MACsec Encryption Commands

This module describes the commands used to configure MACsec encryption.

For detailed information about MACsec concepts, configuration tasks, and examples, see the *Configuring MACsec* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series RoutersSystem Security Configuration Guide for Cisco 8000 Series Routers*.

allow (macsec)

To specify MACsec policy exception to allow packets in clear text, use **allow** command under MACsec policy configuration mode. To remove this configuration, use the **no** form of this command.

allow { **lacp-in-clear** | **pause-frames-in-clear** | **lldp-in-clear** }

Syntax Description

lacp-in-clear	Allows Link Aggregation Control Plane protocol (LACP) packets in clear text.
pause-frames-in-clear	Allows Ethernet PAUSE frame packets in clear text.
lldp-in-clear	Allows Link Layer Discovery Protocol (LLDP) packets in clear text.

Command Default

None

Command Modes

MACsec policy configuration mode

Command History

Release	Modification
Release 7.11.1	This command was modified to include the **lldp-in-clear** option.
Release 7.3.15	This command was modified to include the **pause-frames-in-clear** option.
Release 7.3.1	This command was introduced.

Usage Guidelines

The **policy-exception lacp-in-clear** command under MACsec policy configuration mode is deprecated. Hence, it is recommended to use the **allow lacp-in-clear** command instead, to allow LACP packets in clear-text format.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to create a MACsec policy exception to allow LACP, LLDP, and Ethernet PAUSE frame packets in clear text:

```
Router#configure
Router(config)#macsec-policy test-macsec-policy
Router(config-macsec-policy)#allow lacp-in-clear
Router(config-macsec-policy)#allow pause-frames-in-clear
Router(config-macsec-policy)#allow lldp-in-clear
Router(config-macsec-policy)#commit
```

cipher-suite

Configures the cipher suite for encrypting traffic with MACsec in the MAcsec policy configuration mode.

The first portion of the cipher name indicates the encryption method, the second portion indicates the hash or integrity algorithm, and the third portion indicates the length of the cipher (128/256).

To remove this configuration, use the **no** form of this command.

cipher-suite *encryption_ suite*

Syntax Description

encryption_suite	The GCM encryption method that uses the AES encryption algorithm. The available encryption suites are: • GCM-AES-128 • GCM-AES-256 • GCM-AES-XPN-128 • GCM-AES-XPN-256

Command Default

The default cipher suite chosen for encryption is GCM-AES-XPN-256.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **cipher-suite** command:

```
RP/0/RP0RSP0/CPU0:router# configure t
RP/0/RP0RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# cipher-suite GCM-AES-XPN-256
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#commit
```

conf-offset

Configures the confidentiality offset for MACsec encryption in the MACsec policy configuration mode.

To remove this configuration, use the **no** form of this command.

conf-offset *offset_value*

Syntax Description

offset_value	Configures the offset value. The options are: • CONF-OFFSET-0 : Does not offset the encryption. • CONF-OFFSET-30: Offsets the encryption by 30 bytes. • CONF-OFFSET-50: Offsets the encryption by 50 bytes.

Command Default

Default value is 0.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **conf-offset** command:

```
RP/0/RP0RSP0/CPU0:router# configure t
RP/0/RP0RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# conf-offset CONF-OFFSET-30
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

crypto-sks-kme

To display details of the Quantum Key Distribution (QKD) server, use the **crypto-sks-kme** command in EXEC mode.

crypto-sks-kme *profile-name* { **entropy** | **capability** }

Syntax Description

profile-name	Specifies the key string in clear-text form.
entropy	Specifies the key in encrypted form.
capability	Specifies the key in Type 6 encrypted form.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operations
system	read, write

Examples

The following examples shows how to use the **crypto-sks-kme** command:

```
Router# crypto sks kme remote_qkd_prof1 entropy
Entropy Details:
Key details Dump: 0000 - 406b004c9c7f000000000000000000280c71794fa6f029d0ee2f6c4cd01b46
Key : 406b004c9c7f000000000000000000280c71794fa6f029d0ee2f6c4cd01b46
Entropy Length: 32
```

```
Router# crypto sks kme QkdIP capability
Capability Details:
  Entropy supported : False
  Key supported     : False
  Algorithm         : QKD
  Local identifier  : Alice1
  Remote identifier : Alice1, Bob1,
```

enable-legacy-fallback

To enable interoperability with peer devices that do not support MACsec active fallback feature, use the **enable-legacy-fallback** command in MACsec policy configuration mode. To remove the configuration, use the **no** form of this command.

enable-legacy-fallback

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled, by default.

Command Modes

MACsec policy configuration mode

Command History

Release	Modification
Release 7.0.14	This command was introduced.

Usage Guidelines

For more details on MACsec active fallback feature, see the *Fallback PSK* section in the *Configuring MACsec Encryption* chapter in the *System Security Configuration Guide for Cisco ASR 9000 Series RoutersSystem Security Configuration Guide for Cisco 8000 Series Routers*.

Task ID

Task ID	Operation
system	read, write

This example shows how to enable interoperability with peer devices that do not support MACsec active fallback feature:

```
Router#configure
Router(config)#macsec-policy P1
Router(config-macsec-policy)#enable-legacy-fallback
Router(config-macsec-policy)#commit
```

hw-module macsec-fips-post

To enable the power-on self-test (POST) known answer test (KAT) for the physical layer transceiver (PHY) of a line card, use the **hw-module macsec-fips-post** command in Global Configuration modeXR Config mode mode. To remove this configuration, use the no form of this command.

hw-module macsec-fips-post location { *location* | **all** }

Syntax Description

location	Enables POST KAT for a specific node location.
location	Specifies the node location to enable POST KAT.
all	Enables POST KAT for all nodes.

Command Default

Disabled by default

Command Modes

Global Configuration modeXR Config mode

Command History

Release	Modification
Release 7.0.14	This command was introduced.

Usage Guidelines

You must reload the line card for this configuration to take effect.

You can use the **show hw-module macsec-fips-post** command to know the current mode of POST KAT configuration, and what action is to be performed.

Note If power-on self-test (POST) known answer test (KAT) is already enabled on the PHY, then the system does not allow you to configure the **hw-module macsec-fips-post location all** command again. This restriction is in place to prevent conflicts in configuration, especially in a configuration restore scenario. In such scenarios, you can make use of the **show hw-module macsec-mode fips-post** command to know of the respective running configurations in place.

Task ID

Task ID	Operation
system	read, write

This example shows how to enable power-on self-test KAT for the physical layer transceiver (PHY) of a line card:

```
Router# configure
Router(config)# hw-module macsec-fips-post location 0/4/CPU0
```

