MPLS Label Distribution Protocol Configuration Guide, Cisco IOS Release 12.4T

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

MPLS Label Distribution Protocol (LDP)

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding in an MPLS network. This module explains the concepts related to MPLS LDP and describes how to configure MPLS LDP in a network.

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.

Prerequisites for MPLS LDP

Label switching on a router requires that Cisco Express Forwarding (CEF) be enabled on that router.

Information About MPLS LDP

Introduction to MPLS LDP

MPLS LDP provides the means for LSRs to request, distribute, and release label prefix binding information to peer routers in a network. LDP enables LSRs to discover potential peers and to establish LDP sessions with those peers for the purpose of exchanging label binding information.

MPLS LDP enables one LSR to inform another LSR of the label bindings it has made. Once a pair of routers communicate the LDP parameters, they establish a label-switched path (LSP). MPLS LDP enables LSRs to distribute labels along normally routed paths to support MPLS forwarding. This method of label distribution is also called hop-by-hop forwarding. With IP forwarding, when a packet arrives at a router the router looks at the destination address in the IP header, performs a route lookup, and forwards the packet to the next hop. With MPLS forwarding, when a packet arrives at a router the router looks at the incoming label, looks up the label in a table, and then forwards the packet to the next hop. MPLS LDP is useful for applications that require hop-by-hop forwarding, such as MPLS VPNs.

MPLS LDP Functional Overview

Cisco MPLS LDP provides the building blocks for MPLS-enabled applications, such as MPS Virtual Private Networks (VPNs).

LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward label traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

LDP and TDP Support

LDP supercedes Tag Distribution Protocol (TDP). See the table below for information about LDP and TDP support in Cisco IOS releases.

Use caution when upgrading the image on a router that uses TDP. Ensure that the TDP sessions are established when the new image is loaded. You can accomplish this by issuing the **mpls label protocol tdp** global configuration command. Issue this command and save it to the startup configuration before loading the new image. Alternatively, you can enter the command and save the running configuration immediately after loading the new image.

Table 1 LDP and TDP Support

Train and Release	LDP/TDP Support
12.0S Train	• TDP is enabled by default. • Cisco IOS Release 12.0(29)S and earlier releases: TDP is supported for LDP features. • Cisco IOS Release 12.0(30)S and later releases: TDP is not support for LDP features.

Train and Release	LDP/TDP Support
12.2S, SB, and SR Trains	• LDP is enabled by default. • Cisco IOS Release 12.2(25)S and earlier releases: TDP is supported for LDP features. • Cisco IOS Releases 12.2(27)SBA, 12.2(27)SRA, 12.2(27)SRB and later releases: TDP is not supported for LDP features.
12.T/Mainline Trains	• Cisco IOS Release 12.3(14)T and earlier releases: TDP is enabled by default. • Cisco IOS Releases 12.4 and 12.4T and later releases: LDP is enabled by default. • Cisco IOS Release 12.3(11)T and earlier releases: TDP is supported for LDP features. • Cisco IOS Release 12.3(14)T and later releases: TDP is not support ed for LDP features.

Introduction to LDP Sessions

When you enable MPLS LDP, the LSRs send out messages to try to find other LSRs with which they can create LDP sessions. The following sections explain the differences between directly connected LDP sessions and nondirectly connected LDP sessions.

Directly Connected MPLS LDP Sessions

If an LSR is one hop from its neighbor, it is directly connected to its neighbor. The LSR sends out LDP link Hello messages as User Datagram Protocol (UDP) packets to all the routers on the subnet (multicast). A neighboring LSR may respond to the link Hello message, allowing the two routers to establish an LDP session. This is called basic discovery.

To initiate an LDP session between routers, the routers determine which router will take the active role and which router will take the passive role. The router that takes the active role establishes the LDP TCP connection session and initiates the negotiation of the LDP session parameters. To determine the roles, the two routers compare their transport addresses. The router with the higher IP address takes the active role and establishes the session.

After the LDP TCP connection session is established, the LSRs negotiate the session parameters, including the method of label distribution to be used. Two methods are available:

- Downstream Unsolicited: An LSR advertises label mappings to peers without being asked to.
- Downstream on Demand: An LSR advertises label mappings to a peer only when the peer asks for them.

For information about creating LDP sessions, see the Enabling Directly Connected LDP Sessions, page 6.

Nondirectly Connected MPLS LDP Sessions

If the LSR is more than one hop from its neighbor, it is nondirectly connected to its neighbor. For these nondirectly connected neighbors, the LSR sends out a targeted Hello message as a UDP packet, but as a unicast message specifically addressed to that LSR. The nondirectly connected LSR responds to the Hello message and the two routers begin to establish an LDP session. This is called extended discovery.

An MPLS LDP targeted session is a label distribution session between routers that are not directly connected. When you create an MPLS traffic engineering tunnel interface, you need to establish a label distribution session between the tunnel headend and the tailend routers. You establish nondirectly connected MPLS LDP sessions by enabling the transmission of targeted Hello messages.

You can use the **mpls ldp neighbor targeted** command to set up a targeted session when other means of establishing targeted sessions do not apply, such as configuring **mpls ip** on a traffic engineering (TE) tunnel or configuring Any Transport over MPLS (AToM) virtual circuits (VCs). For example, you can use this command to create a targeted session between directly connected MPLS label switch routers (LSRs) when MPLS label forwarding convergence time is an issue.

The **mpls ldp neighbor targeted** command can improve label convergence time for directly connected neighbor LSRs when the link(s) directly connecting them are down. When the links between the neighbor LSRs are up, both the link and targeted Hellos maintain the LDP session. If the links between the neighbor LSRs go down, the targeted Hellos maintain the session, allowing the LSRs to retain labels learned from each other. When a link directly connecting the LSRs comes back up, the LSRs can immediately reinstall labels for forwarding use without having to reestablish their LDP session and exchange labels.

The exchange of targeted Hello messages between two nondirectly connected neighbors can occur in several ways, including the following:

- Router 1 sends targeted Hello messages carrying a response request to Router 2. Router 2 sends targeted Hello messages in response if its configuration permits. In this situation, Router 1 is considered to be active and Router 2 is considered to be passive.
- Router 1 and Router 2 both send targeted Hello messages to each other. Both routers are considered to be active. Both, one, or neither router can also be passive, if they have been configured to respond to requests for targeted Hello messages from each other.

The default behavior of an LSR is to ignore requests from other LSRs that send targeted Hello messages. You can configure an LSR to respond to requests for targeted Hello messages by issuing the **mpls ldp discovery targeted-hello accept** command.

The active LSR mandates the protocol that is used for a targeted session. The passive LSR uses the protocol of the received targeted Hello messages.

For information about creating MPLS LDP targeted sessions, see the Establishing Nondirectly Connected MPLS LDP Sessions, page 8.

Introduction to LDP Label Bindings Label Spaces and LDP Identifiers

An LDP label binding is an association between a destination prefix and a label. The label used in a label binding is allocated from a set of possible labels called a label space.

LDP supports two types of label spaces:

- Interface-specific--An interface-specific label space uses interface resources for labels. For example, label-controlled ATM (LC-ATM) interfaces use virtual path identifiers/virtual circuit identifiers (VPIs/VCIs) for labels. Depending on its configuration, an LDP platform may support zero, one, or more interface-specific label spaces.

- Platform-wide--An LDP platform supports a single platform-wide label space for use by interfaces that can share the same labels. For Cisco platforms, all interface types, except LC-ATM, use the platform-wide label space.

LDP uses a 6-byte quantity called an LDP Identifier (or LDP ID) to name label spaces. The LDP ID is made up of the following components:

- The first four bytes, called the LDP router ID, identify the LSR that owns the label space.
- The last two bytes, called the local label space ID, identify the label space within the LSR. For the platform-wide label space, the last two bytes of the LDP ID are always both 0.

The LDP ID takes the following form:

<LDP router ID> : <local label space ID>

The following are examples of LDP IDs:

- 172.16.0.0:0
- 192.168.0.0:3

The router determines the LDP router ID as follows, if the **mpls ldp router-id** command is not executed,

1. The router examines the IP addresses of all operational interfaces.
2. If these IP addresses include loopback interface addresses, the router selects the largest loopback address as the LDP router ID.
3. Otherwise, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

The normal (default) method for determining the LDP router ID may result in a router ID that is not usable in certain situations. For example, the router might select an IP address as the LDP router ID that the routing protocol cannot advertise to a neighboring router. The **mpls ldp router-id** command allows you to specify the IP address of an interface as the LDP router ID. Make sure the specified interface is operational so that its IP address can be used as the LDP router ID.

When you issue the **mpls ldp router-id** command without the **force** keyword, the router select selects the IP address of the specified interface (provided that the interface is operational) the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is configured.

When you issue the **mpls ldp router-id** command with the **force** keyword, the effect of the **mpls ldp router-id** command depends on the current state of the specified interface:

- If the interface is up (operational) and if its IP address is not currently the LDP router ID, the LDP router ID changes to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down (not operational) when the **mpls ldp router-id** *interface* **force** command is issued, when the interface transitions to up, the LDP router ID changes to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

How to Configure MPLS LDP

Enabling Directly Connected LDP Sessions

This procedure explains how to configure MPLS LDP sessions between two directly connected routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. mpls label protocol {ldp | tdp | both}
5. Router(config)# **interface** *type number*
6. **mpls ip**
7. **exit**
8. **exit**
9. **show mpls interfaces** [*interface*] [**detail**]
10. **show mpls ldp discovery** [**all** | **vrf** *vpn-name*] [**detail**]
11. **show mpls ldp neighbor** [[**vrf** *vpn-name*] [*address* | *interface*] [**detail**] | [**all**]]

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	**mpls ip** **Example:** `Router(config)# mpls ip`	Configures MPLS hop-by-hop forwarding globally. • The **mpls ip** command is enabled by default; you do not have to specify this command. • Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.

	Command or Action	Purpose
Step 4	mpls label protocol {ldp | tdp | both} **Example:** `Router(config)# mpls label protocol ldp`	Configures the use of LDP on all interfaces. LDP is the default. • 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 5	Router(config)# **interface** *type number* **Example:** `Router(config)# interface ethernet3/0`	Specifies the interface to be configured and enters interface configuration mode.
Step 6	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding on the interface. • You must enable MPLS forwarding on the interfaces as well as for the router.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 9	**show mpls interfaces** [*interface*] [**detail**] **Example:** `Router# show mpls interfaces`	Verifies that the interfaces have been configured to use LDP, TDP, or both.
Step 10	**show mpls ldp discovery** [**all** | **vrf** *vpn-name*] [**detail**] **Example:** `Router# show mpls ldp discovery`	Verifies that the interface is up and is sending Discovery Hello messages.

Command or Action	Purpose
Step 11 **show mpls ldp neighbor** [[**vrf** *vpn-name*] [*address* | *interface*] [**detail**] | [**all**]] **Example:** `Router# show mpls ldp neighbor`	Displays the status of LDP sessions.

Examples

The following **show mpls interfaces** command verifies that interfaces Ethernet 1/0 and 1/1 have been configured to use LDP:

```
Router# show mpls interfaces
Interface              IP           Tunnel   BGP Static Operational
Ethernet3/0            Yes (ldp)    No       No  No     Yes
Ethernet3/1            Yes          No       No  No     Yes
```

The following **show mpls ldp discovery** command verifies that the interface is up and is sending LDP Discovery Hello messages (as opposed to TDP Hello messages):

```
Router# show mpls ldp discovery
Local LDP Identifier:
    172.16.12.1:0
    Discovery Sources:
    Interfaces:
        Ethernet3/0 (ldp): xmit
```

The following example shows that the LDP session between routers was successfully established:

```
Router# show mpls ldp neighbor
Peer LDP Ident: 10.1.1.2:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.1.1.2.18 - 10.1.1.1.66
State: Oper; Msgs sent/rcvd: 12/11; Downstream
Up time: 00:00:10
LDP discovery sources:
FastEthernet1/0, Src IP addr: 10.20.10.2
Addresses bound to peer LDP Ident:
10.1.1.2    10.20.20.1    10.20.10.2
```

For examples on configuring directly connected LDP sessions, see the Configuring Directly Connected MPLS LDP Sessions Example, page 21.

Establishing Nondirectly Connected MPLS LDP Sessions

This section explains how to configure nondirectly connected MPLS LDP sessions, which enable you to establish an LDP session between routers that are not directly connected.

- MPLS requires CEF.
- You must configure the routers at both ends of the tunnel to be active or enable one router to be passive with the **mpls ldp discovery targeted-hello accept** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol** {**ldp** | **tdp** | **both**}
5. **interface** *tunnelnumber*
6. **tunnel destination** *ip-address*
7. **mpls ip**
8. **exit**
9. **exit**
10. **show mpls ldp discovery** [**all** | **vrf** *vpn-name*] [**detail**]

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	**mpls ip** **Example:** `Router(config)# mpls ip`	Configures MPLS hop-by-hop forwarding globally. • The **mpls ip** command is enabled by default; you do not have to specify this command. • Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.
Step 4	**mpls label protocol** {**ldp**	**tdp**	**both**} **Example:** `Router(config)#  mpls label protocol ldp`	Configures the use of LDP on all interfaces. LDP is the default. • 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.

	Command or Action	Purpose
Step 5	**interface** *tunnelnumber* **Example:** `Router(config)# interface tunnel1`	Configures a tunnel interface and enters interface configuration mode.
Step 6	**tunnel destination** *ip-address* **Example:** `Router(config-if)# tunnel destination 172.16.1.1`	Assigns an IP address to the tunnel interface.
Step 7	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding on the interface. • You must enable MPLS forwarding on the interfaces as well as for the router.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 9	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 10	**show mpls ldp discovery** [**all** | **vrf** *vpn-name*] [**detail**] **Example:** `Router# show mpls ldp discovery`	Verifies that the interface is up and is sending Discovery Hello messages.

Example

The following example shows the output of the **show mpls ldp discovery** command for a nondirectly connected LDP session.

```
Router# show mpls ldp discovery
Local LDP Identifier:
          172.16.0.0:0
Discovery Sources:
Interfaces:
POS2/0 (ldp): xmit/recv
LDP Id: 172.31.255.255:0
```

```
Tunnel1 (ldp): Targeted -> 192.168.255.255
Targeted Hellos:
172.16.0.0 -> 192.168.255.255 (ldp): active, xmit/recv
LDP Id: 192.168.255.255:0
172.16.0.0 -> 192.168.0.0 (tdp): passive, xmit/recv
TDP Id: 192.168.0.0:0
```

This command output indicates that:

- The local LSR (172.16.0.0) sent LDP link Hello messages on interface POS2/0 and discovered neighbor 172.31.255.255.
- The local LSR sent LDP targeted Hello messages associated with interface Tunnel1 to target 192.168.255.255. The LSR was configured to use LDP.
- The local LSR is active for targeted discovery activity with 192.168.255.255; this means that the targeted Hello messages it sends to 192.168.255.255 carry a response request. The local LSR was configured to have an LDP session with the nondirectly connected LSR 192.168.255.255.
- The local LSR is not passive from the discovery activity with 192.168.255.255 for one of the following reasons:
  - The targeted Hello messages it receives from 192.168.255.255 do not carry a response request.
  - The local LSR has not been configured to respond to such requests.
- The local LSR sent TDP directed Hello messages to the target LSR 192.168.0.0. This LSR uses TDP because the Hello messages received from the target LSR 192.168.0.0 were TDP directed Hello messages.
- The local LSR is passive in discovery activity with LSR 192.168.0.0. This means that the directed Hello messages it receives from LSR 192.168.0.0 carry a response request and that the local LSR has been configured with the **mpls ldp discovery targeted-hello accept** command to respond to such requests from LSR 192.168.0.0.
- The local LSR is not active in discovery activity with LSR 192.168.0.0, because no application that requires an LDP session with LSR 192.168.0.0 has been configured on the local LSR.

For examples of configuring LDP targeted sessions, see the Establishing Nondirectly Connected MPLS LDP Sessions Example, page 23.

Saving Configurations MPLS Tag Switching Commands

In releases of Cisco IOS software prior to 12.4(2)T, some MPLS commands had both a tag-switching version and an MPLS version. For example, the two commands **tag-switching ip** and **mpls ip** were the same. To support backward compatibility, the tag-switching form of the command was written to the saved configuration.

Starting in Cisco IOS Release 12.4(2)T, the MPLS form of the command is written to the saved configuration.

For example, if an ATM interface is configured using the following commands, which have both a tag-switching form and an MPLS form:

```
Router(config)# interface ATM3/0
Router(config-if)# ip unnumbered Loopback0
router(config-if)# tag-switching ip
Router(config-if)# mpls label protocol ldp
```

After you enter these commands and save this configuration or display the running configuration with the **show running-config** command, the commands saved or displayed appear as follows:

```
interface ATM3/0
ip unnumbered Loopback0
```

```
mpls ip
mpls label protocol ldp
```

Specifying the LDP Router ID

The **mpls ldp router-id** command allows you to establish the IP address of an interface as the LDP router ID.

The following steps describe the normal process for determining the LDP router ID:

1. The router considers all the IP addresses of all operational interfaces.
2. If these addresses include loopback interface addresses, the router selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the router, because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each router is not required.

The loopback IP address does not become the router ID of the local LDP ID under the following circumstances:

- ◦ If the loopback interface has been explicitly shut down.
  ◦ If the **mpls ldp router-id** command specifies that a different interface should be used as the LDP router ID.

If you use a loopback interface, make sure that the IP address for the loopback interface is configured with a /32 network mask. In addition, make sure that the routing protocol in use is configured to advertise the corresponding /32 network.

1. Otherwise, the router selects the largest interface address.

The router might select a router ID that is not usable in certain situations. For example, the router might select an IP address that the routing protocol cannot advertise to a neighboring router.

The router implements the router ID the next time it is necessary to select an LDP router ID. The effect of the command is delayed until the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is deconfigured.

If you use the **force** keyword with the **mpls ldp router-id** command, the router ID takes effect more quickly. However, implementing the router ID depends on the current state of the specified interface:

- If the interface is up (operational) and its IP address is not currently the LDP router ID, the LDP router ID is forcibly changed to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down, the LDP router ID is forcibly changed to the IP address of the interface when the interface transitions to up. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

Make sure the specified interface is operational before assigning it as the LDP router ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol** {**ldp** | **tdp** | **both**}
5. **mpls ldp router-id** *interface* [**force**]
6. **exit**
7. **show mpls ldp discovery** [**all** | **detail** | **vrf** *vpn-name*]

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	**mpls ip** **Example:** `Router(config)# mpls ip`	Configures MPLS hop-by-hop forwarding globally. • The **mpls ip** command is enabled by default; you do not have to specify this command. • Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.
Step 4	**mpls label protocol** {**ldp**	**tdp**	**both**} **Example:** `Router(config)# mpls label protocol ldp`	Configures the use of LDP on all interfaces. LDP is the default. • 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 5	**mpls ldp router-id** *interface* [**force**] **Example:** `Router(config)# mpls ldp router-id pos2/0/0`	Specifies the preferred interface for determining the LDP router ID.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 7	**show mpls ldp discovery** [**all** | **detail** | **vrf** *vpn-name*] **Example:** `Router# show mpls ldp discovery`	Displays the LDP identifier for the local router.

Example

The following example assigns interface pos2/0/0 as the LDP router ID:

```
Router> enable
Router# configure terminal
Router(config)# mpls ip
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp router-id pos2/0/0 force
```

The following example displays the LDP router ID (10.15.15.15):

```
Router# show mpls ldp discovery
Local LDP Identifier:
    10.15.15.15:0
Discovery Sources:
    Interfaces:
        Ethernet4 (ldp): xmit/recv
            LDP Id: 10.14.14.14:0
```

Preserving QoS Settings with MPLS LDP Explicit Null

Normally, LDP advertises an Implicit Null label for directly connected routes. The Implicit Null label causes the second last (penultimate) label switched router (LSR) to remove the MPLS header from the packet. In this case, the penultimate LSR and the last LSR do not have access to the quality of service (QoS) values that the packet carried before the MPLS header was removed. To preserve the QoS values, you can configure the LSR to advertise an explicit NULL label (a label value of zero). The LSR at the penultimate hop forwards MPLS packets with a NULL label instead of forwarding IP packets.

