



MPLS LDP Session Protection

Last Updated: May 29, 2012

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.

- [Finding Feature Information, page 1](#)
- [Restrictions for MPLS LDP Session Protection, page 1](#)
- [Information About MPLS LDP Session Protection, page 2](#)
- [How to Configure MPLS LDP Session Protection, page 3](#)
- [Configuration Examples for MPLS LDP Session Protection, page 6](#)
- [Additional References, page 9](#)
- [Command Reference, page 10](#)

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 Toolkit 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.

Restrictions for MPLS LDP Session Protection

This feature is not supported under the following circumstances:

- With TDP sessions
- With extended access lists
- With LC-ATM routers



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

Information About MPLS LDP Session Protection

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 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 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. 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 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 Customizations, page 2](#)

MPLS LDP Session Protection Customizations

You can modify MPLS LDP Session Protection by using the keywords in the `mpls ldp session protection` command.

Specifying 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.

Specifying 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 for for** keyword to limit the number of neighbor sessions that are protected.

Enabling MPLS LDP Session Protection on Specified VPN Routing and Forwarding Instances

If the router is configured with at least one VPN routing and forwarding (VRF) instance, you can use the **vrf** keyword to select which VRF is to be protected. You cannot specify more than one VRF with the `mpls ldp session protection` command. To specify multiple VRFs, issue the command multiple times.

Enabling MPLS LDP Session Protection on Specified Peer Routers

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, page 3](#)
- [Verifying MPLS LDP Session Protection, page 5](#)
- [Troubleshooting Tips, page 6](#)

Enabling MPLS LDP Session Protection

You use the `mpls ldp session protection` command to enable MPLS LDP Session Protection. This command enables LDP sessions to be protected during a link failure. By default, the command protects all LDP sessions. The command has several options that enable you to specify which LDP sessions to protect. The **vrf** keyword lets you protect LDP sessions for a specified VRF. The **for** keyword lets you specify a standard IP access control list (ACL) of prefixes that should be protected. 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.

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.

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | <p>enable</p> <p>Example:</p> <pre>Router> enable</pre> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre> | <p>Enters global configuration mode.</p> |
| Step 3 | <p>ip cef [distributed]</p> <p>Example:</p> <pre>Router(config)# ip cef</pre> | <p>Configures Cisco Express Forwarding.</p> |
| Step 4 | <p>interface loopback-number</p> <p>Example:</p> <pre>Router(config)# interface Loopback0</pre> | <p>Configures a loopback interface and enters interface configuration mode.</p> |
| Step 5 | <p>ip address {prefix mask}</p> <p>Example:</p> <pre>Router(config-if)# ip address 10.25.0.11 255.255.255.255</pre> | <p>Assigns an IP address to the loopback interface.</p> |
| Step 6 | <p>interface interface</p> <p>Example:</p> <pre>Router(config-if)# interface POS3/0</pre> | <p>Specifies the interface to configure.</p> |
| Step 7 | <p>mpls ip</p> <p>Example:</p> <pre>Router(config-if)# mpls ip</pre> | <p>Configures MPLS hop-by-hop forwarding for a specified interface.</p> |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 8 | mpls label protocol {ldp tdp both} Example: <pre>Router(config-if)# mpls label protocol ldp</pre> | Configures the use of LDP on a specific interface or on all interfaces. In interface configuration mode, the command sets the default label distribution protocol for the interface to be LDP, overriding any default set by the global mpls label protocol command. In global configuration mode, the command sets all the interfaces to LDP. |
| Step 9 | exit Example: <pre>Router(config-if)# exit</pre> | Exits from interface configuration mode. |
| Step 10 | mpls ldp session protection [vrf vpn-name] [for acl] [duration seconds] Example: <pre>Router(config)# mpls ldp session protection</pre> | Enables MPLS LDP Session Protection. |

Verifying MPLS LDP Session Protection

SUMMARY STEPS

1. show mpls ldp discovery
2. show mpls ldp neighbor
3. show mpls ldp neighbor detail

DETAILED STEPS

- Step 1** **show mpls ldp discovery**
Issue this command and check that the output contains xmit/recv to the peer router.

