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.

- Finding Feature Information, on page 1
- Prerequisites for MPLS LDP Session Protection, on page 1
- Restrictions for MPLS LDP Session Protection, on page 2
- Information About MPLS LDP Session Protection, on page 2
- How to Configure MPLS LDP Session Protection, on page 3
- Configuration Examples for MPLS LDP Session Protection, on page 7
- Additional References, on page 10
- Feature Information for MPLS LDP Session Protection, on page 11

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and 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 feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MPLS LDP Session Protection

Label switch routers (LSRs) must be able to respond to Label Distribution Protocol (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 or one device must be configured for session protection and the other device must be configured to respond to targeted hellos.

Restrictions for MPLS LDP Session Protection

The MPLS LDP Session Protection feature is not supported under the following circumstances:

- With extended access lists
- With LC-ATM devices
- With Tag Distribution Protocol (TDP) sessions

Information About MPLS LDP Session Protection

How MPLS LDP Session Protection Works

MPLS LDP Session Protection maintains Label Distribution Protocol (LDP) bindings when a link fails. MPLS LDP sessions are protected through the use of LDP hello messages. When you enable Multiprotocol Label Switching (MPLS) LDP, the label switch 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 out LDP Hello messages as User Datagram Protocol (UDP) packets to all the devices on the subnet. The hello message is called an LDP Link Hello. A neighboring LSR responds to the hello message, and the two devices 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 out a directed hello message as a UDP packet but as a unicast message specifically addressed to that specific LSR. The hello message is called an LDP Targeted Hello. The nondirectly connected LSR responds to the Hello message and the two devices establish an LDP session. (If the path between two LSRs has been traffic engineered and has LDP enabled, the LDP session between them is called a targeted session.)

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. An LDP session that exists between two devices is called an LDP Link Hello Adjacency. 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 devices 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 devices. 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.

MPLS LDP Session Protection Customization

You can modify MPLS LDP Session Protection by using keywords in the **mpls ldp session protection** command. The following sections explain how to customize the feature:

How Long an LDP Targeted Hello Adjacency Should Be Retained

The default behavior of the **mpls ldp session protection** command allows a Label Distribution Protocol (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 either the **vrf** or **for** keyword to limit the number of neighbor sessions that are protected:

- You can use the **vrf** keyword to select which virtual routing and forwarding (VRF) instance is to be protected if the device is configured with at least one virtual private network (VPN) VRF instance. You cannot specify more than one VRF with the **mpls ldp session protection** command. To specify multiple VRFs, issue the command multiple times.
- You can create an access list that includes several peer devices. You can specify that access list with the **for** keyword to enable LDP Session Protection for the peer devices in the access control list.

How to Configure MPLS LDP Session Protection

Enabling MPLS LDP Session Protection

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **interface loopback** *number*
5. **ip address** *prefix mask*
6. **exit**
7. **interface** *type number*
8. **mpls ip**
9. **mpls label protocol** [**ldp** | **tdp** | **both**]
10. **exit**
11. **mpls ldp session protection** [**vrf** *vpn-name*] [**for** *acl*] [**duration** {**infinite** | *seconds*}]
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**ip cef** [**distributed**] **Example:** `Device(config)# ip cef distributed`	Configures distributed Cisco Express Forwarding or Cisco Express Forwarding.
Step 4	**interface loopback** *number* **Example:** `Device(config)# interface Loopback 0`	Configures a loopback interface and enters interface configuration mode.
Step 5	**ip address** *prefix mask* **Example:** `Device(config-if)# ip address 10.25.0.11 255.255.255.255`	Assigns an IP address to the loopback interface.
Step 6	**exit** **Example:** `Device(config-if) exit`	Returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface POS 0/3/0`	Specifies the interface to configure and enters interface configuration mode.
Step 8	**mpls ip** **Example:** `Device(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding for the specified interface.
Step 9	**mpls label protocol** [**ldp** | **tdp** | **both**] **Example:** `Device(config-if)# mpls label protocol ldp`	Configures the use of LDP on a specific interface or on all interfaces. • The keywords that are available depend on the hardware platform. • If you set all interfaces globally to LDP, you can override specific interfaces with either the **tdp** or **both** keyword by specifying the command in interface configuration mode.
Step 10	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.

	Command or Action	Purpose
Step 11	**mpls ldp session protection** [**vrf** *vpn-name*] [**for** *acl*] [**duration** {**infinite** | *seconds*}] **Example:** `Device(config)# mpls ldp session protection`	Enables MPLS LDP session protection. • The **vrf** *vpn-name* keyword and argument protects Label Distribution Protocol (LDP) sessions for a specified virtual routing and forwarding (VRF) interface. • 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. The **mpls ldp session protection** command entered without a keyword protects all LDP sessions.
Step 12	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Troubleshooting Tips

Use the **clear mpls ldp neighbor** command if you need to terminate a Label Distribution Protocol (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.

Verifying MPLS LDP Session Protection

SUMMARY STEPS

1. **enable**
2. **show mpls ldp discovery**
3. **show mpls ldp neighbor**
4. **show mpls ldp neighbor detail**
5. **exit**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password, if prompted.

Example:

```
Device> enable
Device#
```

Step 2 **show mpls ldp discovery**

Verifies that the output contains the term xmit/recv for the peer device.

