MPLS LDP Session Protection

First Published: November 8, 2004
Last Updated: May 31, 2007

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 in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for MPLS LDP Session Protection" section on page 22.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

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.

How to Configure MPLS LDP Session Protection

This section explains how to configure and verify MPLS LDP Session Protection:

- Enabling MPLS LDP Session Protection, page 2 (required)
- Customizing MPLS LDP Session Protection, page 4 (optional)
- Verifying MPLS LDP Session Protection, page 6 (optional)

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.

Prerequisites

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.

Restrictions

This feature is not supported under the following circumstances:

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

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	**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`	Configures Cisco Express Forwarding.

	Command or Action	Purpose
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	**interface** *interface* **Example:** `Router(config-if)# interface POS3/0`	Specifies the interface to configure.
Step 7	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding for a specified interface.
Step 8	**mpls label protocol** {**ldp** | **tdp** | **both**} **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 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:** `Router(config-if)# exit`	Exits from interface configuration mode.
Step 10	**mpls ldp session protection** [**vrf** *vpn-name*] [**for** *acl*] [**duration** *seconds*] **Example:** `Router(config)# mpls ldp session protection`	Enables MPLS LDP Session Protection.

Customizing MPLS LDP Session Protection

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

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** or **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.

Verifying MPLS LDP Session Protection

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

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.

```
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/recv
            LDP Id: 10.0.0.3:0
```

Step 2 show mpls ldp neighbor

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

```
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.

```
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

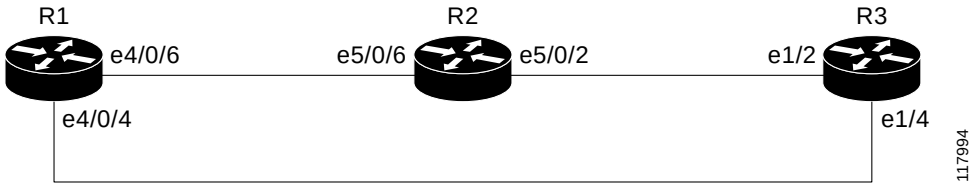
Use the **clear mpls ldp neighbor** command if you need to terminate an LDP session after a link goes down. This is useful for situations where the link needs to be taken out of service or needs to be connected to a different neighbor.

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

Figure 1 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

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*

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

This section documents only commands that are new or modified.

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

debug mpls ldp session protection

To enable the display of events related to MPLS LDP Session Protection, use the **debug mpls ldp session protection** command in privileged EXEC mode. To disable this feature, use the **no** form of this command.

debug mpls ldp session protection [**peer-acl** *acl*]

no debug mpls ldp session protection [**peer-acl** *acl*]

Syntax Description

peer-acl *acl*	(Optional) Enables the display of events for the peers whose router IDs are listed in the access control list.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

In the following example, the display of events related to MPLS LDP Session Protection are enabled:

```
Router# debug mpls ldp session protection
```

Related Commands

Command	Description
clear mpls ldp neighbor	Forcibly resets an LDP session.
show mpls ldp neighbor	Displays the contents of the LDP.

mpls ldp session protection

To enable MPLS LDP Session Protection for existing Label Distribution Protocol (LDP) sessions or when new sessions are established, use the **mpls ldp session protection** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ldp session protection [**vrf** *vpn-name*] [**for** *acl*] [**duration** {**infinite** | *seconds*}]

no mpls ldp session protection [**vrf** *vpn-name*] [**for** *acl*] [**duration** {**infinite** | *seconds*}]

Syntax Description

vrf *vpn-name*	(Optional) Specifies a VPN routing and forwarding instance (*vpn-name*) for accepting labels. This keyword is available when the router has at least one VRF configured.
for *acl*	(Optional) Specifies a standard IP access control list that contains the prefixes that are to be protected.
duration	(Optional) Specifies the time that the LDP Targeted Hello Adjacency should be retained after a link is lost. **Note** If you use this keyword, you must select either the **infinite** keyword or the *seconds* argument.
infinite	Specifies that the LDP Targeted Hello Adjacency should be retained forever after a link is lost.
seconds	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.