Note An explicit NULL label is not needed when the penultimate hop receives MPLS packets with a label stack that contains at least two labels and penultimate hop popping is performed. In that case, the inner label can still carry the QoS value needed by the penultimate and edge LSR to implement their QoS policy.

When you issue the **mpls ldp explicit-null** command, Explicit Null is advertised in place of Implicit Null for directly connected prefixes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol** {**ldp** | **tdp** | **both**}
5. **interface** *type number*
6. **mpls ip**
7. **exit**
8. **mpls ldp explicit-null** [**for** *prefix-acl* | **to** *peer-acl* | **for** *prefix-acl* **to** *peer-acl*]
9. **exit**
10. **show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label*[-*label*] | **interface** *interface* | *next-hop address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vpn-name*] [**detail**]

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	**mpls ip** **Example:** `Router(config)# mpls ip`	Configures MPLS hop-by-hop forwarding globally. • The **mpls ip** command is enabled by default; you do not have to specify this command. • Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.
Step 4	**mpls label protocol** {**ldp**	**tdp**	**both**} **Example:** `Router(config)# mpls label protocol ldp`	Configures the use of LDP on all interfaces. LDP is the default. • 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.

	Command or Action	Purpose
Step 5	**interface** *type number* **Example:** `Router(config)# interface atm2/0`	Specifies the interface to be configured and enters interface configuration mode.
Step 6	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding on the interface. • You must enable MPLS forwarding on the interfaces as well as for the router.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 8	**mpls ldp explicit-null** [**for** *prefix-acl* | **to** *peer-acl* | **for** *prefix-acl* **to** *peer-acl*] **Example:** `Router(config)# mpls ldp explicit-null`	Advertises an Explicit Null label in situations where it would normally advertise an Implicit Null label.
Step 9	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enter privileged EXEC mode.
Step 10	**show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label*[-*label*] | **interface** *interface* | *next-hop address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vpn-name*] [**detail**] **Example:** `Router# show mpls forwarding-table`	Verifies that MPLS packets are forwarded with an explicit-null label (value of 0).

Examples

Enabling explicit-null on an egress LSR causes that LSR to advertise the explicit-null label to all adjacent MPLS routers.

```
Router# configure terminal
Router(config)# mpls ldp explicit-null
```

If you issue the **show mpls forwarding-table** command on an adjacent router, the output shows that MPLS packets are forwarded with an explicit-null label (value of 0). In the following example, the second column shows that entries have outgoing labels of 0, where once they were marked “Pop label”.

```
Router# show mpls forwarding-table
Local  Outgoing    Prefix           Bytes label Outgoing   Next Hop
label  label or VC or Tunnel Id     switched   interface
19     Pop tag     10.12.12.12/32   0          Fa2/1/0    172.16.0.1
22     0           10.14.14.14/32   0          Fa2/0/0    192.168.0.2
23     0           172.24.24.24/32  0          Fa2/0/0    192.168.0.2
24     0           192.168.0.0/8    0          Fa2/0/0    192.168.0.2
25     0           10.15.15.15/32   0          Fa2/0/0    192.168.0.2
26     0           172.16.0.0/8     0          Fa2/0/0    192.168.0.2
27     25          10.16.16.16/32   0          Fa2/0/0    192.168.0.22
28     0           10.34.34.34/32   0          Fa2/0/0    192.168.0.2
```

Enabling explicit-null and specifying the **for** keyword with a standard access control list (ACL) changes all adjacent MPLS routers' tables to swap an explicit-null label for only those entries specified in the access-list. In the following example, an access-list is created that contains the 10.24.24.24/32 entry. Explicit null is configured and the access list is specified.

```
Router# configure terminal
Router(config)# mpls label protocol ldp
Router(config)# access-list 24 permit host 10.24.24.24
Router(config)# mpls ldp explicit-null for 24
```

If you issue the **show mpls forwarding-table** command on an adjacent router, the output shows that the only the outgoing labels for the addresses specified (172.24.24.24/32) change from Pop label to 0. All other Pop label outgoing labels remain the same.

```
Router# show mpls forwarding-table
Local  Outgoing    Prefix           Bytes label Outgoing   Next Hop
label  label or VC or Tunnel Id     switched   interface
19     Pop tag     10.12.12.12/32   0          Fa2/1/0    172.16.0.1
22     0           10.14.14.14/32   0          Fa2/0/0    192.168.0.2
23     0           172.24.24.24/32  0          Fa2/0/0    192.168.0.2
24     0           192.168.0.0/8    0          Fa2/0/0    192.168.0.2
25     0           10.15.15.15/32   0          Fa2/0/0    192.168.0.2
26     0           172.16.0.0/8     0          Fa2/0/0    192.168.0.2
27     25          10.16.16.16/32   0          Fa2/0/0    192.168.0.22
28     0           10.34.34.34/32   0          Fa2/0/0    192.168.0.2
```

Enabling explicit null and adding the **to** keyword and an access list enables you to advertise explicit-null labels to only those adjacent routers specified in the access-list.To advertise explicit-null to a particular router, you must specify the router's LDP ID in the access-list.

In the following example, an access-list contains the 10.15.15.15/32 entry, which is the LDP ID of an adjacent MPLS router. The router that is configured with explicit null advertises explicit-null labels only to that adjacent router.

```
Router# show mpls ldp discovery
Local LDP Identifier:
    10.15.15.15:0
Discovery Sources:
    Interfaces:
        Ethernet4 (ldp): xmit/recv
            TDP Id: 10.14.14.14:0
Router# configure terminal
Router(config)# mpls label protocol ldp
Router(config)# access-list 15 permit host 10.15.15.15
Router(config)# mpls ldp explicit-null to 15
```

If you issue the **show mpls forwarding-table** command, the output shows that explicit null labels are going only to the router specified in the access list.

```
Router# show mpls forwarding-table
```

```
Local  Outgoing    Prefix           Bytes label Outgoing   Next Hop
label  label or VC or Tunnel Id     switched   interface
19     Pop tag     10.12.12.12/32   0          Fa2/1/0    172.16.0.1
22     0           10.14.14.14/32   0          Fa2/0/0    192.168.0.2
23     0           172.24.24.24/32  0          Fa2/0/0    192.168.0.2
24     0           192.168.0.0/8    0          Fa2/0/0    192.168.0.2
25     0           10.15.15.15/32   0          Fa2/0/0    192.168.0.2
26     0           172.16.0.0/8     0          Fa2/0/0    192.168.0.2
27     25          10.16.16.16/32   0          Fa2/0/0    192.168.0.22
28     0           10.34.34.34/32   0          Fa2/0/0    192.168.0.2
```

Enabling explicit-null with both the **for** and **to** keywords enables you to specify which routes to advertise with explicit-null labels and to which adjacent routers to advertise these explicit-null labels.

```
Router# show access 15
Standard IP access list 15
     permit 10.15.15.15 (7 matches)
Router# show access 24
Standard IP access list 24
     permit 10.24.24.24 (11 matches)
Router# configure terminal
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp explicit-null for 24 to 15
```

If you issue the **show mpls forwarding-table** command on the router called 47K-60-4, the output shows that it receives explicit null labels for 10.24.24.24/32.

```
Router# show mpls forwarding-table
Local  Outgoing    Prefix           Bytes label Outgoing   Next Hop
label  label or VC or Tunnel Id     switched   interface
17     0  <---     10.24.24.24/32    0          Et4        172.16.0.1
20     Pop tag     172.16.0.0/8     0          Et4       172.16.0.1
21     20          10.12.12.12/32    0          Et4        172.16.0.1
22     16          10.0.0.0/8        0          Et4        172.16.0.1
23     21          10.13.13.13/32    0          Et4        172.16.0.1
25     Pop tag     10.14.14.14/32    0          Et4        172.16.0.1
27     Pop tag     192.168.0.0/8     0          Et4        172.16.0.1
28     25          10.16.16.16/32    0          Et4        172.16.0.1
29     Pop tag     192.168.34.34/32   0         Et4        172.16.0.1
```

Protecting Data Between LDP Peers with MD5 Authentication

You can enable authentication between two LDP peers, which verifies each segment sent on the TCP connection between the peers. You must configure authentication on both LDP peers using the same password; otherwise, the peer session is not established.

Authentication uses the Message Digest 5 (MD5) algorithm to verify the integrity of the communication and authenticate the origin of the message.

To enable authentication, issue the **mpls ldp neighbor** command with the **password** keyword. This causes the router to generate an MD5 digest for every segment sent on the TCP connection and check the MD5 digest for every segment received from the TCP connection.

When you configure a password for an LDP neighbor, the router tears down existing LDP sessions and establishes new sessions with the neighbor.

If a router has a password configured for a neighbor, but the neighboring router does not have a password configured, a message such as the following appears on the console who has a password configured while the two routers attempt to establish an LDP session. The LDP session is not established.

%TCP-6-BADAUTH: No MD5 digest from [peer's IP address](11003) to [local router's IP address](646)

Similarly, if the two routers have different passwords configured, a message such as the following appears on the console. The LDP session is not established.

%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address](11004) to [local router's IP address] (646)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol** {**ldp** | **tdp** | **both**}
5. **mpls ldp neighbor** [**vrf** *vpn-name*] *ip-address* [**password** [**0**-**7**] *password-string*]
6. **exit**
7. **show mpls ldp neighbor** [[**vrf** *vpn-name*] [*address* | *interface*] [**detail** | [**all**]]

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	**mpls ip** **Example:** `Router(config)# mpls ip`	Configures MPLS hop-by-hop forwarding globally. • The **mpls ip** command is enabled by default; you do not have to specify this command. • Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.
Step 4	**mpls label protocol** {**ldp**	**tdp**	**both**} **Example:** `Router(config)# mpls label protocol ldp`	Configures the use of LDP on all interfaces. LDP is the default. • 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.

	Command or Action	Purpose
Step 5	**mpls ldp neighbor** [**vrf** *vpn-name*] *ip-address* [**password** [**0**-**7**] *password-string*] **Example:** `Router(config)# mpls ldp neighbor 172.27.0.15 password onethirty9`	Specifies authentication between two LDP peers.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 7	**show mpls ldp neighbor** [[**vrf** *vpn-name*] [*address* | *interface*] [**detail** | [**all**]] **Example:** `Router# show mpls ldp neighbor detail`	Displays the status of LDP sessions. If the passwords have been set on both LDP peers and the passwords match, the **show mpls ldp neighbor** command displays that the LDP session was successfully established.

Examples

The following example configures a router with the password cisco:

```
Router> enable
Router# configure terminal
Router(config)# mpls ip
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp neighbor 10.1.1.1 password cisco
Router(config)# exit
```

The following example shows that the LDP session between routers was successfully established:

```
Router# show mpls ldp neighbor
Peer LDP Ident: 10.1.1.2:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.1.1.2.11118 - 10.1.1.1.646
State: Oper; Msgs sent/rcvd: 12/11; Downstream
Up time: 00:00:10
LDP discovery sources:
FastEthernet1/0, Src IP addr: 10.20.10.2
Addresses bound to peer LDP Ident:
10.1.1.2    10.20.20.1    10.20.10.2
```

The following **show mpls ldp neighbor detail** command shows that MD5 (shown in bold) is used for the LDP session.

```
Router# show mpls ldp neighbor 10.0.0.21 detail
    Peer LDP Ident: 10.0.0.21:0; Local LDP Ident 10.0.0.22:0
        TCP connection: 10.0.0.21.646 - 10.0.0.22.14709; MD5 on
        State: Oper; Msgs sent/rcvd: 1020/1019; Downstream; Last TIB rev sent 2034
        Up time: 00:00:39; UID: 3; Peer Id 1;
        LDP discovery sources:
          FastEthernet1/1; Src IP addr: 172.16.1.1
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          10.0.0.21       10.0.38.28       10.88.88.2      172.16.0.1
```

```
  172.16.1.1
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

MPLS LDP Configuration Examples

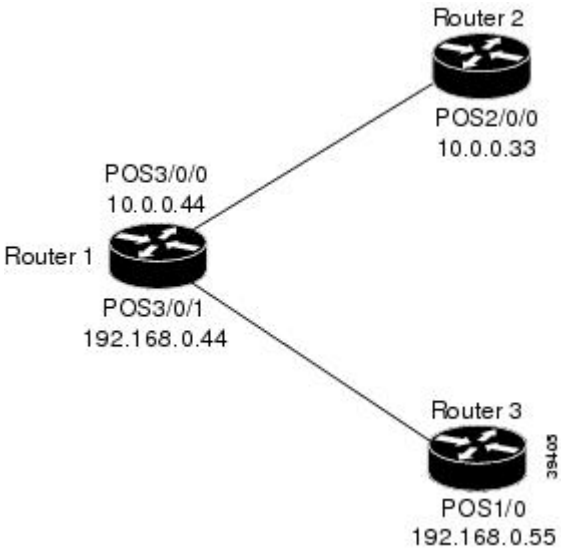
Configuring Directly Connected MPLS LDP Sessions Example

The figure below shows a sample network for configuring directly connected LDP sessions.

This example configures the following:

- MPLS hop-by-hop forwarding for the POS links between Router 1 and Router 2 and between Router 1 and Router 3.
- LDP for label distribution between Router 1 and Router 2.
- TDP for label distribution between Router 1 and Router 3.
- A loopback interface and IP address for each LSR that can be used as the LDP router ID.

Figure 1 Configuration of MPLS LDP



Note The configuration examples below show only the commands related to configuring LDP for Router 1, Router 2, and Router 3 in the sample network shown in the figure above.

Router 1 Configuration

```
ip cef distributed                                  !Assumes R1 supports distributed CEF
interface Loopback0                                 !Loopback interface for LDP ID.
ip address 172.16.0.11 255.255.255.255
!
interface POS3/0/0
ip address 10.0.0.44 255.0.0.0
mpls ip                                              !Enable hop-by-hop MPLS forwarding
```

```
mpls label protocol ldp                          !Use LDP for this interface
!
interface POS3/0/1
ip address 192.168.0.44 255.0.0.0
mpls ip                                          !Enable hop-by-hop MPLS forwarding
mpls label protocol tdp                          !Use TDP for this interface
```

Router 2 Configuration

```
ip cef distributed                               !Assumes R2 supports distributed CEF
!
interface Loopback0                              !Loopback interface for LDP ID.
ip address 172.16.0.22 255.255.255.255
!
interface POS2/0/0
ip address 10.0.0.33 255.0.0.0
mpls ip                                          !Enable hop-by-hop MPLS forwarding
mpls label protocol ldp                          !Use LDP for this interface
```

Router 3 Configuration

```
ip cef                                            !Assumes R3 does not support dCEF
!
interface Loopback0                               !Loopback interface for LDP ID.
ip address 172.16.0.33 255.255.255.255
!
interface POS1/0
ip address 192.168.0.55 255.0.0.0
mpls ip                                           !Enable hop-by-hop MPLS forwarding
mpls label protocol tdp                           !Use tDP for this interface
```

The LDP configuration for Router 1 uses the **mpls label protocol ldp** command in interface configuration mode, because some of its interfaces use LDP and some use TDP. Another way to configure Router 1 is to use the **mpls label protocol ldp** command in global configuration mode to configure LDP as the default protocol for interfaces and use the **mpls label protocol tdp** command in interface configuration mode to configure TDP for the POS3/0/1 link to Router 3. This alternative way to configure Router 1 is shown below:

Router 1 Configuration

```
ip cef distributed                                  !Assumes R1 supports dCEF
mpls label protocol ldp                             !Use LDP for the default protocol
!
interface Loopback0                                 !Loopback interface for LDP ID.
ip address 172.16.0.11 255.255.255.255
interface POS3/0/0
ip address 10.0.0.44 255.0.0.0
mpls ip                                             !Enable hop-by-hop MPLS forwarding
                                                    !Use LDP (configured i/f default)
interface POS3/0/1
ip address 192.168.0.44 255.0.0.0
mpls ip                                             !Enable hop-by-hop MPLS forwarding
mpls label protocol tdp                             !Use TDP for this interface
```

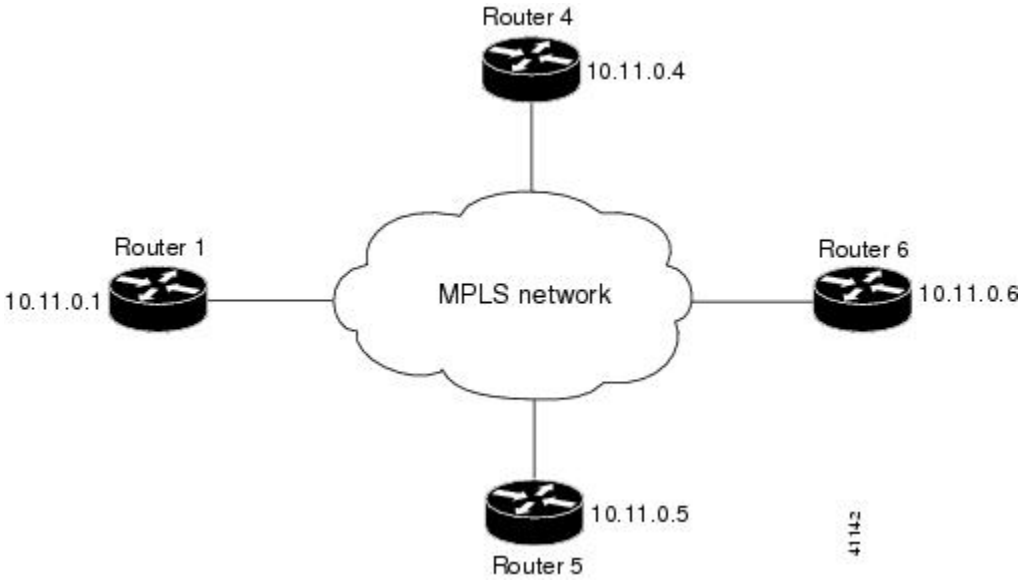
The configuration of Router 2 also uses the **mpls label protocol ldp** command in interface configuration mode. To specify LDP for all interfaces, use the **mpls label protocol ldp** command in global configuration mode without any interface **mpls label protocol** commands.

Configuring the **mpls ip** command on an interface triggers the transmission of discovery Hello messages for the interface.

Establishing Nondirectly Connected MPLS LDP Sessions Example

The following examples illustrate the configuration of platforms for MPLS LDP nondirectly connected sessions using the sample network shown in the figure below. Note that Routers 1, 4, 5, and 6 in this sample network are not directly connected to each other.

Figure 2 Sample Network for Configuring LDP for Targeted Sessions



The configuration example shows the following:

- Targeted sessions between Routers 1 and 4 use LDP. Routers 1 and 4 are both active.
- Targeted sessions between Routers 1 and 6 use LDP. Router 1 is active and Router 6 is passive.
- Targeted sessions between Routers 1 and 5 use TDP. Router 5 is active.

These examples assume that the active ends of the nondirectly connected sessions are associated with tunnel interfaces, such as MPLS traffic engineering tunnels. They show only the commands related to configuring LDP targeted sessions. The examples do not show configuration of the applications that initiate the targeted sessions.

Router 1 Configuration

Tunnel interfaces Tunnel14 and Tunnel16 specify LDP for targeted sessions associated with these interfaces. The targeted session for Router 5 requires TDP. The **mpls label protocol ldp** command in global configuration mode makes it unnecessary to explicitly specify LDP as part of the configuration from the Tunnel14 and Tunnel16.

