MPLS Label Distribution Protocol Configuration Guide, Cisco IOS Release 12.2SY

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for MPLS LDP

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 global configuration command **mpls label protocol tdp**. 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, page 3
- Nondirectly Connected MPLS LDP Sessions, page 4

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 LPD 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 LPD 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, page 6

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**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

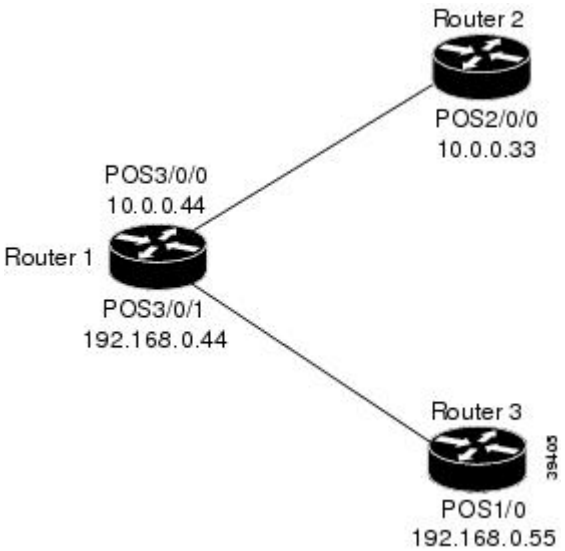
Configuring Directly Connected MPLS LDP Sessions Example

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
```

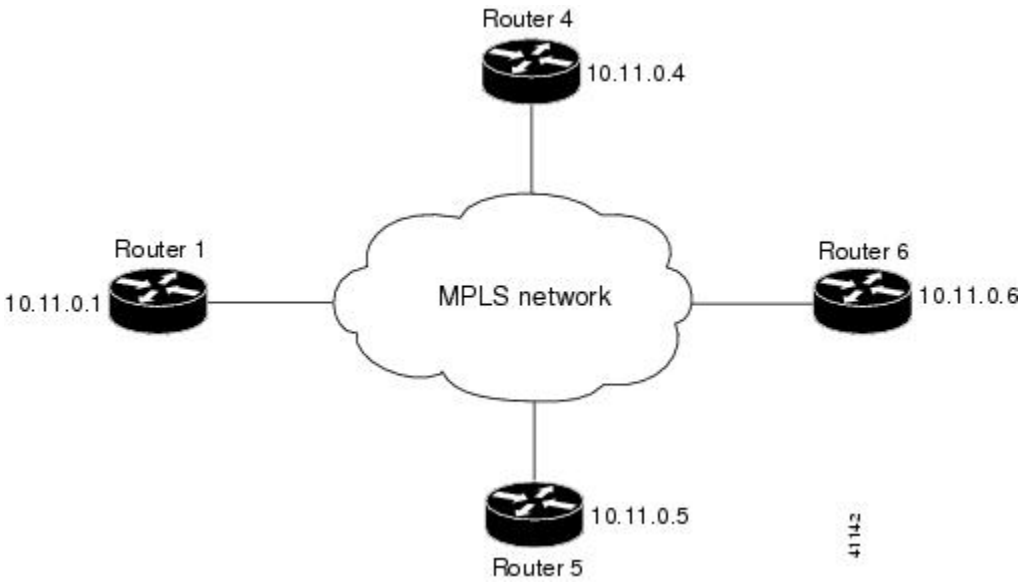
The configuration of Router 2 also uses the **mpls label protocol ldp**command in interface configuration mode. To specify LDP for all interfaces, use the **mpls label protocol ldp**command in global configuration mode without any interface **mpls label protocol** commands.

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 tdp**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
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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

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

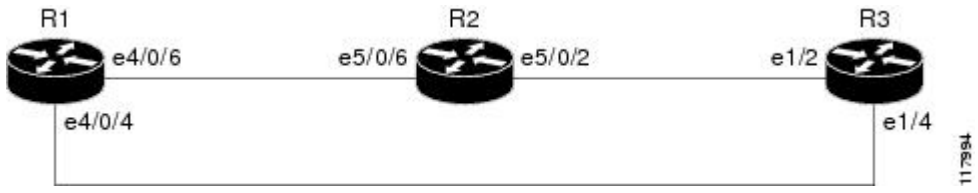
Use the **clear mpls ldp neighbor** command if you need to terminate an LDP session after a link goes down. This is useful for situations where the link needs to be taken out of service or needs to be connected to a different neighbor.

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-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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

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* argumentis 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 3 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.

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

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:** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip access-list standard** *access-list-number* **Example:** **Example:** `Router(config)# ip access-list standard 1`	Defines a standard IP access list with a number.
Step 4	**permit** {*source* [*source-wildcard*] | **any**} [**log**] **Example:** **Example:** `Router(config-std-nacl)# permit 10.0.0.0`	Specifies one or more prefixes permitted by the access list.
Step 5	**exit** **Example:** **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:** **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 access-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 access-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 4 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.