MACsec Encryption Commands

This module describes the commands used to configure MACsec encryption.

Command History

Release	Modification
Release 5.3.2	The following commands were introduced. • cipher-suite • conf-offset • key-server-priority • lifetime • macsec • macsec-policy • security-policy • window-size
Release 6.0.1	The vlan-tags-in-clear command was introduced.
Release 6.1.2	macsec-service command was introduced.
Release 6.1.3	The following commands were introduced. • key chain • fallback-psk-keychain

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 disable this feature, 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 5.3.2	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/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# cipher-suite GCM-AES-XPN-256
RP/0/RSP0/CPU0:router(config-mac_policy)#
```

conf-offset

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

To disable this feature, 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 characters • CONF-OFFSET-50: Offsets the encryption by 50 characters.

Command Default

Default value is 0.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 5.3.2	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/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# conf-offset CONF-OFFSET-30
RP/0/RSP0/CPU0:router(config-mac_policy)#
```

cryptographic-algorithm

Configures the cryptographic algorithm used for authenticating a peer for MACsec encryption in the Keychain-key configuration mode.

To disable this feature, use the **no** form of this command.

cryptographic-algorithm *authentication algorithm*

Syntax Description

authentication algorithm	Configures the 128-bit or 256-bit AES encryption algorithm.

Command Default

No default behavior or values.

Command Modes

Keychain-key configuration.

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

If you do not specify the cryptographic algorithm, MAC computation and API verification would be invalid.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **cryptographic-algorithm** command for MACsec Encryption:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
11111111111111111111111111111111 cryptographic-algorithm aes-256-cmac
```

Examples

The following example shows how to use the **AES-128-CMAC authentication algorithm** command:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678 cryptographic-algorithm aes-128-cmac
```

Examples

The following example shows how to use the **AES-256-CMAC authentication algorithm** command:

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec) # key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
aes-256-cmac
```

fallback-psk-keychain

To create or modify a fallback psk keychain key, use the **fallback-psk-keychain** command in keychain-key configuration mode.

To disable this feature, use the **no** form of this command.

fallback-psk-keychain *key-id*

Syntax Description

key-id	64-character hexadecimal string.

Command Default

No default behavior or values.

Command Modes

Key chain configuration

Command History

Release	Modification
Release 6.1.3	This command is introduced.

Usage Guidelines

The key must be of even number of 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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# fallback-psk-keychain fallback_mac_chain
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
```

key

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

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

Syntax Description

key-id	64-character hexadecimal string.

Command Default

No default behavior or values.

Command Modes

Key chain configuration

Command History

Release	Modification
Release 3.7.2	This command was introduced.

Usage Guidelines

The key must be of even number of 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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
```

key chain

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

To disable this feature, use the **no** form of this command.

key chain *key-chain-name*
no key chain *key-chain-name*

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.

Note If you are configuring MACsec to interoperate with a MACsec server that is running software prior to IOS XR 6.1.3, then ensure that the MACsec key length is of 64 characters. If the key length is lesser than 64 characters, authentication will fail.

Command Modes

Key chain configuration

Command Default

No default behavior or values

Command History

Release	Modification
Release 3.7.2	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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)#
```

key-string

To specify the text string for the key, use the **key-string** command in keychain-key configuration mode.

To disable this feature, use the **no** form of this command.

key-string [{**clear** | **password**}] *key-string-text*
no key-string [{**clear** | **password**}] *key-string-text*

Syntax Description

clear	Specifies the key string in clear-text form.
passwordpassword	Specifies the key in 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 chain configuration

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 **keystring** command:

```
! For AES 128-bit encryption

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678 cryptographic-algorithm AES-128-CMAC
```

```
! For AES 256-bit encryption

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
AES-256-CMAC
```

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 disable this feature, 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 5.3.2	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/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# key-server-priority 16
RP/0/RSP0/CPU0:router(config-mac_policy)#
```

lifetime

Configures the validity period for the MACsec key or CKN in the Keychain-key configuration mode. To disable this feature, 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 2014 to Dec 31 2014), 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 that the key becomes valid.
end_date	The date in DD month YYYY format that the key becomes invalid.
duration *validity*	The key chain is valid for the duration you configure. You can configure duration in seconds.
infinite	The key chain is valid indefinitely.

Command Default

No default behavior or values

Command Modes

Keychain-key configuration

Command History

Release	Modification
Release 5.3.2	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/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
12345678123456781234567812345678 cryptographic-algorithm AES-128-CMAC
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# lifetime 05:00:00 20 february
 2015 12:00:00 30 september 2016

! For AES 256-bit encryption

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# key-string
1234567812345678123456781234567812345678123456781234567812345678 cryptographic-algorithm
AES-256-CMAC
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)# lifetime 05:00:00 20 february
 2015 12:00:00 30 september 2016
```

macsec

Enables MACsec on the router in the keychain configuration mode. To disable this feature, use the **no** form of this command.

macsec [**key** *key-id*]

Syntax Description

key-id	The key can be up to 64 bytes in length. The configured key is the CKN that is exchanged between the peers.

Command Default

No default behavior or values.

Command Modes

Keychain configuration

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

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

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# key chain mac_chain macsec
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec)# key 1234abcd5678
RP/0/RSP0/CPU0:router(config-mac_chain-MacSec-1234abcd5678)#
```

macsec-policy

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

macsec-policy *policy_name*

Syntax Description

policy_name	Name of the MACsec policy for encryption.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **macsec-policy** command:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)#
```

security-policy

Configures the type of data that is allowed to transit out of the interface configured with MACsec in the MACsec policy configuration mode. To disable this feature, use the **no** form of this command.

security-policy {**should-secure** | **must-secure**}

Syntax Description

should-secure	Configures the interface on which the MACsec policy is applied, to permit all data.
must-secure	Configures the interface on which the MACsec policy is applied, to permit only MACsec encrypted data.

Command Default

Default value is **must-secure**.

Command Modes

MACsec policy configuration.

Command History

Release	Modification
Release 5.3.2	This command was introduced.

Task ID

Task ID	Operations
system	read, write

Examples

The following example shows how to use the **security-policy** command:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# security-policy must-secure
RP/0/RSP0/CPU0:router(config-mac_policy)#
```

vlan-tags-in-clear

Configures the number of VLAN tags in clear for MACsec encryption in the MACsec policy configuration mode. To disable this feature, use the **no** form of this command.

vlan-tags-in-clear *number*

Syntax Description

number	Specifies the number of VLAN tags in clear. For 802.1q encapsulation with a single tag, the value is 1. For 802.1q encapsulation with two tags, the value is 2. For 802.1ad encapsulation with a single tag, the value is 1. For 802.1ad encapsulation with a two tags, the value is 2.

Command Default

Default value is 1.

Command Modes

MACsec policy configuration mode

Command History

Release	Modification
Release 6.0.1	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:

```
RP/0/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# vlan-tags-in-clear 1
```

window-size

Configures the replay protection window size in MACsec policy configuration mode. To disable this feature, 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 5.3.2	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/RSP0/CPU0:router# configure t
RP/0/RSP0/CPU0:router(config)# macsec-policy mac_policy
RP/0/RSP0/CPU0:router(config-mac_policy)# window-size 64
```