Configuring MACsec

This document describes how to configure MACsec on Cisco NX-OS devices.

Configuring MACsec

This document describes how to configure MACsec on Cisco NX-OS devices.

About MACsec

Media Access Control Security (MACsec) an IEEE 802.1AE along with MACsec Key Agreement (MKA) protocol provide secure communications on Ethernet links. It offers the following :

- Provides line rate encryption capabilities.
- Helps to ensure data confidentiality by providing strong encryption at Layer 2.
- Provides integrity checking to help ensure that data cannot be modified in transit.
- Can be selectively enabled using a centralized policy to help ensure that it is enforced where required while allowing non-MACsec-capable components to access the network.
- Encrypts packets on a hop-by-hop basis at Layer 2, allowing the network to inspect, monitor, mark, and forward traffic according to your existing policies, unlike end-to-end Layer 3 encryption techniques that hide the contents of packets from the network devices they cross.

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 expires. The time zone of the key can be local or UTC. The default time zone is UTC.

To configure a MACsec keychain, see Configuring a MACsec Keychain and Keys, on page 5.

A key can roll over to a second key within the same keychain by configuring the second key and 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.

Fallback Key

A MACsec session can fail due to a key/key name (CKN) mismatch or a finite key duration between the switch and a peer. If a MACsec session does fail, 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.

To configure a MACsec fallback key, see Configuring MACsec Fallback Key, on page 7.

Guidelines and Limitations for MACsec

MACsec has the following guidelines and limitations:

- MACsec is supported on the following interface types:
  - Layer 2 switch ports (access and trunk)
  - Layer 3 routed interfaces (no subinterfaces)

Note Enabling MACsec on the Layer 3 routed interface also enables encryption on all the subinterfaces that are defined under that interface. However, selectively enabling MACsec on a subset of subinterfaces of the same Layer 3 routed interface is not supported.

  - Individual Layer 2 and Layer 3-port channel members (no subinterfaces)
- Secure Channel Identified (SCI) encoding cannot be disabled on Cisco Nexus 3600 Series switches.
- Support for MACsec is not available for Cisco Nexus ToR switches when you downgrade from Release 10.x.
- MKA is the only supported key exchange protocol for MACsec. The Security Association Protocol (SAP) is not supported.
- Link-level flow control (LLFC) and priority flow control (PFC) are not supported with MACsec.
- Multiple MACsec peers (different SCI values) for the same interface are not supported.
- You can retain the MACsec configuration when you disable MACsec using the **macsec shutdown** command.
- MACsec sessions are liberal in accepting packets from a key server whose latest Rx and latest Tx flags have been retired after Tx SA installation for the first time. The MACsec session then converges into a secure state.
- Beginning with Cisco NX-OS Release 10.1(1), you can modify MACSec policy while the policy is referenced by an interface.
- Beginning with Cisco Nexus Release 10.1(1), MACsec is supported on the Cisco Nexus N3KC3636C-R platform switches.

- N3K-C3636C-R—MACsec is supported on the following eight ports of N3K-C3636C-R, marked in green [Ports 29–36].

Note On the Cisco N3K-C3636C-R platform switches, when MACsec is either configured or unconfigured on a port, there will be a port-flap occurrence irrespective of MACsec security-policy type.

- Cisco Nexus 3600 Series switches do not support MACsec on any of the MACsec capable ports when QSA is being used.
- MACsec is not supported on breakout ports, and breakout is not supported on the following eight ports, from Port 29 to Port 36, of N3K-C3636C-R when MACsec is configured.
- Packet drops for a short period when the conf-offset parameter is changed dynamically for a MACsec policy. Change the conf-offset parameter only in static configuration when the policy is not active on the port.
- Beginning with Cisco Nexus Release 10.3(3)F, MACsec is supported on Cisco N3K-C36180YC-R switches with the following limitations:
  - MACsec is supported only on the Eth1/49, Eth1/51, Eth1/52, Eth1/53, and Eth1/54 ports.
  - MACsec must not be configured on the Eth1/50 port, as it brings the link down.

Keychain Restrictions:

- You cannot overwrite the octet string for a MACsec key. Instead, you must create a new key or a new keychain.
- A new key in the keychain is configured when you enter end or exit. The default timeout for editor mode is 6 seconds. If the key is not configured with the key octet string or/and the send lifetime within the 6-second window, incomplete information may be used to bring up the MACsec session and could result in the session being stuck in an Authorization Pending state. If the MACsec sessions are not converged after the configuration is complete, you might be advised to shut/no shut the ports.
- For a given keychain, key activation times should 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 Restrictions:

- 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 will show as rekeying on the old CA under status. And the MACsec session on the new key on primary PSK will be in 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 any of the key IDs (CKNs) used in the primary key chain.

- Once configured, fallback configuration on an interface cannot be removed, unless the complete MACsec configuration on the interface is removed.

MACsec Policy Restrictions:

- BPDU packets can be transmitted before a MACsec session becomes secure.

Layer 2 Tunneling Protocol (L2TP) Restrictions:

- MACsec is not supported on ports configured for dot1q tunneling or L2TP.
- L2TP does not work if STP is enabled on trunk ports for non-native VLANs.

Statistics Restrictions:

- Few CRC errors should 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 MACsec

Before you can access the MACsec and MKA commands, you must enable the MACsec feature.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature macsec** **Example:** `switch(config)# feature macsec`	Enables MACsec and MKA on the device.
Step 3	(Optional) copy running-config startup-config **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Disabling MACsec

Beginning with Cisco NX-OS Release 10.1(1), disabling the MACsec feature only deactivates this feature and does not remove the associated MACsec configurations.

Disabling MACsec has the following conditions:

- MACsec shutdown is global command and is not available at the interface level.
- The macsec shutdown, show macsec mka session/summary, show macsec mka session detail, and show macsec mka/secy statistics commands will display the 'Macsec is shutdown' message. However, the show macsec policy and show key chain commands will display the output.
- Consecutive MACsec status changes from macsec shutdown to no macsec shutdown and vice versa needs a 30 seconds time interval in between the status change.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**macsec shutdown** **Example:** `switch(config)# macsec shutdown`	Disables the MACsec configuration on the device. The **no** option restores the MACsec feature.
Step 3	(Optional) copy running-config startup-config **Example:** `switch(config)# copy running-config startup-config`	Copies the running configuration to the startup configuration. This step is required only if you want to retain the MACsec in the shutdown state after the switch reload. **Note** You can also disable the MACsec feature using the **no feature macsec** command.

Configuring a MACsec Keychain and Keys

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

Note Only MACsec keychains will result in converged MKA sessions.

Before you begin

Make sure that MACsec is enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose
Step 2	(Optional) [**no**] **key-chain macsec-psk no-show** **Example:** `switch(config)# key-chain macsec-psk no-show`	Hides the encrypted key octet string in the output of the **show running-config** and **show startup-config** by replacing the string with a wildcard character. By default, PSK keys are displayed in encrypted format and can be easily decrypted. This command applies only to MACsec keychains. **Note** The octet string is also hidden when you save the configuration to a file.

Step 3	**key chain** *name* **macsec**
	Example:
	`switch(config)# key chain 1 macsec`
	`switch(config-macseckeychain)#`
		Creates a MACsec keychain to hold a set of MACsec keys and enters MACsec keychain configuration mode.

Step 4	**key** *key-id*
	Example:
	`switch(config-macseckeychain)# key 1000`
	`switch(config-macseckeychain-macseckey)#`
		Creates a MACsec key and enters MACsec key configuration mode. The range is from 1 to 32 octets, and the maximum size is 64.
		Note The key must consist of an even number of characters.