```
Router(config)# commit
```

Related Commands

Command	Description
show hw-module macsec-fips-post, on page 24	Displays the power-on self-test (POST) known answer test (KAT) configurations of nodes in a router.

hw-module macsec-mode

To enable the MACsec mode for the physical layer transceiver (PHY) of a line card, use the **hw-module macsec-mode** command in Global Configuration modeXR Config mode mode. To remove this configuration, use the no form of this command.

hw-module macsec-mode location {**all** | *location*}

Syntax Description

location	Specifies the node location to enable the MACsec mode.
all	Enables MACsec mode for all nodes.
location	Enables MACsec mode for a specific node.

Command Default

Disabled by default

Command Modes

Global Configuration modeXR Config mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

This configuration helps to avoid interface flap when MACsec is configured on an interface.

You must reload the line card for this configuration to take effect.

You can use the **show hw-module macsec-mode** command to know the current mode of MACsec, and what action is to be performed.

Note If the MACsec mode is already enabled on a node such as a line card, then the system does not allow you to configure the **hw-module macsec-mode location all** command again. This restriction is in place to prevent conflicts in configuration, especially in a configuration restore scenario. In such scenarios, you can make use of the **show hw-module macsec-mode** command to know of the respective running configurations in place.

Task ID

Task ID	Operation
system	read, write

This example shows how to enable the MACsec mode for the physical layer transceiver (PHY) of a line card:

```
Router# configure
Router(config)# hw-module macsec-mode location 0/1/CPU0
```

```
Router(config)# commit
```

Related Commands

Command	Description
show hw-module macsec-mode, on page 26	Displays the MACsec mode of a line card and the user action to be performed.

key

To create or modify a keychain key, use the **key** command in keychain-key configuration mode. To remove this configuration, use the **no** form of this command.

key *key-id*
no key *key-id*

Syntax Description

key-id	Hexadecimal string of 2-64 characters.

Command Default

No default behavior or values.

Command Modes

Key chain configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

The key must be of even number of hex characters. Entering an odd number of characters will exit the MACsec configuration mode.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **key** command:

```
RP/0/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router# key chain mac_chain macsec
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
```

key-server-priority

Configures the preference for a device to serve as the key server for MACsec encryption in the MACsec policy configuration mode. To remove this configuration, use the **no** form of this command.

key-server-priority *value*

Syntax Description

value	Indicates the priority for a device to become the key server. Lower the value, higher the preference. The range is 0-255.

Command Default

Default value is 16.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **key-server-priority** command:

```
RP/0/RP0RSP0/CPU0:router# configure t
RP/0/RP0RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# key-server-priority 16
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

key chain

To create or modify a key chain, use the **key chain** command in the key chain configuration mode.

To remove this configuration, use the **no** form of this command.

key chain *key-chain-name* **macsec**

Syntax Description

key-chain-name	Specifies the name of the keychain. The maximum length is 32 (128-bit encryption)/64 (256-bit encryption) character hexadecimal string.
macsec	Specifies the key chain for MACsec encryption.

Command Modes

Key chain configuration

Command Default

No default behavior or values

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how you can configure a key chain for MACsec encryption:

```
RP/0/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec)#
```

key-string

To specify the text string for the key, use the **key-string** command in key configuration submode under the macsec key chain mode.

To remove this configuration, use the **no** form of this command.

key-string [{**clear** | **password** | **password6**}] *key-string-text* **cryptographic-algorithm** {**aes-128-cmac** | **aes-256-cmac**}

Syntax Description

clear	Specifies the key string in clear-text form.
passwordpassword	Specifies the key in encrypted form.
password6	Specifies the key in Type 6 encrypted form.
key-string-text	Text string for the key, which is encrypted by the parser process before being saved to the configuration. The text string has the following character limitations: • Plain-text key strings—Minimum of 1 character and a maximum of 32 (128-bit encryption)/64 (256-bit encryption) characters (hexadecimal string). • Encrypted key strings—Minimum of 4 characters and no maximum.

Command Default

The default value is clear.

Command Modes

Key configuration submode under the macsec key chain mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

For an encrypted password to be valid, the following statements must be true:

- String must contain an even number of characters, with a minimum of four.
- The first two characters in the password string must be decimal numbers and the rest must be hexadecimals.
- The first two digits must not be a number greater than 53.

Either of the following examples would be valid encrypted passwords:

1234abcd

or

50aefd

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **key-string** command:

```
! For AES 128-bit encryption

RP/0/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678 cryptographic-algorithm AES-128-CMAC

! For AES 256-bit encryption with clear-text CAK:

RP/0/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string clear
1234567812345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
AES-256-CMACRP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)#commit
```

lifetime

Configures the validity period for the MACsec key or CKN in the Keychain-key configuration mode. To remove this configuration, use the **no** form of this command.

The lifetime period can be configured with a duration in seconds, as a validity period between two dates (for example, Jan 01 2020 to Dec 31 2020), or with an infinite validity.

The key is valid from the time you configure in HH:MM:SS format. Duration is configured in seconds.

When a key has expired, the MACsec session is torn down and running the **show macsec mka session** command does not display any information. If you run the **show macsec mka interface** and **show macsec mka interface detail** commands, you can see that the session is unsecured.

lifetime *start_time start_date* {*end_time end_date* | **duration** *validity* | **infinite**}

Syntax Description

start-time	Start time in hh:mm:ss from which the key becomes valid. The range is from 0:0:0 to 23:59:59.
end-time	End time in hh:mm:ss at which point the key becomes invalid. The range is from 0:0:0 to 23:59:59.
start_date	The date in DD month YYYY format when the key becomes valid.
end_date	The date in DD month YYYY format when the key becomes invalid.
duration *validity*	The key chain is valid for the duration you configure. You can configure duration in seconds. The range is from 1 to 2147483646.
infinite	The key chain is valid indefinitely.

Command Default

No default behavior or values

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **lifetime** command:

```
! For AES 128-bit encryption
```

```
RP/0/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678 cryptographic-algorithm AES-128-CMAC
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# lifetime 05:00:00 20 february
 2020 12:00:00 30 september 2020
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)#commit

! For AES 256-bit encryption, with lifetime specified as duration:

RP/0/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
1234567812345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
AES-256-CMAC
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# lifetime 05:00:00 20 february
 2020 duration 2592000
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# commit

! Lifetime specified as infinite:

RP/0/RP0RSP0/CPU0:router# configure
RP/0/RP0RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
1234567812345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
AES-256-CMAC
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# lifetime 05:00:00 20 february
 2020 infinite
RP/0/RP0RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# commit
```

macsec-policy

Creates a MACsec policy for MACsec encryption in the global configuration mode. To remove this configuration, use the **no** form of this command.

