MPLS LDP Session Protection

The MPLS LDP session protection feature provides faster Label Distribution Protocol (LDP) convergence when a link recovers following an outage. MPLS LDP session protection protects an LDP session between directly connected neighbors or an LDP session established for a traffic engineering (TE) tunnel. This module explains the concepts related to MPLS LDP session protection and describes how to configure MPLS LDP session protection in a network.

Feature history for MPLS LDP session protection

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature name and description	Supported platform
Cisco IOS XE 17.18.2	MPLS LDP session protection	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

MPLS LDP session protection

MPLS LDP session protection is an MPLS LDP feature that

- provides faster LDP convergence when a link recovers from an outage
- protects an LDP session between directly connected neighbors, and
- protects an LDP session established for a traffic engineering (TE) tunnel.

MPLS LDP session protection customization

This section explains how to customize MPLS LDP session protection feature.

You can modify MPLS LDP session protection by using specific keywords in the **mpls ldp session protection** command.

How long should an LDP Targeted Hello Adjacency be retained

The default behavior of the **mpls ldp session protection** command allows an LDP Targeted Hello Adjacency to exist indefinitely following the loss of an LDP Link Hello Adjacency. You can issue the **duration** keyword to specify the number of seconds that the LDP Targeted Hello Adjacency is retained after the loss of the LDP Link Hello Adjacency. When the link is lost, a timer starts. If the timer expires, the LDP Targeted Hello Adjacency is removed.

Which devices should have MPLS LDP session protection

The default behavior of the **mpls ldp session protection** command allows MPLS LDP session protection for all neighbor sessions. You can issue the **for** keyword to limit the number of neighbor sessions that are protected. You can create an access list that includes several peer devices. Specify that access list with the **for** keyword to enable LDP session protection for the peer devices in the access control list.

How MPLS LDP session protection works

MPLS LDP session protection feature allows LDP sessions to remain active during temporary link failures by leveraging Targeted Hello adjacency in addition to standard Link Hello adjacency.

This process is used in MPLS networks to improve LDP session resiliency and convergence time after link failures.

Summary

These are the key components involved in the MPLS LDP session protection process:

- Label switch routers (LSRs): network devices that send and receive LDP messages
- LDP Hello messages: used by LSRs to discover neighbors and establish LDP sessions
- LDP Link Hello: a UDP packet sent to all devices on a subnet for directly connected neighbors
- LDP Targeted Hello: a unicast UDP packet specifically addressed to a non-directly connected LSR
- LDP Link Adjacency: an LDP session between directly connected devices
- LDP Targeted Hello Adjacency: an LDP session established using Targeted Hellos, also used for session protection

MPLS LDP session protection uses LDP Targeted Hellos to protect LDP sessions. For example, two directly connected devices have LDP enabled and can reach each other through alternate IP routes in the network.

Workflow

These stages describe how MPLS LDP session protection works:

1. LSRs send LDP Hello messages to discover other LSRs for LDP session creation.

If...	Then...
LSRs are directly connected or one hop	they send LDP Link Hellos as UDP packets to all devices on the subnet. A neighboring LSR responds, and an LDP session is established, forming an LDP Link adjacency.
LSRs are not directly connected or more than one hop	they send LDP Targeted Hellos as unicast UDP packets to specific LSRs. The non-directly connected LSR responds, and an LDP session is established—a targeted session, often for traffic-engineered paths.

2. When MPLS LDP session protection is enabled, an LDP Targeted Hello adjacency is established for the LDP session in addition to the LDP Link Hello adjacency.

If...	Then...
the directly connected link between two devices fails	the LDP Link adjacency also fails.
if the LDP peer is still reachable through alternate IP routes in the network	the LDP session remains active because the LDP Targeted Hello adjacency persists between the devices.

3. When the directly connected link recovers, the LDP session does not need to be reestablished. And, LDP bindings for prefixes do not need to be relearned, leading to faster convergence.

Result

MPLS LDP session protection feature ensures LDP sessions remain active during temporary link failures, preventing the need for re-establishment and relearning of LDP bindings when the link recovers.

Restrictions for MPLS LDP session protection

The MPLS LDP session protection feature is not supported in certain scenarios:

- with extended access lists
- with LC-ATM devices, and
- with Tag Distribution Protocol (TDP) sessions.

Configure MPLS LDP session protection

This task involves configuring basic IP and MPLS settings before enabling LDP session protection to ensure faster LDP convergence when a link recovers following an outage.