Step 5	**key-octet-string** *octet-string* **cryptographic-algorithm** {**AES_128_CMAC** | **AES_256_CMAC**}
	Example:
	`switch(config-macseckeychain-macseckey)#`
	`key-octet-string`
	`abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789`
	`cryptographic-algorithm AES_256_CMAC`
		Configures the octet string for the key. The octet-string argument can contain up to 64 hexadecimal characters. The octet key is encoded internally, so the key in clear text does not appear in the output of the **show running-config macsec** command.
		The key octet string includes the following:
		• 0 Encryption Type - No encryption (default)
		• 6 Encryption Type - Proprietary (Type-6 encrypted). For more information, see *Enabling Type-6 Encryption on MACsec Keys*.
		• 7 Encryption Type - Proprietary WORD key octet string with maximum 64 characters
		Note MACsec peers must run the same Cisco NX-OS release in order to use the AES_128_CMAC cryptographic algorithm. To interoperate between previous releases and Cisco NX-OS Release 7.0(3)I7(2) or a later release, you must use keys with the AES_256_CMAC cryptographic algorithm.

Step 6	**send-lifetime** *start-time* **duration** *duration*
	Example:
	`switch(config-macseckeychain-macseckey)#`
	`send-lifetime 00:00:00 Oct 04 2016 duration 100000`
		Configures a send lifetime for the key. By default, the device treats the start time as UTC.
		The *start-time* argument is the time of day and date that the key becomes active. The *duration* argument is the length

	Command or Action	Purpose
		of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).
Step 7	(Optional) **show key chain** *name* **Example:** `switch(config-macseckeychain-macseckey)# show key chain 1`	Displays the keychain configuration.
Step 8	(Optional) copy running-config startup-config **Example:** `switch(config-macseckeychain-macseckey)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring MACsec Fallback Key

Beginning with Cisco NX-OS Release 10.1(1), you can configure a fallback key on the device to initiate a backup session if the primary session fails as a result of a key/key name (CKN) mismatch or a finite key duration between the switch and peer.

Before you begin

Make sure that MACsec is enabled and a primary and fallback keychain and key ID are configured. See Configuring a MACsec Keychain and Keys, on page 5.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *name*
	Example:
	`switch(config)# interface ethernet 1/29`
	`switch(config-if)#`
		Specifies the interface that you are configuring. You can specify the interface type and identity. For an Ethernet port, use ethernet slot/port.

Step 3	**macsec keychain** *keychain-name* **policy** *policy-name* **fallback-keychain** *keychain-name* **Example:** `switch(config-if)# macsec keychain kc2 policy abc fallback-keychain fb_kc2`	Specifies the fallback keychain to use after a MACsec session failure due to a key/key ID mismatch or a key expiration. The fallback key ID should not match any key ID from a primary keychain. Fallback keychain configuration for each interface can be changed on the corresponding interface, without removing the MACsec configuration, by reissuing the same command with the fallback keychain name changed.

	Command or Action	Purpose
		Note The command must be entered exactly the same as the existing configuration command for the interface, except for the fallback keychain name. See Configuring a MACsec Keychain and Keys, on page 5.
Step 4	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring 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

Make sure that MACsec is enabled.

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**macsec policy** *name*
	Example:
	`switch(config)# macsec policy abc`
	`switch(config-macsec-policy)#`
		Creates a MACsec policy.

Step 3	**cipher-suite** *name* **Example:** `switch(config-macsec-policy)# cipher-suite GCM-AES-256`	Configures one of the following ciphers: GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128, or GCM-AES-XPN-256.
Step 4	**key-server-priority** *number* **Example:** `switch(config-macsec-policy)# key-server-priority 0`	Configures the key server priority to break the tie between peers during a key exchange. The range is from 0 (highest) and 255 (lowest), and the default value is 16.
Step 5	**security-policy** *name* **Example:**	Configures one of the following security policies to define the handling of data and control packets:

	Command or Action	Purpose
	`switch(config-macsec-policy)# security-policy should-secure`	• **must-secure**—Packets not carrying MACsec headers will be dropped. • **should-secure**—Packets not carrying MACsec headers will be permitted. This is the default value.
Step 6	**window-size** *number* **Example:** `switch(config-macsec-policy)# window-size 512`	Configures the replay protection window such that the secured interface will not accept any packet that is less than the configured window size. The range is from 0 to 596000000.
Step 7	**sak-expiry-time** *time* **Example:** `switch(config-macsec-policy)# sak-expiry-time 100`	Configures the time in seconds to force an SAK rekey. This command can be used to change the session key to a predictable time interval. The default is 0.
Step 8	**conf-offset** *name* **Example:** `switch(config-macsec-policy)# conf-offset CONF-OFFSET-0`	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. This command might be necessary for intermediate switches to use packet headers {dmac, smac, etype} like MPLS tags.
Step 9	(Optional) **show macsec policy** **Example:** `switch(config-macsec-policy)# show macsec policy`	Displays the MACsec policy configuration.
Step 10	(Optional) **copy running-config startup-config** **Example:** `switch(config-macsec-policy)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Rotating PSKs

Follow this procedure to rotate PSKs when the SAK expiry time is configured for 60 seconds in the MACsec policy.

Step 1 Use the **no sak-expiry-time** command to remove the SAK expiry timer from the MACsec policy.

You need to remove the SAK expiry timer only for the number of policies in the configuration. You do not need to remove it for each interface. If you have defined only one policy and applied it to all interfaces, you need to remove the SAK expiry timer only from this policy.

Step 2 Wait for 2 minutes.

Step 3 Use the **key** *key-id* command to program the new key under the keychain.

Step 4 Once the session with the new key is secured, use the **no key** *key-id* command to delete the old key.

Step 5 Wait for 2 minutes.

Step 6 Use the **sak-expiry-timer 60** command to add the SAK rekey timer to the MACsec policy.

Verifying the MACsec Configuration

To display MACsec configuration information, perform one of the following tasks:

Command	Purpose
show key chain *name*	Displays the keychain configuration.
show macsec mka session [**interface** *type slot/port*] [**detail**]	Displays information about the MACsec MKA session for a specific interface or for all interfaces.
show macsec mka session details	Displays information about the MAC address.
show macsec mka summary	Displays the MACsec MKA configuration.
show macsec policy [*policy-name*]	Displays the configuration for a specific MACsec policy or for all MACsec policies.
show running-config macsec	Displays the running configuration information for MACsec.

The following example displays information about the MACsec MKA session for all interfaces.

```
switch(config)# show macsec mka session
Interface          Local-TxSCI                     # Peers           Status
Key-Server         Auth Mode
------------------ ------------------------------- ------------------ ------------------
------------------ ------------------
Ethernet1/29       6c8b.d3db.e968/0001             1                  Secured
No                 PRIMARY-PSK
Ethernet1/30       6c8b.d3db.e96c/0001             1                  Secured
No                 PRIMARY-PSK
Ethernet1/31       6c8b.d3db.e970/0001             1                  Secured
Yes                PRIMARY-PSK
Ethernet1/32       6c8b.d3db.e974/0001             1                  Secured
Yes                PRIMARY-PSK
Ethernet1/33       6c8b.d3db.e978/0001             1                  Secured
Yes                PRIMARY-PSK
Ethernet1/34       6c8b.d3db.e97c/0001             1                  Secured
Yes                PRIMARY-PSK
Ethernet1/35       6c8b.d3db.e980/0001             1                  Secured
Yes                PRIMARY-PSK
Ethernet1/36       6c8b.d3db.e984/0001             1                  Secured
No                 PRIMARY-PSK
------------------ ------------------------------- ------------------ ------------------
------------------ ------------------
Total Number of Sessions : 8
        Secured Sessions : 8
        Pending Sessions : 0
switch(config)#
```

The following example displays information about the MACsec MKA session for a specific interface. In addition to the common elements of the table as described in the previous example, the following also identifies the authentication mode which defines the current MACsec session type.

```
switch(config)# show macsec mka session interface e1/35
Interface          Local-TxSCI                     # Peers            Status
Key-Server         Auth Mode
------------------ ------------------------------- ------------------ ------------------
------------------ ------------------
Ethernet1/35       6c8b.d3db.e980/0001             1                  Secured
Yes                PRIMARY-PSK
switch(config)#
```