Example:

```
Router# show mpls ldp discovery
Local LDP Identifier:
 10.0.0.5:0
Discovery Sources:
Interfaces:
  ATM5/1/0.5 (ldp): xmit/recv
                   LDP Id: 10.0.0.1:0
Targeted Hellos:
```

```
10.0.0.5 -> 10.0.0.3 (ldp): active, xmit/rcv
LDP Id: 10.0.0.3:0
```

Step 2 **show mpls ldp neighbor**

Issue this command to check that the targeted hellos are active.

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 3 **show mpls ldp neighbor detail**

Issue this command to check 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:

```
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
```

Troubleshooting Tips

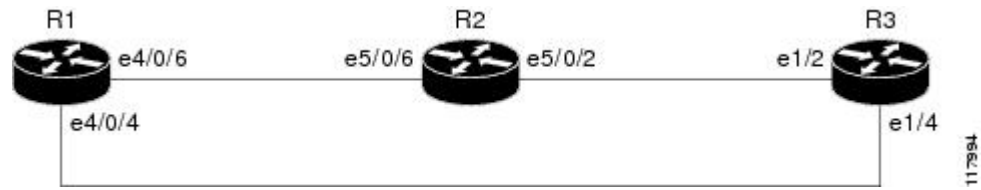
Use the **clear mpls ldp neighbor** command if you need to terminate an LDP session after a link goes down. This is useful for situations where the link needs to be taken out of service or needs to be connected to a different neighbor.

To enable the display of events related to MPLS LDP Session Protection, use the **debug mpls ldp session protection** command.

Configuration Examples for MPLS LDP Session Protection

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

Figure 1 MPLS LDP Session Protection Example



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
tag-switching tdp 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 Ethernet1/0/0
  ip address 10.3.123.1 255.255.0.0
  no ip directed-broadcast
!
interface Ethernet4/0/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Ethernet4/0/1
  description -- ip address 10.0.0.2 255.255.255.0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Ethernet4/0/4
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
  mpls label protocol ldp
  tag-switching ip
!
interface Ethernet4/0/6
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
  mpls label protocol ldp
  tag-switching ip
!
interface Ethernet4/0/7
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
  
```

```

mpls label protocol ldp
tag-switching 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
tag-switching tdp router-id Loopback0 force
!
interface Loopback0
ip address 10.0.0.3 255.255.255.255
no ip directed-broadcast
!
interface Ethernet5/0/0
no ip address
no ip directed-broadcast
shutdown
full-duplex
!
interface Ethernet5/0/2
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
full-duplex
mpls label protocol ldp
tag-switching ip
!
interface Ethernet5/0/6
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
tag-switching ip
!
interface FastEthernet5/1/0
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
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
tag-switching tdp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.5 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet1/0
 no ip address
 no ip directed-broadcast
 shutdown
 half-duplex
!
interface Ethernet1/2
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
 tag-switching ip
!
interface Ethernet1/4
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
 tag-switching 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 |
|------------------------------|----------------------------------|
| MPLS LDP | MPLS Label Distribution Protocol |
| MPLS LDP-IGP synchronization | MPLS LDP-IGP Synchronization |
| LDP autoconfiguration | LDP Autoconfiguration |

Standards

| Standards | Title |
|-----------|-------|
| None | -- |

MIBs

| MIBs | MIBs Link |
|--------------|--|
| MPLS LDP MIB | To locate and download MIBs for selected platforms, Cisco IOS 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com. | http://www.cisco.com/techsupport |

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html . For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug mpls ldp session protection**
- **mpls ldp session protection**
- **show mpls ldp neighbor**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.