Defaults

LDP sessions are not established.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is not supported under the following circumstances:

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

If you issue the **mpls ldp session protection** command without the **duration** keyword, then session protection is enabled for 86400 seconds (24 hours) meaning that the LDP Targeted Hello Adjacency is retained for 24 hours after a link is lost. This is the default timeout.

If you issue the **mpls ldp session protection duration infinite** command, then session protection is enabled forever meaning that the LDP Targeted Hello Adjacency is retained forever after a link is lost.

If you issue the **mpls ldp session protection duration** *seconds* command, then session protection is enabled for the number of seconds indicated meaning that the LDP Targeted Hello Adjacency is retained for that amount of time. For example, if you issued **mpls ldp session protection duration 100**, then the LDP Targeted Hello Adjacency is retained for 100 seconds after a link is lost.

Examples

In the following example, MPLS LDP Session Protection is enabled for LDP sessions for peers whose router IDs are listed in access control list rtr4:

```
Router(config)# mpls ldp session protection for rtr4
```

Related Commands

Command	Description
clear mpls ldp neighbor	Forcibly resets an LDP session.
show mpls ldp neighbor	Displays the contents of the LDP.

show mpls ldp neighbor

To display the status of Label Distribution Protocol (LDP) sessions, use the **show mpls ldp neighbor** command in user EXEC or privileged EXEC mode.

show mpls ldp neighbor [**vrf** *vrf-name* | **all**] [*address* | *interface*] [**detail**] [**graceful-restart**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the LDP neighbors for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance (*vrf-name*).
all	(Optional) Displays LDP neighbor information for all VPNs, including those in the default routing domain.
address	(Optional) Identifies the neighbor with this IP address.
interface	(Optional) Defines the LDP neighbors accessible over this interface.
detail	(Optional) Displays information in long form.
graceful-restart	(Optional) Displays per-neighbor graceful restart information.

Defaults

This command displays information about LDP neighbors for the default routing domain if you do not specify the optional **vrf** keyword.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CT	This command was introduced.
12.0(10)ST	The command was modified to reflect Multiprotocol Label Switching (MPLS) Internet Engineering Task Force (IETF) command syntax and terminology.
12.0(14)ST	This command was modified to reflect MPLS VPN support for LDP and the **vrf** and **all** keywords were added.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(26)S	The **detail** keyword was updated to display information about inbound filtering.
12.2(25)S	The **graceful-restart** keyword was added.
12.3(14)T	The command output was updated so that the **detail** keyword displays information about MPLS LDP Session Protection.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(28)SB	The **detail** keyword was updated to include Message Digest 5 (MD5) password information and the command was implemented on the Cisco 10000 Series Routers.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show mpls ldp neighbor** command can provide information about all LDP neighbors, or the information can be limited to the following:

- Neighbor with specific IP address
- LDP neighbors known to be accessible over a specific interface

Note This command displays information about LDP and Tag Distribution Protocol (TDP) neighbor sessions.

Examples

For explanations of the significant fields shown in the displays, see Table 1.

The following is sample output from the **show mpls ldp neighbor** command:

```
Router# show mpls ldp neighbor

Peer LDP Ident: 10.0.7.7:2; Local LDP Ident 10.1.1.1:1
        TCP connection: 10.0.7.7.11032 - 10.1.1.1.646
        State: Oper; Msgs sent/rcvd: 5855/6371; Downstream on demand
        Up time: 13:15:09
        LDP discovery sources:
          ATM3/0.1
Peer LDP Ident: 10.1.1.1:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.1.1.1.646 - 10.1.1.1.11006
        State: Oper; Msgs sent/rcvd: 4/411; Downstream
        Up time: 00:00:52
        LDP discovery sources:
          Ethernet1/0/0
        Addresses bound to peer LDP Ident:
          10.0.0.29        10.1.1.1         10.0.0.199      10.10.1.1
          10.205.0.9
```