The following example displays detailed information about the MACsec MKA session for a specific Ethernet interface:

```
switch(config)# show macsec mka session interface e1/35 details
Detailed Status for MKA Session
---------------------------------
Interface Name                         : Ethernet1/35
    Session Status                     : SECURED - Secured MKA Session with MACsec
    Local Tx-SCI                       : 6c8b.d3db.e980/0001
    Local Tx-SSCI                      : 2
    MKA Port Identifier                : 2
    CAK Name (CKN)                     : 2006
    CA Authentication Mode             : PRIMARY-PSK
    Member Identifier (MI)             : 50BE8367F1C6D0AB1C442229
    Message Number (MN)                : 1048
    MKA Policy Name                    : mpsr1
    Key Server Priority                : 1
    Key Server                         : Yes
    Include ICV                        : Yes
    SAK Cipher Suite                   : GCM-AES-128
    SAK Cipher Suite (Operational)     : GCM-AES-128
    Replay Window Size                 : 148809600
    Confidentiality Offset             : CONF-OFFSET-30
    Confidentiality Offset (Operational): CONF-OFFSET-30
    Latest SAK Status                  : Rx & TX
    Latest SAK AN                      : 0
    Latest SAK KI                      : 50BE8367F1C6D0AB1C44222900000021
    Latest SAK KN                      : 33
    Last SAK key time                  : 11:23:53 pst Tue Dec 15 2020
    CA Peer Count                      : 1
    Eapol dest mac                     : 0180.c200.0003
    Ether-type                         : 0x888e
Peer Status:
    Peer MI                            : 37AFE73EC8617FD32F70E21A
    RxSCI                              : 6c8b.d3db.e984/0001
    Peer CAK                           : Match
    Latest Rx MKPDU                    : 11:24:52 pst Tue Dec 15 2020
Fallback Data:
    Fallback CKN                       : FB2004
    Fallback MI                        : 849D72D5F6A900F5B0718C78
    Fallback MN                        : 0x3d6
Fallback Peer:
    Peer MI                            : 8DCE8CBE67B474D2C2955F58
    RxSCI                              : 6c8b.d3db.e984/0001
    Peer CAK                           : Match
    Latest Rx MKPDU                    : 11:24:52 pst Tue Dec 15 2020
switch(config)#
```

The following example displays the MACsec MKA configuration:

```
switch# show macsec mka summary
Interface          MACSEC-policy                  Keychain
------------------ ------------------------------- ------------------------
Ethernet2/13       1                               1/10000000000000000
Ethernet2/14       1                               1/10000000000000000
switch#
```

The following example displays the configuration for all MACsec policies:

```
switch# show macsec policy
MACSec Policy Cipher Pri Window Offset Security SAK Rekey time ICV Indicator
------------------------------ ---------------- ---- ------------ -------- --------------
-------------- -------------
system-default-macsec-policy GCM-AES-XPN-256 16 148809600 0 should-secure
pn-rollover FALSE
tests1 GCM-AES-XPN-256 16 148809600 0 should-secure
pn-rollover FALSE
tests2 GCM-AES-XPN-256 16 148809600 0 should-secure
pn-rollover FALSE
tests3 GCM-AES-256 16 148809600 0 should-secure
pn-rollover FALSE
```

The following example displays the key octet string in the output of the **show running-config** and **show startup-config** commands when the **key-chain macsec-psk no-show** command is not configured:

```
key chain KC256-1 macsec
    key 2000
      key-octet-string 7
075e701e1c5a4a5143475e5a527d7c7c706a6c724306170103555a5c57510b051e47080
a05000101005e0e50510f005c4b5f5d0b5b070e234e4d0a1d0112175b5e cryptographic-algorithm
AES_256_CMAC
```

The following example displays the key octet string in the output of the **show running-config** and **show startup-config** commands when the **key-chain macsec-psk no-show** command is configured:

```
key chain KC256-1 macsec
    key 2000
      key-octet-string 7 ****** cryptographic-algorithm AES_256_CMAC
```

Displaying MACsec Statistics

You can display MACsec statistics using the following commands.

Command	Purpose
show macsec mka statistics [**interface** *type slot/port*]	Displays MACsec MKA statistics.
show macsec secy statistics [**interface** *type slot/port*]	Displays MACsec security statistics.

The following example shows the MACsec MKA statistics for a specific Ethernet interface:

```
switch# show macsec mka statistics interface ethernet 1/29
MKA Statistics for Session on interface (Ethernet1/29)
======================================================
CA Statistics
   Pairwise CAK Rekeys..... 0

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

MKPDU Statistics
   MKPDUs Transmitted...... 41
      "Distributed SAK".. 0
   MKPDUs Validated & Rx... 41
      "Distributed SAK".. 0

MKA IDB Statistics
```

```
   MKPDUs Tx Success.......... 82
   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.......... 82

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

switch(config)#
```

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
  - Common = Encrypted and unencrypted

```
switch(config)# show macsec secy statistics interface e1/29
Interface Ethernet1/29 MACSEC SecY Statistics:
-----------------------------------------
Interface Rx Statistics:
```

```
   Unicast Uncontrolled Pkts: 8067779
   Multicast Uncontrolled Pkts: 14
   Broadcast Uncontrolled Pkts: 0
   Uncontrolled Pkts - Rx Drop: 0
   Uncontrolled Pkts - Rx Error: 0
   Unicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Multicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Broadcast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Controlled Pkts: 8056748
   Controlled Pkts - Rx Drop: N/A (N3K-C3636C-R not supported)
   Controlled Pkts - Rx Error: N/A (N3K-C3636C-R not supported)
   In-Octets Uncontrolled: 37641828280 bytes
   In-Octets Controlled: 37324295914 bytes
   Input rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Input rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Input rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Input rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)

Interface Tx Statistics:
   Unicast Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Multicast Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Broadcast Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Uncontrolled Pkts - Rx Drop: N/A (N3K-C3636C-R not supported)
   Uncontrolled Pkts - Rx Error: N/A (N3K-C3636C-R not supported)
   Unicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Multicast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Broadcast Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Controlled Pkts: 8049279
   Controlled Pkts - Rx Drop: N/A (N3K-C3636C-R not supported)
   Controlled Pkts - Rx Error: N/A (N3K-C3636C-R not supported)
   Out-Octets Uncontrolled: N/A (N3K-C3636C-R not supported)
   Out-Octets Controlled: 37262189352 bytes
   Out-Octets Common: 37699748491 bytes
   Output rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Output rate for Uncontrolled Pkts: N/A (N3K-C3636C-R not supported)
   Output rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)
   Output rate for Controlled Pkts: N/A (N3K-C3636C-R not supported)

SECY Rx Statistics:
   Transform Error Pkts: N/A (N3K-C3636C-R not supported)
   Control Pkts: 0
   Untagged Pkts: N/A (N3K-C3636C-R not supported)
   No Tag Pkts: 0
   Bad Tag Pkts: 0
   No SCI Pkts: 0
   Unknown SCI Pkts: 0
   Tagged Control Pkts: N/A (N3K-C3636C-R not supported)

SECY Tx Statistics:
   Transform Error Pkts: N/A (N3K-C3636C-R not supported)
   Control Pkts: 0
   Untagged Pkts: N/A (N3K-C3636C-R not supported)

SAK Rx Statistics for AN [0]:
   Unchecked Pkts: 0
   Delayed Pkts: 0
   Late Pkts: 0
   OK Pkts: 8056748
   Invalid Pkts: 0
   Not Valid Pkts: 0
   Not-Using-SA Pkts: 0
   Unused-SA Pkts: 0
   Decrypted In-Octets: 36952542946 bytes
   Validated In-Octets: 0 bytes
```

```
SAK Tx Statistics for AN [0]:
   Encrypted Protected Pkts: 8049279
   Too Long Pkts: N/A (N3K-C3636C-R not supported)
   SA-not-in-use Pkts: N/A (N3K-C3636C-R not supported)
   Encrypted Protected Out-Octets: 36909704659 bytes

switch(config)#
```