```
ip cef distributed             !Router1 supports distributed CEF
mpls label protocol ldp       !Use LDP as default for all interfaces
interface Loopback0            !Loopback interface for LDP ID.
ip address 10.25.0.11 255.255.255.255
interface Tunnel14             !Tunnel to Router 4 requiring label distribution
tunnel destination 10.11.0.4  !Tunnel endpoint is Router 4
mpls ip                        !Enable hop-by-hop forwarding on the interface
interface Tunnel15             !Tunnel to Router 5 requiring label distribution
tunnel destination 10.11.0.5  !Tunnel endpoint is Router 5
mpls label protocol tdp        !Use TDP for session with Router 5
```

```
mpls ip                          !Enable hop-by-hop forwarding on the interface
interface Tunnel16               !Tunnel to Router 6 requiring label distribution
tunnel destination 10.11.0.6  !Tunnel endpoint is Router 6
mpls ip                          !Enable hop-by-hop forwarding on the interface
```

Router 4 Configuration

The **mpls label protocol ldp** command in global configuration mode makes it unnecessary to explicitly specify LDP as part of the configuration for the Tunnel41 targeted session with Router 1.

```
ip cef distributed           !Router 4 supports distributed CEF
mpls label protocol ldp       !Use LDP as default for all interfaces
interface Loopback0           !Loopback interface for LDP ID.
ip address 10.25.0.44 255.255.255.255
interface Tunnel41            !Tunnel to Router 1 requiring label distribution
tunnel destination 10.11.0.1 !Tunnel endpoint is Router 1
mpls ip                       !Enable hop-by-hop forwarding on the interface
```

Router 5 Configuration

Router 5 must use TDP for all targeted sessions. Therefore, its configuration includes the **mpls label protocol ldp** command.

```
ip cef                       !Router 5 supports CEF
mpls label protocol tdp       !Use TDP as default for all interfaces
interface Loopback0          !Loopback interface for LDP ID.
ip address 10.25.0.55 255.255.255.255
interface Tunnel51             !Tunnel to Router 1 requiring label distribution
tunnel destination 10.11.0.1  !Tunnel endpoint is Router 1
mpls ip                       !Enable hop-by-hop forwarding on the interface
```

Router 6 Configuration

By default, a router cannot be a passive neighbor in targeted sessions. Therefore, Router 1, Router 4, and Router 5 are active neighbors in any targeted sessions. The **mpls ldp discovery targeted-hello accept** command permits Router 6 to be a passive target in targeted sessions with Router 1. Router 6 can also be an active neighbor in targeted sessions, although the example does not include such a configuration.

```
ip cef distributed                       !Router 6 supports distributed CEF
interface Loopback0                      !Loopback interface for LDP ID.
ip address 10.25.0.66 255.255.255.255
mpls ldp discovery targeted-hellos accept from LDP_SOURCES
                                         !Respond to requests for targeted hellos
                                         !from sources permitted by acl LDP_SOURCES
ip access-list standard LDP_SOURCES      !Define acl for targeted hello sources.
permit 10.11.0.1                        !Accept targeted hello request from Router 1.
deny any                                 !Deny requests from other sources.
```

Additional References

Related Documents

Related Topic	Document Title
Configures LDP on every interface associated with a specified IGP instance.	MPLS LDP Autoconfiguration

Related Topic	Document Title
Ensures that LDP is fully established before the IGP path is used for switching.	MPLS LDP-IGP Synchronization
Allows ACLs to control the label bindings that an LSR accepts from its peer LSRs.	MPLS LDP Inbound Label Binding Filtering
Enables standard, SNMP-based network management of the label switching features in Cisco IOS.	MPLS Label Distribution Protocol MIB Version 8 Upgrade

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• MPLS Label Distribution Protocol MIB (draft-ietf-mpls-ldp-mib-08.txt) • SNMP-VACM-MIB The View-based Access Control Model (ACM) MIB for SNMP	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

RFC	Title
RFC 3036	*LDP Specification*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for MPLS Label Distribution Protocol

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 2 Feature Information for MPLS Label Distribution Protocol Overview

Feature Name	Releases	Feature Information
MPLS Label Distribution Protocol	12.0(10)ST 12.0(14)ST 12.1(2)T 12.1(8a)E 12.2(2)T 12.2(4)T 12.2(8)T 12.0(21)ST 12.0(22)S 12.0(23)S 12.2(13)T 12.4(3) 12.4(5)	This feature was introduced in Cisco IOS Release 12.0(10)ST, incorporating a new set of Multiprotocol Label Switching (MPLS) CLI commands implemented for use with Cisco routers and switches. The CLI commands in this release reflected MPLS command syntax and terminology, thus facilitating the orderly transition from a network using the Tag Distribution Protocol (TDP) to one using the Label Distribution Protocol (LDP). In Cisco IOS Release 12.0(14)ST, several new MPLS CLI commands were introduced, support for MPLS VPNs was added by means of a new **vrf** *vpn-name* parameter in certain existing commands, and other commands were modified to ensure consistent interpretation of associated *prefix-access-list* arguments by Cisco IOS software. In Cisco IOS 12.1(2)T, this feature was integrated into this release. Also, the **debug mpls atm-ldp api**, **debug mpls atm-ldp routes**, and **debug mpls atm-ldp states** commandswere modified. This feature was integrated into Cisco IOS Release 12.1(8a)E. This feature was integrated into Cisco IOS Release 12.2(2)T. The following commands were introduced or modified by this feature: **mpls label protocol** (global configuration), **mpls ldp router-id**

Feature Name	Releases	Feature Information
		In Cisco IOS Release 12.2(4)T, support was added for Cisco MGX 8850 and MGX 8950 switches equipped with a Cisco MGX RPM-PR card, and the VPI range in the **show mpls atm-ldp bindings** and **show mpls ip binding** commands was changed to 4095. In Cisco IOS Release 12.2(8)T, the **debug mpls atm-ldp failure** command was introduced. In Cisco IOS Release 12.0(21)ST, the **mpls ldp neighbor implicit-withdraw** command was introduced. This feature was integrated into Cisco IOS Release 12.0(22)S. The **mpls ldp neighbor targeted-session** command and the **interface** keyword for the **mpls ldp advertise-labels** command were added. This feature was integrated into Cisco IOS Release 12.0(23)S. Default values for the **mpls ldp discovery** command **holdtime** and **interval** keywords were changed. This feature was integrated into Cisco IOS Release 12.2(13)T. In Cisco IOS Release 12.4(3), the default MPLS label distribution protocol changed from TDP to LDP. See LDP and TDP Support, page 2 for more information. If no protocol is explicitly configured by the **mpls label protocol** command, LDP is the default label distribution protocol. See the **mpls label protocol** (global configuration) command for more information. Also in Cisco IOS Release 12.4(3), LDP configuration commands are saved by using the MPLS form of the command

Feature Name	Releases	Feature Information
		rather than the tag-switching form. Previously, commands were saved by using the tag-switching form of the command, for backward compatibility. See the Saving Configurations MPLS Tag Switching Commands, page 11 for more information. In Cisco IOS Release 12.4(5), the **vrf** *vrf-name* keyword/argument pair was added for the **mpls ldp router-id** command to allow you to associate the LDP router ID with a nondefault VRF.

MPLS LDP Session Protection

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

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

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 32

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**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.

How to Configure MPLS LDP Session Protection

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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
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.
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.

	Command or Action	Purpose
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.

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/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.

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

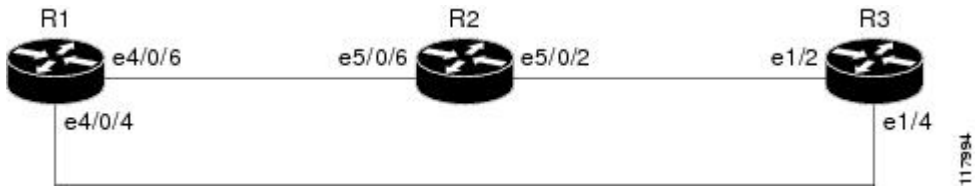
Use the **clear mpls ldp neighbor** command if you need to terminate an LDP session after a link goes down. This is useful for situations where the link needs to be taken out of service or needs to be connected to a different neighbor.

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 3 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**

MPLS LDP Inbound Label Binding Filtering

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) supports inbound label binding filtering. You can use the MPLS LDP Inbound Label Binding Filtering feature to configure access control lists (ACLs) for controlling the label bindings a label switch router (LSR) accepts from its peer LSRs.

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

Inbound label binding filtering does not support extended ACLs; it only supports standard ACLs.

Information about MPLS LDP Inbound Label Binding Filtering

The MPLS LDP Inbound Label Binding Filtering feature may be used to control the amount of memory used to store LDP label bindings advertised by other routers. For example, in a simple MPLS Virtual Private Network (VPN) environment, the VPN provider edge (PE) routers may require LSPs only to their peer PE routers (that is, they do not need LSPs to core routers). Inbound label binding filtering enables a PE router to accept labels only from other PE routers.

How to Configure MPLS LDP Inbound Label Binding Filtering

Configuring MPLS LDP Inbound Label Binding Filtering

Perform this task to configure a router for inbound label filtering. The following configuration allows the router to accept only the label for prefix 25.0.0.2 from LDP neighbor router 10.12.12.12.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list standard** *access-list-number*
4. **permit** {*source* [*source-wildcard*] | **any**} [**log**]
5. **exit**
6. **mpls ldp neighbor** [**vrf** *vpn-name*] *nbr-address* **labels accept** *acl*
7. **end**

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 access-list standard** *access-list-number* **Example:** `Router(config)# ip access-list standard 1`	Defines a standard IP access list with a number.

	Command or Action	Purpose
Step 4	**permit** {*source* [*source-wildcard*] | **any**} [**log**] **Example:** `Router(config-std-nacl)# permit 10.0.0.0`	Specifies one or more prefixes permitted by the access list.
Step 5	**exit** **Example:** `Router(config-std-nacl)# exit`	Exits the current mode and goes to the next higher level.
Step 6	**mpls ldp neighbor** [**vrf** *vpn-name*] *nbr-address* **labels accept** *acl* **Example:** `Router(config)# mpls ldp neighbor 10.12.12.12 labels accept 1`	Specifies the ACL to be used to filter label bindings for the specified LDP neighbor.
Step 7	**end** **Example:** `Router(config)# end`	Exits the current mode and enters privileged Exec mode.

Verifying that MPLS LDP Inbound Label Bindings are Filtered

If inbound filtering is enabled, perform the following steps to verify that inbound label bindings are filtered:

SUMMARY STEPS

1. Enter the **show mpls ldp neighbor** command to show the status of the LDP session, including the name or number of the ACL configured for inbound filtering.
2. Enter the **show ip acess-list** command to display the contents of all current IP access lists or of a specified access list.
3. Enter the **show mpls ldp bindings** command to verify that the LSR has remote bindings only from a specified peer for prefixes permitted by the access list.

DETAILED STEPS

Step 1 Enter the **show mpls ldp neighbor** command to show the status of the LDP session, including the name or number of the ACL configured for inbound filtering.

Example:

```
show mpls ldp neighbor
 [vrf

vpn-name
][
address
 |
interface
] [detail
```

Note To display information about inbound label binding filtering, you must enter the **detail** keyword.

Following is sample output from the **show mpls ldp neighbor** command.

Example:

```
Router# show mpls ldp neighbor 10.12.12.12 detail
 Peer LDP Ident: 10.12.12.12:0; Local LDP Ident 10.13.13.13:0
   TCP connection: 10.12.12.12.646 - 10.13.13.13.12592
   State: Oper; Msgs sent/rcvd: 49/45; Downstream; Last TIB rev sent 1257
   Up time: 00:32:41; UID: 1015; Peer Id 0;
   LDP discovery sources:
    Serial1/0; Src IP addr: 25.0.0.2
     holdtime: 15000 ms, hello interval: 5000 ms
   Addresses bound to peer LDP Ident:
    10.0.0.129       10.12.12.12     10.0.0.2
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
   LDP inbound filtering accept acl: 1
```

Step 2 Enter the **show ip acess-list** command to display the contents of all current IP access lists or of a specified access list.

Example:

```
show ip access-list
 [
access-list-number
 |
access-list-name
]
```

Note It is important that you enter this command to see how the access list is defined; otherwise, you cannot verify inbound label binding filtering.

The following command output shows the contents of IP access list 1:

Example:

```
Router# show ip access 1
Standard IP access list 1
  permit 10.0.0.0, wildcard bits 0.0.0.255 (1 match)
```

Step 3 Enter the **show mpls ldp bindings** command to verify that the LSR has remote bindings only from a specified peer for prefixes permitted by the access list.

Example:

```
Router# show mpls ldp bindings
 tib entry: 10.0.0.0/8, rev 4
     local binding:  tag: imp-null
```

```
 tib entry: 10.2.0.0/16, rev 1137
     local binding:  tag: 16
 tib entry: 10.2.0.0/16, rev 1139
     local binding:  tag: 17
 tib entry: 10.12.12.12/32, rev 1257
     local binding:  tag: 18
 tib entry: 10.13.13.13/32, rev 14
     local binding:  tag: imp-null
 tib entry: 10.10.0.0/16, rev 711
     local binding:  tag: imp-null
 tib entry: 10.0.0.0/8, rev 1135
     local binding:  tag: imp-null
     remote binding: tsr: 12.12.12.12:0, tag: imp-null
 tib entry: 10.0.0.0/8, rev 8
     local binding:  tag: imp-null
Router#
```

Configuration Examples for MPLS LDP Inbound Label Binding Filtering

In the following example, the mpls ldp neighbor labels accept command is configured with an access control list to filter label bindings received on sessions with the neighbor 10.110.0.10.

Label bindings for prefixes that match 10.b.c.d are accepted, where b is less than or equal to 63, and c and d can be any integer between 0 and 128. Other label bindings received from 10.110.0.10 are rejected.

```
Router# configure terminal
Router(config)# access-list 1 permit 10.63.0.0 0.63.255.255
Router(config)# mpls ldp neighbor 10.110.0.10 labels accept 1
Router(config)# end
```

In the following example, the **show mpls ldp bindings neighbor** command displays label bindings that were learned from 10.110.0.10. This example verifies that the LIB does not contain label bindings for prefixes that have been excluded.

```
Router# show mpls ldp bindings neighbor 10.110.0.10
tib entry: 10.2.0.0/16, rev 4
    remote binding: tsr: 10.110.0.10:0, tag: imp-null
tib entry: 10.43.0.0/16, rev 6
    remote binding: tsr: 10.110.0.10:0, tag: 16
tib entry: 10.52.0.0/16, rev 8
    remote binding: tsr: 10.110.0.10:0, tag: imp-null
```

Additional References

Related Documents

Related Topic	Document Title
MPLS Label Distribution Protocol (LDP)	MPLS Label Distribution Protocol

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
LDP Specification, draft-ietf-mpls-ldp-08.txt	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

RFC	Title
RFC 3036	LDP Specification
RFC 3037	LDP Applicability

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for MPLS LDP Inbound Label Binding Filtering Feature

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 3 Feature Information for MPLS LDP Inbound Label Binding Filtering Feature

Feature Name	Releases	Feature Information
MPLS LDP Inbound Label Binding Filtering Feature	12.0(26)S 12.2(25)S 12.3(14)T 12.2(18)SXE	You can use the MPLS LDP Inbound Label Binding Filtering feature to configure access control lists (ACLs) for controlling the label bindings a label switch router (LSR) accepts from its peer LSRs. In Cisco IOS Release 12.0(26)S, this feature was introduced on the Cisco 7200. This feature was integrated into Cisco IOS Release 12.2(25)S for the Cisco 7500 series router. This feature was integrated into Cisco IOS Release 12.3(14)T. This feature was integrated into Cisco IOS Release 12.2(18)SXE for the Cisco 7600 series router. The following commands were introduced or modified: **clear mpls ldp neighbor** , **mpls ldp neighbor labels accept** , **show mpls ldp neighbor**

Glossary

carrier supporting carrier --A situation where one service provider allows another service provider to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

CE router --customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

inbound label binding filtering --Allows LSRs to control which label bindings it will accept from its neighboring LSRs. Consequently, an LSR does not accept or store some label bindings that its neighbors advertise.

label --A short fixed-length identifier that tells switching nodes how to forward data (packets or cells).

label binding --An association between a destination prefix and a label.

MPLS LDP Autoconfiguration

The MPLS LDP Autoconfiguration feature enables you to globally configure Label Distribution Protocol (LDP) on every interface associated with a specified Interior Gateway Protocol (IGP) instance.

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 Autoconfiguration

- In Cisco IOS Release 12.0(32)SY, the **mpls ldp autoconfig** command is supported only with OSPF. Other IGPs are not supported.
- If LDP is disabled globally, the **mpls ldp autoconfig** command fails and generates a console message explaining that LDP must first be enabled globally by using the **mpls ip** global configuration command.
- If the **mpls ldp autoconfig** command is configured for an IGP instance, you cannot enter **no mpls ip** global configuration command. To disable LDP, you must first issue the **no mpls ldp autoconfig** command.
- For interfaces running IS-IS processes, you can enable Multiprotocol Label Switching (MPLS) for each interface, using the router mode command **mpls ldp autoconfig** or the **mpls ldp igp autoconfig** interface configuration command.
- You specify that the default label distribution protocol is LDP for a router or for an interface. Tag Distribution Protocol (TDP) is not supported.

- The MPLS LDP Autoconfiguration feature is not supported on traffic engineering tunnel interfaces.

Information About MPLS LDP Autoconfiguration

To enable LDP, you should configure it globally and on each interface where it is needed. Configuring LDP on many interfaces can be time-consuming. The following section provides information about autoconfiguration feature on OSPF and IS-IS interfaces:

- MPLS LDP Autoconfiguration on OSPF and IS-IS Interfaces, page 50

MPLS LDP Autoconfiguration on OSPF and IS-IS Interfaces

The MPLS LDP Autoconfiguration feature enables you to globally enable LDP on every interface associated with an IGP instance. This feature is supported on OSPF and IS-IS IGPs. It provides a means to block LDP from being enabled on interfaces that you do not want enabled. The goal of the MPLS LDP Autoconfiguration feature is to make configuration easier, faster, and error free.

You issue the **mpls ldp autoconfig** command to enable LDP on each interface that is running an OSPF or IS-IS process. If you do not want some of the interfaces to have LDP enabled, you can issue the **no mpls ldp igp autoconfig** command on those interfaces.

How to Configure MPLS LDP Autoconfiguration

- Configuring MPLS LDP Autoconfiguration with OSPF Interfaces, page 50
- Disabling MPLS LDP Autoconfiguration from Selected OSPF Interfaces, page 53
- Verifying MPLS LDP Autoconfiguration with OSPF, page 54
- Configuring MPLS LDP Autoconfiguration with IS-IS Interfaces, page 55
- Disabling MPLS LDP Autoconfiguration from Selected IS-IS Interfaces, page 57
- Verifying MPLS LDP Autoconfiguration with IS-IS, page 58

Configuring MPLS LDP Autoconfiguration with OSPF Interfaces

The following steps explain how to configure LDP for interfaces running OSPF processes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol ldp**
5. **interface** *type number*
6. **ip address** *prefix mask*
7. **exit**
8. **router ospf** *process-id*
9. **network** *ip-address wildcard-mask* **area** *area-id*
10. **mpls ldp autoconfig** [**area** *area-id*]
11. **end**

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	**mpls ip** **Example:** `Router(config)# mpls ip`	Globally enables hop-by-hop forwarding.
Step 4	**mpls label protocol ldp** **Example:** `Router(config)# mpls label protocol ldp`	Specifies LDP as the default label distribution protocol.

	Command or Action	Purpose
Step 5	**interface** *type number* **Example:** `Router(config)# interface POS 3/0`	Specifies the interface to configure and enters interface configuration mode.
Step 6	**ip address** *prefix mask* **Example:** `Router(config-if)# ip address 10.0.0.11 255.255.255.255`	Assigns an IP address to the interface.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 8	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Enables OSPF routing and enters router configuration mode.
Step 9	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Router(config-router)# network 10.0.0.0 0.0.255.255 area 3`	Specifies the interface on which OSPF runs and defines the area ID for that interface.
Step 10	**mpls ldp autoconfig** [**area** *area-id*] **Example:** `Router(config-router)# mpls ldp autoconfig area 3`	Enables the MPLS LDP Autoconfiguration feature to enable LDP on interfaces belonging to an OSPF process. • If no area is specified, the command applies to all interfaces associated with the OSPF process. If an area ID is specified, then only interfaces associated with that OSPF area are enabled with LDP.
Step 11	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Disabling MPLS LDP Autoconfiguration from Selected OSPF Interfaces

When you issue the **mpls ldp autoconfig** command, all the interfaces that belong to an OSPF area are enabled for LDP. To remove LDP from some interfaces, use the **no mpls ldp igp autoconfig** command on those interfaces. The following configuration steps show how to disable LDP from some of the interfaces after they were configured with the MPLS LDP Autoconfiguration feature with the **mpls ldp autoconfig** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no mpls ldp igp autoconfig**
5. **end**

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	**interface** *type number* **Example:** `Router(config)# interface POS 3/0`	Specifies the interface to configure and enters interface configuration mode.
Step 4	**no mpls ldp igp autoconfig** **Example:** `Router(config-if)# no mpls ldp igp autoconfig`	Disables LDP for that interface.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying MPLS LDP Autoconfiguration with OSPF

The following steps explain how to verify the MPLS LDP Autoconfiguration feature.

SUMMARY STEPS

1. **enable**
2. **show mpls interfaces** [*type number* | **vrf** *vpn-name*] [**all**] [**detail**] [**internal**]
3. **show mpls ldp discovery** [**vrf** *vpn-name* | **all**] [**detail**]

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **show mpls interfaces** [*type number* | **vrf** *vpn-name*] [**all**] [**detail**] [**internal**]
The **show mpls interfaces** command displays the method used to enable LDP on an interface:

- If LDP is enabled by the **mpls ldp autoconfig** command, the output displays:

Example:

```
IP labeling enabled (ldp):
   IGP config
```

- If LDP is enabled by the **mpls ip** command, the output displays:

Example:

```
IP labeling enabled (ldp):
  Interface config
```

- If LDP is enabled by the **mpls ip** command and the **mpls ldp autoconfig** command, the output displays:

Example:

```
IP labeling enabled (ldp):
  Interface config
  IGP config
```

The following example shows that LDP was enabled on the interface by both the **mpls ip** and **mpls ldp autoconfig** commands:

Example:

```
Router# show mpls interfaces Serial 2/0 detail

Interface Serial2/0:
        IP labeling enabled (ldp):
          Interface config
          IGP config
        LSP Tunnel labeling enabled
        BGP labeling not enabled
        MPLS operational
        Fast Switching Vectors:
          IP to MPLS Fast Switching Vector
          MPLS Turbo Vector
        MTU = 1500
```

Step 3 **show mpls ldp discovery** [**vrf** *vpn-name* | **all**] [**detail**]

The **show mpls ldp discovery detail** command also shows how LDP was enabled on the interface. In the following example, LDP was enabled by both the **mpls ip** and **mpls ldp autoconfig** commands:

Example:

```
Router# show mpls ldp discovery detail
Local LDP Identifier:
    10.11.11.11:0
    Discovery Sources:
    Interfaces:
        Serial2/0 (ldp): xmit/recv
            Enabled: Interface config, IGP config;
            Hello interval: 5000 ms; Transport IP addr: 10.11.11.11
            LDP Id: 10.10.10.10:0
              Src IP addr: 10.0.0.1; Transport IP addr: 10.10.10.10
              Hold time: 15 sec; Proposed local/peer: 15/15 sec
```

Configuring MPLS LDP Autoconfiguration with IS-IS Interfaces

The following steps explain how to configure the MPLS LDP Autoconfiguration feature for interfaces that are running IS-IS processes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *prefix mask*
5. **ip router isis**
6. **exit**
7. **mpls ip**
8. **mpls label protocol ldp**
9. **router isis**
10. **mpls ldp autoconfig** [**level-1** | **level-2**]
11. **end**

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	**interface** *type number* **Example:** `Router(config)# interface POS 0/2`	Specifies the interface to configure and enters interface configuration mode.
Step 4	**ip address** *prefix mask* **Example:** `Router(config-if)# ip address 10.50.72.4 255.0.0.0`	Assigns an IP address to the interface.
Step 5	**ip router isis** **Example:** `Router(config-if)# ip router isis`	Enables IS-IS for IP on the interface.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 7	**mpls ip** **Example:** `Router(config)# mpls ip`	Globally enables hop-by-hop forwarding.

	Command or Action	Purpose
Step 8	**mpls label protocol ldp** **Example:** `Router(config)# mpls label protocol ldp`	Specifies LDP as the default label distribution protocol.
Step 9	**router isis** **Example:** `Router(config)# router isis`	Enables an IS-IS process on the router and enters router configuration mode.
Step 10	**mpls ldp autoconfig** [**level-1** | **level-2**] **Example:** `Router(config-router)# mpls ldp autoconfig`	Enables the LDP for interfaces that belong to an IS-IS process.
Step 11	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Disabling MPLS LDP Autoconfiguration from Selected IS-IS Interfaces

When you issue the **mpls ldp autoconfig** command, all the interfaces that belong to an IS-IS process are enabled for LDP. To remove LDP from some interfaces, use the **no mpls ldp igp autoconfig** command on those interfaces. The following configuration steps show how to disable LDP from some of the interfaces after they were configured with the MPLS LDP Autoconfiguration feature with the **mpls ldp autoconfig** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no mpls ldp igp autoconfig**
5. **end**

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	**interface** *type number* **Example:** `Router(config)# interface POS 3/0`	Specifies the interface to configure and enters interface configuration mode.
Step 4	**no mpls ldp igp autoconfig** **Example:** `Router(config-if)# no mpls ldp igp autoconfig`	Disables LDP for that interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying MPLS LDP Autoconfiguration with IS-IS

You can verify that the MPLS LDP Autoconfiguration feature is working correctly with the **show isis mpls ldp** command.

SUMMARY STEPS

1. **enable**
2. **show isis mpls ldp**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

Step 2 **show isis mpls ldp**

The output of the following **show isis mpls ldp** command shows that IS-IS is configured on the interface and that LDP is enabled:

Example:

```
Router# show isis mpls ldp
Interface: POS0/2; ISIS tag null enabled
 ISIS is UP on interface
 AUTOCONFIG Information :
   LDP enabled: YES
 SYNC Information :
   Required: NO
```

The output shows:

- IS-IS is up.
- LDP is enabled.

If the MPLS LDP Autoconfiguration feature is not enabled on an interface, the output looks like the following:

Example:

```
Interface: Ethernet0; ISIS tag null enabled
 ISIS is UP on interface
 AUTOCONFIG Information :
   LDP enabled: NO
 SYNC Information :
   Required: NO
```

- Troubleshooting Tips, page 59

Troubleshooting Tips

You can use the **debug mpls ldp autoconfig** command to display events that are related to the MPLS LDP Autoconfiguration feature.

Configuration Examples for MPLS LDP Autoconfiguration

The following sections show examples for the MPLS LDP Autoconfiguration feature with OSPF and IS-IS processes.

MPLS LDP Autoconfiguration with OSPF Example

The following configuration commands enable LDP for OSPF process 1 area 3. The **mpls ldp autoconfig area 3** command and the OSPF **network** commands enable LDP on POS interfaces 0/0, 0/1, and 1/1. The

no mpls ldp igp autoconfig command on POS interface 1/0 prevents LDP from being enabled on POS interface 1/0, even though OSPF is enabled for that interface.

```
configure terminal
 interface POS 0/0
  ip address 10.0.0.1 255.0.0.0
!
 interface POS 0/1
  ip address 10.0.1.1 255.0.0.1
!
 interface POS 1/1
  ip address 10.1.1.1 255.255.0.0
!
 interface POS 1/0
  ip address 10.1.0.1 0.1.0.255
  exit
!
 router ospf 1
  network 10.0.0.0 0.0.255.255 area 3
  network 10.1.0.0 0.0.255.255 area 3
  mpls ldp autoconfig area 3
  end
 interface POS 1/0
  no mpls ldp igp autoconfig
```

MPLS LDP Autoconfiguration with IS-IS Examples

The following example shows the configuration of the MPLS LDP Autoconfiguration feature on POS0/2 and 0/3 interfaces, which are running IS-IS processes:

```
configure terminal
 interface POS 0/2
  ip address 10.0.0.1 255.0.0.1
  ip router isis
!
 interface POS 0/3
  ip address 10.1.1.1 255.0.1.0
  ip router isis
  exit
mpls ip
mpls label protocol ldp
router isis
mpls ldp autoconfig
```

Additional References

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

Related Documents

Related Topic	Document Title
MPLS commands	*Cisco IOS Multiprotocol Label Switching Command Reference*
MPLS LDP	MPLS Label Distribution Protocol
The MPLS LDP-IGP Synchronization feature	MPLS LDP-IGP Synchronization
The MPLS LDP Session Protection feature	MPLS LDP Session Protection

Related Topic	Document Title
Configuring integrated IS-IS	Integrated IS-IS Routing Protocol Overview

Standards

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

MIBs

MIB	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

RFC	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 Autoconfiguration

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 4 Feature Information for MPLS LDP Autoconfiguration

Feature Name	Releases	Feature Information
MPLS LDP Autoconfiguration	12.0(30)S 12.0(32)SY 12.2(28)SB 12.2(33)SRB 12.3(14)T 15.0(1)M 12.2(33)XNE	This feature enables you to globally configure LDP on every interface associated with a specified Interior Gateway Protocol (IGP) instance. In Cisco IOS Release 12.0(30)S, this feature was introduced with support for OSPF. In Cisco IOS Release 12.0(32)SY, support for IS-IS was added. This feature was integrated into Cisco IOS Release 12.2(28)SB with support for OSPF. This feature was integrated into Cisco IOS Release 12.2(33)SRB. This feature was integrated into Cisco IOS Release 12.3(14)T with support for OSPF. In Release 15.0(1)M, support for IS-IS was added. This feature was integrated into Cisco IOS Release 12.2(33)XNE with support for IS-IS on the Cisco 10000 series router. The following commands were modified: **mpls ldp autoconfig**, **mpls ldp igp autoconfig**, **show isis mpls ldp**, **show mpls ldp discovery**.

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.

MPLS LDP Graceful Restart

When a router is configured with Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Graceful Restart (GR), it assists a neighboring router that has MPLS LDP Stateful Switchover/ Nonstop Forwarding (SSO/NSF) Support and Graceful Restart to recover gracefully from an interruption in service. In this Cisco IOS release, MPLS LDP GR functions strictly in helper mode, which means it can only help other routers that are enabled with MPLS SSO/NSF and GR to recover. If the router with LDP GR fails, its peer routers cannot help it recover.

Notes:

- MPLS LDP SSO/NSF Support and Graceful Restart is supported in Cisco IOS Release 12.2(25)S. For brevity, this feature is called LDP SSO/NSF in this document.
- The MPLS LDP GR feature described in this document refers to helper mode.

When you enable MPLS LDP GR on a router that peers with an MPLS LDP SSO/NSF-enabled router, the SSO/NSF-enabled router can maintain its forwarding state when the LDP session between them is interrupted. While the SSO/NSF-enabled router recovers, the peer router forwards packets using stale information. This enables the SSO/NSF-enabled router to become operational more quickly.

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

- MPLS LDP GR is supported in strict helper mode.
- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- MPLS LDP GR cannot be configured on label-controlled ATM (LC-ATM) interfaces.
- MPLS LDP SSO/NSF is supported in IOS Release 12.2(25)S. It is not supported in this release.

Information About MPLS LDP Graceful Restart

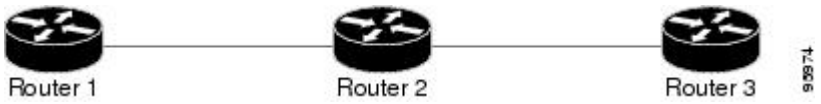
How MPLS LDP Graceful Restart Works

MPLS LDP GR works in strict helper mode, which means it helps a neighboring route processor that has MPLS LDP SSO/NSF to recover from disruption in service without losing its MPLS forwarding state. The disruption in service could be the result of a TCP or UDP event or the stateful switchover of a route processor. When the neighboring router establishes a new session, the LDP bindings and MPLS forwarding states are recovered.

In the topology shown in the figure below, the following elements have been configured:

- LDP sessions are established between Router 1 and Router 2, as well as between Router 2 and Router 3.
- Router 2 has been configured with MPLS LDP SSO/NSF. Routers 1 and 3 have been configured with MPLS LDP GR.
- A label switched path (LSP) has been established between Router 1 and Router 3.

Figure 4 Example of a Network Using LDP Graceful Restart



The following process shows how Routers 1 and 3, which have been configured with LDP GR help Router 2, which has been configured with LDP SSO/NSF recover from a disruption in service:

1. Router 1 notices an interruption in service with Router 2. (Router 3 also performs the same actions in this process.)
2. Router 1 marks all the label bindings from Router 2 as stale, but it continues to use the bindings for MPLS forwarding.

Router 1 reestablishes an LDP session with Router 2, but keeps its stale label bindings. If you issue a **show mpls ldp neighbor** command with the **graceful-restart** keyword, the command output displays the recovering LDP sessions.

1. Both routers readvertise their label binding information. If Router 1 relearns a label from Router 2 after the session has been established, the stale flags are removed. The **show mpls forwarding-table**command displays the information in the MPLS forwarding table, including the local label, outgoing label or VC, prefix, label-switched bytes, outgoing interface, and next hop.

You can set various graceful restart timers. See the following commands for more information:

- **mpls ldp graceful-restart timers neighbor-liveness**
- **mpls ldp graceful-restart timers max-recovery**

How a Route Processor Advertises That It Supports MPLS LDP Graceful Restart

A route processor that is configured to perform MPLS LDP GR includes the Fault Tolerant (FT) Type Length Value (TLV) in the LDP initialization message. The route processor sends the LDP initialization message to a neighbor to establish an LDP session.

The FT session TLV includes the following information:

- The Learn from Network (L) flag is set to 1, which indicates that the route processor is configured to perform MPLS LDP GR.
- The Reconnect Timeout field shows the time (in milliseconds) that the neighbor should wait for a reconnection if the LDP session is lost. In this release, the timer is set to 0, which indicates that if the local router fails, its peers should not wait for it to recover. The timer setting indicates that the local router is working in helper mode.
- The Recovery Time field shows the time (in milliseconds) that the neighbor should retain the MPLS forwarding state during a recovery. If a neighbor did not preserve the MPLS forwarding state before the restart of the control plane, the neighbor sets the recovery time to 0.

What Happens If a Route Processor Does Not Have LDP Graceful Restart

If two route processors establish an LDP session and one route processor is not configured for MPLS LDP GR, the two route processors create a normal LDP session but do not have the ability to perform MPLS LDP GR. Both route processors must be configured for MPLS LDP GR.

How to Configure MPLS LDP Graceful Restart

Configuring MPLS LDP Graceful Restart

You must enable MPLS LDP GR on all route processors for an LDP session to be preserved during an interruption in service.

MPLS LDP GR is enabled globally. When you enable MPLS LDP GR, it has no effect on existing LDP sessions. New LDP sessions that are established can perform MPLS LDP GR.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [**distributed**]
4. **mpls ldp graceful-restart**
5. **interface** *type slot/port*
6. **mpls ip**
7. **mpls label protocol** {**ldp** | **tdp** | **both**}

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`	Enables Cisco Express Forwarding (CEF).
Step 4	**mpls ldp graceful-restart** **Example:** `Router(config)# mpls ldp graceful-restart`	Enables the router to protect the LDP bindings and MPLS forwarding state during a disruption in service.
Step 5	**interface** *type slot/port* **Example:** `Router(config)# interface pos 3/0`	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 6	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding for an interface.
Step 7	**mpls label protocol** {**ldp** | **tdp** | **both**} **Example:** `Router(config-if)# mpls label protocol ldp`	Configures the use of LDP for an interface. You must use LDP.

Note You can also issue the **mpls label protocol ldp** command in global configuration mode, which enables LDP on all interfaces configured for MPLS.

Verifying the Configuration

The following commands help verify that MPLS LDP GR has been configured correctly:

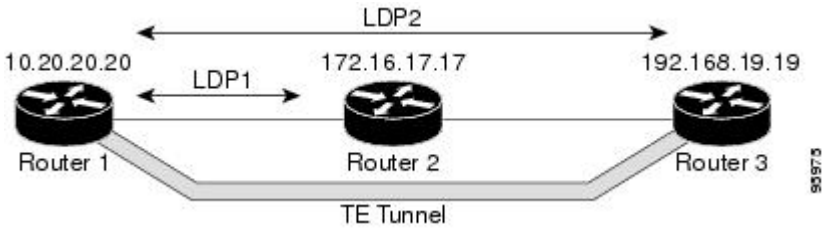
show mpls ldp neighbor with the **graceful-restart** keyword	Displays the Graceful Restart information for LDP sessions.
show mpls ldp graceful-restart	Displays Graceful Restart sessions and session parameters.

Configuration Example for MPLS LDP Graceful Restart

The figure below shows a configuration where MPLS LDP GR is enabled on Router 1 and MPLS LDP SSO/NSF is enabled on Routers 2 and 3. In this configuration example, Router 1 creates an LDP session with Router 2. Router 1 also creates a targeted session with Router 3 through a traffic engineering tunnel using Router 2.

Note MPLS LDP SSO/NSF is supported in Cisco IOS Release 12.2(25)S. It is not supported in this release.

Figure 5 MPLS LDP Graceful Restart Configuration Example



Router 1 configured with LDP GR:

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
!
ip subnet-zero
ip cef
mpls label range 16 10000 static 10001 1048575
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 20.20.20.20 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
 tunnel destination 19.19.19.19
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth  500
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface ATM5/1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/1/0.5 point-to-point
 ip address 12.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 6/100
  encapsulation aal5snap
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ip
ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
 redistribute connected
     network 12.0.0.0 0.255.255.255 area 100
 network 20.20.20.20 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
```

Router 2 configured with LDP SSO/NSF:

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
redundancy
  mode sso
!
ip cef
no ip domain-lookup
mpls label range 17 10000 static 10001 1048575
mpls label protocol ldp
```

```
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
no mpls advertise-labels
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 17.17.17.17 255.255.255.255
 no ip directed-broadcast
!
interface ATM4/0/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM4/0/0.5 point-to-point
 ip address 12.0.0.1 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 6/100
  encapsulation aal5snap
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ip
ip rsvp bandwidth 1000
!
interface POS5/1/0
 ip address 11.0.0.1 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls traffic-eng tunnels
 mpls ip
 no peer neighbor-route
 clock source internal
 ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 nsf enforce global
 network 11.0.0.0 0.255.255.255 area 100
 network 12.0.0.0 0.255.255.255 area 100
 network 17.17.17.17 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
!
ip classless
```

Router 3 configured with LDP SSO/NSF:

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
redundancy
  mode sso
!
ip subnet-zero
ip cef
!
no ip finger
no ip domain-lookup
mpls label protocol ldp
mpls ldp neighbor 11.11.11.11 targeted ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
```

```
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp discovery directed-hello interval 12
mpls ldp discovery directed-hello holdtime 130
mpls ldp discovery directed-hello accept
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 19.19.19.19 255.255.255.255
 no ip directed-broadcast
!
interface POS1/0
 ip address 11.0.0.2 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls traffic-eng tunnels
 mpls ip
 no peer neighbor-route
 clock source internal
 ip rsvp bandwidth 1000
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 nsf enforce global
network 11.0.0.0 0.255.255.255 area 100
network 19.19.19.19 0.0.0.0 area 100
mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 100
!
ip classless
```

Additional References

Related Documents

Related Topic	Document Title
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP)

Standards

Standards	Title
None	—

MIBs

MIBs[1]	MIBs Link
• MPLS Label Distribution Protocol MIB Version 8 Upgrade	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

1 Not all supported MIBs are listed.

RFCs

RFCs[2]	Title
RFC 3036	*LDP Specification*
RFC 3478	*Graceful Restart Mechanism for Label Distribution*

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for MPLS LDP Graceful Restart

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.