Example:

```
Device# show mpls ldp discovery

 Local LDP Identifier:
    10.0.0.5:0
    Discovery Sources:
    Interfaces:
        ATM50/1/0.5 (ldp): xmit/recv
            LDP Id: 10.0.0.1:0
    Targeted Hellos:
        10.0.0.5 -> 10.0.0.3 (ldp): active, xmit/recv
            LDP Id: 10.0.0.3:0
```

Step 3 **show mpls ldp neighbor**

Verifies that the targeted hellos are active.

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
```

Step 4 **show mpls ldp neighbor detail**

Verifies that the MPLS LDP Session Protection state is Ready or Protecting. If the second last line of the output shows Incomplete, the Targeted Hello Adjacency is not up yet.

Example:

```
Device# show mpls ldp neighbor detail

    Peer LDP Ident: 10.16.16.16:0; Local LDP Ident 10.15.15.15:0
        TCP connection: 10.16.16.16.11013 - 10.15.15.15.646
        State: Oper; Msgs sent/rcvd: 53/51; Downstream; Last TIB rev sent 74
        Up time: 00:11:32; UID: 1; Peer Id 0;
        LDP discovery sources:
          Targeted Hello 10.15.15.15 -> 10.16.16.16, active, passive;
```

```
    holdtime: infinite, hello interval: 10000 ms
Addresses bound to peer LDP Ident:
  10.0.0.2        10.16.16.16     10.101.101.101 11.0.0.1
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
Clients: Dir Adj Client
LDP Session Protection enabled, state: Protecting
    duration: infinite
```

Step 5 **exit**

Returns to user EXEC mode.

Example:

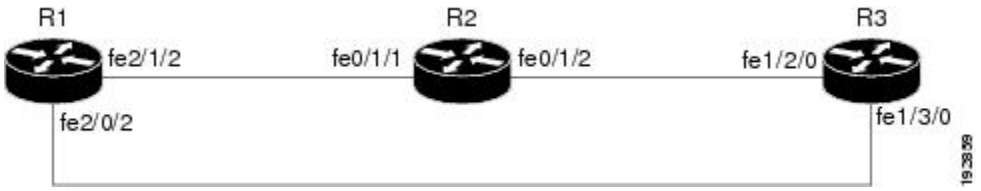
```
Device# exit
Device>
```

Configuration Examples for MPLS LDP Session Protection

Example: Configuring MPLS LDP Session Protection

The figure below shows a sample configuration for MPLS LDP Session Protection.

Figure 1: MPLS LDP Session Protection Example



The following configuration examples for R1, R2, and R3 are based on the figure above.

R1

```
redundancy
 no keepalive-enable
 mode hsa
!
ip cef distributed
no ip domain-lookup
multilink bundle-name both
mpls label protocol ldp
mpls ldp session protection
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Multilink4
```

```
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 load-interval 30
 ppp multilink
 multilink-group 4
!
interface FastEthernet1/0/0
 ip address 10.3.123.1 255.255.0.0
 no ip directed-broadcast
!
interface FastEthernet2/0/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface FastEthernet2/0/1
 description --  ip address 10.0.0.2 255.255.255.0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface FastEthernet2/0/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet2/1/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet2/2/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 10.0.0.1 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
ip classless
```

R2

```
redundancy
 no keepalive-enable
 mode hsa
!
ip subnet-zero
ip cef distributed
mpls label protocol ldp
mpls ldp session protection
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
```

```
!
interface Loopback0
 ip address 10.0.0.3 255.255.255.255
 no ip directed-broadcast
!
interface FastEthernet0/1/0
 no ip address
 no ip directed-broadcast
 shutdown
 full-duplex
!
interface FastEthernet0/1/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/1/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 ip load-sharing per-packet
 full-duplex
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/2/0
 ip address 10.3.123.112 255.255.0.0
 no ip directed-broadcast
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 10.0.0.3 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
ip classless
```

R3

```
ip cef distributed
no ip domain-lookup
mpls label range 200 100000 static 16 199
mpls label protocol ldp
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.5 255.255.255.255
 no ip directed-broadcast
!
interface FastEthernet1/0/0
 no ip address
 no ip directed-broadcast
 shutdown
 half-duplex
!
interface FastEthernet1/2/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
```

```
 mpls ip
!
interface FastEthernet1/3/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 10.0.0.5 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
ip classless
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
MPLS LDP	"MPLS Label Distribution Protocol" module in the *MPLS Label Distribution Protocol Configuration Guide*
MPLS LDP IGP synchronization	"MPLS LDP IGP Synchronization" module in the *MPLS Label Distribution Protocol Configuration Guide*
MPLS LDP Autoconfiguration	"MPLS LDP Autoconfiguration" module in the *MPLS Label Distribution Protocol Configuration Guide*

MIBs

MIBs	MIBs Link
MPLS LDP MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mib

RFCs

RFCs	Title
RFC 3036	LDP Specification
RFC 3037	LDP Applicability

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MPLS LDP Session Protection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for MPLS LDP Session Protection

Feature Name	Releases	Feature Information
MPLS LDP Session Protection	12.0(30)S 12.2(27)SBA 12.2(33)SRA 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1	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. In Cisco IOS Release 12.0(30)S, this feature was introduced on the Cisco 7200 series routers. In Cisco IOS Release 12.2(27)SBA, this feature was implemented on the Cisco 10000 and 7500 series routers. In Cisco IOS Release 12.2(33)SRA, this feature was implemented on the Cisco 7600 series routers. In Cisco IOS Release 12.2(33)SXH, this feature was implemented on the Cisco 6500 series routers. In Cisco IOS Release 12.3(14)T, this feature was integrated. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **debug mpls ldp session protection**, **mpls ldp session protection**, **show mpls ldp neighbor**.