The following is sample output from the **show mpls ldp neighbor** command, in which duplicate addresses are detected. They indicate an error because a given address should be bound to only one peer.

```
Router# show mpls ldp neighbor

Peer LDP Ident: 10.0.7.7:2; Local LDP Ident 10.1.1.1:1
        TCP connection: 10.0.7.7.11032 - 10.1.1.1.646
        State: Oper; Msgs sent/rcvd: 5855/6371; Downstream on demand
        Up time: 13:15:09
        LDP discovery sources:
          ATM3/0.1
Peer LDP Ident: 10.1.1.1:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.1.1.1.646 - 10.1.1.1.11006
        State: Oper; Msgs sent/rcvd: 4/411; Downstream
        Up time: 00:00:52
        LDP discovery sources:
          Ethernet1/0/0
        Addresses bound to peer LDP Ident:
          10.0.0.29 10.1.1.1 10.0.0.199 10.10.1.1
          10.205.0.9
        Duplicate Addresses advertised by peer:
          10.10.8.111
```

The following is sample output from the **show mpls ldp neighbor vrf vpn10** command, which displays the LDP neighbor information for the specified VPN routing and forwarding instance named vpn10:

```
Router# show mpls ldp neighbor vrf vpn10

Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.29.0.2:0
        TCP connection:10.14.14.14.646 - 10.29.0.2.11384
        State:Oper; Msgs sent/rcvd:1423/800; Downstream
        Up time:02:38:11
        LDP discovery sources:
          ATM3/0/0.10
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
```

The following shows sample output from the **show mpls ldp neighbor detail** command, which displays information about inbound filtering:

```
Router# show mpls ldp neighbor vrf vpn1 detail

 Peer LDP Ident: 10.13.13.13:0; Local LDP Ident 10.33.0.2:0
   TCP connection: 10.13.13.13.646 - 10.33.0.2.31581
   State: Oper; Msgs sent/rcvd: 11/10; Downstream; Last TIB rev sent 13
   Up time: 00:02:25; UID: 26; Peer Id 0;
   LDP discovery sources:
    Ethernet1/0/2; Src IP addr: 10.33.0.1
     holdtime: 15000 ms, hello interval: 5000 ms
   Addresses bound to peer LDP Ident:
    10.3.105.1       10.13.13.13     10.33.0..1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
   LDP inbound filtering accept acl:1
 Peer LDP Ident: 10.14.14.14:0; Local LDP Ident 10.33.0.2:0
   TCP connection: 10.14.14.14.646 - 10.33.0.2.31601
   State: Oper; Msgs sent/rcvd: 10/9; Downstream; Last TIB rev sent 13
   Up time: 00:01:17; UID: 29; Peer Id 3;
   LDP discovery sources:
    Ethernet1/0/3; Src IP addr: 10.33.0.1
     holdtime: 15000 ms, hello interval: 5000 ms
   Addresses bound to peer LDP Ident:
    10.3.104.1       10.14.14.14     10.32.0.1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
   LDP inbound filtering accept acl:1
```