2 **Not all supported RFCs are listed.**

Table 5 Feature Information for MPLS LDP Graceful Restart

Feature Name	Releases	Feature Information
MPLS LDP Graceful Restart	12.0(29)S 12.3(14)T 12.2(33)SRA	MPLS LDP Graceful Restart assists a neighboring router that has MPLS LDP Stateful Switchover/Nonstop Forwarding (SSO/NSF) Support and Graceful Restart to recover gracefully from an interruption in service. In Cisco IOS Release 12.0(29)S, this feature was introduced. This feature was integrated into Cisco IOS Release 12.3(14)T. This feature was integrated into Cisco IOS Release 12.2(33)SRA. The following sections provide information about this feature: The following commands were introduced or modified: **debug mpls ldp graceful-restart** , **mpls ldp graceful-restart** , **mpls ldp graceful-restart timers max-recovery** , **mpls ldp graceful-restart timers neighbor-liveness**, **show mpls ip binding show mpls ldp bindings** , **show mpls ldp graceful-restart** , **show mpls ldp neighbor** .

MPLS--LDP MD5 Global Configuration

The MPLS--LDP MD5 Global Configuration feature provides enhancements to the Label Distribution Protocol (LDP) implementation of the Message Digest 5 (MD5) password. This feature allows you to enable LDP MD5 globally instead of on a per-peer basis. Using this feature you can set up password requirements for a set of LDP neighbors to help prevent unauthorized peers from establishing LDP sessions and to block spoofed TCP messages.

This document provides information about and configuration information for the global configuration of LDP MD5 protection.

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.

Prerequisites for MPLS--LDP MD5 Global Configuration

- Cisco Express Forwarding or distributed Cisco Express Forwarding must be enabled on the label switch router (LSR).
- Routing (static or dynamic) must be configured for the LSR.

- Multiprotocol Label Switching (MPLS) LDP must be configured on the LSR. However, you can configure LDP MD5 protection before you configure MPLS LDP. You can then use LDP MD5 protection after you configure MPLS LDP.
- A Virtual Private Network (VPN) routing and forwarding instance (VRF) must be configured if you want to configure MPLS LDP MD5 global configuration for a VRF. If you delete a VRF, the LDP MD5 global configuration for that VRF is automatically removed.

Restrictions for MPLS--LDP MD5 Global Configuration

MD5 protection described in this document applies only to the LDP sessions. All enhancements described in this document do not affect Tag Distribution Protocol (TDP) sessions.

Information About MPLS--LDP MD5 Global Configuration

Enhancements to LDP MD5 Protection for LDP Messages Between Peers

The MPLS--LDP MD5 Global Configuration feature provides the following enhancements to the LDP support of MD5 passwords:

- You can specify peers for which MD5 protection is required. This can prevent the establishment of LDP sessions with unexpected peers.
- You can configure passwords for groups of peers. This increases the scalability of LDP password configuration management.
- The established LDP session with a peer is not automatically torn down when the password for that peer is changed. The new password is used the next time an LDP session is established with the peer.
- You can control when the new password is used. You can configure the new password on the peer before forcing the use of the new password.
- If the neighboring nodes support graceful restart, then LDP sessions are gracefully restarted. The LDP MD5 password configuration is checkpointed to the standby Route Processors (RPs). The LDP MD5 password is used by the router when the new active RP attempts to establish LDP sessions with neighbors after the switchover.

LDP session, advertisement, and notification messages are exchanged between two LDP peers over a TCP connection. You can configure the TCP MD5 option to protect LDP messages that are exchanged over a TCP connection. You can configure this protection for each potential LDP peer. As a result, an LDP ignores any LDP hello messages sent from an LSR for which you have not configured a password. (LDP tries to establish an LDP session with each neighbor from which a hello message is received.)

Before the introduction of the MPLS--LDP MD5 Global Configuration feature, you needed to configure a separate password for each LDP peer for which you wanted MD5 protection. This was the case even when the same password was used for multiple LDP peers. Before this feature, LDP would tear down LDP sessions with a peer immediately if a password for that peer had changed.

LDP MD5 Password Configuration Information

Before the introduction of the MPLS--LDP MD5 Global Configuration feature, the command used for configuring a password for an LDP neighbor was **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** [**0** | **7**] *password*. This command configures a password for one neighbor whose router ID is the IP address in the specified VRF. An LSR can have zero or one such configuration for each LDP neighbor.

You can use the commands provided by the MPLS--LDP MD5 Global Configuration feature to configure passwords for LDP neighbors.

You must understand how LDP determines the password for an LDP session between peers before you configure MD5 password protection for your network. LDP determines the passwords for its sessions based on the commands that you enter.

You can enter an **mpls ldp password vrf** *vrf-name* **required** [**for** *acl*] command, either with an optional *acl* argument that permits the LDP router ID of the neighbor or without an *acl* argument. Make sure that you enter a command that configures a password. Otherwise, LDP might not establish a session with the neighbor in question.

For the commands in the following password-determining process, *A.B.C.D:N* represents the LDP neighbor in VRF vpn1 and the neighbor LDP ID:

- *A.B.C.D* is the neighbor router ID.
- *N* is the neighbor label space ID.

To determine the password for an LDP session for the neighbor label space *A.B.C.D:N* , LDP looks at the password commands in the order indicated by the following statements:

- If you configured this command:

mpls ldp neighbor vrf vpn1 *A.B.C.D* **password** *pwd-nbr*

The LDP session password is *pwd-nbr*. LDP looks no further and uses the password you specify.

- Otherwise, LDP looks to see if you configured one or more **mpls ldp vrf vpn1 password option** commands. LDP considers the commands in order of the ascending *number* arguments (*number-1st to number-n*). For example:

mpls ldp vrf vpn1 password option *number-1st* **for** *acl-1st pwd-1st*

LDP compares the peer router ID of the neighbor (*A.B.C.D)* with this command. If *A.B.C.D* is permitted by the command access list *acl-1st* , the session password is the command password, that is, *pwd-1st* .

If A.B.C.D is not permitted by *acl-1st* , LDP looks at the command with the next ascending *number* argument (*number-2nd*):

mpls ldp vrf vpn1 password option *number-2nd* **for** *acl-2nd pwd-2nd*

If *A.B.C.D* is permitted by the command access list *acl-2nd*, the session password is *pwd-2nd*.

If *A.B.C.D* is not permitted by the access list *acl-2nd*, LDP continues checking *A.B.C.D* against access lists until LDP:

- ◦ Finds *A.B.C.D* permitted by an access list. Then the command password is the session password.
  ◦ Has processed the *number-nth* argument of this command (*n* being the highest *number* argument you configured for this command).
- If the **mpls ldp vrf vpn1 password option** *number-nth* **for** *acl-nth pwd-nth* command produces no match and, therefore no password, LDP looks to see if you configured the following command:

mpls ldp password vrf vpn1 fallback *pwd-fback*

If you configured this command, the session password is *pwd-fback*.

- Otherwise, if LDP has not found a password, you did not configure a password for the session. LDP does not use MD5 protection for the session TCP connection.

LDP MD5 Password Configuration for Routing Tables

The MPLS--LDP MD5 Global Configuration feature introduces commands that can establish password protection for LDP sessions between LDP neighbors or peers. These commands can apply to routes in the global routing table or in a VRF.

By default, if the **vrf** keyword is not specified in the command, the command applies to the global routing table. The following sample commands would apply to routes in the global routing table:

```
Router# mpls ldp password required
Router# mpls ldp password option 15 for 99 pwd-acl
Router# mpls ldp password fallback pwd-fbck
```

You can configure LDP MD5 password protection for routes in a VRF only when the VRF is configured on the LSR. If you specify a VRF name and a VRF with that name is not configured on the LSR, LDP prints out a warning and discards the command. If you remove a VRF, LDP deletes the password configuration for that VRF. The following sample commands would apply to routes in a VRF, for example, VRF vpn1:

```
Router# mpls ldp vrf vpn1 password required
Router# mpls ldp vrf vpn1 password option 15 for 99 pwd-acl
Router# mpls ldp vrf vpn1 password fallback pwd-flbk
```

How to Configure the MPLS--LDP MD5 Global Configuration Feature

You might require password protection for a certain set of neighbors for security reasons (for example, to prevent LDP sessions being established with unauthorized peers, or to block spoofed TCP messages). To enforce this security, you can configure a password requirement for LDP sessions with those neighbors that must have MD5 protection (TCP session uses a password).

If you configure a password requirement for a neighbor and you did not configure a password for the neighbor, LDP tears down the LDP sessions with the neighbor. LDP also tears down the LDP sessions with the neighbor if you configured a password requirement and a password and the password is not used in the LDP sessions.

If a password is required for a neighbor and the LDP sessions with the neighbor are established to use a password, any configuration that removes the password for the neighbor causes the LDP sessions to be torn down.

To avoid unnecessary LDP session flapping, you should perform the task as described in this section and use caution when you change LDP passwords.

- Identifying LDP Neighbors for LDP MD5 Password Protection, page 78
- Configuring an LDP MD5 Password for LDP Sessions, page 80
- Verifying the LDP MD5 Configuration, page 86

Identifying LDP Neighbors for LDP MD5 Password Protection

Perform the following task to identify LDP neighbors for LDP MD5 password protection.

Before you start to configure passwords for LDP sessions, you must identify neighbors or groups of peers for which you want to provide MD5 protection. For example:

- You might have several customers that all use the same core routers. To ensure security you might want to provide each customer with a different password.
- You could have defined several departmental VRFs in your network. You could provide password protection for each VRF.
- Certain groups of peers might require password protection for security reasons. Password protection prevents unwanted LDP sessions.

Before you start to configure passwords for LDP sessions, you must identify neighbors or groups of peers for which you want to provide LDP MD5 password protection. This task uses the network in the figure below to show how you might identify LDP neighbors for LDP MD5 protection.

After you identify LDP neighbors or a group of peers for LDP MD5 protection, you must decide if password protection is mandatory and what password commands to use for each peer.

SUMMARY STEPS

1. Identify LDP neighbors or groups of peers for LDP MD5 password protection.
2. Decide what LDP MD5 protection is required for each neighbor or group of peers.

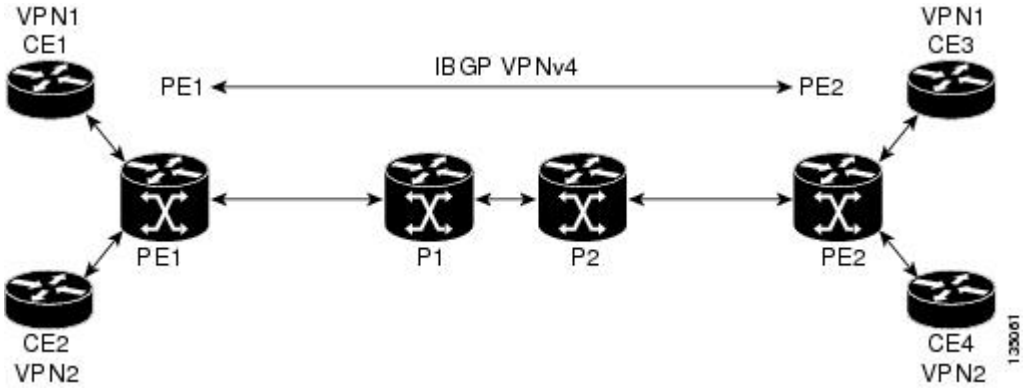
DETAILED STEPS

Step 1 Identify LDP neighbors or groups of peers for LDP MD5 password protection.
This task uses the network in the figure below to show how you might identify LDP neighbors for LDP MD5 protection.

The figure below shows a sample network that has the following topology:

- Carrier Supporting Carrier (CSC) is configured between provider edge (PE) router PE1 and customer edge (CE) router CE1 and between PE1 and CE2.
- Internal Border Gateway Protocol (IBGP) Virtual Private Network (VPN) IPv4 (VPNv4) to support Layer 3 VPNs is configured between PE1 and PE2.
- CE1 and CE3 are in VRF VPN1. CE2 and CE4 are in a different VRF, VPN2.

Figure 6 Sample Network: Identifying LDP Neighbors for LDP MD5 Protection



For the sample network in the figure above, you could configure separate passwords on PE1 for the following:

- VRF VPN1
- VRF VPN2

You could also configure a password requirement on PE1 for P1, P2, CE1 and CE2.

Step 2 Decide what LDP MD5 protection is required for each neighbor or group of peers.

Configuring an LDP MD5 Password for LDP Sessions

This section contains information about and instructions for configuring an LDP MD5 password for LDP sessions. You configure an LDP MD5 password to protect your routers from unwanted LDP sessions and provide LDP session security. You can provide LDP session security for a specific neighbor, or for LDP peers from a specific VRF or from the global routing table, or for a specific set of LDP neighbors.

After you have identified the LDP neighbor, LDP neighbors, or LDP peers in your network for which you want LDP MD5 password protection, perform the following procedures, as you require, to configure an LDP MD5 password for LDP sessions:

- Configuring an LDP MD5 Password for a Specified Neighbor, page 80
- Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF, page 82
- Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers, page 84

Configuring an LDP MD5 Password for a Specified Neighbor

Perform the following task to configure an LDP MD5 password for a specified neighbor.

LDP looks first for a password between the router and neighbor that is configured with the **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** *pwd-string* command. If a password is configured with this command, LDP uses that password before checking passwords configured by other commands.

You must add a configuration command for each neighbor or peer for which you want password protection.

Identify the LDP neighbor or peer for which you want MD5 password protection.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** [**0** | **7**] *password-string*
4. **end**
5. **show mpls ldp neighbor** [**vrf** *vrf-name* | **all**] [*ip-address* | [*interface*] [**detail**] [**graceful-restart**]
6. **show mpls ldp neighbor** [**vrf** *vrf-name*] [*ip-address* | *interface*] **password** [**pending** | **current**]
7. **show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**]

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	**mpls ldp neighbor** [**vrf** *vrf-name*] *ip-address* **password** [**0** | **7**] *password-string* **Example:** `Router(config)# mpls ldp neighbor vrf vpn1 10.1.1.1 password nbrce1pwd`	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor. • The **vrf** *vrf-name* keyword-argument pair specifies the VPN routing and forwarding instance for the specified neighbor. • The *ip-address* argument specifies the router ID (IP address) that identifies a neighbor. • The [**0** | **7**] keywords specify whether the password that follows is encrypted: ◦ **0** specifies a clear-text (nonencrypted) password. ◦ **7** specifies a Cisco proprietary encrypted password. • The *password-string* argument defines the password key to be used for computing MD5 checksums for the session TCP connection with the specified neighbor.
Step 4	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Command or Action	Purpose
Step 5 **show mpls ldp neighbor** [**vrf** *vrf-name* | **all**] [*ip-address* | [*interface*] [**detail**] [**graceful-restart**] **Example:** `Router# show mpls ldp neighbor vrf vpn1 detail`	Displays the status of LDP sessions. • The **vrf** *vrf-name* keyword-argument pair displays the LDP neighbors for the specified VRF instance (*vrf-name*). • The **all** keyword displays LDP neighbor information for all VPNs, including those in the default routing domain. • The *ip-address* argument identifies the neighbor with the IP address for which you configured password protection. • The *interface* argument defines the LDP neighbors accessible over this interface. • The **detail** keyword displays information in long form, including password information for this neighbor. Here are the items displayed: ◦ An indication as to whether a password is mandatory for this neighbor (required or not required) ◦ The password source (neighbor, fallback or number [option number]) ◦ An indication as to whether the latest configured password for this neighbor is used by the TCP session (in use) or the TCP session uses an old password (stale) • The **graceful-restart** keyword displays per-neighbor graceful restart information.
Step 6 **show mpls ldp neighbor** [**vrf** *vrf-name*] [*ip-address* | *interface*] **password** [**pending** | **current**] **Example:** `Router# show mpls ldp neighbor vrf vpn1 password`	Displays password information used in established LDP sessions. • The **vrf** *vrf-name* keyword-argument pair displays the LDP neighbors for the specified VRF instance (*vrf-name*). • The*ip-address* argument identifies the neighbor with the IP address for which you configured password protection. • The *interface* argument defines the LDP neighbors accessible over this interface. • The **pending** keyword displays LDP sessions whose passwords are different from that in the current configuration. • The **current** keyword displays LDP sessions whose password is the same as that in current configuration. If you do not specify an optional keyword for this command, password information for all established LDP sessions is displayed.
Step 7 **show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**] **Example:** `Router# show mpls ldp discovery vrf vpn1 detail`	Displays the status of the LDP discovery process. • The **vrf** *vrf-name* keyword-argument pair displays the neighbor discovery information for the specified VRF instance (*vrf-name*). • The **all** keyword displays LDP discovery information for all VPNs, including those in the default routing domain. • The **detail** keyword displays detailed information about all LDP discovery sources on an LSR.

Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF

Perform the following task to configure an LDP MD5 password for LDP sessions with peers from a specified VRF. You can also use this task to configure an LDP MD5 password for LDP sessions with peers from the global routing table.

This task provides you with LDP session protection with peers from a particular VRF or the global routing table. If you want a password requirement, you can use the **mpls ldp password required** command.

If only LDP sessions with a set of LDP neighbors need MD5 protection, configure a standard IP access list that permits the desired set of LDP neighbors and denies the rest. See the Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers, page 84.

Identify LDP peers for which you want MD5 password protection.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp** [**vrf** *vrf-name*] **password fallback** [**0** | **7**] *password*
4. **mpls ldp** [**vrf** *vrf-name*] **password required** [**for** *acl*]
5. **end**
6. **show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**]

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	**mpls ldp** [**vrf** *vrf-name*] **password fallback** [**0**	**7**] *password* **Example:** `Router(config)# mpls ldp vrf vpn1 password fallback 0 vrfpwdvppn1` **Example:**	Configures an MD5 password for LDP sessions with peers. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The [**0**	**7**] keywords specify whether the password that follows is encrypted: ◦ **0** specifies a clear-text (nonencrypted) password. ◦ **7** specifies a Cisco proprietary encrypted password. • The *password* argument specifies the MD5 password to be used for the LDP sessions with peers whose connections are established through a named VRF or the global routing table. The example sets up an MD5 password for a VRF.

	Command or Action	Purpose
Step 4	**mpls ldp** [**vrf** *vrf-name*] **password required** [**for** *acl*] **Example:** `Router(config)# mpls ldp vrf vpn1 password required`	Specifies that LDP must use a password when establishing a session between LDP peers. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The **for** *acl* keyword-argument pair names an access list that specifies that a password is mandatory only for LDP sessions with neighbors whose LDP router IDs are permitted by the list. Only standard IP access lists can be used for the *acl* argument.
Step 5	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.
Step 6	**show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**] **Example:** `Router# show mpls ldp discovery detail`	Displays the status of the LDP discovery process. • The **vrf** *vrf-name* keyword-argument pair displays the neighbor discovery information for the specified VPN routing and forwarding instance (*vrf-name*). • The **all** keyword displays LDP discovery information for all VPNs, including those in the default routing domain. • The **detail** keyword displays detailed information about all LDP discovery sources on an LSR. Use this command to verify that password configuration is correct for all LDP neighbors.

Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers

Perform the following task to configure an LDP MD5 password for LDP sessions with a selected group of peers.

If only LDP sessions with a selected group of peers need MD5 protection, configure a standard IP access list that permits sessions with the desired group of peers (identified by LDP router IDs) and denies session with the rest. Configuring a password and password requirement for these neighbors or peers provides security by preventing LDP sessions from being established with unauthorized peers.

