MPLS LDP Session Protection

Last Updated: November 29, 2011

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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 LDP targeted hellos. Otherwise, the LSRs cannot establish a targeted adjacency. All routers that participate in MPLS LDP Session Protection must be enabled to respond to targeted hellos. Both neighbor routers must be configured for session protection or one router must be configured for session protection and the other router must be configured to respond to targeted hellos.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for MPLS LDP Session Protection

This feature is not supported under the following circumstances:

- With extended access lists
- With LC-ATM routers

Information About MPLS LDP Session Protection

How MPLS LDP Session Protection Works

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 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 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 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 routers 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 routers 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 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 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.

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 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 (from 30 to 2,147,483) 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 Routers 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 VRF is to be protected, if the router is configured with at least one VPN routing and forwarding (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 routers. You can specify that access list with the **for** keyword to enable LDP Session Protection for the peer routers in the access control list.

How to Configure MPLS LDP Session Protection

Enabling MPLS LDP Session Protection

To enable MPLS LDP session protection, perform the following task.

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 slot* / *subslot* / *port* [**.** *subinterface-number*]
8. **mpls ip**
9. **mpls label protocol ldp**
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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef distributed** **Example:** `Router(config)# ip cef distributed`	Configures distributed Cisco Express Forwarding.
Step 4	**interface loopback** number **Example:** `Router(config)# interface Loopback0`	Configures a loopback interface and enters interface configuration mode.
Step 5	**ip address** *prefix mask* **Example:** `Router(config-if)# ip address 10.25.0.11 255.255.255.255`	Assigns an IP address to the loopback interface.
Step 6	**exit** **Example:** `Router(config-if) exit`	Exits to global configuration mode.
Step 7	**interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*] **Example:** `Router(config)# interface POS0/3/0`	Specifies the interface to configure and enters interface configuration mode.

	Command or Action	Purpose
Step 8	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding for a specified interface.
Step 9	**mpls label protocol ldp** **Example:** `Router(config-if)# mpls label protocol ldp`	Configures the use of LDP on a specific interface or on all interfaces. • In interface configuration mode, the command sets the the label distribution protocol for the interface. • In global configuration mode, the command sets all the interfaces to LDP.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits from interface configuration mode and returns to global configuration mode.
Step 11	**mpls ldp session protection** [**vrf** *vpn-name*] [**for** *acl*] [**duration** {**infinite** | *seconds*}] **Example:** `Router(config)# mpls ldp session protection`	Enables MPLS LDP session protection. • The **vrf** *vpn-name*keyword-argument pair protects LDP sessions for a specified VRF. • The **for** *acl* keyword-argument pair specifies a standard IP access control list (ACL) of prefixes to be protected. • The **duration** keyword specifies how long the router 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 valid range of values 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:** `Router(config)# exit`	Exits to privileged EXEC mode.

• Troubleshooting Tips, page 5

Troubleshooting Tips

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.

Verifying MPLS LDP Session Protection

To verify that LDP Session Protection has been correctly configured, perform the following steps.

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**

Use this command to enable privileged EXEC mode. Enter your password, if prompted. For example:

Example:

```
Router> enable
Router#
```

Step 2 **show mpls ldp discovery**

Use this command to verify that the output contains the term xmit/recv for the peer router. For example:

Example:

```
Router# 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**

Use this command to verify that the targeted hellos are active. For example:

Example:

```
Router# 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**

Use this command to verify 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. For example:

Example:

```
Router# 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**

Use this command to exit to user EXEC. For example:

Example:

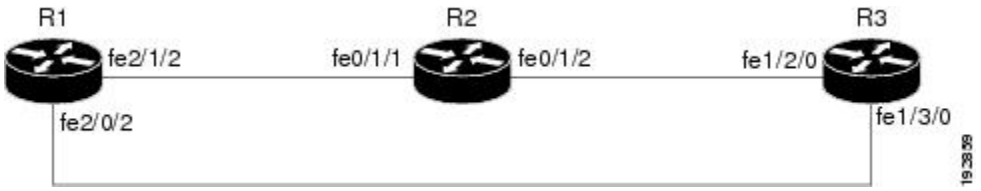
```
Router# exit
Router>
```

Configuration Examples for MPLS LDP Session Protection

Configuring MPLS LDP Session Protection Example

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

The following sections provide references related to the MPLS LDP Session Protection feature.

Related Documents

Related Topic	Document Title
MPLS LDP	MPLS Label Distribution Protocol
MPLS LDP-IGP synchronization	MPLS LDP-IGP Synchronization
LDP autoconfiguration	LDP Autoconfiguration
MPLS LDP commands	*Cisco IOS Multiprotocol Label Switching Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

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

RFCs

RFCs	Title
RFC 3036	LDP Specification
RFC 3037	LDP Applicability

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

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	Cisco IOS XE Release 2.1	The MPLS LDP Session Protection feature provides faster label distribution protocol convergence when a link recovers following an outage. MPLS LDP Session Protection protects a label distribution protocol (LDP) session between directly connected neighbors or an LDP session established for a traffic engineering (TE) tunnel. 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**.