Configuring MPLS LDP Session Protection

This chapter describes how to configure Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) session protection on Cisco NX-OS devices.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information" chapter or the Feature History table below.

Information About MPLS LDP Session Protection

The session protection feature provides faster LDP convergence when a link recovers following an outage. It protects an LDP session between directly connected neighbors or an LDP session established for a traffic engineering (TE) tunnel.

MPLS LDP session protection maintains LDP bindings when a link fails. MPLS LDP sessions are protected through the use of LDP hello messages. When you enable MPLS LDP, the label switched routers (LSRs) send messages to find other LSRs with which they can create LDP sessions.

- If the LSR is one hop from its neighbor, it is directly connected to its neighbor. The LSR sends LDP hello messages as User Datagram Protocol (UDP) packets to all the routers on the subnet. The hello message is called an *LDP link hello*. A neighboring LSR responds to the hello message, and the two routers begin to establish an LDP session.
- If the LSR is more than one hop from its neighbor, it is not directly connected to its neighbor. The LSR sends a directed hello message as a UDP packet but as a unicast message specifically addressed to that LSR. The hello message is called an *LDP targeted hello*. The nondirectly connected LSR responds to the hello message, and the two routers establish a targeted LDP session.

MPLS LDP session protection uses LDP targeted hellos to protect LDP sessions. Take, for example, two directly connected routers that have LDP enabled and can reach each other through alternate IP routes in the network. An LDP session that exists between two routers is called an *LDP link session*. When MPLS LDP session protection is enabled, an LDP targeted hello adjacency is also established for the LDP session. If the link between the two routers fails, the LDP link adjacency also fails. However, if the LDP peer is still reachable through IP, the LDP session stays up because the LDP targeted hello adjacency still exists between the routers. When the directly connected link recovers, the session does not need to be reestablished, and LDP bindings for prefixes do not need to be relearned.

Licensing Requirements for MPLS LDP Session Protection

Product	License Requirement
Cisco NX-OS	MPLS LDP session protection requires an MPLS license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

Prerequisites for MPLS LDP Session Protection

MPLS LDP session protection has the following prerequisites:

- You must enable MPLS LDP.
- You must enable all routers that participate in MPLS LDP session protection to respond to targeted hellos. Otherwise, the LSRs cannot establish a targeted adjacency. You must configure both neighbor routers for session protection or configure one router for session protection and the other router to respond to targeted hellos.

Default Settings for MPLS LDP Session Protection

Table 5-1 lists the default settings for MPLS LDP session protection parameters.

Table 5-1 Default MPLS LDP Session Protection Parameters

Parameters	Default
MPLS LDP session protection	Disabled

Configuring MPLS LDP Session Protection

You can configure the Cisco NX-OS device for MPLS LDP session protection.

Prerequisites

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that MPLS LDP is enabled.

SUMMARY STEPS

1. **configure terminal**
2. mpls ldp configuration
3. **session protection** *[***for** *prefix-list] [***duration** *{seconds* | **infinite***}]*
4. **(Optional) show mpls ldp neighbor detail**
5. **(Optional) copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

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

Step 2	**mpls ldp configuration**
	
	Example:
	`switch(config)# mpls ldp configuration`
	`switch(config-ldp)#`
		Enters LDP configuration mode.

Step 3	**session protection** *[***for** *prefix-list]* *[***duration** *{seconds* | **infinite***}]* **Example:** `switch(config-ldp)# session protection for prefix1 duration 100`	Enables MPLS LDP session protection. This command enables LDP sessions to be protected during a link failure. It protects all LDP sessions, unless you specify a prefix list. You can use these keywords to limit the number of protected LDP sessions: • **The for** keyword allows you to specify a prefix list that should be protected. Session protection is then enabled for the peer routers in that prefix list. • **The duration** keyword enables you to specify how long the router should retain the LDP targeted hello adjacency following the loss of the LDP link hello adjacency. The range is from 30 to 2,147,483 seconds. When the link is lost, a timer starts. If the timer expires, the LDP targeted hello adjacency is removed. The **infinite** keyword allows the LDP targeted hello adjacency to exist indefinitely following the loss of the LDP link hello adjacency.
Step 4	**show mpls ldp neighbor detail** **Example:** `switch(config-ldp)# show mpls ldp neighbor detail`	(Optional) Displays the configuration status and current state of MPLS LDP session protection. The state can be “Ready” or “Protecting.” **Note** If the state is “Incomplete,” then the targeted hello adjacency is not yet up.
Step 5	**copy running-config startup-config** **Example:** `switch(config-ldp)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Clearing an MPLS LDP Session

You can terminate an MPLS LDP session after a link goes down. This procedure is useful when the link needs to be taken out of service or needs to be connected to a different neighbor.