Identify the groups of peers for which you want MD5 password protection and define an access list that permits LDP sessions with the group of peers you require.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* [**0** | **7**] *password*
4. **mpls ldp** [**vrf** *vrf-name*] **password required** [**for** *acl*]
5. **end**
6. **show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**]

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	**mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* [**0**	**7**] *password* **Example:** `Router(config)# mpls ldp password option 25 for 10 aclpwdfor10`	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The *number* argument defines the order in which the access lists are evaluated in the determination of a neighbor password. The valid range is 1-32767. • The **for** *acl* keyword-argument pair specifies the name of the access list that includes the LDP router IDs of those neighbors for which the password applies. Only standard IP access list values (1-99) can be used for the *acl* argument. • The [**0**	**7**] keywords specifies whether the password that follows is encrypted: ◦ **0** specifies a clear-text (nonencrypted) password. ◦ **7** specifies a Cisco proprietary encrypted password. • The *password* argument specifies the MD5 password to be used for the specified LDP sessions.

	Command or Action	Purpose
Step 4	**mpls ldp** [**vrf** *vrf-name*] **password required** [**for** *acl*] **Example:** `Router(config)# mpls ldp password required for 10`	Specifies that LDP must use a password when establishing a session between LDP peers. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The **for** *acl* keyword-argument pair names an access list. The access list specifies a password is mandatory only for LDP sessions with neighbors whose LDP router IDs are permitted by the list. Only standard IP access lists can be used for the *acl* argument.
Step 5	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.
Step 6	**show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**] **Example:** `Router# show mpls ldp discovery detail`	Displays the status of the LDP discovery process. • The **vrf** *vrf-name* keyword-argument pair displays the neighbor discovery information for the specified VPN routing and forwarding instance (*vrf-name*). • The **all** keyword displays LDP discovery information for all VPNs, including those in the default routing domain. • The **detail** keyword displays detailed information about all LDP discovery sources on an LSR. Use this command to verify password configuration is correct for all LDP neighbors.

Verifying the LDP MD5 Configuration

Perform the following task to verify that the LDP MD5 secure sessions are as you configured for all LDP neighbors.

SUMMARY STEPS

1. **enable**
2. **show mpls ldp discovery detail**
3. **show mpls ldp neighbor detail**
4. **show mpls ldp neighbor password** [**pending** | **current**]
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 detail**

Use this command to verify that the LDP MD5 password information is as you configured for each neighbor. For example:

Example:

```
Router# show mpls ldp discovery detail
 Local LDP Identifier:
    10.1.1.1:0
    Discovery Sources:
    Interfaces:
        Ethernet1/0 (ldp): xmit/recv
            Hello interval: 5000 ms; Transport IP addr: 10.1.1.1
            LDP Id: 10.4.4.4:0
              Src IP addr: 10.0.20.4; Transport IP addr: 10.4.4.4
              Hold time: 15 sec; Proposed local/peer: 15/15 sec
              Password: not required, none, stale
    Targeted Hellos:
        10.1.1.1 -> 10.3.3.3 (ldp): passive, xmit/recv
            Hello interval: 10000 ms; Transport IP addr: 10.1.1.1
            LDP Id: 10.3.3.3:0
              Src IP addr: 10.3.3.3; Transport IP addr: 10.3.3.3
              Hold time: 90 sec; Proposed local/peer: 90/90 sec
              Password: required, neighbor, in use
```

The Password field might display any of the following for the status of the password:

- 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.

Look at the output of the command to verify your configuration.

Step 3 **show mpls ldp neighbor detail**

Use this command to verify that the password information for a neighbor is as you configured. For example:

Example:

```
Router# show mpls ldp neighbor detail
    Peer LDP Ident: 10.3.3.3:0; 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
```

Step 4 **show mpls ldp neighbor password** [**pending** | **current**]

Use this command to verify that LDP sessions are using the password configuration that you expect, either the same as or different from that in the current configuration. The **pending** keyword displays information for LDP sessions whose password is different from that in the current configuration. The **current** keyword displays information for LDP sessions whose password is the same as that in the current configuration.

For example:

Example:

```
Router# show mpls ldp neighbor password
    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: 57/57
    Peer LDP Ident: 10.3.3.3:0; 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: 216/215
Router# show mpls ldp neighbor password pending
    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: 57/57
Router# show mpls ldp neighbor password current
    Peer LDP Ident: 10.3.3.3:0; 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: 216/215
```

This command displays password information used in established LDP sessions. If you do not enter an optional **pending** or **current** keyword for the command, password information for all established LDP sessions is displayed.

Step 5 **exit**

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

Example:

```
Router# exit
Router>
```

Configuration Examples for Configuring the MPLS--LDP MD5 Global Configuration Feature

Configuring an LDP MD5 Password for LDP Sessions Examples

The section contains the following examples for configuring an LDP MD5 password for LDP sessions:

Configuring an LDP MD5 Password for LDP Sessions for a Specified Neighbor Example

The following example shows how to configure an LDP MD5 password for LDP sessions for a specified neighbor:

```
enable
configure terminal
mpls ldp vrf vpn1 10.1.1.1 password nbrscrtpwd
end
```

This sets up nbrscrtpwd as the password to use for LDP sessions for the neighbor whose LDP router ID is 10.1.1.1. Communication with this neighbor is through VRF vpn1.

Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF Example

The following example shows how to configure an LDP MD5 password for LDP sessions with peers from a specified VRF. The password vrfpwdvpn1 is configured for use with LDP peers that communicate using VRF vpn1. A password is required; otherwise, LDP tears down the session.

```
enable
configure terminal
mpls ldp vrf vpn1 password fallback vrfpwdvpn1
mpls ldp vrf vpn1 password required
end
```

The following example shows how to configure a password that is used for sessions for peers that communicate using the global routing table:

```
enable
configure terminal
mpls ldp password fallback vrfpwdvppn1
end
```

Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers Example

The following example shows how to configure an LDP MD5 password for LDP sessions with a selected group of peers. The required password aclpwdfor10 is configured for access list 10. Only those LDP router IDs permitted in access list 10 are required to use the password.

```
enable
configure terminal
mpls ldp password option 25 for 10 aclpwdfor10
mpls ldp password required for 10
end
```

Access list 10 might look something like this:

```
enable
configure terminal
access-list 10 permit 10.1.1.1
access-list 10 permit 10.3.3.3
access-list 10 permit 10.4.4.4
access-list 10 permit 10.1.1.1
access-list 10 permit 10.2.2.2
end
```

Additional References

The following sections provide references related to the MPLS--LDP MD5 Global Configuration feature.

Related Documents

Related Topic	Document Title
Configuration tasks for LDP	MPLS LDP MD5 Global Configuration

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

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

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 MD5 Global Configuration

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 6 Feature Information for MPLS--LDP MD5 Global Configuration

Feature Name	Releases	Feature Information
MPLS-LDP MD5 Global Configuration	12.2(28)SB 12.0(32)SY 12.2(33)SRB 12.4(20)T	The MPLS--LDP MD5 Global Configuration feature provides enhancements to the Label Distribution Protocol (LDP) implementation of the Message Digest 5 (MD5) password. This feature allows you to enable LDP MD5 globally instead of on a per-peer basis. Using this feature you can set up password requirements for a set of LDP neighbors to help prevent unauthorized peers from establishing LDP sessions and to block spoofed TCP messages. In 12.2(28)SB, this feature was introduced. In 12.0(32)SY, this feature was integrated into Cisco IOS Release 12.0(32)SY. This feature was integrated into Cisco IOS Release 12.2(33)SRB. This feature was integrated into Cisco IOS Release 12.4(20)T.
		The following commands were modified by this feature: **mpls ldp password fallback**, **mpls ldp password option**, **mpls ldp password required**, **show mpls ldp discovery**, **show mpls ldp neighbor**, **show mpls ldp neighbor password**.

Glossary

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces External Gateway Protocol (EGP). BGP systems exchange reachability information with other BGP systems. BGP is defined by RFC 1163.

EGP --Exterior Gateway Protocol. An internet protocol for exchanging routing information between autonomous systems. EGP is documented in RFC 904. EGP is not to be confused with the general term exterior gateway protocol. EGP is an obsolete protocol that was replaced by Border Gateway Protocol (BGP).

CE router--customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

CSC --Carrier Supporting Carrier. A situation where one service provider allows another service provider to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

LDP --Label Distribution Protocol. A standard protocol between Multiprotocol Label Switching (MPLS)-enabled routers that is uses in the negotiation of the labels used to forward packets. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

LDP peer--A label switch router (LSR) that is the receiver of label space information from another LSR. If an LSR has a label space to advertise to another LSR, or to multiple LSRs, one Label Distribution Protocol (LDP) session exists for each LSR (LDP peer) receiving the label space information.

MD5 --Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. SNMP v.2 uses MD5 for message authentication, to verify the integrity of the communication, to authenticate the message origin, and to check its timeliness.

MPLS --Multiprotocol Label Switching. A switching method that forwards IP traffic through use of labels. Each label instructs the routers and the switches in the network where to forward a packet based on preestablished IP routing information.

PE router--provider edge router. A router that is part of a service provider's network connected to a customer edge (CE) router. All Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) processing occurs in the PE router.

VPN --Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic forwarded from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

VRF --A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

MPLS LDP--Lossless MD5 Session Authentication

The MPLS LDP--Lossless MD5 Session Authentication feature enables a Label Distribution Protocol (LDP) session to be password-protected without tearing down and reestablishing the LDP session.

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.

Prerequisites for MPLS LDP--Lossless MD5 Session Authentication

The MPLS LDP--Lossless MD5 Session Authentication feature is an enhancement to the MPLS LDP MD5 Global Configuration feature. Before configuring the MPLS LDP--Lossless MD5 Session Authentication feature, refer to the *MPLS--LDP MD5 Global Configuration* feature module for more information on how the message digest algorithm 5 (MD5) works with MPLS LDP to ensure that LDP segments remain properly protected.

Note The MPLS LDP--Lossless MD5 Session Authentication feature must be configured before MPLS LDP is configured.

Configure the following features on the label switch router (LSR) before configuring the MPLS LDP--Lossless MD5 Session Authentication feature:

- Cisco Express Forwarding or distributed Cisco Express Forwarding
- Static or dynamic routing
- MPLS Virtual Private Network (VPN) routing and forwarding (VRFs) instances for MPLS VPNs
- MPLS LDP--Lossless MD5 Session Authentication for the MPLS VPN VRFs

Note If a VRF is deleted, then the lossless MD5 session authentication for that VRF is automatically removed.

Restrictions for MPLS LDP--Lossless MD5 Session Authentication

MD5 protection applies to LDP sessions between peers. Tag Distribution Protocol (TDP) sessions between peers are not protected.

Information About MPLS LDP--Lossless MD5 Session Authentication

How MPLS LDP Messages in MPLS LDP--Lossless MD5 Session Authentication are Exchanged

MPLS LDP messages (discovery, session, advertisement, and notification messages) are exchanged between LDP peers through two channels:

- LDP discovery messages are transmitted as User Datagram Protocol (UDP) packets to the well-known LDP port.
- Session, advertisement, and notification messages are exchanged through a TCP connection established between two LDP peers.

The MPLS LDP--Lossless MD5 Session Authentication feature allows an LDP session to be password-protected without tearing down and reestablishing the LDP session. The MD5 password can be implemented and changed without interrupting the LDP session.

The Evolution of MPLS LDP MD5 Password Features

The initial version of LDP MD5 protection allowed authentication to be enabled between two LDP peers and each segment sent on the TCP connection was verified between the peers. Authentication was configured on both LDP peers using the same password; otherwise, the peer session was not established. The **mpls ldp neighbor** command was issued with the **password** keyword. When MD5 protection was enabled, the router tore down the existing LDP sessions and established new sessions with the neighbor router.

An improved MD5 protection feature, called MPLS--LDP MD5 Global Configuration, was later introduced that allowed LDP MD5 to be enabled globally instead of on a per-peer basis. Using this feature, password requirements for a set of LDP neighbors could be configured. The MPLS LDP MD5 Global Configuration feature also improved the ability to maintain the LDP session. The LDP session with a peer was not automatically torn down when the password for that peer was changed. The new password was implemented the next time an LDP session was established with the peer.

The MPLS LDP--Lossless MD5 Session Authentication feature is based on the MPLS LDP MD5 Global Configuration feature. However, the MPLS LDP--Lossless MD5 Session Authentication feature provides the following enhancements:

- Activate or change LDP MD5 session authentication without interrupting the LDP session.
- Configure multiple passwords, so one password can be used now and other passwords later.
- Configure asymmetric passwords, which allows one password to be used for incoming TCP segments and a different password to be used for outgoing TCP segments.
- Configure passwords so that they overlap for a period of time. This functionality is beneficial when the clocks on two LSRs are not synchronized.

These enhancements are available by using the **key-chain** command, which allows different key strings to be used at different times according to the keychain configuration.

Keychains Use with MPLS LDP--Lossless MD5 Session Authentication

The MPLS LDP--Lossless MD5 Session Authentication feature allows keychains to be used to specify different MD5 keys to authenticate LDP traffic exchanged in each direction.

In the following example, three passwords are configured:

- Key 1 specifies the lab password. The **send-lifetime** command enables the lab password to authenticate the outgoing TCP segments from November 2, 2007, at 10:00:00 a.m. until December 2, 2007, at 10:00:00 a.m. The **accept-lifetime** command is configured so that the lab password is never used to authenticate incoming TCP segments. The **accept-lifetime** command enables the lab password for 1 second on January 1, 1970. By setting the date to the past and by enabling a duration of 1 second, the password for incoming TCP segments immediately expires. If the **accept-lifetime** command is omitted from the keychain configuration, then the password is always valid for incoming TCP segments.
- Key 2 and key 3 specify the lab2 and lab3 passwords, respectively. The **send-lifetime** commands enable the passwords for 1 second on January 1, 1970. By setting the date to the past and by enabling a duration of 1 second, the passwords for outgoing TCP segments immediately expire. If the **send-lifetime** commands are omitted from the keychain configuration, the passwords are always valid for outgoing TCP segments. The **accept-lifetime** commands for key 2 and key 3 enable the passwords to

authenticate the incoming TCP segments from November 2, 2007, at 10:00:00 a.m. until November 17, 2007, at 10:00:00 a.m. and from November 17, 2007, at 10:00:00 a.m. until December 2, 2007, at 10:00:00 a.m., respectively.

```
key chain ldp-pwd
 key 1
  key-string lab
  send-lifetime 10:00:00 Nov 2 2007 10:00:00 Dec 2 2007
  accept-lifetime 00:00:00 Jan 1 1970 duration 1
 key 2
  key-string lab2
  send-lifetime 00:00:00 Jan 1 1970 duration 1
  accept-lifetime 10:00:00 Nov 2 2007 10:00:00 Nov 17 2007
 key 3
  key-string lab3
  send-lifetime 00:00:00 Jan 1 1970 duration 1
  accept-lifetime 10:00:00 Nov 17 2007 10:00:00 Dec 2 2007
!
mpls ldp password option 1 for nbr-acl key-chain ldp-pwd
```

Application of Rules to Overlapping Passwords

Overlapping passwords can be useful when two LSRs have clocks that are not synchronized. The overlapping passwords provide a window to ensure that TCP packets are not dropped. The following rules apply to overlapping passwords:

- If the send-lifetime value for the next password begins before the send-lifetime value of the current password expires, the password with the shorter key ID is used during the overlap period. The send-lifetime value of the current password can be shortened by configuring a shorter send-lifetime value. Similarly, the send-lifetime value of the current password can be lengthened by configuring a longer send-lifetime value.
- If the accept-lifetime value for the next password begins before the accept-lifetime value of the current password expires, both the next password and the current password are used concurrently. The next password information is passed to TCP. If TCP fails to authenticate the incoming segments with the current password, it tries authenticating with the next password. If TCP authenticates a segment using the new password, it discards the current password and uses the new password from that point on.
- If a password for incoming or outgoing segments expires and no additional valid password is configured, one of the following actions take place:
  - If a password is required for the neighbor, LDP drops the existing session.
  - If a password is not required for the neighbor, LDP attempts to roll over to a session that does not require authentication. This attempt also fails unless the password expires on both LSRs at the same time.

Password Rollover Period Guidelines

Both old and new passwords are valid during a rollover period. This ensures a smooth rollover when clocks are not synchronized between two LDP neighbors. When passwords are configured using a keychain, the rollover period is equal to the accept-lifetime overlap between two successive receive passwords.

The minimum rollover period (the duration between two consecutive MD5 key updates) must be longer than the value of the LDP keepalive interval time to ensure an update of new MD5 authentication keys. If LDP session hold time is configured to its default value of 3 minutes, the LDP keepalive interval is 1 minute. The minimum rollover period should be 5 minutes. However, we recommend that the minimum rollover period is set to between 15 and 30 minutes.

To ensure a seamless rollover, follow these guidelines:

- Ensure that the local time on the peer LSRs is the same before configuring the keychain.
- Check for error messages (TCP-6-BADAUTH) that indicate keychain misconfiguration.
- Validate the correct keychain configuration by checking for the following password messages:

```
%LDP-5-PWDCFG: Password configuration changed for 10.1.1.1:0
%LDP-5-PWDRO: Password rolled over for 10.1.1.1:0
```

Resolving LDP Password Problems

LDP displays error messages when an unexpected neighbor attempts to open an LDP session, or the LDP password configuration is invalid. Some existing LDP debugs also display password information.

When a password is required for a potential LDP neighbor, but no password is configured for it, the LSR ignores LDP hello messages from that neighbor. When the LSR processes the hello message and tries to establish a TCP connection with the neighbor, it displays the error message and stops establishing the LDP session with the neighbor. The error is rate-limited and has the following format:

```
00:00:57: %LDP-5-PWD: MD5 protection is required for peer 10.2.2.2:0(glbl), no password
configured
```

When passwords do not match between LDP peers, TCP displays the following error message on the LSR that has the lower router ID; that is, the router that has the passive role in establishing TCP connections:

```
00:01:07: %TCP-6-BADAUTH: Invalid MD5 digest from 10.2.2.2(11051) to 10.1.1.1(646)
```

If one peer has a password configured and the other one does not, TCP displays the following error messages on the LSR that has a password configured:

```
00:02:07: %TCP-6-BADAUTH: No MD5 digest from 10.1.1.1(646) to 10.2.2.2(11099)
```

How to Configure MPLS LDP--Lossless MD5 Session Authentication

Configuring MPLS LDP--Lossless MD5 Session Authentication Using a Keychain

Perform this task to configure the MPLS LDP--Lossless MD5 Session Authentication feature using a keychain. Keychains allow a different key string to be used at different times according to the keychain configuration. MPLS LDP queries the appropriate keychain to obtain the current live key and key ID for the specified keychain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} {*type-code wildcard-mask* | *ip-address mask*}
4. **key chain** *name-of-chain*
5. **key** *key-id*
6. **key-string** *string*
7. **accept-lifetime** {*start-time* | **local** *start-time*} {**duration** *seconds* | *end-time* | **infinite**}
8. **send-lifetime** {*start-time* | **local** *start-time*} {**duration** *seconds* | *end-time* | **infinite**}
9. **exit**
10. **exit**
11. **mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* {**key-chain** *keychain-name* | [**0** | **7**] *password*}
12. **exit**
13. **show mpls ldp neighbor** [**vrf** *vrf-name* | **all**] [*ip-address* | *interface*] [**detail**] [**graceful-restart**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter the password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**permit** | **deny**} {*type-code wildcard-mask* | *ip-address mask*} **Example:** `Router(config)# access-list 10 permit 10.2.2.2`	Creates an access list.

