



# 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. <ul style="list-style-type: none"><li>• cipher-suite</li><li>• conf-offset</li><li>• key-server-priority</li><li>• lifetime</li><li>• macsec</li><li>• macsec-policy</li><li>• security-policy</li><li>• window-size</li></ul>
	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. <ul style="list-style-type: none"><li>• key chain</li><li>• fallback-psk-keychain</li></ul>

- [cipher-suite](#), on page 3
- [conf-offset](#), on page 4
- [cryptographic-algorithm](#), on page 5
- [fallback-psk-keychain](#), on page 7
- [key](#), on page 8
- [key chain](#), on page 9
- [key-string](#), on page 10

- [key-server-priority](#), on page 12
- [lifetime](#), on page 13
- [macsec](#), on page 15
- [macsec-service](#), on page 16
- [macsec-policy](#), on page 17
- [security-policy](#), on page 18
- [vlan-tags-in-clear](#), on page 19
- [window-size](#), on page 20

# 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-XPB-128
- GCM-AES-XPB-256

## Command Default

The default cipher suite chosen for encryption is GCM-AES-XPB-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-XPB-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*

<b>Syntax Description</b>	<p><i>offset_value</i> Configures the offset value. The options are:</p> <ul style="list-style-type: none"> <li>• CONF-OFFSET-0 : Does not offset the encryption</li> <li>• CONF-OFFSET-30: Offsets the encryption by 30 characters</li> <li>• CONF-OFFSET-50: Offsets the encryption by 50 characters.</li> </ul>
---------------------------	--

<b>Command Default</b>	Default value is 0.
------------------------	---------------------

<b>Command Modes</b>	MACsec policy configuration.
----------------------	------------------------------

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Release 5.3.2</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Release 5.3.2	This command was introduced.
Release	Modification				
Release 5.3.2	This command was introduced.				

<b>Task ID</b>	<table border="1"> <thead> <tr> <th>Task ID</th> <th>Operations</th> </tr> </thead> <tbody> <tr> <td>system</td> <td>read, write</td> </tr> </tbody> </table>	Task ID	Operations	system	read, write
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)#
```



---

**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
1234567812345678123456781234567812345678123456781234567812345678 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
```

<b>Syntax Description</b>	<i>key-id</i> 64-character hexadecimal string.
---------------------------	--

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Key chain configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.7.2	This command was introduced.

<b>Usage Guidelines</b>	The key must be of even number of characters. Entering an odd number of characters will exit the MACsec configuration mode.
-------------------------	---

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	system	read, write

<b>Examples</b>	The following example shows how to use the <b>key</b> 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	
<b>clear</b>	Specifies the key string in clear-text form.
<b>password</b> <i>password</i>	Specifies the key in encrypted form.
<i>key-string-text</i>	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: <ul style="list-style-type: none"> <li>• Plain-text key strings—Minimum of 1 character and a maximum of 32 (128-bit encryption)/64 (256-bit encryption) characters (hexadecimal string).</li> <li>• Encrypted key strings—Minimum of 4 characters and no maximum.</li> </ul>

**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 hexadecimal.
- 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
1234567812345678123456781234567812345678123456781234567812345678 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*

<b>Syntax Description</b>	<i>value</i> Indicates the priority for a device to become the key server. Lower the value, higher the preference. The range is 0-255.				
<b>Command Default</b>	Default value is 16.				
<b>Command Modes</b>	MACsec policy configuration.				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Release 5.3.2</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Release 5.3.2	This command was introduced.
Release	Modification				
Release 5.3.2	This command was introduced.				
<b>Task ID</b>	<table border="1"> <thead> <tr> <th>Task ID</th> <th>Operations</th> </tr> </thead> <tbody> <tr> <td>system</td> <td>read, write</td> </tr> </tbody> </table>	Task ID	Operations	system	read, write
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