macsec-policy *policy-name* [{ **allow** { **lacp-in-clear** | **pause-frames-in-clear** } | **cipher-suite** { **GCM-AES-128** | **GCM-AES-256** | **GCM-AES-XPN-128** | **GCM-AES-XPN-256** } | **conf-offset** { **CONF-OFFSET-0** | **CONF-OFFSET-30** | **CONF-OFFSET-50** } | **delay-protection** | **enable-legacy-fallback** | **include-icv-indicator** | **key-server-priority** *priority-value* | **policy-exception lacp-in-clear** | **sak-rekey-interval** { *value-in-minutes* | **seconds** *value-in-seconds* } | **security-policy** { **must-secure** | **should-secure** } | **use-eapol-pae-in-icv** | **vlan-tags-in-clear** *value* | **window-size** *window-size* }]

Syntax Description

policy_name	The MACsec policy name with a maximum length of 16.
allow	Specifies MACsec policy exception to allow packets in clear text.
pause-frames-in-clear	Allows Ethernet PAUSE frame packets in clear text.
cipher-suite	Specifies the cipher-suite used for encryption.
conf-offset	Specifies the confidentiality offset value for encryption.
delay-protection	Enables data delay protection.
include-icv-indicator	Includes integrity check value (ICV) indicator parameter set in MACsec Key Agreement PDU (MKPDU).
enable-legacy-fallback	Enables interoperability with peer devices that do not support MACsec active fallback feature.
key-server-priority	Specifies the key-server priority for the node.
policy-exception	Specifies MACsec policy exception to allow packets in clear text.
lacp-in-clear	Allows Link Aggregation Control Plane protocol (LACP) packets in clear text.
sak-rekey-interval	Specifies the interval after which the key-server generates a new Secure Association Key (SAK) for a secured session.
security-policy	Specifies the security policy as must secure or should secure for data encryption.
use-eapol-pae-in-icv	Enables the use of Extensible Authentication Protocol over LAN (EAPoL) port access entity (POE) address in ICV.
vlan-tags-in-clear	Specifies the number of vlan-tags in clear (1 or 2).
window-size	Specifies the window-size used for encryption. The range is from 0 to 1024.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.0.14	This command was modified to include the **enable-legacy-fallback** option.
Release 7.3.1	This command was modified to include the **allow** keyword.
Release 7.3.15	This command was modified to include the **pause-frames-in-clear** option under the **allow** keyword.

Usage Guidelines

The **policy-exception lacp-in-clear** command is deprecated. Hence, it is recommended to use the **allow lacp-in-clear** command instead, to allow LACP packets in clear-text format.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to configure the **macsec-policy** command:

```
RP/0/RP0RSP0/CPU0:router# configure t
RP/0/RP0RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to specify the cipher-suite used for MACsec encryption:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#cipher-suite GCM-AES-128
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to specify the confidentiality offset value used for MACsec encryption:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#conf-offset CONF-OFFSET-30
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to enable data delay protection under the macsec policy:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#delay-protection
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to include ICV indicator under the macsec policy:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# include-icv-indicator
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to specify the key-server priority for the node:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# key-server-priority 10
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to specify the macsec policy exception to allow packets in clear text:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# policy-exception lacp-in-clear
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to specify the SAK rekey interval under the macsec policy:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# sak-rekey-interval seconds 86400
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to specify the security policy as must-secure or should-secure under the macsec policy:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# security-policy must-secure
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to enable the use of EAPoL PAE address in ICV:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# use-eapol-pae-in-icv
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to specify the number of vlan-tags in clear:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# vlan-tags-in-clear 1
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to specify the window-size under the macsec-policy:

```
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# window-size 256
RP/0/RP0RSP0/CPU0:router(config-mac_policy)#
```

This example shows how to create a MACsec policy exception to allow LACP and Ethernet PAUSE frame packets in clear text:

```
Router#configure
Router(config)#macsec-policy test-macsec-policy
Router(config-macsec-policy)#allow lacp-in-clear
Router(config-macsec-policy)#allow pause-frames-in-clear
Router(config-macsec-policy)#commit
```

macsec shutdown

To enable MACsec shutdown, use the **macsec shutdown** command. To disable MACsec shutdown, use the **no** form of the command.

macsec shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

The **macsec shutdown** command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Usage Guidelines

Enabling the **macsec shutdown** command, brings down all macsec sessions on the MACsec-enabled interfaces and resets ports to non-macsec mode. The already existing MACsec configurations remain unaffected by enabling this feature.

Disabling the **macsec shutdown** command, brings up MACsec sessions for the configured interfaces and enforces MACsec policy on the port.

Warning Configuring **macsec shutdown** command disables MACsec on all data ports, system wide. Execute **clear** command to erase cached configuration or **commit** command to continue.

Task ID

Task ID	Operation
system	read, write

Example

The following example shows how to enable MACsec shutdown:

```
RP/0/RSP0/CPU0:router# configure terminal
RP/0/RSP0/CPU0:router(config)# macsec shutdown
```

sak-rekey-interval

To set a timer value to rekey the MACsec secure association key (SAK) at a specified interval, use the **sak-rekey-interval** command in the macsec-policy configuration mode. To disable this feature, use the **no** form of this command.

sak-rekey-interval *timer-value*

Syntax Description

timer-value	Specifies the timer value, in seconds. Range is 60 to 2592000.

Command Default

The timer is set to OFF, by default

Command Modes

MACsec policy configuration mode.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

This example shows how to set a timer value to rekey the MACsec SAK:

```
Router#configure
Router(config)#macsec-policy test-policy
Router(config-macsec-policy)#sak-rekey-interval 120
Router(config-macsec-policy)#commit
```

show hw-module macsec-fips-post

To display the power-on self-test (POST) known answer test (KAT) configurations of nodes in a router, use the **show hw-module macsec-mode** command in the EXEC modeXR EXEC mode.

show hw-module macsec-fips-post [**location** { *location* | **all** }]

Syntax Description

location	Displays the POST KAT configuration for a node location.
location	Specifies the node location for which the POST KAT configuration is to be displayed.
all	Displays the POST KAT configuration for all nodes.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.14	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
system	read

This example shows how to view the POST KAT configuration of all nodes in a router:

Before location reload:

```
Router#show hw-module macsec-fips-post location all
Wed Jun 17 09:36:31.932 UTC

Location       Configured     Applied          Action
--------------------------------------------------------------
0/0/CPU0       NO             NO               NONE
0/11/CPU0      YES            NO               RELOAD
```

After location reload:

```
Router#show hw-module macsec-fips-post location all
Wed Jun 17 10:03:57.263 UTC

Location       Configured     Applied          Action
--------------------------------------------------------------
0/0/CPU0       NO             NO               NONE
```