Configuration Example for MACsec

The following example shows how to configure a user-defined MACsec policy and then apply the policy to interfaces:

```
switch(config)# macsec policy mpsr1
switch(config-macsec-policy)# cipher-suite GCM-AES-128
switch(config-macsec-policy)# key-server-priority 1
switch(config-macsec-policy)# window-size 1000
switch(config-macsec-policy)# conf-offset CONF-OFFSET-30
switch(config-macsec-policy)# security-policy must-secure
switch(config-macsec-policy)# sak-expiry-time 60
switch(config-macsec-policy)# include-icv-indicator

switch(config-macsec-policy)# interface e1/35-36
switch(config-if-range)# macsec keychain ksr policy mpsr1
switch(config-if-range)# show macsec mka session
Interface          Local-TxSCI                     # Peers            Status
Key-Server         Auth Mode
------------------ ------------------------------- ------------------ ------------------
------------------ ------------------
Ethernet1/35       6c8b.d3db.e980/0001             1                  Secured
Yes                PRIMARY-PSK
Ethernet1/36       6c8b.d3db.e984/0001             1                  Secured
No                 PRIMARY-PSK
------------------ ------------------------------- ------------------ ------------------
------------------ ------------------

switch(config-if-range)# show macsec mka summary
Interface          Status   Cipher (Operational)   Key-Server   MACSEC-policy
       Keychain                        Fallback-keychain
------------------ -------- ---------------------- ------------
-------------------------------- --------------------------------
--------------------------------
Ethernet1/35       Secured  GCM-AES-128            Yes          mpsr1
       ksr                              no keychain
Ethernet1/36       Secured  GCM-AES-128            No           mpsr1
       ksr                              no keychain

switch(config-if-range)# show running-config macsec
!Command: show running-config macsec
!Running configuration last done at: Tue Dec 15 11:41:53 2020
!Time: Tue Dec 15 11:45:06 2020

version 10.1(1) Bios:version 01.14
feature macsec

macsec policy mpsr1
   cipher-suite GCM-AES-128
   key-server-priority 1
   window-size 1000
   conf-offset CONF-OFFSET-30
   sak-expiry-time 60
   include-icv-indicator
```

```
interface Ethernet1/35
   macsec keychain ksr policy mpsr1

interface Ethernet1/36
   macsec keychain ksr policy mpsr1
```

The following example shows how to configure a MACsec keychain and then add the system default MACsec policy to the interfaces:

```
switch(config)# key chain ksr macsec
switch(config-macseckeychain)# key 2006
switch(config-macseckeychain-macseckey)# key-octet-string
1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef cryptographic-algorithm
AES_256_CMAC
switch(config-macseckeychain-macseckey)# interface e1/35-36
switch(config-if-range)# macsec keychain ksr

switch(config-if-range)# show running-config macsec
!Command: show running-config macsec
!Running configuration last done at: Tue Dec 15 11:53:10 2020
!Time: Tue Dec 15 11:54:40 2020

version 10.1(1) Bios:version 01.14
feature macsec

interface Ethernet1/35
   macsec keychain ksr policy system-default-macsec-policy

interface Ethernet1/36
   macsec keychain ksr policy system-default-macsec-policy

switch(config-if-range)# show macsec mka summary
Interface          Status   Cipher (Operational)   Key-Server   MACSEC-policy
       Keychain                        Fallback-keychain
------------------ -------- ---------------------- ------------
--------------------------------- ---------------------------------
---------------------------------
Ethernet1/35       Secured  GCM-AES-XPN-256       Yes          system-default-macsec-policy
     ksr                              no keychain
Ethernet1/36       Secured  GCM-AES-XPN-256       No           system-default-macsec-policy
     ksr                              no keychain

switch(config-if-range)# show macsec mka session
Interface          Local-TxSCI                      # Peers            Status
Key-Server         Auth Mode
------------------ -------------------------------- ------------------ ------------------
------------------ ------------------
Ethernet1/35       6c8b.d3db.e980/0001              1                  Secured
Yes                PRIMARY-PSK
Ethernet1/36       6c8b.d3db.e984/0001              1                  Secured
No                 PRIMARY-PSK
------------------ -------------------------------- ------------------ ------------------
------------------ ------------------

Total Number of Sessions : 2
   Secured Sessions : 2
   Pending Sessions : 0

switch(config-if-range)#
```

XML Examples

MACsec supports XML output for the following **show** commands for scripting purposes using | **xml**:

- **show key chain** *name* | **xml**
- **show macsec mka session** *interface interface slot/port* **details** |**xml**
- **show macsec mka statistics interface** *interface slot/port* |**xml**
- **show macsec mka summary** |**xml**
- **show macsec policy** *name* |**xml**
- **show macsec secy statistics interface** *interface slot/port* |**xml**
- **show running-config macsec** |**xml**

The following are example outputs for each of the preceding **show** commands:

Example 1: Displays the keychain configuration

```
switch(config)# show key chain "ksr" | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:rpm"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <key>
    <chain>
     <__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
      <keychain>ksr</keychain>
      <__XML__OPT_Cmd_rpm_show_keychain_cmd___readonly__>
       <__readonly__>
        <TABLE_keychain>
         <ROW_keychain>
          <chain_name>ksr</chain_name>
          <TABLE_key>
           <ROW_key>
            <key_id>2006</key_id>
<key_string>075e731f1a5c4f524f4cfb0d0629f212e62677147524054590f09595170a061e470b0b030604020c520b07055b530115575685f535976141759180714160e0a</key_string>
            <crypto_algo>AES_256_CMAC</crypto_algo>
            <send_valid>true</send_valid>
           </ROW_key>
          </TABLE_key>
         </ROW_keychain>
        </TABLE_keychain>
       </__readonly__>
      </__XML__OPT_Cmd_rpm_show_keychain_cmd___readonly__>
     </__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
    </chain>
   </key>
  </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

Example 2: Displays information about the MACsec MKA session for a specific interface

```
switch(config)# show macsec mka session interface e1/35 details | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <macsec>
    <mka>
     <session>
      <__XML__OPT_Cmd_show_macsec_mka_session_interface>
       <interface>
        <__XML__INTF_ifname>
         <__XML__PARAM_value>
          <__XML__INTF_output>Ethernet1/35</__XML__INTF_output>
         </__XML__PARAM_value>
        </__XML__INTF_ifname>
       </interface>
       <__XML__OPT_Cmd_show_macsec_mka_session_details>
        <details/>
        <__XML__OPT_Cmd_show_macsec_mka_session___readonly__>
         <__readonly__>
          <TABLE_mka_session_details>
           <ROW_mka_session_details>
            <ifname>Ethernet1/35</ifname>
            <status>SECURED - Secured MKA Session with MACsec</status>
            <sci>6c8b.d3db.e980/0001</sci>
            <ssci>2</ssci>
            <port_id>2</port_id>
            <ckn>2006</ckn>
            <ca_auth_mode>PRIMARY-PSK</ca_auth_mode>
            <mi>5AABE0AB9CC867AB0FF40F7D</mi>
            <mn>3550</mn>
            <policy>system-default-macsec-policy</policy>
            <ks_prio>16</ks_prio>
            <keyserver>Yes</keyserver>
            <include_icv_indicator>No</include_icv_indicator>
            <cipher>GCM-AES-XPN-256</cipher>
            <cipher_operational>GCM-AES-XPN-256</cipher_operational>
            <window>148809600</window>
            <conf_offset>CONF-OFFSET-0</conf_offset>
            <conf_offset_operational>CONF-OFFSET-0</conf_offset_operational>
            <sak_status>Rx &amp;amp; TX</sak_status>
            <sak_an>0</sak_an>
            <sak_ki>5AABE0AB9CC867AB0FF40F7D00000001</sak_ki>
            <sak_kn>1</sak_kn>
            <last_sak_rekey_time>11:53:25 pst Tue Dec 15 2020</last_sak_rekey_time>
            <peer_count>1</peer_count>
            <mac_addr>0180.c200.0003</mac_addr>
            <ether_type>0x888e</ether_type>
            <TABLE_mka_peer_status>
             <ROW_mka_peer_status>
              <peer_mi>27FC36C2BFAFBDBC65419A40</peer_mi>
              <rxsci>6c8b.d3db.e984/0001</rxsci>
              <icv_status>Match</icv_status>
              <last_rx_time>13:51:39 pst Tue Dec 15 2020</last_rx_time>
             </ROW_mka_peer_status>
            </TABLE_mka_peer_status>
           </ROW_mka_session_details>
          </TABLE_mka_session_details>
         </__readonly__>
        </__XML__OPT_Cmd_show_macsec_mka_session___readonly__>
       </__XML__OPT_Cmd_show_macsec_mka_session_details>
```