Before you begin

Follow these guidelines for configuring MPLS LDP session protection:

- Label switch routers (LSRs) must be able to respond to LDP Targeted Hellos. Otherwise, the LSRs cannot establish a Targeted adjacency. All devices that participate in MPLS LDP session protection must be enabled to respond to Targeted Hellos.
- Both neighbor devices must be configured for session protection. If not, one device must be configured for session protection and the other device must be configured to respond to Targeted Hellos.

Procedure

Step 1 Configure Cisco Express Forwarding (CEF).

Example:

```
Device> enable
Device# configure terminal
Device(config)# ip cef
```

You can also configure distributed CEF.

Step 2 Configure a loopback interface and assign an IP address to the loopback interface.

Example:

```
Device(config)# interface Loopback 0
Device(config-if)# ip address 10.25.0.11 255.255.255.255
Device(config-if)# exit
```

Step 3 Configure MPLS hop-by-hop forwarding on an interface.

Example:

```
Device(config)# interface HundredGigE 1/0/1
Device(config-if)# mpls ip
Device(config-if)# mpls label protocol ldp
Device(config-if)# exit
Device(config)# exit
```

Step 4 Enable MPLS LDP session protection.

Example:

```
Device(config)# mpls ldp session protection
Device(config)# end
```

Entering the **mpls ldp session protection** command without a keyword protects all LDP sessions.

Specify the keywords for the command, as applicable:

- The **for acl** keyword and argument specifies a standard IP access control list (ACL) of prefixes to be protected.
- The **duration** keyword specifies how long the device should retain the LDP Targeted Hello Adjacency following the loss of the LDP Link Hello Adjacency.

- The **infinite** keyword specifies that the LDP Targeted Hello Adjacency should be retained forever after a link is lost.
- The **seconds** argument specifies the time in seconds that the LDP Targeted Hello Adjacency should be retained after a link is lost. The range is 30 to 2,147,483 seconds.

Verify MPLS LDP session protection

Use this procedure to confirm the operational status of MPLS LDP session protection feature.

Procedure

Step 1 Verify information of the LDP neighbors.

Example:

```
Device# show mpls ldp neighbor

Peer LDP Ident: 10.0.0.3:0; Local LDP Ident 10.0.0.5:0
TCP connection: 10.0.0.3.646 - 10.0.0.5.11005
State: Oper; Msgs sent/rcvd: 1453/1464; Downstream
Up time: 21:09:56
LDP discovery sources:
 Targeted Hello 10.0.0.5 -> 10.0.0.3, active
Addresses bound to peer LDP Ident:
 10.3.104.3       10.0.0.2        10.0.0.3
```

Check if the output contains the term `xmit/recv` for the peer device.

Step 2 Verify that the MPLS LDP session protection state is `Ready` or `Protecting`.

Example:

```
Device#show mpls ldp neighbor detail
    Peer LDP Ident: 44.44.44.44:0; Local LDP Ident 1.1.1.1:0
        TCP connection: 44.44.44.44.29723 - 1.1.1.1.646
        Password: not required, none, in use
        State: Oper; Msgs sent/rcvd: 11085/11089; Downstream; Last TIB rev sent 81942
        Up time: 00:17:46; UID: 3; Peer Id 2
        LDP discovery sources:
         Port-channel44; Src IP addr: 104.1.1.5
           holdtime: 15000 ms, hello interval: 5000 ms
         Targeted Hello 1.1.1.1 -> 44.44.44.44, active, passive;
           holdtime: infinite, hello interval: 10000 ms
        Addresses bound to peer LDP Ident:
          44.44.44.44     43.44.43.44     104.11.1.2      50.255.102.3
          104.1.34.3      104.77.1.4      104.88.44.3     104.1.1.11
          104.10.11.3     104.1.1.5
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
        Clients: Dir Adj Client
        LDP Session Protection enabled, state: Ready
            duration: 86400 seconds
```

If the second last line of the output shows `Incomplete`, the Targeted Hello Adjacency is not up yet.

What to do next

These are some troubleshooting steps for MPLS LDP session protection feature:

- Use the **clear mpls ldp neighbor** command if you need to terminate an LDP session after a link goes down. This is useful for situations where the link needs to be taken out of service or needs to be connected to a different neighbor.
- To enable the display of events related to MPLS LDP session protection, use the **debug mpls ldp session protection** command.