Prerequisites

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

Ensure that MPLS LDP is enabled.

SUMMARY STEPS

1. **clear mpls ldp neighbor {* | *neighbor-address*}**

DETAILED STEPS

	Command	Purpose
Step 1	**clear mpls ldp neighbor {* |** *neighbor-address*} **Example:** switch# clear mpls ldp neighbor 10.0.0.13	Clears all LDP neighbor sessions or a specific LDP neighbor session. • **The *** keyword clears all LDP neighbor sessions. • **The** *neighbor-address* **argument** specifies the IP address of the LDP neighbor whose session should be cleared.

Verifying the MPLS LDP Session Protection Configuration

To display the MPLS LDP session protection configuration, perform one of the following tasks:

Command	Purpose
show mpls ldp discovery [detail]	Displays the sources for locally generated LDP targeted hellos.
show mpls ldp neighbor	Displays the status of the LDP session and shows whether the targeted hellos are active.
show mpls ldp neighbor detail	Displays the configuration status and current state of MPLS LDP session protection.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 7000 Series NX-OS MPLS Command Reference*.

Configuration Examples for MPLS LDP Session Protection

The following example shows how to configure MPLS LDP session protection for prefix list “prefix1” and verify the results:

```
switch# configure terminal
switch(config)# mpls ldp configuration
switch(config-ldp)# session protection for prefix1 duration 100
switch(config-ldp)# show mpls ldp discovery
 Local LDP Identifier:
    10.0.0.13:0
    Discovery Sources:
    Interfaces:
    Ethernet2/6 (ldp): xmit/recv
            LDP Id: 10.0.0.22:0
    Targeted Hellos:
        10.0.0.13 -> 10.0.0.22 (ldp): active, xmit/recv
```

```
            LDP Id: 10.0.0.22:0
switch(config-ldp)# show mpls ldp neighbor detail
Peer LDP Ident: 10.0.0.22:0; Local LDP Ident 10.0.0.13:0
        TCP connection: 10.0.0.22.36624 - 10.0.0.13.646
        Password: not required, none, in use
        Adj pwd Rx/Tx: [nil]/[nil]
        TCP pwd Rx/Tx: [nil]/[nil]
        State: Oper; Msgs sent/rcvd: 17/20; Downstream; Last TIB rev sent 9
        Up time: 00:10:25; UID: 3; Peer Id 0
        LDP discovery sources:
          Ethernet2/6; Src IP addr: 168.6.6.22
            holdtime: 15000 ms, hello interval: 5000 ms
          Targeted Hello 10.0.0.13 -> 10.0.0.22, active;
            holdtime: infinite, hello interval: 10000 ms
        Addresses bound to peer LDP Ident:
          10.0.0.22       10.0.0.122      2.0.0.73        168.6.6.22
          192.168.1.22
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
        Clients: Dir Adj Client
        LDP Session Protection enabled, state: Protecting
            duration: 100 seconds
           holdup time remaining: 60 seconds

Capabilities Sent:
          [Dynamic Announcement (0x0506)]
          [Typed Wildcard (0x0970)]
        Capabilities Received:
          [None]
```

Additional References for MPLS LDP Session Protection

For additional information related to implementing MPLS LDP session protection, see the following sections:

- Related Documents, page 5-7
- MIBs, page 5-7

Related Documents

Related Topic	Document Title
CLI commands	*Cisco Nexus 7000 Series NX-OS MPLS Command Reference*
Cisco IOS MPLS LDP session protection	MPLS LDP Session Protection

MIBs

MIB	MIBs Link
MPLS-LDP-STD-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for MPLS LDP Session Protection

Table 5-2 lists the release history for this feature.

Table 5-2 Feature History for MPLS LDP Session Protection

Feature Name	Releases	Feature Information
MPLS LDP session protection	5.2(1)	This feature was introduced.