```
0/11/CPU0       YES             YES               NONE
```

Related Commands

Command	Description
hw-module macsec-fips-post, on page 8	Enables power-on self-test known answer test (KAT) for the physical layer transceiver (PHY) of a line card

show hw-module macsec-mode

To display the MACsec mode of line cards, and the user action to be performed, use the **show hw-module macsec-mode** command in the EXEC modeXR EXEC mode.

show hw-module macsec-mode [**location** { *location* | **all** }]

Syntax Description

location	*location*	Specifies the location of the line card for which the MACsec mode and the user action to be performed are to be displayed.
all		Displays the MACsec mode information for all the nodes.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.0.12	This command was introduced.
Release 7.0.14	This command was modified to include the **all** option.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
system	read

This example shows how to view the MACsec mode of all nodes and the user action to be performed:

```
Router#show hw-module macsec-mode
Sun Feb 16 21:06:07.726 UTC

Location       Configured     Running          Action
--------------------------------------------------------------
0/0/CPU0       NO             NO               NONE
0/7/CPU0       YES            YES              NONE
```

You can also use the **show hw-module macsec-mode location all** command to display the MACsec mode information of all nodes. This **location all** option is available starting Cisco IOS XR Software Release 7.0.14.

This example shows how to view the MACsec mode of a specific node and the user action to be performed:

```
Router#show hw-module macsec-mode location 0/1/CPU0
Sat Dec  7 14:31:52.668 UTC
Location       Configured     Running          Action
```

```
-------------------------------------------------------------
0/1/CPU0       YES            NO               RELOAD
```

After performing the specified action (reload, in this case):

```
Router#show hw-module macsec-mode location 0/1/CPU0
Sat Dec  7 15:01:00.463 UTC

Location       Configured     Running          Action
-------------------------------------------------------------
0/1/CPU0       YES            YES              NONE
```

Related Commands

Command	Description
hw-module macsec-mode, on page 10	Enables the MACsec mode for the physical layer transceiver (PHY) of a line card.

show crypto sks profile

To display the details or statistics of the Session Key Service (SKS) profiles in the router, use the **show crypto sks profile** command in the EXEC mode.

show crypto sks profile { *profile-name* | **all** } [**stats**]

Syntax Description

profile name	Specifies the name of the SKS profile.
all	Specifies all the SKS profiles in the router.
stats	Displays the statistics of the SKS profiles.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.9.1	This command was introduced.

Usage Guidelines

No specific guidelines impact the use of this command.

Task ID

Task ID	Operation
system	read

The following example shows how to view the SKS profile details in a router:

```
Router# show crypto sks profile all
Profile Name         :ProfileR1toR2
Myidentifier        :Router1
Type                :Remote
Reg Client Count     :1

Server
IP                   :192.0.2.35
Port                 :10001
Vrf                  :Notconfigured
Source Interface     :Notconfigured
Status               :Connected
Entropy              :true
Key                  :true
Algorithm            :QKD
Local identifier     :Alice
Remote identifier    :Alice

Peerlist
QKD ID               :Bob
State                :Connected
```

```
Peerlist
QKD ID                :Alice
State                 :Connected
```

The following example shows how to view the SKS profile statistics in a router:

```
Router# show crypto sks profile all stats
Profile Name            : ProfileR1toR2
My identifier           : Router1
Server
 IP                     : 192.0.2.35
 Port                   : 10001
 Status                 : connected
Counters
 Capability request         : 1
 Key request                : 3
 Key-id request             : 0
 Entropy request            : 0
 Capability response        : 1
 Key response               : 3
 Key-id response            : 0
 Entropy response           : 0
 Total request              : 4
 Request failed             : 0
 Request success            : 4
 Total response             : 4
 Response failed            : 0
 Response success           : 4
 Retry count                : 0
 Response Ignored           : 0
 Cancelled count            : 0
Response time
 Max Time                   : 100 ms
 Avg Time                   : 10  ms
 Min Time                   : 50  ms
Last transaction
 Transaction Id             : 9
 Transaction type           : Get key
 Transaction status         : Response data received, successfully
 Http code                  : 200 OK (200)
```

show macsec mka summary

To display the Summary of MACsec Sessions, use the **show macsec mka summary** command in EXEC mode.

show macsec mka summary

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka summary** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec mka summary information for a specific interface.

```
 Router# show macsec mka summary
Fri Dec 15 06:41:13.299 UTC

NODE: node0_RP0_CPU0
================================================================================================
   Interface-Name     Status     Cipher-Suite       KeyChain       PSK/EAP       CKN
================================================================================================
     TF0/0/0/24       Secured  GCM-AES-XPN-256         kc1          PRIMARY     1111
     TF0/0/0/25       Secured  GCM-AES-XPN-256         kc1          PRIMARY     1111
     TF0/0/0/26       Secured  GCM-AES-XPN-256         kc1          PRIMARY     1111
     TF0/0/0/27       Secured  GCM-AES-XPN-256         kc1          PRIMARY     1111

Total MACSec Sessions  : 4
    Secured Sessions   : 4
    Pending Sessions   : 0
    Suspended Sessions : 0
    Active  Sessions   : 0
```

show macsec mka session

To display the detailed Information of MACsec Sessions, use the **show macsec mka session** command in EXEC mode.

show macsec mka session interface *interface name* **location** *location name* **detail**

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.
detail	(Optional) Detailed information specific to session.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka session** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec mka session information for a specific interface.

```
 Router# show macsec mka session
Fri Dec 15 06:31:38.457 UTC

NODE: node0_RP0_CPU0
==============================================================================================

   Interface-Name        Local-TxSCI       #Peers   Status   Key-Server   PSK/EAP      CKN
==============================================================================================

     TF0/0/0/24      ac3a.67ee.281c/0001     1      Secured      YES      PRIMARY     1111
     TF0/0/0/25      ac3a.67ee.281d/0001     1      Secured      YES      PRIMARY     1111
     TF0/0/0/26      ac3a.67ee.281e/0001     1      Secured      YES      PRIMARY     1111
     TF0/0/0/27      ac3a.67ee.281f/0001     1      Secured      YES      PRIMARY     1111
```

show macsec mka interface detail

To display detailed information on MACsec interfaces, use the **show macsec mka interface detail** command in the EXEC modeXR EXEC mode.

show macsec mka interface *interface name* **detail**

Syntax Description

interface name	Specifies the name of the interface for which you want to view the MACsec details.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.11.1	The **lldp-in-clear** counter was introduced.
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka interface detail** command is available only with the installation of the k9sec rpm.

The **show macsec mka interface detail** command displays information about all MACsec-enabled interfaces across all nodes. If you need MACsec information for a specific interface, use the **show macsec mka interface** *interface name* **detail** command.

Task ID

Task ID	Operation
system	read

This example shows how to view the MACsec information for a specific interface:

```
 Router# show macsec  mka interface HundredGigE 0/0/0/29 detail
Interface Name : HundredGigE0/0/0/29
    Interface Namestring     : HundredGigE0/0/0/29
    Interface short name     : Hu0/0/0/29
    Interface handle         : 0x3c000008
    Interface number         : 0x3c000008
    MacSecControlledIfh      : 0x3c008110
    MacSecUnControlledIfh    : 0x3c008118
    Interface MAC            : ac4a.6730.0624
    Ethertype                : 888E
    EAPoL Destination Addr   : 0180.c200.0003
    MACsec Shutdown          : FALSE
    Config Received          : TRUE
    IM notify Complete       : TRUE
    MACsec Power Status      : N/A
    Interface CAPS Add       : TRUE
    RxSA CAPS Add            : TRUE
    TxSA CAPS Add            : TRUE
    lldp-in-clear            : TRUE
```

```
Principal Actor          : Primary
MKA PSK Info
  Key Chain Name         : kc
  MKA Cipher Suite       : AES-256-CMAC
  CKN                    : 12 34
MKA fallback_PSK Info
  fallback keychain Name : fb
  MKA Cipher Suite       : AES-256-CMAC
  CKN                    : 99 99
Policy                   : mp
SKS Profile              : N/A
Traffic Status           : Protected
Rx SC 1
  Rx SCI                 : ac3a67ee28240001
  Rx SSCI                : 2
  Peer MAC               : ac:3a:67:ee:28:24
  Is XPN                 : YES
  SC State               : Provisioned
  SAK State[3]           : Provisioned
  Rx SA Program Req[3]   : 2023 Nov 08 10:45:16.000
  Rx SA Program Rsp[3]   : 2023 Nov 08 10:45:16.054
  SAK Data
    SAK[3]               : ***
    SAK Len              : 32
    SAK Version          : 1861
    HashKey[3]           : ***
    HashKey Len          : 16
    Conf offset          : 0
    Cipher Suite         : GCM-AES-XPN-256
    CtxSalt[3]           : 0e 43 04 9b 46 92 b2 5a 56 95 c2 af
    CtxSalt Len          : 12
    ssci                 : 2

Tx SC
  Tx SCI                 : ac4a673006240001
  Tx SSCI                : 1
  Active AN              : 3
  Old AN                 : 2
  Is XPN                 : YES
  Next PN                : 1, 1, 1, 1
  SC State               : Provisioned
  SAK State[3]           : Provisioned
  Tx SA Program Req[3]   : 2023 Nov 08 10:45:16.104
  Tx SA Program Rsp[3]   : 2023 Nov 08 10:45:16.154
  SAK Data
    SAK[3]               : ***
    SAK Len              : 32
    SAK Version          : 1861
    HashKey[3]           : ***
    HashKey Len          : 16
    Conf offset          : 0
    Cipher Suite         : GCM-AES-XPN-256
    CtxSalt[3]           : 0e 43 04 98 46 92 b2 5a 56 95 c2 af
    CtxSalt Len          : 12
    ssci                 : 1
```

show macsec mka statistics

To display MKA interface and session statistics, use the **show macsec mka statistics** command in EXEC mode.

show macsec mka statistics [**interface** *interface name* | **location** *location name*]

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location *location name*	(Optional) Location of the node to view global statistics of the MKA instance.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka statistics** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows the output for **show macsec mka statistics**:

```
 Router# show macsec mka statistics location 0/RP0/CPU0
Fri Dec 15 06:43:21.985 UTC


MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 10
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 6
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated............. 10
   SAKs Rekeyed............... 0
   SAKs Received.............. 0
```

```
   SAK Responses Received..... 10
   PPK Tuple Generated........ 0
   PPK Retrieved.............. 0

MKPDU Statistics
   MKPDUs Validated & Rx...... 480156
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0
      "Distributed PPK"..... 0
      "PPK Capable"......... 0
   MKPDUs Transmitted......... 480167
      "Distributed SAK"..... 10
      "Distributed CAK"..... 0
      "Distributed PPK"..... 0
      "PPK Capable"......... 0
```

show macsec mka client

To display MACsec MKA client traces, use the **show macsec mka client** command in EXEC mode.

show macsec mka client [trace {all | errors | events | info}]

Syntax Description

all	(Optional) Show all MACsec MKA client traces for the specified node, or the current node if none is specified.
errors	(Optional) Show MACsec MKA client error traces for the specified node, or the current node if none is specified.
events	(Optional) Show MACsec MKA client event traces for the specified node, or the current node if none is specified
info	(Optional) Show MACsec MKA client info traces for the specified node, or the current node if none is specified

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka trace** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows the output for **show macsec mka client trace all**:

```
 Router# show macsec mka client trace all
Tue Dec  5 10:32:14.266 UTC
1 wrapping entries (10432 possible, 192 allocated, 0 filtered, 1 total)
Dec  4 09:56:25.544 macsec_mka/client/events 0/RP0/CPU0 t5544 TP257:aipc, server:driver,
client:default, init from pid:4779
```

show macsec mka standby

To display MACsec MKA information from hot standby node, use the **show macsec mka standby** command in EXEC mode.

show macsec mka standby [interface | session | statistics] { *interface name* **detail** } **[summary]**

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
detail	(Optional) detailed information specific to Interface/Session

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka standby** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows the output for **show macsec mka standby summary**:

```
 Router# show macsec mka standby summary
Tue Dec  5 10:38:29.004 UTC

Total MACSec Sessions  : 0
    Secured Sessions   : 0
    Pending Sessions   : 0
    Suspended Sessions : 0
     Active  Sessions : 0
```

show macsec mka trace

To display MACsec MKA traces, use the **show macsec mka trace** command in EXEC mode.

show macsec mka trace [all | base | config | errors | events | new-errors | new-events]

Syntax Description

all	(Optional) Show all MACsec MKA traces for the specified node, or the current node if none is specified.
base	(Optional) Show MACsec MKA base traces for the specified node, or the current node if none is specified.
config	(Optional) Show MACsec MKA config traces for the specified node, or the current node if none is specified.
errors	(Optional) Show MACsec MKA error traces for the specified node, or the current node if none is specified.
events	(Optional) Show MACsec MKA event traces for the specified node, or the current node if none is specified.
new-errors	(Optional) Show MACsec MKA new-errors traces for the specified node, or the current node if none is specified.
new-events	(Optional) Show MACsec MKA new-event traces for the specified node, or the current node if none is specified.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec mka trace** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows the output for **show macsec mka trace all**:

```
 Router# show macsec mka trace all
Fri Dec 15 06:42:04.919 UTC
2385 wrapping entries (8576 possible, 3968 allocated, 0 filtered, 2385 total)
Dec 12 15:12:30.077 macsec_mka/base 0/RP0/CPU0 t10778 TP1002: ********** MacSec MKA(10778)
 init start ********.
Dec 12 15:12:30.077 macsec_mka/new_events 0/RP0/CPU0 t10778 TP1002: ********** MacSec
MKA(10778) init start ********.
```