<i>start-time</i>	Start time in hh:mm:ss from which the key becomes valid. The range is from 0:0:0 to 23:59:59.
<i>end-time</i>	End time in hh:mm:ss at which point the key becomes invalid. The range is from 0:0:0 to 23:59:59.
<i>start_date</i>	The date in DD month YYYY format that the key becomes valid.
<i>end_date</i>	The date in DD month YYYY format that the key becomes invalid.
<b>duration</b> <i>validity</i>	The key chain is valid for the duration you configure. You can configure duration in seconds.
<b>infinite</b>	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
123456781234567812345678123456781234567812345678123456781234567812345678 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* ]

<b>Syntax Description</b>	<i>key-id</i> The key can be up to 64 bytes in length. The configured key is the CKN that is exchanged between the peers.				
<b>Command Default</b>	No default behavior or values.				
<b>Command Modes</b>	Keychain configuration				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Release 5.3.2</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Release 5.3.2	This command was introduced.
Release	Modification				
Release 5.3.2	This command was introduced.				
<b>Task ID</b>	<table border="1"> <thead> <tr> <th>Task ID</th> <th>Operations</th> </tr> </thead> <tbody> <tr> <td>system</td> <td>read, write</td> </tr> </tbody> </table>	Task ID	Operations	system	read, write
Task ID	Operations				
system	read, write				
<b>Examples</b>	<p>The following example shows how to use the <b>macsec</b> command:</p> <pre>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)#</pre>				

## macsec-service

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

**macsec-service decrypt-port** *interface\_number /port\_number* **psk-keychain** *key\_chain\_name* [**policy**] [*policy\_name*]

Syntax Description		
<i>interface_number /port_number</i>		The port or interface number. The interfaces or ports are: The port configured to face the Customer Edge router. The MACsec encryption port The MACsec decryption port
<i>key-chain_name</i>		Name of the key chain configured using the <b>key chain</b> command.
<i>(optional) policy_name</i>		Name of the MACsec policy for encryption configured using the <b>mac-sec policy</b> command. This is an optional keyword.

**Command Default** No default behavior or values.

**Command Modes** Global configuration

Command History	Release	Modification
	Release 6.1.1	This command was introduced.

Task ID	Task ID	Operations
	system	read, write

### Examples

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

```
RP/0/RSP0/CPU0:router# interface <interface>15.10 l2transport
RP/0/RSP0/CPU0:router(config)# encapsulation dot1q 10
RP/0/RSP0/CPU0:router macsec-service decrypt-port <intf>17.10 psk-keychain
<keychain_name> [policy <macsec_policy>]
```



# 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*

<b>Syntax Description</b>	<i>policy_name</i> Name of the MACsec policy for encryption.
---------------------------	--

<b>Command Default</b>	No default behavior or values.
------------------------	--------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 5.3.2	This command was introduced.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	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	
<b>should-secure</b>	Configures the interface on which the MACsec policy is applied, to permit all data.
<b>must-secure</b>	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*

<b>Syntax Description</b>	<p><i>number</i> Specifies the number of VLAN tags in clear.</p> <p>For 802.1q encapsulation with a single tag, the value is 1.</p> <p>For 802.1q encapsulation with two tags, the value is 2.</p> <p>For 802.1ad encapsulation with a single tag, the value is 1.</p> <p>For 802.1ad encapsulation with a two tags, the value is 2.</p>
---------------------------	--

<b>Command Default</b>	Default value is 1.
------------------------	---------------------

<b>Command Modes</b>	MACsec policy configuration mode
----------------------	----------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 6.0.1	This command was introduced.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	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*

<b>Syntax Description</b>	<i>value</i> Number of out-of-sequence frames that can be accepted at the interface without being dropped. The range is 0-1024.
---------------------------	---

<b>Command Default</b>	Default value is 64.
------------------------	----------------------

<b>Command Modes</b>	MACsec policy configuration.
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 5.3.2	This command was introduced.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	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
```