```
      </__XML__OPT_Cmd_show_macsec_mka_session_interface>
     </session>
    </mka>
   </macsec>
  </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

Example 3: Displays MACsec MKA statistics

```
switch(config)# show macsec mka statistics interface e1/29 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <macsec>
    <mka>
     <statistics>
      <__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
       <interface>
        <__XML__INTF_ifname>
         <__XML__PARAM_value>
          <__XML__INTF_output>Ethernet1/29</__XML__INTF_output>
         </__XML__PARAM_value>
        </__XML__INTF_ifname>
       </interface>
       <__XML__OPT_Cmd_some_macsec_mka_statistics___readonly__>
        <__readonly__>
         <TABLE_mka_intf_stats>
          <ROW_mka_intf_stats>
           <ifname2>Ethernet1/29</ifname2>
           <TABLE_ca_stats>
            <ROW_ca_stats>
             <ca_stat_ckn>2002</ca_stat_ckn>
             <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
             <sa_stat_sak_generated>0</sa_stat_sak_generated>
             <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
             <sa_stat_sak_received>2</sa_stat_sak_received>
             <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
             <mkpdu_stat_mkpdu_tx>4335</mkpdu_stat_mkpdu_tx>
             <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
             <mkpdu_stat_mkpdu_rx>4335</mkpdu_stat_mkpdu_rx>
             <mkpdu_stat_mkpdu_rx_distsak>2</mkpdu_stat_mkpdu_rx_distsak>
            </ROW_ca_stats>
           </TABLE_ca_stats>
           <TABLE_idb_stats>
            <ROW_idb_stats>
             <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
             <sa_stat_sak_generated>0</sa_stat_sak_generated>
             <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
             <sa_stat_sak_received>2</sa_stat_sak_received>
             <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
             <mkpdu_stat_mkpdu_tx>4335</mkpdu_stat_mkpdu_tx>
             <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
             <mkpdu_stat_mkpdu_rx>4335</mkpdu_stat_mkpdu_rx>
             <mkpdu_stat_mkpdu_rx_distsak>2</mkpdu_stat_mkpdu_rx_distsak>
             <idb_stat_mkpdu_tx_success>8666</idb_stat_mkpdu_tx_success>
             <idb_stat_mkpdu_tx_fail>0</idb_stat_mkpdu_tx_fail>
             <idb_stat_mkpdu_tx_pkt_build_fail>0</idb_stat_mkpdu_tx_pkt_build_fail>
             <idb_stat_mkpdu_no_tx_on_intf_down>0</idb_stat_mkpdu_no_tx_on_intf_down>
             <idb_stat_mkpdu_no_rx_on_intf_down>0</idb_stat_mkpdu_no_rx_on_intf_down>
```

```
                <idb_stat_mkpdu_rx_ca_notfound>0</idb_stat_mkpdu_rx_ca_notfound>
                <idb_stat_mkpdu_rx_error>0</idb_stat_mkpdu_rx_error>
                <idb_stat_mkpdu_rx_success>8666</idb_stat_mkpdu_rx_success>
<idb_stat_mkpdu_failure_rx_integrity_check_error>0</idb_stat_mkpdu_failure_rx_integrity_check_error>
<idb_stat_mkpdu_failure_invalid_peer_mn_error>0</idb_stat_mkpdu_failure_invalid_peer_mn_error>
<idb_stat_mkpdu_failure_nonrecent_peerlist_mn_error>0</idb_stat_mkpdu_failure_nonrecent_peerlist_mn_error>
<idb_stat_mkpdu_failure_sakuse_kn_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_kn_mismatch_error>
<idb_stat_mkpdu_failure_sakuse_rx_not_set_error>0</idb_stat_mkpdu_failure_sakuse_rx_not_set_error>
<idb_stat_mkpdu_failure_sakuse_key_mi_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_key_mi_mismatch_error>
<idb_stat_mkpdu_failure_sakuse_an_not_in_use_error>0</idb_stat_mkpdu_failure_sakuse_an_not_in_use_error>
<idb_stat_mkpdu_failure_sakuse_ks_rx_tx_not_set_error>0</idb_stat_mkpdu_failure_sakuse_ks_rx_tx_not_set_error>
<idb_stat_mkpdu_failure_sakuse_eapol_ethertype_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_eapol_ethertype_mismatch_error>
<idb_stat_mkpdu_failure_sakuse_eapol_destmac_mismatch_error>0</idb_stat_mkpdu_failure_sakuse_eapol_destmac_mismatch_error>
<idb_stat_sak_failure_sak_generate_error>0</idb_stat_sak_failure_sak_generate_error>
<idb_stat_sak_failure_hash_generate_error>0</idb_stat_sak_failure_hash_generate_error>
<idb_stat_sak_failure_sak_encryption_error>0</idb_stat_sak_failure_sak_encryption_error>
<idb_stat_sak_failure_sak_decryption_error>0</idb_stat_sak_failure_sak_decryption_error>
<idb_stat_sak_failure_ick_derivation_error>0</idb_stat_sak_failure_ick_derivation_error>
<idb_stat_sak_failure_kek_derivation_error>0</idb_stat_sak_failure_kek_derivation_error>
<idb_stat_sak_failure_invalid_macsec_capability_error>0</idb_stat_sak_failure_invalid_macsec_capability_error>
<idb_stat_macsec_failure_rx_sa_create_error>0</idb_stat_macsec_failure_rx_sa_create_error>
<idb_stat_macsec_failure_tx_sa_create_error>0</idb_stat_macsec_failure_tx_sa_create_error>
            </ROW_idb_stats>
           </TABLE_idb_stats>
          </ROW_mka_intf_stats>
         </TABLE_mka_intf_stats>
        </__readonly__>
       </__XML__OPT_Cmd_some_macsec_mka_statistics___readonly__>
      </__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
     </statistics>
    </mka>
   </macsec>
  </show>
</nf:data>
```

```
</nf:rpc-reply>
]]>]]>
switch(config)#
```

Example 4: Displays the MACsec MKA configuration

```
switch(config)# show macsec mka summary | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <macsec>
    <mka>
     <__XML__OPT_Cmd_some_macsec_summary>
      <__XML__OPT_Cmd_some_macsec___readonly__>
       <__readonly__>
        <TABLE_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/29</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>No</keyserver>
          <policy>mpd1</policy>
          <keychain>kd</keychain>
          <fallback_keychain>fbkd</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/30</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>No</keyserver>
          <policy>mpd2</policy>
          <keychain>kd</keychain>
          <fallback_keychain>fbkd</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/31</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>Yes</keyserver>
          <policy>mps1</policy>
          <keychain>ks</keychain>
          <fallback_keychain>fbks</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/32</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>Yes</keyserver>
          <policy>mps2</policy>
          <keychain>ks</keychain>
          <fallback_keychain>fbks</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/33</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>Yes</keyserver>
          <policy>mpsr1</policy>
          <keychain>ksr</keychain>
          <fallback_keychain>fbksr</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
```

```
          <ifname>Ethernet1/34</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-128</cipher>
          <keyserver>Yes</keyserver>
          <policy>mpsr2</policy>
          <keychain>ksr</keychain>
          <fallback_keychain>fbksr</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/35</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-XPN-256</cipher>
          <keyserver>Yes</keyserver>
          <policy>system-default-macsec-policy</policy>
          <keychain>ksr</keychain>
          <fallback_keychain>no keychain</fallback_keychain>
         </ROW_mka_summary>
         <ROW_mka_summary>
          <ifname>Ethernet1/36</ifname>
          <status>Secured</status>
          <cipher>GCM-AES-XPN-256</cipher>
          <keyserver>No</keyserver>
          <policy>system-default-macsec-policy</policy>
          <keychain>ksr</keychain>
          <fallback_keychain>no keychain</fallback_keychain>
         </ROW_mka_summary>
        </TABLE_mka_summary>
       </__readonly__>
      </__XML__OPT_Cmd_some_macsec___readonly__>
     </__XML__OPT_Cmd_some_macsec_summary>
    </mka>
   </macsec>
  </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

Example 5: Displays the configuration for a specific MACsec policy