```
Dec 12 15:12:30.077 macsec_mka/events 0/RP0/CPU0 t10778 TP18: MKA_EVENT: Successfully created
 mka event queue
Dec 12 15:12:30.077 macsec_mka/base 0/RP0/CPU0 t10778 TP10: Timer init Success
Dec 12 15:12:30.077 macsec_mka/base 0/RP0/CPU0 t10778 TP801: process respawn_count:1
Dec 12 15:12:30.080 macsec_mka/base 0/RP0/CPU0 t10778 TP164: platform_capa : macsec:1,
macsec-service:0, macsec-subif:0, if_capa:1, ddp:1, secy_intf:1
Dec 12 15:12:30.080 macsec_mka/base 0/RP0/CPU0 t10778 TP164: platform_capa : ea_ha:0,
driver_ha:1, ea_retry:1, plt_sci:0, persist:0, max_an:3, no_secure_loc:1
Dec 12 15:12:30.080 macsec_mka/base 0/RP0/CPU0 t10778 TP164: platform_capa : issu:0,
ppk_support:1, pl_if_data:0, power_status:0, hot_stdby:0
Dec 12 15:12:30.080 macsec_mka/base 0/RP0/CPU0 t10778 TP1341: HA role: Active
```

show macsec policy detail

To display details on the MACsec policies configured on the router, use the **show macsec policy detail** command in the EXEC modeXR EXEC mode.

show macsec policy *policy name* **detail**

Syntax Description

policy name	Specifies the name of the MACsec policy that you want to view.

Command Default

None

Command Modes

EXEC modeXR EXEC mode

Command History

Release	Modification
Release 7.11.1	The **lldp-in-clear** counter was introduced.
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec policy detail** command is available only with the installation of the k9sec rpm.

The **show macsec policy detail** command displays information about all MACsec policies in the router. If you need details of a specific, use the **show macsec policy** *policy name* **detail** command.

Task ID

Task ID	Operation
system	read

This example shows the output for **show macsec policy** *policy name* **detail**:

```
Router# show macsec policy mp detail
Policy Name                 : mp
      Cipher Suite          : GCM-AES-XPN-256
      Key-Server Priority   : 16
      Window Size           : 64
      Conf Offset           : 0
      Replay Protection     : TRUE
      Delay Protection      : FALSE
      Security Policy       : Must Secure
      Vlan Tags In Clear    : 1
      LACP In Clear         : FALSE
      LLDP In Clear         : FALSE
      Pause Frame In Clear  : FALSE
      Sak Rekey Interval    : 60 seconds
      Include ICV Indicator : FALSE
      Use Eapol PAE in ICV  : FALSE
      Disable Suspend On Request    : FALSE
      Disable Suspend For           : FALSE
      Enable legacy fallback        : FALSE
      SKS Profile                   : N/A
```

```
      Max AN                        : 3
```

This example shows the output for **show macsec policy detail**:

```
Router# show macsec policy detail

Total Number of Policies = 2
-------------------------------------------------------
Policy Name                 : DEFAULT-POLICY
      Cipher Suite          : GCM-AES-XPN-256
      Key-Server Priority   : 16
      Window Size           : 64
      Conf Offset           : 0
      Replay Protection     : TRUE
      Delay Protection      : FALSE
      Security Policy       : Must Secure
      Vlan Tags In Clear    : 1
      LACP In Clear         : FALSE
      LLDP In Clear         : FALSE
      Pause Frame In Clear  : FALSE
      Sak Rekey Interval    : OFF
      Include ICV Indicator : FALSE
      Use Eapol PAE in ICV  : FALSE
      Disable Suspend On Request    : FALSE
      Disable Suspend For           : FALSE
      Enable legacy fallback        : FALSE
      SKS Profile                   : N/A
      Max AN                        : 3

Policy Name                 : mp
      Cipher Suite          : GCM-AES-XPN-256
      Key-Server Priority   : 16
      Window Size           : 64
      Conf Offset           : 0
      Replay Protection     : TRUE
      Delay Protection      : FALSE
      Security Policy       : Must Secure
      Vlan Tags In Clear    : 1
      LACP In Clear         : FALSE
      LLDP In Clear         : FALSE
      Pause Frame In Clear  : FALSE
      Sak Rekey Interval    : 60 seconds
      Include ICV Indicator : FALSE
      Use Eapol PAE in ICV  : FALSE
      Disable Suspend On Request    : FALSE
      Disable Suspend For           : FALSE
      Enable legacy fallback        : FALSE
      SKS Profile                   : N/A
      Max AN                        : 3
```

show macsec secy

To display Interface based MACsec dataplane (SecY) statistics, use the **show macsec secy** command in EXEC mode.

show macsec secy [**stats** { **interface** *interface name* **sc** }]

Syntax Description

interface name	MACsec enabled Interface to be specified..
sc	(Optional) Display Secure Channel Statistics for both Rx-SC,SA and Tx-SC,SA specific to the given interface

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec secy** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows the output for **show macsec secy**:

```
 Router# show macsec mka secy stats interface HundredGigE 0/0/0/29 sc
Interface Stats
    InPktsUntagged     :  0
    InPktsNoTag        :  0
    InPktsBadTag       :  0
    InPktsUnknownSCI   :  0
    InPktsNoSCI        :  0
    InPktsOverrun      :  0
    InOctetsValidated  :  0
    InOctetsDecrypted  :  3510182
    OutPktsUntagged    :  0
    OutPktsTooLong     :  0
    OutOctetsProtected :  0
    OutOctetsEncrypted :  1827580
```

show macsec ea

To display MACsec programming details for each interface, use the **show macsec ea** command in EXEC mode.

show macsec ea [idb { **interface** *interface name* | | **location** *location name* } **| trace {all | errors | events| base}**

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.
all	(Optional) Show **all** MACsec EA traces for the specified node, or the current node if none is specified.
base	(Optional) Show MACsec EA **base** traces for the specified node, or the current node if none is specified.
errors	(Optional) Show MACsec EA **error** traces for the specified node, or the current node if none is specified.
events	(Optional) Show MACsec EA **event** traces for the specified node, or the current node if none is specified.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec ea** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec information for a specific interface located on location 0/RP0/CPU0.

