MACsec policy exceptions

This chapter explains how to configure MACsec policy exceptions to permit specific packet types—such as LACP, pause frames, and LLDP packets—to bypass MACsec encryption and be transmitted in clear text. It provides step-by-step procedures, example commands, and important security considerations for enabling these exceptions in Cisco environments.

MACsec policy exception

A MACsec policy exception is a mechanism within a MACsec security policy that

- bypasses MACsec encryption or decryption for specific data packets,
- allows these packets to be sent in clear-text format, and
- supports interoperability scenarios and certain network topologies.

By default, a MACsec security policy uses the **must-secure** option, which mandates data encryption for all traffic. Specific commands can optionally bypass MACsec encryption or decryption, enabling certain packet types to be transmitted in clear text.

Within the **macsec-policy** configuration mode, the **allow** option is available to permit clear-text transmission for designated packet types.

Table 1: MACsec Policy Options: Must-Secure vs. Allow

Feature / Behavior	must-secure	allow
Encryption enforcement	Required for all traffic	Mandatory except for packets explicitly allowed
Use case	Provides maximum security	Allows interoperability in mixed environments
Packet exceptions	Not permitted	Specific packet types can bypass encryption
Example commands	N/A	`allow lacp-in-clear` `allow pause-frames-in-clear`

Feature / Behavior	must-secure	allow
Security level	Highest (no clear-text transmission)	Slightly reduced (clear text allowed for selected frames)

MACsec policy exceptions

- Using the `allow lacp-in-clear` command to bypass MACsec for Link Aggregation Control Protocol (LACP) packets. This is beneficial in scenarios where bundles are terminated at an intermediate node and MACsec is enforced only at end nodes or when the remote node expects clear text.
- Using the `allow pause-frames-in-clear` command to transmit Ethernet PAUSE frame packets in clear text.

Create a MACsec policy exception

Allow specific MACsec policy exceptions to enable or permit particular packet types in clear-text format.

Procedure

Step 1 Use the **macsec-policy** command to access the desired MACsec policy configuration by specifying the policy name.

Example:

```
Router# configure
Router(config)# macsec-policy mp1
```

Step 2 Use the **allow lacp-in-clear** command to permit LACP packets in clear-text format.

Example:

```
Router(config-macsec-policy)# allow lacp-in-clear
```

Step 3 Use the **allow pause-frames-in-clear** command to permit pause frames in clear-text.

Example:

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

Step 4 Use the **show running config** command to confirm the policy exception.

Example:

```
Router# show running-config macsec-policy mp1
macsec-policy mp1
…
allow lacp-in-clear
allow pause-frames-in-clear
!
```

Step 5 Use the **show macsec policy detail** command to verify detailed MACsec policy status.

Example:

```
Router# show macsec policy detail
Total Number of Policies = 1
-------------------------------------------------------
Policy Name : mp1
Cipher Suite : GCM-AES-XPN-256
Key-Server Priority : 10
Window Size : 64
Conf Offset : 50
Replay Protection : TRUE
Delay Protection : FALSE
Security Policy : Must Secure
Vlan Tags In Clear : 1
LACP In Clear : TRUE
LLDP In Clear : FALSE
Pause Frame In Clear : TRUE
Sak Rekey Interval : 60 seconds
```

The MACsec policy is updated to allow the specified packet exceptions in clear text, using the recommended **allow** commands for new configurations.

MACsec policy exceptions for LLDP packets

A MACsec policy exception for LLDP packets is a MACsec configuration mechanism that

- allows the transmission of LLDP (Link Layer Discovery Protocol) packets in clear text even when MACsec encryption is enabled,
- enables network administrators to facilitate neighbor discovery and troubleshooting by making LLDP packets visible on the network, and
- maintains MACsec encryption for all other traffic, ensuring the overall security of the data link layer.

Table 2: Feature History Table

Feature Name	Release Information	Feature Description
MACsec Policy Exception for Link Layer Discovery Protocol Packets	Release 25.1.1	Introduced in this release on: Fixed Systems (8700 [ASIC: K100])(select variants only*) *This feature is supported on the Cisco 8712-MOD-M routers.

Feature Name	Release Information	Feature Description
MACsec Policy Exception for Link Layer Discovery Protocol Packets	Release 24.4.1	Introduced in this release on: Fixed Systems (8200 [ASIC: P100], 8700 [ASIC: P100])(select variants only*); Modular Systems (8800 [LC ASIC: P100])(select variants only*) *This feature is supported on: • 88-LC1-36EH • 88-LC1-12TH24FH-E • 88-LC1-52Y8H-EM • 8212-48FH-M • 8711-32FH-M