```
switch(config)# show macsec policy mpsr1 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <macsec>
    <policy>
     <__XML__OPT_Cmd_show_macsec_policy_policy_name>
      <policy_name>mpsr1</policy_name>
      <__XML__OPT_Cmd_show_macsec_policy___readonly__>
       <__readonly__>
        <TABLE_macsec_policy>
         <ROW_macsec_policy>
          <name>mpsr1</name>
          <cipher_suite>GCM-AES-128</cipher_suite>
          <keyserver_priority>1</keyserver_priority>
          <window_size>1000</window_size>
          <conf_offset>30</conf_offset>
          <security_policy>should-secure</security_policy>
          <sak-expiry-time>60</sak-expiry-time>
          <include_icv_indicator>TRUE</include_icv_indicator>
         </ROW_macsec_policy>
        </TABLE_macsec_policy>
```

```
       </__readonly__>
      </__XML__OPT_Cmd_show_macsec_policy___readonly__>
     </__XML__OPT_Cmd_show_macsec_policy_policy_name>
    </policy>
   </macsec>
  </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

Example 6: Displays MACsec Security statistics

```
switch(config)# show macsec secy statistics interface e1/29 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns="http://www.cisco.com/nxos:1.0:cts"
xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0">
<nf:data>
  <show>
   <macsec>
    <secy>
     <statistics>
      <__XML__OPT_Cmd_some_macsec_secy_statistics_interface>
       <interface>
        <__XML__INTF_ifname>
         <__XML__PARAM_value>
          <__XML__INTF_output>Ethernet1/29</__XML__INTF_output>
         </__XML__PARAM_value>
        </__XML__INTF_ifname>
       </interface>
       <__XML__OPT_Cmd_some_macsec_secy_statistics___readonly__>
        <__readonly__>
         <TABLE_statistics>
          <ROW_statistics>
           <ifname2>Ethernet1/29</ifname2>
           <in_pkts_unicast_uncontrolled>6536205587</in_pkts_unicast_uncontrolled>
           <in_pkts_multicast_uncontrolled>10775</in_pkts_multicast_uncontrolled>
           <in_pkts_broadcast_uncontrolled>0</in_pkts_broadcast_uncontrolled>
           <in_rx_drop_pkts_uncontrolled>0</in_rx_drop_pkts_uncontrolled>
           <in_rx_err_pkts_uncontrolled>0</in_rx_err_pkts_uncontrolled>
           <in_pkts_unicast_controlled>N/A (N3K-C3636C-R not
supported)</in_pkts_unicast_controlled>
           <in_pkts_multicast_controlled>N/A (N3K-C3636C-R not
supported)</in_pkts_multicast_controlled>
           <in_pkts_broadcast_controlled>N/A (N3K-C3636C-R not
supported)</in_pkts_broadcast_controlled>
           <in_pkts_controlled>5173107800</in_pkts_controlled>
           <in_rx_drop_pkts_controlled>N/A (N3K-C3636C-R not
supported)</in_rx_drop_pkts_controlled>
           <in_rx_err_pkts_controlled>N/A (N3K-C3636C-R not
supported)</in_rx_err_pkts_controlled>
           <in_octets_uncontrolled>30491280431357</in_octets_uncontrolled>
           <in_octets_controlled>23935220809548</in_octets_controlled>
           <input_rate_uncontrolled_pps>N/A (N3K-C3636C-R not
supported)</input_rate_uncontrolled_pps>
           <input_rate_uncontrolled_bps>N/A (N3K-C3636C-R not
supported)</input_rate_uncontrolled_bps>
           <input_rate_controlled_pps>N/A (N3K-C3636C-R not
supported)</input_rate_controlled_pps>
           <input_rate_controlled_bps>N/A (N3K-C3636C-R not
supported)</input_rate_controlled_bps>
           <out_pkts_unicast_uncontrolled>N/A (N3K-C3636C-R not
supported)</out_pkts_unicast_uncontrolled>
           <out_pkts_multicast_uncontrolled>N/A (N3K-C3636C-R not
```

```
supported)</out_pkts_multicast_uncontrolled>
           <out_pkts_broadcast_uncontrolled>N/A (N3K-C3636C-R not
supported)</out_pkts_broadcast_uncontrolled>
           <out_rx_drop_pkts_uncontrolled>N/A (N3K-C3636C-R not
supported)</out_rx_drop_pkts_uncontrolled>
           <out_rx_err_pkts_uncontrolled>N/A (N3K-C3636C-R not
supported)</out_rx_err_pkts_uncontrolled>
           <out_pkts_unicast_controlled>N/A (N3K-C3636C-R not
supported)</out_pkts_unicast_controlled>
           <out_pkts_multicast_controlled>N/A (N3K-C3636C-R not
supported)</out_pkts_multicast_controlled>
           <out_pkts_broadcast_controlled>N/A (N3K-C3636C-R not
supported)</out_pkts_broadcast_controlled>
           <out_pkts_controlled>5173113173</out_pkts_controlled>
           <out_rx_drop_pkts_controlled>N/A (N3K-C3636C-R not
supported)</out_rx_drop_pkts_controlled>
           <out_rx_err_pkts_controlled>N/A (N3K-C3636C-R not
supported)</out_rx_err_pkts_controlled>
         <out_octets_uncontrolled>N/A (N3K-C3636C-R not supported)</out_octets_uncontrolled>

           <out_octets_controlled>23946219872208</out_octets_controlled>
           <out_octets_common>30664229104600</out_octets_common>
           <output_rate_uncontrolled_pps>N/A (N3K-C3636C-R not
supported)</output_rate_uncontrolled_pps>
           <output_rate_uncontrolled_bps>N/A (N3K-C3636C-R not
supported)</output_rate_uncontrolled_bps>
           <output_rate_controlled_pps>N/A (N3K-C3636C-R not
supported)</output_rate_controlled_pps>
           <output_rate_controlled_bps>N/A (N3K-C3636C-R not
supported)</output_rate_controlled_bps>
         <in_pkts_transform_error>N/A (N3K-C3636C-R not supported)</in_pkts_transform_error>

           <in_pkts_control>0</in_pkts_control>
           <in_pkts_untagged>N/A (N3K-C3636C-R not supported)</in_pkts_untagged>
           <in_pkts_no_tag>0</in_pkts_no_tag>
           <in_pkts_badtag>0</in_pkts_badtag>
           <in_pkts_no_sci>0</in_pkts_no_sci>
           <in_pkts_unknown_sci>0</in_pkts_unknown_sci>
           <in_pkts_tagged_ctrl>N/A (N3K-C3636C-R not supported)</in_pkts_tagged_ctrl>
           <out_pkts_transform_error>N/A (N3K-C3636C-R not
supported)</out_pkts_transform_error>
           <out_pkts_control>0</out_pkts_control>
           <out_pkts_untagged>N/A (N3K-C3636C-R not supported)</out_pkts_untagged>
           <TABLE_rx_sa_an>
            <ROW_rx_sa_an>
             <rx_sa_an>2</rx_sa_an>
             <in_pkts_unchecked>0</in_pkts_unchecked>
             <in_pkts_delayed>0</in_pkts_delayed>
             <in_pkts_late>0</in_pkts_late>
             <in_pkts_ok>1951781408</in_pkts_ok>
             <in_pkts_invalid>0</in_pkts_invalid>
             <in_pkts_not_valid>0</in_pkts_not_valid>
             <in_pkts_not_using_sa>0</in_pkts_not_using_sa>
             <in_pkts_unused_sa>0</in_pkts_unused_sa>
             <in_octets_decrypted>8952613134278</in_octets_decrypted>
             <in_octets_validated>0</in_octets_validated>
            </ROW_rx_sa_an>
           </TABLE_rx_sa_an>
           <TABLE_tx_sa_an>
            <ROW_tx_sa_an>
             <tx_sa_an>2</tx_sa_an>
             <out_pkts_encrypted_protected>1951773387</out_pkts_encrypted_protected>
             <out_pkts_too_long>N/A (N3K-C3636C-R not supported)</out_pkts_too_long>
           <out_pkts_sa_not_inuse>N/A (N3K-C3636C-R not supported)</out_pkts_sa_not_inuse>
```

```
            <out_octets_encrypted_protected>8952606203313</out_octets_encrypted_protected>

            </ROW_tx_sa_an>
           </TABLE_tx_sa_an>
          </ROW_statistics>
         </TABLE_statistics>
        </__readonly__>
       </__XML__OPT_Cmd_some_macsec_secy_statistics___readonly__>
      </__XML__OPT_Cmd_some_macsec_secy_statistics_interface>
     </statistics>
    </secy>
   </macsec>
  </show>
</nf:data>
</nf:rpc-reply>
]]>]]>
switch(config)#
```