```
 Router# show macsec ea idb location 0/RP0/CPU0
Mon Dec  4 03:59:07.481 UTC
```

```
IDB Details:
  if_sname                : TF0/0/0/23
  if_handle               : 0x3c000068
  MacSecControlledIfh     : 0x3c008120
  MacSecUnControlledIfh   : 0x3c008128
  Replay window size      : 64
  Local MAC               : ac:4a:67:30:06:1b
  Rx SC Option(s)         : Validate-Frames Replay-Protect
  Tx SC Option(s)         : Protect-Frames Always-Include-SCI
  Security Policy         : MUST SECURE
  Delay Protection        : FALSE
  Sectag offset           : 0
  db_init Req             : 2023 Dec 03 09:36:22.656
  db_init Rsp             : 2023 Dec 03 09:36:22.662
  if_enable Req           : 2023 Dec 03 09:36:22.663
  if_enable Rsp           : 2023 Dec 03 09:36:23.127
  Rx SC 1
    Rx SCI                : ac3a67ee281b0001
    Peer MAC              : ac:3a:67:ee:28:1b
    Stale                 : NO
    SAK Data
      SAK[2]              : ***
      SAK Len             : 32
      SAK Version         : 1
      HashKey[2]          : ***
      HashKey Len         : 16
      Conf offset         : 0
      Cipher Suite        : GCM-AES-XPN-256
      CtxSalt[2]          : e8 5c ca 8f b3 7a 9d 65 2a 35 ac f8
      ssci                : 2
      Rx SA Program Req[2]: 2023 Dec 03 09:36:27.632
      Rx SA Program Rsp[2]: 2023 Dec 03 09:36:27.712
```

This example shows how to view events associated with the MACsec ea command.

```
Router#show macsec ea trace events

Mon Dec  4 03:57:58.463 UTC
59 wrapping entries (18496 possible, 320 allocated, 0 filtered, 59 total)
Dec  3 09:36:02.903 macsec_ea/events 0/RP0/CPU0 t6945 TP155: ********** MacSec EA(0x1b21)
process START ********.
Dec  3 09:36:02.926 macsec_ea/events 0/RP0/CPU0 t6945 TP180: macsec_ea_programming_conn_up_cb
 received.
Dec  3 09:36:02.966 macsec_ea/events 0/RP0/CPU0 t6945 TP191: macsec_ea_platform_init success
Dec  3 09:36:03.050 macsec_ea/events 0/RP0/CPU0 t6945 TP208: ea_plat_cb_evq:
event_async_attach success, pulse_code:0x7c
Dec  3 09:36:03.050 macsec_ea/events 0/RP0/CPU0 t6945 TP211: ea_plat_cb_evq: created
successfully
Dec  3 09:36:03.083 macsec_ea/events 0/RP0/CPU0 t6945 TP121: ********** Started MacSec
EA(0x1b21) Successfully ********.
```

show macsec open-config

To display Open-config MACSEC traces, use the **show macsec open-config** command in EXEC mode.

show macsec opwn-config trace

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec open-config** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
cisco-support	read

This example shows the output for **show macsec open-config trace**:

```
 Router#show macsec open-config trace
Fri Dec 15 09:08:37.760 UTC
20 wrapping entries (320 possible, 64 allocated, 0 filtered, 20 total)
Dec 12 12:42:43.823 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_edm_open:313, Successful
Dec 12 12:42:43.823 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_mka_oper_gl_sysdb_bind:173,
sysdb_bind successful
Dec 12 12:42:43.823 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_if_sysdb_bind:315, sysdb bind
 successful
Dec 12 12:42:43.827 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_mka_sysdb_bind:343, sysdb
bind: success
Dec 12 12:42:43.827 oc_macsec/all 0/RP0/CPU0 t16252
oc_macsec_mka_gl_stats_oper_sysdb_bind:372, sysdb_bind success
Dec 12 12:42:43.847 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_reg_cfg_notif:250, Successful
Dec 12 15:12:31.317 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_20: notif macsec_if_config, create/update
Dec 12 15:13:52.560 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_21: notif macsec_if_config, create/update
Dec 12 15:16:41.447 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_22: notif macsec_if_config, create/update
Dec 12 15:18:12.700 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_23: notif macsec_if_config, create/update
Dec 12 15:47:30.887 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TenGigE0_0_0_24: notif macsec_if_config, create/update
Dec 13 08:39:35.878 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TenGigE0_0_0_24: notif macsec_if_config, delete
Dec 13 08:46:15.995 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_20: notif macsec_if_config, delete
Dec 13 08:46:15.995 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
```

```
TwentyFiveGigE0_0_0_21: notif macsec_if_config, delete
Dec 13 08:46:15.995 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_22: notif macsec_if_config, delete
Dec 13 08:46:15.995 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_23: notif macsec_if_config, delete
Dec 13 09:25:40.478 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_24: notif macsec_if_config, create/update
Dec 13 09:27:59.242 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_25: notif macsec_if_config, create/update
Dec 13 09:29:32.355 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_26: notif macsec_if_config, create/update
Dec 13 09:31:03.658 oc_macsec/all 0/RP0/CPU0 t16252 oc_macsec_notify_if_macsec:74,
TwentyFiveGigE0_0_0_27: notif macsec_if_config, create/update
```

show macsec platform hardware

To display hardware-specific details for MACsec on each interface, use the **show macsec platform hardware** command in EXEC mode.

show macsec platform hardware [flow | sa | stats] { **interface** *interface name* | **location** *location name* }

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec platform hardware** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec platform hardware information for a specific interface located on location 0/RP0/CPU0.

```
 Router# show macsec platform hardware flow location 0/RP0/CPU0
Wed Dec 20 08:39:18.958 UTC
------------------------------------------
Interface : TwentyFiveGigE0_0_0_27


------------------------------------------
Interface : TwentyFiveGigE0_0_0_26


------------------------------------------
Interface : TwentyFiveGigE0_0_0_25


------------------------------------------
```

```
Interface : TwentyFiveGigE0_0_0_24
```

show macsec platform idb

To display interface database (IDB) details specific to MACsec, use the **show macsec platform idb** command in EXEC mode.

show macsec platform idb { **interface** *interface name* | **location** *location name* }

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec platform idb** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec platform idb information for a specific interface located on location 0/RP0/CPU0.

```
 Router# show macsec platform idb location 0/RP0/CPU0
Wed Dec 20 08:55:47.745 UTC

------------------------------------------------------------------
        EA IDB Details:
------------------------------------------------------------------
    IF Handle             : 0x3c000048
    IF Name               : TF0/0/0/27

------------------------------------------------------------------
        EA IDB Details:
------------------------------------------------------------------
    IF Handle             : 0x3c000050
    IF Name               : TF0/0/0/26

------------------------------------------------------------------
        EA IDB Details:
```

```
------------------------------------------------------------------
    IF Handle             : 0x3c000058
    IF Name               : TF0/0/0/25

------------------------------------------------------------------
        EA IDB Details:
------------------------------------------------------------------
    IF Handle             : 0x3c000060
    IF Name               : TF0/0/0/24
```

show macsec platform stats

To display MACsec platform statistics, use the **show macsec platform stats** command in EXEC mode.

show macsec platform stats { **interface** *interface name* | **location** *location name* }

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec platform stats** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec platform statistics information for a specific interface located on location 0/RP0/CPU0.