Feature Name	Release Information	Feature Description
MACsec Policy Exception for Link Layer Discovery Protocol Packets	Release 7.11.1	We have introduced an option in MACsec policy exceptions to accommodate Link Layer Discovery Protocol (LLDP) packets in an unencrypted format. LLDP packets in clear text format help you troubleshoot LLDP neighbor discovery network issues on MAcsec-enabled ports. By default, MACsec always operates in must-secure mode, allowing encrypted traffic flow including LLDP packets only after securing the MACsec Key Agreement (MKA) session. The feature introduces these changes: CLI: • The **lldp-in-clear** keyword is introduced in the **allow** command. • The **lldp-in-clear** status is displayed in the **show macsec policy detail** command. • The **lldp-in-clear** status is displayed in the **show macsec mka interface detail** command. YANG Data Models: • `Cisco-IOS-XR-crypto-macsec-mka-cfg.yang` • `Cisco-IOS-XR-crypto-macsec-mka-oper.yang` • `Cisco-IOS-XR-um-macsec-cfg.yang` (See GitHub, YANG Data Models Navigator)

By default, when MACsec is enabled, it encrypts all network traffic at the data link layer, including LLDP packets. This ensures that communications between peers remain secure. The router stores information learned from LLDP exchanges in the Management Information Base (MIB).

However, starting from Cisco IOS XR Software Release 7.11.1, routers provide an option to transmit LLDP packets in clear text even when MACsec is enabled. Administrators can enable this exception using the **allow lldp-in-clear** command in the MACsec policy. This functionality is useful for troubleshooting LLDP neighbor

discovery issues, as it allows network administrators to view LLDP packets unencrypted for diagnostic purposes.

By default, MACsec operates in must-secure mode, permitting encrypted traffic flow—including LLDP packets—only after the MACsec Key Agreement (MKA) session is secured.

Note We strongly advise against enabling the MACsec exception to retain LLDP packets unencrypted unless necessary for network maintenance. You must ensure to configure LLDP packets in clear text at both ends of the MACsec link.

Table 3: LLDP packet handling in MACsec: default encryption versus clear-text exception

Feature	Default MACsec behavior	With LLDP exception enabled
LLDP packet encryption	Encrypted	Clear text (unencrypted)
Troubleshooting support	Limited (due to encryption)	Enhanced (LLDP packets visible in plain text)
Security posture	Highest (all packets encrypted)	Slightly reduced for LLDP, others encrypted

LLDP packet handling in MACsec: default encryption and clear-text exception

- An administrator enables the **allow lldp-in-clear** command to transmit LLDP packets in clear text on a MACsec-enabled port for troubleshooting neighbor discovery issues.
- By default, a router encrypts LLDP packets with MACsec, ensuring all data link layer communications are secured.

MACsec LLDP clear-text: troubleshooting challenges and security risks

- Without enabling the LLDP exception, LLDP packets remain encrypted under MACsec, making it difficult to diagnose neighbor discovery problems using packet captures.
- Transmitting all protocol packets, including LLDP, in clear text on a MACsec-enabled port would compromise the security provided by MACsec, which is not the default or recommended configuration.

Configure MACsec policy exception for LLDP packets

Configure a MACsec policy to allow LLDP packets to be transmitted in clear-text format without encryption.

By default, MACsec encrypts all traffic on a link. This task enables an exception for Link Layer Discovery Protocol (LLDP) packets, allowing them to pass through unencrypted while maintaining encryption for other traffic types.

Procedure

Step 1 Use the **macsec-policy** command to access the desired MACsec policy configuration by specifying the policy name.

Example:

```
Router# configure
Router(config)# macsec-policy test-macsec
```

Step 2 Use the **allow lldp-in-clear** command to enable the LLDP clear-text exception.

Example:

```
Router(config-macsec-policy)# allow lldp-in-clear
```

Step 3 Use the **show running config** command to confirm the policy exception.

Example:

```
Router# show running-config macsec-policy test-macsec
macsec-policy mp1
…
allow lldp-in-clear
!
```

Step 4 Use the **show macsec policy detail** and **show macsec mka interface detail** commands to verify the policy details reflect the LLDP clear-text setting.

Example:

```
Router# show macsec policy detail
Total Number of Policies = 1
------------------------------------------------------
Policy Name : mp1
Cipher Suite : GCM-AES-XPN-256
Key-Server Priority : 10
Window Size : 64
Conf Offset : 50
Replay Protection : TRUE
Delay Protection : FALSE
Security Policy : Must Secure
Vlan Tags In Clear : 1
LACP In Clear : FALSE
LLDP In Clear : TRUE
Pause Frame In Clear : FALSE
Sak Rekey Interval : 60 seconds
```

```
Router# show macsec mka interface detail
Number of interfaces on node node0_3_CPU0 : 1
------------------------------------------------------
Interface Name : HundredGigE0/3/0/5
Interface Namestring : HundredGigE0/3/0/5
Interface short name : Hu0/3/0/5
Interface handle : 0x1800238
Interface number : 0x1800238
MacSecControlledIfh : 0x18005e0
MacSecUnControlledIfh : 0x18005e8
Interface MAC : 5cb1.2ede.7648
Ethertype : 888E
EAPoL Destination Addr : 0180.c200.0003
MACsec Shutdown : FALSE
Config Received : TRUE
IM notify Complete : TRUE
```

```
MACsec Power Status : Allocated
Interface CAPS Add : TRUE
RxSA CAPS Add : TRUE
TxSA CAPS Add : TRUE
lldp-in-clear : TRUE
```

The MACsec policy is updated to allow LLDP packets in clear-text, confirmed by showing running configuration and interface details.