	Command or Action	Purpose
Step 4	**key chain** *name-of-chain* **Example:** `Router(config)# key chain ldp-pwd`	Enables authentication for routing protocols and identifies a group of authentication keys. • Enters keychain configuration mode.
Step 5	**key** *key-id* **Example:** `Router(config-keychain)# key 1`	Identifies an authentication key on a keychain. • The *key-id* value must be a numeral. • Enters keychain key configuration mode.
Step 6	**key-string** *string* **Example:** `Router(config-keychain-key)# key-string pwd1`	Specifies the authentication string for a key. • The *string* value can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral.
Step 7	**accept-lifetime** {*start-time* | **local** *start-time*} {**duration** *seconds* | *end-time* | **infinite**} **Example:** `Router(config-keychain-key)# accept-lifetime 10:00:00 Jan 13 2007 10:00:00 Jan 13 2009`	Specifies the time period during which the authentication key on a keychain can be used for verifying incoming TCP segments. The *start-time* argument identifies the time to start and the local *start-time* argument identifies the time to start in the local time zone. Both arguments have the same parameters: **Note** The time reference depends on the clock time zone configuration on the router. If no time zone configured, then the default time zone uses the Coordinated Universal Time (UTC) time. If it is configured, either the Eastern Standard Time (EST) or Pacific Standard Time (PST) time zone is used. • *hh:mm:ss* is the time format. • Enter the number of days from 1 to 31. • Enter the name of the month. • Enter the year from the present to 2035. Once the start time is entered, select from the following: • The **duration** keyword sets the key lifetime duration in seconds. • The *end-time* argument sets the time to stop. These parameters are the same as those used for the *start-time* argument. • The **infinite** keyword allows the accept-lifetime period to never expire. If the **no accept-lifetime** value is defined, the associated receive password is valid for authenticating incoming TCP segments.

	Command or Action	Purpose
Step 8	**send-lifetime** {*start-time* | **local** *start-time*} {**duration** *seconds* | *end-time* | **infinite**} **Example:** `Router(config-keychain-key)# send-lifetime 10:00:00 Jan 13 2007 10:00:00 Jan 13 2009`	Specifies the time period during which the authentication key on a keychain can be used for verifying outgoing TCP segments. The *start-time* argument identifies the time to start and the local *start-time* argument identifies the time to start in the local time zone. Both arguments have the same parameters: **Note** The time reference depends on the clock time zone configuration on the router. If no time zone configured, then the default time zone uses the UTC time. If it is configured, either the EST or PST time zone is used. • *hh*:*mm*:*ss* is the time format. • Enter the number of days from 1 to 31. • Enter the name of the month. • Enter the year from 1993 to 2035. Once the start time is entered, select from the following: • The **duration** keyword sets the send lifetime duration in seconds. • The *end-time* argument sets the time to stop. These parameters are the same as those used for the *start-time* argument. • The **infinite** keyword allows the send lifetime period to never expire. If the **no send-lifetime** value is defined, the associated send password is valid for authenticating outgoing TCP segments.
Step 9	**exit** **Example:** `Router(config-keychain-key)# exit`	Exits from keychain key configuration mode.
Step 10	**exit** **Example:** `Router(config-keychain)# exit`	Exits from keychain configuration mode.

	Command or Action	Purpose
Step 11	**mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* {**key-chain** *keychain-name* | [**0** | **7**] *password*} **Example:** `Router(config)# mpls ldp password option 1 for 10 keychain ldp-pwd`	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The *number* argument defines the order in which the access lists are evaluated in the determination of a neighbor password. The valid range is 1 to 32767. • The **for** *acl* keyword-argument pair specifies the name of the access list that includes the LDP router IDs of those neighbors for which the password applies. Only standard IP access list values (1 to 99) can be used for the *acl* argument. • The **key-chain** *keychain-name* keyword-argument pair specifies the name of the keychain to use. • The **0** and **7** keywords specify whether the password that follows is hidden (encrypted); ◦ **0** specifies an unencrypted password. ◦ **7** specifies an encrypted password. • The *password* argument specifies the MD5 password to be used for the specified LDP sessions.
Step 12	**exit** **Example:** `Router(config)# exit`	Exits from global configuration mode.
Step 13	**show mpls ldp neighbor** [**vrf** *vrf-name* | **all**] [*ip-address* | *interface*] [**detail**] [**graceful-restart**] **Example:** `Router# show mpls ldp neighbor detail`	Displays the status of LDP sessions. • The **vrf** *vrf-name* keyword-argument pair displays the LDP neighbors for the specified VRF instance. • The *ip-address* argument identifies the neighbor with the IP address for which password protection is configured. • The *interface* argument identifies the LDP neighbors accessible over this interface. • The **detail** keyword displays information in long form, including password information for this neighbor. Here are the items displayed: ◦ An indication as to whether a password is mandatory for this neighbor (required/not required) ◦ The password source (neighbor/fallback/number [option number]) ◦ An indication as to whether the latest configured password for this neighbor is used by the TCP session (in use) or the TCP session uses an old password (stale) • The **graceful-restart** keyword displays per-neighbor graceful restart information.

Enabling the Display of MPLS LDP Password Rollover Changes and Events

When a password is required for a neighbor, but no password is configured for the neighbor, the following debug message is displayed:

00:05:04: MDSym5 protection is required for peer 10.2.2.2:0(glbl), but no password configured.

To enable the display of events related to configuration changes and password rollover events, perform this task.

or

debug mpls ldp transport connections

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp logging password configuration** [**rate-limit** *number*]
4. **mpls ldp logging password rollover** [**rate-limit** *number*]
5. **exit**
6. **debug mpls ldp transport events**

DETAILED STEPS

Step 1 **enable**
This command enables privileged EXEC mode. Enter the password if prompted.

Step 2 **configure terminal**
This command enables global configuration mode.

Step 3 **mpls ldp logging password configuration** [**rate-limit** *number*]
This command is used to enable the display of events related to configuration changes. The output displays events when a new password is configured or an existing password has been changed or deleted. A rate limit of 1 to 60 messages a minute can be specified.

Step 4 **mpls ldp logging password rollover** [**rate-limit** *number*]
This command is used to enable the display of events related to password rollover events. Events are displayed when a new password is used for authentication or when authentication is disabled. A rate limit of 1 to 60 messages a minute can be specified.

Step 5 **exit**
This command exits global configuration mode.

Step 6 **debug mpls ldp transport events**
or

debug mpls ldp transport connections

Either command displays notifications when a session TCP MD5 option is changed.

For example:

Example:

```
00:03:44: ldp: MD5 setup for peer 10.2.2.2:0(glbl); password changed to adfas
00:05:04: ldp: MD5 setup for peer 10.52.52.2:0(vpn1(1)); password changed to [nil]
```

Changing MPLS LDP--Lossless MD5 Session Authentication Passwords

The MPLS LDP--Lossless MD5 Session Authentication feature allows MD5 passwords to be changed for LDP session authentication without having to close and reestablish an existing LDP session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp** [**vrf** *vrf-name*] **password rollover duration** *minutes*
4. **mpls ldp** [**vrf** *vrf-name*] **password fallback** {**key-chain** *keychain-name* | [**0** | **7**] *password*}
5. **no mpls ldp neighbor** [**vrf** *vpn-name*] *ip-address* **password** *password*
6. **exit**
7. **show mpls ldp neighbor** [**vrf** *vrf-name*] [*ip-address* | *interface*] [**detail**] [**graceful-restart**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter the password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls ldp** [**vrf** *vrf-name*] **password rollover duration** *minutes* **Example:** `Router(config)# mpls ldp password rollover duration 7`	Configures the duration before the new password takes effect. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The *minutes* argument specifies the number of minutes from 5 to 65535 before the password rollover occurs on this router.

	Command or Action	Purpose
Step 4	**mpls ldp** [**vrf** *vrf-name*] **password fallback** {**key-chain** *keychain-name* | [**0** | **7**] *password*} **Example:** `Router(config)# mpls ldp password fallback key-chain fallback`	Configures an MD5 password for LDP sessions with peers. • The **vrf** *vrf-name* keyword-argument pair specifies a VRF configured on the LSR. • The **key-chain** *keychain-name* keyword-argument pair specifies the name of the keychain used to specify the MD5 key that authenticates the exchange of bidirectional LDP traffic. • The **0** and **7** keywords specify whether the password that follows is hidden (encrypted); ◦ **0** specifies an unencrypted password. ◦ **7** specifies an encrypted password. • The *password* argument specifies the MD5 password to be used for the specified LDP sessions.
Step 5	**no mpls ldp neighbor** [**vrf** *vpn-name*] *ip-address* **password** *password* **Example:** `Router(config)# no mpls ldp neighbor 10.11.11.11 password lab1`	Disables the configuration of a password for computing MD5 checksums for the session TCP connection with the specified neighbor. • The **vrf** *vpn-name* keyword-argument pair optionally specifies the VRF instance for the specified neighbor. • The *ip-address* argument identifies the neighbor router ID. • The **password** *password* keyword-argument pair is necessary so that the router computes MD5 checksums for the session TCP connection with the specified neighbor.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits from global configuration mode.

Command or Action	Purpose
Step 7 **show mpls ldp neighbor** [**vrf** *vrf-name*] [*ip-address* | *interface*] [**detail**] [**graceful-restart**] **Example:** `Router# show mpls ldp neighbor detail`	Displays the status of LDP sessions. • The **vrf** *vrf-name* keyword-argument pair displays the LDP neighbors for the specified VRF instance. • The *ip-address* argument identifies the neighbor with the IP address for which password protection is configured. • The *interface* argument lists the LDP neighbors accessible over this interface. • The **detail** keyword displays information in long form, including password information for this neighbor. Here are the items displayed: ◦ An indication as to whether a password is mandatory for this neighbor (required/not required) ◦ The password source (neighbor/fallback/number [option number]) ◦ An indication as to whether the latest configured password for this neighbor is used by the TCP session (in use) or the TCP session uses an old password (stale) • The **graceful-restart** keyword displays per-neighbor graceful restart information.

Configuration Examples for MPLS LDP--Lossless MD5 Session Authentication

Configuring MPLS LDP--Lossless MD5 Session Authentication Using a Keychain (Symmetrical) Example

The following example shows a configuration of two peer LSRs that use symmetrical MD5 keys:

LSR1

```
access-list 10 permit 10.2.2.2
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
 key 1
  key-string pwd1
  send-lifetime 10:00:00 Jan 1 2007 10:00:00 Feb 1 2007
  accept-lifetime 09:00:00 Jan 1 2007 11:00:00 Feb 1 2007
!
interface loopback0
  ip address 10.1.1.1 255.255.255.255
!
interface Ethernet0/0
  ip address 10.0.1.1 255.255.255.254
  mpls label protocol ldp
  tag-switching ip
```

LSR2

```
access-list 10 permit 10.1.1.1
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
 key 1
  key-string pwd1
  send-lifetime 10:00:00 Jan 1 2007 10:00:00 Feb 1 2007
  accept-lifetime 09:00:00 Jan 1 2007 11:00:00 Feb 1 2007
!
interface loopback0
  ip address 10.2.2.2 255.255.255.255
!
interface Ethernet0/0
  ip address 10.0.1.2 255.255.255.254
  mpls label protocol ldp
  tag-switching ip
```

Configuring MPLS LDP--Lossless MD5 Session Authentication Using a Keychain (Asymmetrical) Example

The following example shows a configuration of two peer LSRs that use asymmetrical MD5 keys:

LSR1

```
access-list 10 permit 10.2.2.2
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
 key 1
  key-string pwd1
  accept-lifetime 00:00:00 Jan 1 2005 duration 1
  send-lifetime 10:00:00 Jan 1 2007 10:00:00 Feb 1 2007
 key 2
  key-string pwd2
  accept-lifetime 09:00:00 Jan 1 2007 11:00:00 Feb 1 2007
  send-lifetime 00:00:00 Jan 1 2005 duration 1
!
interface loopback0
  ip address 10.1.1.1 255.255.255.255
!
interface Ethernet0/0
  ip address 10.0.1.1 255.255.255.254
  mpls label protocol ldp
  tag-switching ip
```

LSR2

```
access-list 10 permit 10.1.1.1
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
 key 1
  key-string pwd2
  accept-lifetime 00:00:00 Jan 1 2005 duration 1
  send-lifetime 10:00:00 Jan 1 2007 10:00:00 Feb 1 2007
 key 2
  key-string pwd1
  accept-lifetime 09:00:00 Jan 1 2007 11:00:00 Feb 1 2007
  send-lifetime 00:00:00 Jan 1 2005 duration 1
!
interface loopback0
```

```
  ip address 10.2.2.2 255.255.255.255
!
interface Ethernet0/0
  ip address 10.0.1.2 255.255.255.254
  mpls label protocol ldp
  tag-switching ip
```

Changing MPLS LDP--Lossless MD5 Session Authentication Password Example

The following example shows the existing password configuration for LSR A, LSR B, and LSR C:

LSR A Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.11.11.11 password lab1
mpls ldp neighbor 10.12.12.12 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.10.10.10 255.255.255.255
!
interface Ethernet1/0
ip address 10.2.0.1 255.255.0.0
mpls ip
!
interface Ethernet2/0
ip address 10.0.0.1 255.255.0.0
mpls ip
```

LSR B Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.10.10.10 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.11.11.11 255.255.255.255
!
interface Ethernet1/0
ip address 10.2.0.2 255.255.0.0
mpls ip
```

LSR C Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.10.10.10 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.12.12.12 255.255.255.255
!
interface Ethernet2/0
ip address 10.0.0.2 255.255.0.0
mpls ip
!
```

The following example shows how the lossless password change is configured using the **mpls ldp password rollover duration** command for LSR A, LSR B, and LSR C so there is enough time to change all the passwords on all of the routers:

LSR A New Configuration

```
mpls ldp password rollover duration 10
mpls ldp password fallback lab2
no mpls ldp neighbor 10.11.11.11 password lab1
no mpls ldp neighbor 10.12.12.12 password lab1
```

LSR B New Configuration

```
mpls ldp password rollover duration 10
mpls ldp password fallback lab2
no mpls ldp neighbor 10.10.10.10 password lab1
```

LSR C New Configuration

```
mpls ldp password rollover duration 10
mpls ldp password fallback lab2
no mpls ldp neighbor 10.10.10.10 password lab1
```

After 10 minutes has elapsed, the password changes. The following system logging message for LSR A confirms that the password rollover was successful:

```
%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
%LDP-5-PWDRO: Password rolled over for 10.12.12.12:0
```

Changing MPLS LDP--Lossless MD5 Session Authentication Password Using a Rollover Without Keychain Example

The MPLS LDP--Lossless MD5 Session Authentication password can be changed in a lossless way (without tearing down an existing LDP session) by using a password rollover without a keychain.

The following example shows the existing password configuration for LSR A and LSR B:

LSR A Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.11.11.11 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.10.10.10 255.255.255.255
!
interface Ethernet1/0
ip address 10.2.0.1 255.255.0.0
mpls ip
```

LSR B Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.10.10.10 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.11.11.11 255.255.255.255
!
interface Ethernet1/0
ip address 10.2.0.2 255.255.0.0
mpls ip
```

The following example shows the new password configuration for LSR A and LSR B:

Note The rollover duration should be large enough so that the passwords can be changed on all impacted routers.

LSR A New Configuration

```
mpls ldp password rollover duration 10
mpls ldp neighbor 10.11.11.11 password lab2
```

LSR B New Configuration

```
mpls ldp password rollover duration 10
mpls ldp neighbor 10.10.10.10 password lab2
```

After 10 minutes (rollover duration), the password changes and the following system logging message confirms the password rollover at LSR A:

```
%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
```

Changing MPLS LDP--Lossless MD5 Session Authentication Password Using a Rollover with a Keychain Example

The MPLS LDP--Lossless MD5 Session Authentication password can be changed in a lossless way by using a password rollover with a keychain. The following configuration example shows the new password keychain configuration for LSR A, LSR B, and LSR C, in which the new password is ldp-pwd.

In the example, the desired keychain is configured first. The first pair of keys authenticate incoming TCP segments (recv key) and compute MD5 digests for outgoing TCP segments (**xmit key**). These keys should be the same keys as those currently in use; that is, in **lab 1**. The second **recv key** in the keychain should be valid after a few minutes. The second **xmit key** becomes valid at a future time.

Note The rollover duration should be large enough so that the passwords can be changed on all impacted routers.

LSR A New Configuration

```
mpls ldp password rollover duration 10
access-list 10 permit 10.11.11.11
access-list 10 permit 10.12.12.12
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
accept-lifetime 10:15:00 Jan 1 2007 10:45:00 Feb 1 2007
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
accept-lifetime 10:15:00 Feb 1 2007 10:45:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

```
no mpls ldp neighbor 10.11.11.11 password lab1
no mpls ldp neighbor 10.12.12.12 password lab1
```

LSR B New Configuration

```
mpls ldp password rollover duration 10
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
accept-lifetime 10:15:00 Jan 1 2007 10:45:00 Feb 1 2007
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
accept-lifetime 10:15:00 Feb 1 2007 10:45:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
no mpls ldp neighbor 10.10.10.10 password lab1
```

LSR C New Configuration

```
mpls ldp password rollover duration 10
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
accept-lifetime 10:15:00 Jan 1 2007 10:45:00 Feb 1 2007
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
accept-lifetime 10:15:00 Feb 1 2007 10:45:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
no mpls ldp neighbor 10.10.10.10 password lab1
```

After 10 minutes, the password changes and the following system logging message confirms the password rollover at LSR A.

```
%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
%LDP-5-PWDRO: Password rolled over for 10.12.12.12:0
```

Changing MPLS LDP--Lossless MD5 Session Authentication Password Using a Fallback Password With a Keychain Example

The MPLS LDP--Lossless MD5 Session AuthenticationMPLS LDP--Lossless MD5 Session Authentication password can be changed in a lossless way by using a fallback password when doing a rollover with a keychain.

Note The fallback password is used only when there is no other keychain configured. If there is a keychain configured, then the fallback password is not used.