Example 7: Displays the running configuration information for MACsec

```
switch(config)# show running-config macsec | xml

!Command: show running-config macsec
!Running configuration last done at: Tue Dec 15 11:53:10 2020
!Time: Tue Dec 15 13:58:58 2020

version 10.1(1) Bios:version 01.14
****************************************
This may take time. Please be patient.
****************************************
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://www.cisco.com/nxos:10.1.1.:configure_"
xmlns:m="http://www.cisco.com/nxos:10.1.1.:_exec"
xmlns:m1="http://www.cisco.com/nxos:10.1.1.:configure__macsec-policy"
xmlns:m2="http://www.cisco.com/nxos:10.1.1.:configure__if-ethernet-all" message-id="1">
  <nf:get-config>
    <nf:source>
      <nf:running/>
    </nf:source>
    <nf:filter>
      <m:configure>
        <m:terminal>
          <feature>
            <macsec/>
          </feature>
          <macsec>
            <policy>
              <__XML__PARAM__policy_name>
                <__XML__value>mpd1</__XML__value>
                <m1:cipher-suite>
                  <m1:__XML__PARAM__suite>
                    <m1:__XML__value>GCM-AES-128</m1:__XML__value>
                  </m1:__XML__PARAM__suite>
                </m1:cipher-suite>
                <m1:conf-offset>
                  <m1:__XML__PARAM__offset>
                    <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
                  </m1:__XML__PARAM__offset>
                </m1:conf-offset>
              </__XML__PARAM__policy_name>
            </policy>
          </macsec>
```

```
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mpd2</__XML__value>
      <m1:cipher-suite>
        <m1:__XML__PARAM__suite>
          <m1:__XML__value>GCM-AES-128</m1:__XML__value>
        </m1:__XML__PARAM__suite>
      </m1:cipher-suite>
      <m1:conf-offset>
        <m1:__XML__PARAM__offset>
          <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
        </m1:__XML__PARAM__offset>
      </m1:conf-offset>
      <m1:security-policy>
        <m1:__XML__PARAM__policy>
          <m1:__XML__value>must-secure</m1:__XML__value>
        </m1:__XML__PARAM__policy>
      </m1:security-policy>
    </__XML__PARAM__policy_name>
  </policy>
</macsec>
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mps1</__XML__value>
      <m1:cipher-suite>
        <m1:__XML__PARAM__suite>
          <m1:__XML__value>GCM-AES-128</m1:__XML__value>
       </m1:__XML__PARAM__suite>
      </m1:cipher-suite>
      <m1:key-server-priority>
        <m1:__XML__PARAM__pri>
          <m1:__XML__value>1</m1:__XML__value>
        </m1:__XML__PARAM__pri>
      </m1:key-server-priority>
      <m1:conf-offset>
        <m1:__XML__PARAM__offset>
          <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
        </m1:__XML__PARAM__offset>
      </m1:conf-offset>
      <m1:sak-expiry-time>
        <m1:__XML__PARAM__ts>
          <m1:__XML__value>60</m1:__XML__value>
        </m1:__XML__PARAM__ts>
      </m1:sak-expiry-time>
      <m1:include-icv-indicator/>
    </__XML__PARAM__policy_name>
  </policy>
</macsec>
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mps2</__XML__value>
      <m1:cipher-suite>
        <m1:__XML__PARAM__suite>
          <m1:__XML__value>GCM-AES-128</m1:__XML__value>
        </m1:__XML__PARAM__suite>
      </m1:cipher-suite>
      <m1:key-server-priority>
        <m1:__XML__PARAM__pri>
          <m1:__XML__value>1</m1:__XML__value>
        </m1:__XML__PARAM__pri>
      </m1:key-server-priority>
```

```
      <m1:window-size>
        <m1:__XML__PARAM__size>
          <m1:__XML__value>1000</m1:__XML__value>
        </m1:__XML__PARAM__size>
      </m1:window-size>
      <m1:conf-offset>
        <m1:__XML__PARAM__offset>
          <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
        </m1:__XML__PARAM__offset>
      </m1:conf-offset>
      <m1:security-policy>
        <m1:__XML__PARAM__policy>
          <m1:__XML__value>must-secure</m1:__XML__value>
        </m1:__XML__PARAM__policy>
      </m1:security-policy>
      <m1:sak-expiry-time>
        <m1:__XML__PARAM__ts>
          <m1:__XML__value>60</m1:__XML__value>
        </m1:__XML__PARAM__ts>
      </m1:sak-expiry-time>
      <m1:include-icv-indicator/>
    </__XML__PARAM__policy_name>
  </policy>
</macsec>
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mpsr1</__XML__value>
      <m1:cipher-suite>
        <m1:__XML__PARAM__suite>
          <m1:__XML__value>GCM-AES-128</m1:__XML__value>
        </m1:__XML__PARAM__suite>
      </m1:cipher-suite>
      <m1:key-server-priority>
        <m1:__XML__PARAM__pri>
          <m1:__XML__value>1</m1:__XML__value>
        </m1:__XML__PARAM__pri>
      </m1:key-server-priority>
      <m1:window-size>
        <m1:__XML__PARAM__size>
          <m1:__XML__value>1000</m1:__XML__value>
        </m1:__XML__PARAM__size>
      </m1:window-size>
      <m1:conf-offset>
        <m1:__XML__PARAM__offset>
          <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
        </m1:__XML__PARAM__offset>
      </m1:conf-offset>
      <m1:sak-expiry-time>
        <m1:__XML__PARAM__ts>
          <m1:__XML__value>60</m1:__XML__value>
        </m1:__XML__PARAM__ts>
      </m1:sak-expiry-time>
      <m1:include-icv-indicator/>
    </__XML__PARAM__policy_name>
  </policy>
</macsec>
<macsec>
  <policy>
    <__XML__PARAM__policy_name>
      <__XML__value>mpsr2</__XML__value>
      <m1:cipher-suite>
        <m1:__XML__PARAM__suite>
          <m1:__XML__value>GCM-AES-128</m1:__XML__value>
```

```
        </m1:__XML__PARAM__suite>
      </m1:cipher-suite>
      <m1:key-server-priority>
        <m1:__XML__PARAM__pri>
          <m1:__XML__value>1</m1:__XML__value>
        </m1:__XML__PARAM__pri>
      </m1:key-server-priority>
      <m1:window-size>
        <m1:__XML__PARAM__size>
          <m1:__XML__value>1000</m1:__XML__value>
        </m1:__XML__PARAM__size>
      </m1:window-size>
      <m1:conf-offset>
        <m1:__XML__PARAM__offset>
          <m1:__XML__value>CONF-OFFSET-30</m1:__XML__value>
        </m1:__XML__PARAM__offset>
      </m1:conf-offset>
      <m1:security-policy>
        <m1:__XML__PARAM__policy>
          <m1:__XML__value>must-secure</m1:__XML__value>
        </m1:__XML__PARAM__policy>
      </m1:security-policy>
      <m1:sak-expiry-time>
        <m1:__XML__PARAM__ts>
          <m1:__XML__value>60</m1:__XML__value>
        </m1:__XML__PARAM__ts>
      </m1:sak-expiry-time>
      <m1:include-icv-indicator/>
    </__XML__PARAM__policy_name>
  </policy>