The following is sample output from the **show mpls ldp neighbor all** command, which displays the LDP neighbor information for all VPN routing and forwarding instances, including those in the default routing domain. In this example, note that the same neighbor LDP ID (10.14.14.14) appears in all the listed VRF interfaces, highlighting the fact that the same IP address can coexist in different VPN routing and forwarding instances.

```
Router# show mpls ldp neighbor all

Peer TDP Ident:10.11.11.11:0; Local TDP Ident 10.12.12.12:0
        TCP connection:10.11.11.11.711 - 10.12.12.12.11003
        State:Oper; PIEs sent/rcvd:185/187; Downstream
        Up time:02:40:02
        TDP discovery sources:
          ATM1/1/0.1
        Addresses bound to peer TDP Ident:
          10.3.38.3        10.1.0.2        10.11.11.11
VRF vpn1:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.7.0.2:0
        TCP connection:10.14.14.14.646 - 10.7.0.2.11359
        State:Oper; Msgs sent/rcvd:952/801; Downstream
        Up time:02:38:49
        LDP discovery sources:
          ATM3/0/0.1
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn2:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.13.0.2:0
        TCP connection:10.14.14.14.646 - 10.13.0.2.11361
        State:Oper; Msgs sent/rcvd:964/803; Downstream
        Up time:02:38:50
        LDP discovery sources:
          ATM3/0/0.2
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.7.0.1        10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn3:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.15.0.2:0
        TCP connection:10.14.14.14.646 - 10.15.0.2.11364
```

```
        State:Oper; Msgs sent/rcvd:1069/800; Downstream
        Up time:02:38:52
        LDP discovery sources:
          ATM3/0/0.3
        Addresses bound to peer LDP Ident:
          10.3.36.9       10.17.0.1       10.14.14.14     10.13.0.1
          10.15.0.1       10.17.0.1       10.19.0.1       10.21.0.1
          10.23.0.1       10.25.0.1       10.27.0.1       10.29.0.1
          10.31.0.1       10.33.0.1       10.35.0.1       10.37.0.1
          10.39.0.1       10.41.0.1       10.43.0.1       10.45.0.1
          10.47.0.1       10.49.0.1       10.51.0.1       10.53.0.1
          10.55.0.1       10.57.0.1       10.59.0.1       10.61.0.1
          10.63.0.1       10.65.0.1       10.67.0.1       10.69.0.1
          10.71.0.1       10.73.0.1       10.75.0.1       10.77.0.1
          10.79.0.1       10.81.0.1       10.83.0.1       10.85.0.1
          10.87.0.1       10.89.0.1       10.91.0.1       10.93.0.1
          10.95.0.1       10.97.0.1       10.99.0.1       10.101.0.1
          10.103.0.1      10.105.0.1      10.107.0.1      10.109.0.1
          10.4.0.2        10.3.0.2
VRF vpn4:
    Peer LDP Ident:10.14.14.14:0; Local LDP Ident 10.17.0.2:0
        TCP connection:10.14.14.14.646 - 10.17.0.2.11366
        State:Oper; Msgs sent/rcvd:1199/802; Downstream
```

The following example shows the Graceful Restart status of the LDP neighbors:

```
Router# show mpls ldp neighbor graceful-restart

Peer LDP Ident: 10.20.20.20:0; Local LDP Ident 10.17.17.17:0
   TCP connection: 10.20.20.20.16510 - 10.17.17.17.646
    State: Oper; Msgs sent/rcvd: 8/18; Downstream
    Up time: 00:04:39
    Graceful Restart enabled; Peer reconnect time (msecs): 120000
Peer LDP Ident: 10.19.19.19:0; Local LDP Ident 10.17.17.17:0
    TCP connection: 10.19.19.19.11007 - 10.17.17.17.646
    State: Oper; Msgs sent/rcvd: 8/38; Downstream
    Up time: 00:04:30
    Graceful Restart enabled; Peer reconnect time (msecs): 120000
```