```
 Router# show macsec platform stats location 0/RP0/CPU0
Wed Dec 20 08:56:13.285 UTC

------------------------------------------
Interface : TwentyFiveGigE0_0_0_27

------------------------------------------------------------------
    Global Statistics: Ingress
------------------------------------------------------------------
    Rx Ctrl Pkts                          : 47300
    Rx Ctrl Octets                        : 6905732
    Rx Data Pkts                          : 13
    Rx Data Octets                        : 894
    Rx OverSized Pkts                     : 0
    Rx Pkts Bad Tag                       : 0
    Rx Pkts No SCI                        : 0
    Rx Pkts No Tag                        : 0
    Rx Pkts Tagged                        : 0
    Rx Pkts Untagged                      : 0
```

```
    Rx Pkts Unknown SCI                     : 0
    Rx Pkts Untagged Miss                   : 0
    Rx Transform Error Pkts                 : 0
    Rx Pkts SA Not In Use                   : 0

-------------------------------------------------------------------
    Global Statistics: Egress
-------------------------------------------------------------------
    Tx Ctrl Pkts                            : 47308
    Tx Ctrl Octets                          : 6906216
    Tx Data Pkts                            : 16
    Tx Data Octets                          : 894
    Tx Pkts SA Not In Use                   : 0
    Tx Untagged Pkts                        : 0
    Tx Transform Error Pkts                 : 0

-------------------------------------------------------------------
    SA Statistics:Ingress
-------------------------------------------------------------------
    Index                                   : 0
    SCI                                     : ac3a67ee281f0001
    Current AN                              : 0
    Port                                    : 27
    Rx Data Pkts Decrypted                  : 13
    Rx Data Octets Decrypted                : 894
    Rx Pkts Delayed                         : 0
    Rx Pkts Invalid                         : 0
    Rx Pkts Late                            : 0
    Rx Pkts Not Using SA                    : 0
    Rx Pkts Not Valid                       : 0
    Rx Pkts Unchecked                       : 0
    Rx Pkts Untagged Hit                    : 0
    Rx Pkts Unused SA                       : 0
```

show macsec platform trace

To display MACsec platform trace logs, use the **show macsec platform trace** command in EXEC mode.

show macsec platform hardware trace [all | detail | errors | events] { **interface** *interface name* | **location** *location name* }

Syntax Description

interface	Specifies the interface name to view MACsec details.
interface name	Enables MACsec mode for a specified interface.
location	Specifies the node location to enable the MACsec details.
location name	Enables MACsec mode for a specific node.
all	(Optional) Show **all** MACsec Platform traces for the specified node, or the current node if none is specified.
detail	(Optional) Show MACsec Platform**detail** traces for the specified node, or the current node if none is specified.
errors	Optional) Show MACsec Platform **error** traces for the specified node, or the current node if none is specified.
events	(Optional) Show MACsec Platform **event** traces for the specified node, or the current node if none is specified.

Command Default

No default behavior or values.

Command Modes

EXEC mode

Command History

Release	Modification
Release 7.0.1	This command was introduced.

Usage Guidelines

The **show macsec platform trace** command is available only with the installation of the k9sec rpm.

Task ID

Task ID	Operation
interface	read

This example shows how to view MACsec platform trace information for a specific interface located on location 0/RP0/CPU0.

```
 Router# show macsec platform trace detail location 0/RP0/CPU0
Wed Dec 20 08:57:03.178 UTC
2023-12-19:06.28.09.556530212:34390:secydrv_client_commu_ipc_common_fvt_init:COMMU_IPC_DET_36:secydrv_client_commu_ipc_common_fvt_init
```

```
 called
2023-12-19:06.28.09.556530980:34390:secydrv_client_commu_ipc_fvt_init:COMMU_IPC_DET_53:secydrv_client_commu_ipc_fvt_init
 called
2023-12-19:06.28.09.558317574:34390:secydrv_commu_ipc_platform_init:COMMU_IPC_DET_83:secydrv_commu_ipc_platform_init
 called
2023-12-19:06.28.10.579426302:34390:secydrv_commu_ipc_resync_start:COMMU_IPC_DET_106:secydrv_commu_ipc_resync_start
 called
2023-12-19:06.28.10.596378984:34390:secydrv_commu_ipc_resync_stop:COMMU_IPC_DET_129:secydrv_commu_ipc_resync_stop
 called
2023-12-19:06.28.19.598852376:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.28.29.598939886:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.28.39.599043710:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-49:06.28.49.599136368:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.28.59.599221556:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.09.599315246:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.19.599396186:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.29.599470492:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.39.599542858:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.49.599616712:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.29.59.599691262:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.30.09.599768752:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.30.19.599842944:34390:macsec_ea_platform_poll_pn_exceeded:EAPD_DET_3192:PN
Threshold Check:No active sessions
2023-12-19:06.30.27.011625732:34390:macsec_ea_platform_idb_init:EAPD_DET_1026:IDB Init:
ifh: 0x3c000060, if_name TF0/0/0/24, slot 0
2023-12-19:06.30.27.011632184:34390:secydrv_commu_ipc_if_init:COMMU_IPC_DET_151:secydrv_commu_ipc_if_init
 called
```

vlan-tags-in-clear

To configure the number of VLAN tags to be unencrypted (in clear) in MACsec, use the **vlan-tags-in-clear** command in the MACsec policy configuration mode.

vlan-tags-in-clear *number*

Syntax Description

number	Specifies the number of VLAN tags in clear. For single VLAN tag with 802.1q encapsulation, the value is 1. For double VLAN tags with 802.1ad outer tag and 802.1q inner tag encapsulation, the value is 2.

Command Default

Default value is 1.

Command Modes

MACsec policy configuration mode

Command History

Release	Modification
Release 7.11.1	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **vlan-tags-in-clear** command:

```
Router# configure
Router(config)# macsec-policy mac_policy
Router(config-mac_policy)# vlan-tags-in-clear 1
Router(config-mac_policy)# commit
```

window-size

Configures the replay protection window size in MACsec policy configuration mode. To remove this configuration, use the **no** form of this command.

The replay protection window size indicates the number of out-of-sequence frames that can be accepted at the interface configured with MACsec, without being dropped.

window-size *value*

Syntax Description

value	Number of out-of-sequence frames that can be accepted at the interface without being dropped. The range is 0-1024.

Command Default

Default value is 64.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 7.0.12	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **window-size** command:

```
RP/0/RP0RSP0/CPU0:router# configure t
RP/0/RP0RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RP0RSP0/CPU0:router(config-mac_policy)# window-size 64
```