</macsec>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/29</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>kd</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>mpd1</m2:__XML__value>
              <m2:fallback-keychain>
                <m2:__XML__PARAM__fallback_kc_name>
                  <m2:__XML__value>fbkd</m2:__XML__value>
                </m2:__XML__PARAM__fallback_kc_name>
              </m2:fallback-keychain>
            </m2:__XML__PARAM__policy_name>
          </m2:policy>
        </m2:__XML__PARAM__keychain_name>
      </m2:keychain>
    </m2:macsec>
  </__XML__PARAM__interface>
</interface>
<interface>
  <__XML__PARAM__interface>
    <__XML__value>Ethernet1/30</__XML__value>
    <m2:macsec>
      <m2:keychain>
        <m2:__XML__PARAM__keychain_name>
          <m2:__XML__value>kd</m2:__XML__value>
          <m2:policy>
            <m2:__XML__PARAM__policy_name>
              <m2:__XML__value>mpd2</m2:__XML__value>
              <m2:fallback-keychain>
```

```
                    <m2:__XML__PARAM__fallback_kc_name>
                      <m2:__XML__value>fbkd</m2:__XML__value>
                    </m2:__XML__PARAM__fallback_kc_name>
                  </m2:fallback-keychain>
                </m2:__XML__PARAM__policy_name>
              </m2:policy>
            </m2:__XML__PARAM__keychain_name>
          </m2:keychain>
        </m2:macsec>
      </__XML__PARAM__interface>
    </interface>
    <interface>
      <__XML__PARAM__interface>
        <__XML__value>Ethernet1/31</__XML__value>
        <m2:macsec>
          <m2:keychain>
            <m2:__XML__PARAM__keychain_name>
              <m2:__XML__value>ks</m2:__XML__value>
              <m2:policy>
                <m2:__XML__PARAM__policy_name>
                  <m2:__XML__value>mps1</m2:__XML__value>
                  <m2:fallback-keychain>
                    <m2:__XML__PARAM__fallback_kc_name>
                      <m2:__XML__value>fbks</m2:__XML__value>
                    </m2:__XML__PARAM__fallback_kc_name>
                  </m2:fallback-keychain>
                </m2:__XML__PARAM__policy_name>
              </m2:policy>
            </m2:__XML__PARAM__keychain_name>
          </m2:keychain>
        </m2:macsec>
      </__XML__PARAM__interface>
    </interface>
    <interface>
      <__XML__PARAM__interface>
        <__XML__value>Ethernet1/32</__XML__value>
        <m2:macsec>
          <m2:keychain>
            <m2:__XML__PARAM__keychain_name>
              <m2:__XML__value>ks</m2:__XML__value>
              <m2:policy>
                <m2:__XML__PARAM__policy_name>
                  <m2:__XML__value>mps2</m2:__XML__value>
                  <m2:fallback-keychain>
                    <m2:__XML__PARAM__fallback_kc_name>
                      <m2:__XML__value>fbks</m2:__XML__value>
                    </m2:__XML__PARAM__fallback_kc_name>
                  </m2:fallback-keychain>
                </m2:__XML__PARAM__policy_name>
              </m2:policy>
            </m2:__XML__PARAM__keychain_name>
          </m2:keychain>
        </m2:macsec>
      </__XML__PARAM__interface>
    </interface>
    <interface>
      <__XML__PARAM__interface>
        <__XML__value>Ethernet1/33</__XML__value>
        <m2:macsec>
          <m2:keychain>
            <m2:__XML__PARAM__keychain_name>
              <m2:__XML__value>ksr</m2:__XML__value>
              <m2:policy>
                <m2:__XML__PARAM__policy_name>
```

```
                    <m2:__XML__value>mpsr1</m2:__XML__value>
                    <m2:fallback-keychain>
                      <m2:__XML__PARAM__fallback_kc_name>
                        <m2:__XML__value>fbksr</m2:__XML__value>
                      </m2:__XML__PARAM__fallback_kc_name>
                    </m2:fallback-keychain>
                  </m2:__XML__PARAM__policy_name>
                </m2:policy>
              </m2:__XML__PARAM__keychain_name>
            </m2:keychain>
          </m2:macsec>
        </__XML__PARAM__interface>
      </interface>
      <interface>
        <__XML__PARAM__interface>
          <__XML__value>Ethernet1/34</__XML__value>
          <m2:macsec>
            <m2:keychain>
              <m2:__XML__PARAM__keychain_name>
                <m2:__XML__value>ksr</m2:__XML__value>
                <m2:policy>
                  <m2:__XML__PARAM__policy_name>
                    <m2:__XML__value>mpsr2</m2:__XML__value>
                    <m2:fallback-keychain>
                      <m2:__XML__PARAM__fallback_kc_name>
                        <m2:__XML__value>fbksr</m2:__XML__value>
                      </m2:__XML__PARAM__fallback_kc_name>
                    </m2:fallback-keychain>
                  </m2:__XML__PARAM__policy_name>
                </m2:policy>
              </m2:__XML__PARAM__keychain_name>
            </m2:keychain>
          </m2:macsec>
        </__XML__PARAM__interface>
      </interface>
      <interface>
        <__XML__PARAM__interface>
          <__XML__value>Ethernet1/35</__XML__value>
          <m2:macsec>
            <m2:keychain>
              <m2:__XML__PARAM__keychain_name>
                <m2:__XML__value>ksr</m2:__XML__value>
                <m2:policy>
                  <m2:__XML__PARAM__policy_name>
                    <m2:__XML__value>system-default-macsec-policy</m2:__XML__value>
                  </m2:__XML__PARAM__policy_name>
                </m2:policy>
              </m2:__XML__PARAM__keychain_name>
            </m2:keychain>
          </m2:macsec>
        </__XML__PARAM__interface>
      </interface>
      <interface>
        <__XML__PARAM__interface>
          <__XML__value>Ethernet1/36</__XML__value>
          <m2:macsec>
            <m2:keychain>
              <m2:__XML__PARAM__keychain_name>
                <m2:__XML__value>ksr</m2:__XML__value>
                <m2:policy>
                  <m2:__XML__PARAM__policy_name>
                    <m2:__XML__value>system-default-macsec-policy</m2:__XML__value>
                  </m2:__XML__PARAM__policy_name>
                </m2:policy>
```

```
                    </m2:__XML__PARAM__keychain_name>
                  </m2:keychain>
                </m2:macsec>
              </__XML__PARAM__interface>
            </interface>
          </m:terminal>
        </m:configure>
      </nf:filter>
    </nf:get-config>
</nf:rpc>
]]>]]>

switch(config)#
```

MIBs

MACsec supports the following MIBs:

- IEEE8021-SECY-MIB
- CISCO-SECY-EXT-MIB

Related Documentation

Related Topic	Document Title
Keychain management	Cisco Nexus 3600 Series NX-OS Security Configuration Guide
System messages	Cisco Nexus 3600 Series NX-OS System Messages References