The following sample output from the **show mpls ldp neighbor detail** command displays information about the MD5 password configuration:

```
Router# show mpls ldp neighbor detail

    Peer LDP Ident: 10.3.3:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
        Password: required, neighbor, in use
        State: Oper; Msgs sent/rcvd: 167/167; Downstream; Last TIB rev sent 9
        Up time: 02:24:02; UID: 5; Peer Id 3;
        LDP discovery sources:
          Targeted Hello 10.1.1.1 -> 10.3.3.3, passive;
            holdtime: 90000 ms, hello interval: 10000 ms
        Addresses bound to peer LDP Ident:
          10.3.3.3        10.0.30.3
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
    Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
        TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
        Password: not required, none, stale
        State: Oper; Msgs sent/rcvd: 9/9; Downstream; Last TIB rev sent 9
        Up time: 00:05:35; UID: 6; Peer Id 1;
        LDP discovery sources:
          Ethernet1/0; Src IP addr: 10.0.20.4
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
```

```
    10.0.40.4       10.4.4.4         10.0.20.4
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

Table 1 describes the significant fields shown in the displays.

Table 1 show mpls ldp neighbor Field Descriptions

Field	Description
Peer LDP Ident	LDP (or TDP) identifier of the neighbor (peer) for this session.
Local LDP Ident	LDP (or TDP) identifier for the local label switch router (LSR) for this session.
TCP connection	TCP connection used to support the LDP session, shown in the following format: • peer IP address.peer port • local IP address.local port
Password	Indicates if password protection is being used. Password status is as follows: • Required or not required—Indicates whether password configuration is required. • Neighbor, none, option #, or fallback—Indicates the password source when the password was configured. • In use (current) or stale (previous)—Indicates the current LDP session password usage status.
State	State of the LDP session. Generally, this is Oper (operational), but transient is another possible state.
Msgs sent/rcvd	Number of LDP messages sent to and received from the session peer. The count includes the transmission and receipt of periodic keepalive messages, which are required for maintenance of the LDP session.
Downstream on demand	Indicates that the Downstream on Demand method of label distribution is being used for this LDP session. When the Downstream on Demand method is used, an LSR advertises its locally assigned (incoming) labels to its LDP peer only when the peer requests them.
Downstream	Indicates that the downstream method of label distribution is being used for this LDP session. When the downstream method is used, an LSR advertises all of its locally assigned (incoming) labels to its LDP peer (subject to any configured access list restrictions).
Up time	Length of time (in hours, minutes, seconds) the LDP session has existed.
Graceful Restart enabled	Indicates whether the LDP session has Graceful Restart enabled.
Peer reconnect time	The length of time, in milliseconds (msecs), the peer router waits for a router to reconnect.
LDP discovery sources	Sources of LDP discovery activity that led to the establishment of this LDP session.

Table 1 show mpls ldp neighbor Field Descriptions (continued)

Field	Description
Targeted Hello	Lists the platforms to which targeted hello messages are being sent: • The active field indicates that this LSR has initiated targeted hello messages. • The passive field indicates that the neighbor LSR has initiated targeted hello messages and that this LSR is configured to respond to the targeted hello messages from the neighbor.
holdtime	Period of time, in milliseconds (ms), a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor.
hello interval	Period of time, in milliseconds (ms), between the sending of consecutive hello messages.
Addresses bound to peer LDP Ident	Known interface addresses of the LDP session peer. These are addresses that might appear as “next hop” addresses in the local routing table. They are used to maintain the Label Forwarding Information Base (LFIB).
Duplicate Addresses advertised by peer	IP addresses that are bound to another peer. They indicate an error because a given address should be bound to only one peer.
Peer holdtime	The time, in milliseconds (ms), that the neighbor session is retained without the receipt of an LDP message from the neighbor.
KA Interval	Keep Alive Interval. The amount of time, in milliseconds (ms), that a router lets pass without sending an LDP message to its neighbor. If this time elapses and the router has nothing to send, it sends a Keep Alive message.
Peer state	State of the peer; estab means established.
LDP inbound filtering accept acl:1	Access list that is permitted for inbound label binding filtering.

Related Commands

Command	Description
show mpls ldp discovery	Displays the status of the LDP discovery process.

Feature Information for MPLS LDP Session Protection

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2 Feature Information for MPLS LDP Session Protection

Feature Name	Releases	Feature Information
MPLS LDP Session Protection	12.0(30)S 12.3(14)T 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	This feature provides faster label distribution protocol convergence when a link recovers following an outage. The following sections provide information about this feature: • Information About MPLS LDP Session Protection, page 2 • How to Configure MPLS LDP Session Protection, page 2