy from the drop-down list.
MACsec EAPOL Name drop-down list	Allows you to select MACsec EAPOL from the drop-down list.

For more information on MACsec EAPOL, see Configurable EAPOL Destination and Ethernet Type.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec Interface Configuration

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **Interface Configuration**.

Step 3 In the **Actions** area, click **Delete** to delete a MACsec interface configuration.

Step 4 Click **Yes** in the confirmation dialog box .

Configuring MACsec on an Uplink Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > ***Fabric*** > **Uplink Eth Interfaces**.

Step 3 Select an Ethernet Uplink interface.

Step 4 In the **Properties** area, in the **Interface Configuration** field, choose the MACsec interface configuration that was created, and apply it on the interface.

Step 5 Click **Save Changes** to save the configuration change.

Viewing or Modifying MACsec on an Uplink Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > ***Fabric*** > **Uplink Eth Interfaces**.

Step 3 Select an Ethernet Uplink interface.

Step 4 In the **Properties** area, view or modify the properties as required.

Step 5 Click **Save Changes** to save the configuration change.

Deleting MACsec on an Uplink Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > ***Fabric*** > **Uplink Eth Interfaces**.

Step 3 Select an Ethernet Uplink interface.

Step 4 In the **Properties** area, in the **MACsec Interface Configuration** field, choose **<not-set>** to delete an interface.

Step 5 Click **Save Changes** to save the configuration change.

Configuring MACsec on an Uplink Port Channel Member Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > ***Fabric*** > **Port Channels**.

Step 3 Select a Ethernet Port Channel Member interface.

Step 4 In the **Properties** area, in the **MACsec Interface Configuration** field, choose the MACsec interface configuration that was created, and apply it on the interface.

Step 5 Click **Save Changes** to save the configuration change.

Viewing or Modifying MACsec on an Uplink Port Channel Member Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > ***Fabric*** > **Port Channels**.

Step 3 Select a Ethernet Port Channel Member interface.

Step 4 In the **Properties** area, view or modify the properties as required.

Step 5 Click **Save Changes** to save the configuration change.

Deleting MACsec on an Uplink Port Channel Member Interface

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Expand **LAN** > **LAN Cloud** > ***Fabric*** > **Port Channels**.

Step 3 Select a Ethernet Port Channel Member interface.

Step 4 In the **Properties** area, in the **MACsec Interface Configuration** field, choose **<not-set>** to delete an interface.

Step 5 Click **Save Changes** to save the configuration change.

Configurable EAPOL Destination and Ethernet Type

Configurable EAPOL MAC and Ethernet type provides you the ability to change the MAC address and the Ethernet type of the MKA packet, to allow CE device to form MKA sessions over the ethernet networks that consume the standard MKA packets.

The EAPOL destination Ethernet type can be changed from the default Ethernet type of 0x888E to an alternate value or, the EAPOL destination MAC address can be changed from the default DMAC of 01:80:C2:00:00:03 to an alternate value, to avoid being consumed by a provider bridge.

This feature is available at the interface level and the alternate EAPOL configuration can be changed on any interface at any given time as follows:

- If the MACsec is already configured on an interface, the sessions comes up with a new alternate EAPOL configuration.
- When MACsec is not configured on an interface, the EAPOL configuration is applied to the interface and is effective when MACsec is configured on that inferface.

Creating a MACsec EAPOL

You can enable the EAPOL configuration on any available interface.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **EAPOL**.

Step 3 In the **Properties** area, click **Add** to create a MACsec EAPOL configuration.

Step 4 In the **Create MACsec EAPOL** dialog box, complete the following fields:

Name	Description
Name field	Enter a name for the MACsec EAPOL.
Description field	Enter a brief description for the MACsec EAPOL.
MAC Address field	Enter the MAC address where you wish to enable the EAPOL configuration.
Ether Type field	Enter the Ethernet type.

Step 5 Click **OK**.

Viewing or Modifying a MACsec EAPOL

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **EAPOL**.

Step 3 Select the MACsec EAPOL, which you want to view or modify.

Step 4 In the **General** tab, under the **Properties** window, you can view and modify the following:

Name	Description
Name field	Enter a name for the MACsec EAPOL.
Description field	Enter a brief description for the MACsec EAPOL.
MAC Address field	Enter the MAC address where you wish to enable the EAPOL configuration.
Ether Type field	Enter the Ethernet type.

Step 5 Click **Save Changes** to save the configuration change.

Deleting a MACsec EAPOL

Procedure

Step 1 In the **Navigation** pane, click **LAN**.

Step 2 Navigate to **LAN** > **MACsec** > **EAPOL**.

Step 3 In the **Actions** area, click **Delete** to delete a MACsec EAPOL configuration.

Step 4 Click **Yes** in the confirmation dialog box .

Displaying MACsec Sessions

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > **Fabric_Interconnect_Name** > **Fixed Module** > **Ethernet Ports** .

Step 3 Click a port under the Ethernet Ports node.

Step 4 Click the **General** tab.

The Operational states of the MACsec session on an interface are displayed.

The possible values for operational states are as follows:

- MACsec Status—Init, Pending, Secured, Rekeyed
- MACsec Key-server—yes, no
- MACsec Auth-mode—Primary-PSK, Fallback-PSK

Displaying MACsec Statistics

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Fabric Interconnects** > **Fabric_Interconnect_Name** > **Fixed Module** > **Ethernet Ports** .

Step 3 Click a port under the Ethernet Ports node.

Step 4 In the Work pane, click the **Statistics** tab.

The MACsec RX Stats and MACsec TX Stats counters are displayed.

The following example shows the MACsec security statistics for a specific Ethernet interface.

Note The following differences exist for uncontrolled and controlled packets in Rx and Tx statistics:

Rx statistics:

- Uncontrolled = Encrypted and unencrypted
- Controlled = Decrypted

Tx statistics:

- Uncontrolled = Unencrypted
- Controlled = Encrypted