The following example shows the existing password configuration for LSR A, LSR B, and LSR C:

LSR A Existing Configuration

```
mpls ldp router-id loopback0 force
mpls label protocol ldp
!
interface loopback0
ip address 10.10.10.10 255.255.255.255
!
interface Ethernet1/0
ip address 10.2.0.1 255.255.0.0
mpls ip
!
interface Ethernet2/0
ip address 10.0.0.1 255.255.0.0
mpls ip
!
access-list 10 permit 10.11.11.11
access-list 10 permit 10.12.12.12
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR B Existing Configuration

```
mpls ldp router-id loopback0 force
mpls label protocol ldp
!
interface loopback0
ip address 10.11.11.11 255.255.255.255
!
interface Ethernet1/0
ip address 10.2.0.2 255.255.0.0
mpls ip
!
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR C Existing Configuration

```
mpls ldp router-id loopback0 force
mpls label protocol ldp
!
interface loopback0
ip address 10.12.12.12 255.255.255.255
!
interface Ethernet2/0
ip address 10.0.0.2 255.255.0.0
mpls ip
```

```
!
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

Note The fallback keychain is not used unless the keychain **ldp-pwd** is removed using the **no mpls ldp password option 5 for 10 key-chain ldp-pwd** command.

The following example shows the new configuration for LSR A, LSR B, and LSR C, where one keychain is configured with the name **ldp-pwd** and another keychain is configured with the name **fallback** for the fallback password.

Note The rollover duration should be large enough so that the passwords can be changed on all impacted routers.

LSR A New Configuration

```
mpls ldp password rollover duration 10
!
key chain fallback
key 10
key-string fbk1
!
mpls ldp password fallback key-chain fallback
!
no mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR B New Configuration

```
mpls ldp password rollover duration 10
!
key chain fallback
key 10
key-string fbk1
!
mpls ldp password fallback key-chain fallback
!
no mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR C New Configuration

```
mpls ldp password rollover duration 10
key chain fallback
key 10
key-string fbk1
!
mpls ldp password fallback key-chain fallback
!
no mpls ldp password option 5 for 10 key-chain ldp-pwd
```

After 10 minutes, the password changes and the following system logging message confirms the password rollover at LSR A:

```
%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
%LDP-5-PWDRO: Password rolled over for 10.12.12.12:0
```

Changing MPLS LDP--Lossless MD5 Session Authentication Common Misconfiguration Examples

The following sections describe common misconfiguration examples that can occur when the MPLS LDP--Lossless MD5 Session Authentication password is migrated in a lossless way. Misconfigurations can lead to undesired behavior in an LDP session.

Incorrect Keychain LDP Password Configuration Example

Possible misconfigurations can occur when keychain-based commands are used with the **mpls ldp password option for key-chain** command. If the **accept-lifetime** or **send-lifetime** command is not specified in this configuration, then a misconfiguration can occur when more than two keys are in a keychain.

The following example shows an incorrect keychain configuration with three passwords for LSR A and LSR B in the keychain:

LSR A Incorrect Keychain LDP Password Configuration

```
access-list 10 permit 10.11.11.11
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR B Incorrect Keychain LDP Password Configuration

```
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

In the example, for both LSR A and LSR B, during the period of the third **send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007** command, all three configured keys are valid as receive keys, and only the last configured key is valid as a transmit key. The keychain resolution rules dictate that keys 10 and 11 are used as receive keys, and only the last key 12 can be used as the transmit key. Because the transmit and receive keys are mismatched, the LDP session will not stay active.

Note When more than two passwords are configured in a keychain, the configuration needs to have both **accept-lifetime** and **send-lifetime** commands configured correctly for effective rollovers.

The following example shows the correct keychain configuration with multiple passwords in the keychain:

LSR A Correct Keychain LDP Password Configuration

```
access-list 10 permit 10.11.11.11
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
accept-lifetime 10:15:00 Jan 1 2007 10:45:00 Feb 1 2007
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
accept-lifetime 10:15:00 Feb 1 2007 10:45:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

LSR B Correct Keychain LDP Password Configuration

```
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
accept-lifetime 10:15:00 Jan 1 2007 10:45:00 Feb 1 2007
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
accept-lifetime 10:15:00 Feb 1 2007 10:45:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

In the example above, for both LSR A and LSR B, during the period of the third **send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007** command, only the last key 12 is valid as transmit and receive keys. Therefore, the LDP session remains active.

Avoiding Access List Configuration Problems

Use caution when modifying or deleting an access list. Any empty access list implies "permit any" by default. So when either the **mpls ldp password option for key-chain** command or the **mpls ldp password option for** command is used for MPLS LDP MD5 session authentication, if the access list specified in the command becomes empty as a result of a modification or deletion, then all LDP sessions on the router expect a password. This configuration may cause undesired behavior in LDP sessions. To avoid this scenario, ensure that the proper access list is specified for each LSR.

Changing MPLS LDP--Lossless MD5 Session Authentication Using a Second Key to Avoid LDP Session Failure Examples

The MPLS LDP--Lossless MD5 Session Authentication feature works when a specified rollover period is configured. Typically, one rollover period overlaps the two accept lifetime values that are configured for two consecutive receive keys. The LDP process requests an update from the keychain manager for the latest valid transmit and receive keys once every minute. LDP compares the latest key set with the keys from the previous update in its database to determine if a key was removed, changed, or rolled over. When the rollover occurs, the LDP process detects the rollover and programs TCP with the next receive key.

The LDP session can fail if LDP is configured to use two keys for the MPLS LDP--Lossless MD5 Session Authentication feature where the first key uses a send and accept lifetime value and the second key is not configured. The configuration creates a special case where there are two rollovers but there is only one rollover period.

The following sections provide an example of this problem and a solution:

TCP Authentication and LDP Sessions Can Fail When a Second Rollover Period Is Missing Example

In the following configuration, the first rollover is from “secondpass” to “firstpass.” The second rollover is from “firstpass” back to “secondpass.” The only rollover period in this configuration is the overlapping between the “firstpass” and “secondpass.” Because one rollover period is missing, LDP performs only the first rollover and not the second rollover, causing TCP authentication to fail and the LDP session to fail.

```
key chain ldp-pwd
 key 1
   key-string firstpass
   accept-lifetime 01:03:00 Sep 10 2007 01:10:00 Sep 10 2007
   send-lifetime 01:05:00 Sep 10 2007 01:08:00 Sep 10 2007
 key 2
   key-string secondpass
```

TCP authentication and LDP sessions can also fail if the second key has send and accept lifetime configured. In this case the accept lifetime of the first key is a subset of the accept lifetime of the second key. For example:

```
key chain ldp-pwd
 key 1
   key-string firstpass
   accept-lifetime 01:03:00 Sep 10 2007 01:10:00 Sep 10 2007
   send-lifetime 01:05:00 Sep 10 2007 01:08:00 Sep 10 2007
 key 2
   key-string secondpass
   accept-lifetime 01:03:00 Sep 9 2007 01:10:00 Sep 11 2007
   send-lifetime 01:05:00 Sep 9 2007 01:08:00 Sep 11 2007
```

Reconfigure a Keychain to Prevent TCP Authentication and LDP Session Failures Example

If the configuration needs to specify the last key in the keychain to always be valid, then configure the keychain to have at least two keys. Each key must be configured with both the send and accept lifetime period. For example:

```
key chain ldp-pwd
 key 1
   key-string firstpass
   accept-lifetime 01:03:00 Sep 10 2007 01:10:00 Sep 10 2007
```

```
   send-lifetime 01:05:00 Sep 10 2007 01:08:00 Sep 10 2007
 key 2
   key-string secondpass
   accept-lifetime 01:06:00 Sep 10 2007 01:17:00 Sep 10 2007
   send-lifetime 01:08:00 Sep 10 2007 01:15:00 Sep 10 2007
 key 3
   key-string thirdpass
```

If the configuration needs to specify the first keychain for the time interval, then switch to use the second key forever after that interval. This is done by configuring the start time for the second key to begin shortly before the end time of the first key, and by configuring the second key to be valid forever after that interval. For example:

```
key chain ldp-pwd
 key 1
   key-string firstpass
   accept-lifetime 00:03:00 Sep 10 2007 01:10:00 Sep 10 2007
   send-lifetime 00:05:00 Sep 10 2007 01:08:00 Sep 10 2007
 key 2
   key-string secondpass
   accept-lifetime 01:06:00 Sep 10 2007 infinite
   send-lifetime 01:08:00 Sep 10 2007 infinite
```

If the configuration needs to specify the two keys in the order of the second key, first key, and second key again, then specify three keys in that order with the proper rollover period. For example:

```
key chain ldp-pwd
 key 1
   key-string firstpass
   accept-lifetime 00:03:00 Sep 10 2007 01:10:00 Sep 10 2007
   send-lifetime 00:05:00 Sep 10 2007 01:08:00 Sep 10 2007
 key 2
   key-string secondpass
   accept-lifetime 01:06:00 Sep 10 2007 01:17:00 Sep 10 2007
   send-lifetime 01:08:00 Sep 10 2007 01:15:00 Sep 10 2007
 key 3
   key-string firstpass
   accept-lifetime 01:13:00 Sep 10 2007 infinite
   send-lifetime 01:15:00 Sep 10 2007 infinite
```

Additional References

The following sections provide references related to the MPLS LDP--Lossless MD5 Session Authentication feature.

Related Documents

Related Topic	Document Title
MPLS Label Distribution Protocol (LDP)	MPLS Label Distribution Protocol
LDP implementation enhancements for the MD5 password	MPLS LDP MD5 Global Configuration

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

RFC	Title
No new or modified RFCs are supported by this release.	--

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--Lossless MD5 Session Authentication

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 7 Feature Information for MPLS LDP--Lossless MD5 Session Authentication

Feature Name	Releases	Feature Information
MPLS LDP-Lossless MD5 Session Authentication	12.0(33)S 12.2(33)SRC 12.2(33)SB 12.4(20)T	This feature allows an LDP session to be password-protected without tearing down and reestablishing the LDP session. This feature was introduced in Cisco IOS Release12.0(33)S. This feature was integrated into Cisco IOS Release 12.2(33)SRC. This feature was integrated into Cisco IOS Release12.2(33)SB. This feature was integrated ino Cisco IOS Release12.4(20)T. The following commands were introduced or modified: **mpls ldp logging password configuration**, **mpls ldp logging password rollover**, **mpls ldp neighbor password**, **mpls ldp password fallback**, **mpls ldp password option**, **mpls ldp password required**, **mpls ldp password rollover duration**, **show mpls ldp discovery**, **show mpls ldp neighbor**, **show mpls ldp neighbor password**.

MPLS LDP-VRF-Aware Static Labels

This document explains how to configure the MPLS LDP--VRF-Aware Static Labels feature and Multiprotocol Label Switching (MPLS) static labels. Virtual Private Network routing and forwarding (VRF)-aware static labels can be used at the edge of an MPLS Virtual Private Network (VPN), whereas MPLS static labels can be used only in the MPLS VPN provider core.

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.

Information About

To configure and use VRF-aware static labels, you should understand the following concepts:

Overview of MPLS Static Labels and MPLS LDP--VRF-Aware Static Labels

Label switch routers (LSRs) dynamically learn the labels they should use to label-switch packets by means of the following label distribution protocols:

- Label Distribution Protocol (LDP), the Internet Engineering Task Force (IETF) standard used to bind labels to network addresses
- Resource Reservation Protocol (RSVP) used to distribute labels for traffic engineering (TE)

- Border Gateway Protocol (BGP) used to distribute labels for MPLS VPNs

The LSR installs the dynamically learned label into its Label Forwarding Information Base (LFIB).

You can configure static labels for the following purposes:

- To bind labels to IPv4 prefixes to support MPLS hop-by-hop forwarding through neighbor routers that do not implement LDP label distribution. MPLS static labels allow you to configure entries in the MPLS forwarding table and assign label values to forwarding equivalence classes (FECs) learned by LDP. You can manually configure an LSP without running an LDP between the endpoints.
- To create static cross connects to support MPLS label switched path (LSP) midpoints when neighbor routers do not implement the LDP or RSVP label distribution, but do implement an MPLS forwarding path.
- To statically bind a VRF-aware label on a provider edge (PE) router to a customer network prefix (VPN IPv4 prefix). VRF-aware static labels can be used with nonglobal VRF tables, so the labels can be used at the VPN edge. For example, with the Carrier Supporting Carrier (CSC) feature, the backbone carrier can assign specific labels to FECs it advertises to the edge routers of customer carriers. Then, backbone carrier can monitor backbone traffic coming from particular customer carriers for billing or other purposes. Depending on how you configure VRF-aware static labels, they are advertised one of the following ways:
  - By LDP between PE and customer edge (CE) routers within a VRF instance
  - In VPNv4 BGP in the service provider's backbone

Labels Reserved for Static Assignment

Before you can manually assign labels, you must reserve a range of labels to be used for the manual assignment. Reserving the labels ensures that the labels are not dynamically assigned. If you are running Cisco IOS Release 12.0S or an older release, you may need to reload the router for the range of labels you reserve to take effect.

How to Configure MPLS LDP--VRF-Aware Static Labels

Reserving Labels to Use for MPLS Static Labels and MPLS LDP--VRF-Aware Static Labels

The following procedure explains how to reserve the labels that are to be statically assigned so that the labels are not dynamically assigned.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls label range** *minimum-value maximum-value* [**static** *minimum-static-value maximum-static-value*]
4. **end**
5. **show mpls label range**

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	**mpls label range** *minimum-value maximum-value* [**static** *minimum-static-value maximum-static-value*] **Example:** `Router(config)# mpls label range 200 100000 static 16 199`	Reserves a range of labels for static labels assignment. The default is that no labels are reserved for static assignment. **Note** You might need to reload the router for the range of labels you reserve to take effect.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode.
Step 5	**show mpls label range** **Example:** `Router# show mpls label range`	Displays information about the range of values for local labels, including those available for static assignment.

Configuring MPLS Static Labels in the MPLS VPN Provider Core

MPLS static labels allow you to configure entries in the MPLS forwarding table and assign label values to FECs learned by LDP. You can manually configure an LSP without running a label distribution protocol

between the endpoints. In MPLS VPN networks, static labels can be used only in the MPLS VPN provider core.

- Globally enable MPLS on each LSR.
- Enable Cisco Express Forwarding on each LSR.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls static binding ipv4** *prefix mask* {*label* | **input** *label* | **output** *nexthop* {**explicit-null** | **implicit-null** | *label*}}
4. **end**
5. **show mpls static binding ipv4**
6. **show mpls forwarding-table**

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 and returns to privileged EXEC mode.
Step 3	**mpls static binding ipv4** *prefix mask* {*label* | **input** *label* | **output** *nexthop* {**explicit-null** | **implicit-null** | *label*}} **Example:** `Router(config)# mpls static binding ipv4 10.2.2.0 255.255.255.255 input 17`	Specifies static binding of labels to IPv4 prefixes. Specified bindings are installed automatically in the MPLS forwarding table as routing demands.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show mpls static binding ipv4** **Example:** `Router# show mpls static binding ipv4`	Displays the configured static labels.
Step 6	**show mpls forwarding-table** **Example:** `Router# show mpls forwarding-table`	Displays the static labels used for MPLS forwarding.

Configuring MPLS Static Cross Connects

You can configure MPLS static cross connects to support MPLS LSP midpoints when neighbor routers do not implement either the LDP or RSVP label distribution, but do implement an MPLS forwarding path.

- Globally enable MPLS on each LSR.
- Enable Cisco Express Forwarding on each LSR.

Note

- MPLS static cross connect functionality is supported in Cisco IOS Releases 12.0(23)S and 12.3(14)T and later releases. It is not supported in Cisco IOS Release 12.4(20)T.
- MPLS static cross-connect labels remain in the LFIB even if the router to which the entry points goes down.
- MPLS static cross-connect mappings remain in effect even with topology changes.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls static crossconnect** *inlabel out-interface nexthop* {*outlabel* | **explicit-null** | **implicit-null**}
4. **end**
5. **show mpls static crossconnect**

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	**mpls static crossconnect** *inlabel out-interface nexthop* {*outlabel* | **explicit-null** | **implicit-null**} **Example:** `Router(config)# mpls static crossconnect 45 pos5/0 45 explicit-null`	Specifies static cross connects. **Note** The *nexthop* argument is required for multiaccess interfaces.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show mpls static crossconnect** **Example:** `Router# show mpls static crossconnect`	Displays the configured static cross connects.

Configuring MPLS LDP--VRF-Aware Static Labels at the Edge of the VPN

You can statically bind a VRF-aware label on a PE router to a customer network prefix (VPN IPv4 prefix). VRF-aware static labels can be used with nonglobal VRF tables, so the labels can be used at the VPN edge.

Restrictions

- Globally enable MPLS on each LSR.
- Enable Cisco Express Forwarding on each LSR.

- Ensure the MPLS VPN is configured. See MPLS VPN Carrier Supporting Carrier Using LDP and IGP for information about configuring the VPN and VRFs.
- Ensure that the provider network has MPLS LDP installed and running. See MPLS VPN Carrier Supporting Carrier Using LDP and IGP for information about configuring LDP.

Note The MPLS LDP-VRF-Aware Static Labels feature is supported only with MPLS VPN Carrier Supporting Carrier networks that use MPLS LDP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls static binding ipv4 vrf** *vpn-name prefix mask* {**input** *label* | *label*}
4. **end**
5. **show mpls static binding ipv4 vrf** *vpn-name*

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	**mpls static binding ipv4 vrf** *vpn-name prefix mask* {**input** *label* | *label*} **Example:** `Router(config)# mpls static binding ipv4 vrf vpn100 10.2.0.0 255.255.0.0 input 17`	Binds a prefix to a local label. Specified bindings are installed automatically in the MPLS forwarding table as routing demands. **Note** You must configure the MPLS VPN and VRFs before creating VRF-aware static labels.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show mpls static binding ipv4 vrf** *vpn-name* **Example:** `Router(config)# show mpls static binding ipv4 vrf vpn100`	Displays the configured MPLS static bindings.

Troubleshooting Tips

To display information related to static binding events, use the **debug mpls static binding vrf** command.

Configuration Examples for MPLS LDP--VRF-Aware Static Labels

Reserving Labels to Use for MPLS Static Labels and MPLS LDP--VRF-Aware Static Labels Example

In the following example, the mpls label range command reserves a generic range of labels from 200 to 100000 and configures a static label range of 16 to 199:

```
Router(config)# mpls label range 200 100000 static 16 199
% Label range changes take effect at the next reload.
```

In this example, the output from the **show mpls label range** command indicates that the new label ranges do not take effect until a reload occurs:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 16/100000
   [Configured range for next reload: Min/Max label: 200/100000]
Range for static labels: Min/Max/Number: 16/199
```

In the following output, the **show mpls label range** command, executed after a reload, indicates that the new label ranges are in effect:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 200/100000
Range for static labels: Min/Max/Number: 16/199
```

Configuring MPLS Static Labels in the MPLS VPN Provider Core Example

The following example configures input and output labels for several prefixes:

```
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.0.0.66 167
Router(config)# mpls static binding ipv4 10.66.0.0 255.255.0.0 input 17
```

```
Router(config)# mpls static binding ipv4 10.66.0.0 255.255.0.0 output 10.13.0.8 explicit-
null
```

The **show mpls static binding ipv4** command displays the configured static labels:

```
Router# show mpls static binding ipv4

10.0.0.0/8: Incoming label: 55
  Outgoing labels:
      10.0.0.66   167
10.66.0.0/24: Incoming label: 17
  Outgoing labels:
     10.13.0.8  explicit-null
```

Configuring MPLS Static Cross Connects Example

In the following example, the mpls static crossconnect command configures a cross connect from incoming label 45 to outgoing label 46 on the POS interface 5/0:

```
Router(config)# mpls static crossconnect 45 pos5/0 46
```

The show mpls static crossconnect command displays information about cross connects that have been configured:

```
Router# show mpls static crossconnect
Local  Outgoing    Outgoing   Next Hop
label  label       interface
45     46          pos5/0     point2point  (in LFIB)
```

Configuring MPLS LDP--VRF-Aware Static Labels at the VPN Edge Example

In the following example, the **mpls static binding ipv4 vrf** commands configure static label bindings. They also configure input (local) labels for various prefixes.

```
Router(config)# mpls static binding ipv4 vrf vpn100 10.0.0.0 10.0.0.0 55
Router(config)# mpls static binding ipv4 vrf vpn100 10.66.0.0 255.255.0.0 input 17
```

In the following output, the **show mpls static binding ipv4 vrf** command displays the configured VRF-aware static bindings:

```
Router# show mpls static binding ipv4 vrf vpn100
10.0.0.0/8:   (vrf: vpn100)  Incoming label: 55
  Outgoing labels:  None
10.66.0.0/16:   (vrf: vpn100)  Incoming label: 17
  Outgoing labels:  None
```

Additional References

The following sections provide references related to the MPLS LDP--VRF-Aware Static Labels feature.

Related Documents

Related Topic	Document Title
MPLS VPN CSC with LDP and IGP	MPLS VPN Carrier Supporting Carrier Using LDP and IGP

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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

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

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

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, use the Command Lookup Tool at http://tools.cisco.com/

Support/CLILookup or the *Cisco IOS Master Command List, All Releases* , at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html .

- **debug mpls static binding**
- **mpls label range**
- **mpls static binding ipv4**
- **mpls static binding ipv4 vrf**
- **show mpls label range**
- **show mpls static binding ipv4**
- **show mpls static binding ipv4 vrf**

Feature Information for MPLS LDP--VRF-Aware Static Labels

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 8 Feature Information for MPLS LDP--VRF-Aware Static Labels

Feature Name	Releases	Feature Information
MPLS LDP-VRF-Aware Static Labels	12.0(23)S 12.0(26)S 12.3(14)T 12.2(33)SRA 12.2(33)SXH 12.2(33)SB	The MPLS LDP-VRF-Aware Static Labels feature explains how to configure the MPLS LDP--VRF-Aware Static Labels feature and MPLS static labels. VVRF-aware static labels can be used at the edge of an MPLS VPN, whereas MPLS static labels can be used only in the MPLS VPN provider core. In 12.0(23)S, MPLS static labels were introduced, but they supported only global routing tables. In 12.0(26)S, the MPLS LDP--VRF-Aware Static Labels feature was introduced, allowing MPLS static labels to be used for VRF traffic at the VPN edge. In 12.3(14)T, this feature was integrated. In 12.2(33)SRA, this feature was integrated. In 12.2(33)SXH, this feature was integrated. In 12.2(33)SB, support was added for the Cisco 10000 series router.