MPLS Label Distribution Protocol Configuration Guide, Cisco IOS Release 15SY

First Published: October 15, 2012

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

CHAPTER 1

MPLS Label Distribution Protocol

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for MPLS Label Distribution Protocol

Label switching on a device requires that Cisco Express Forwarding be enabled on that device.

Information About MPLS Label Distribution Protocol

Introduction to MPLS Label Distribution Protocol

MPLS Label Distribution Protocol (LDP) provides the means for label switch devices (LSRs) to request, distribute, and release label prefix binding information to peer devices 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.

Multiprotocol Label Switching (MPLS) LDP enables one LSR to inform another LSR of the label bindings it has made. Once a pair of devices 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 device the device 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 device the device 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 Label Distribution Protocol Functional Overview

Cisco Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) provides the building blocks for MPLS-enabled applications, such as MPLS 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 (LIPS), 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

On supported hardware platforms and software releases, the Label Distribution Protocol (LDP) supercedes Tag Distribution Protocol (TDP). See the table below for information about LDP and TDP support in Cisco software releases.

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

Table 1: LDP and TDP Support

Train and Release	LDP and 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.
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 Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), the label switch routers (LSRs) send out messages to try to find other LSRs with which they can create LDP sessions. The following sections explain the differences between directly connected LDP sessions and nondirectly connected LDP sessions.

Directly Connected MPLS LDP Sessions

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

To initiate an LDP session between devices, the devices determine which device will take the active role and which device will take the passive role. The device 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 devices compare their transport addresses. The device 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.

Nondirectly Connected MPLS LDP Sessions

If the label switch router (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 User Datagram Protocol (UDP) packet, but as a unicast message specifically addressed to that LSR. The nondirectly connected LSR responds to the Hello message and the two devices begin to establish a Label Distribution Protocol (LDP) session. This is called extended discovery.

A Multiprotocol Label Switching (MPLS) LDP targeted session is a label distribution session between devices 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 devices. 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 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 links 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, and there is an alternate route between neighbors, the targeted Hellos would 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:

- Device 1 sends targeted Hello messages carrying a response request to Device 2. Device 2 sends targeted Hello messages in response if its configuration permits. In this situation, Device 1 is considered to be active and Device 2 is considered to be passive.
- Device 1 and Device 2 both send targeted Hello messages to each other. Both devices are considered to be active. Both, one, or neither device 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.

Introduction to LDP Label Bindings Label Spaces and LDP Identifiers

A Label Distribution Protocol (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 label switch router (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 device determines the LDP router ID as follows, if the **mpls ldp router-id** command is not executed,

1. The device examines the IP addresses of all operational interfaces.
2. If these IP addresses include loopback interface addresses, the device selects the largest loopback address as the LDP router ID.
3. Otherwise, the device 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 device might select an IP address as the LDP router ID that the routing protocol cannot advertise to a neighboring device. 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 device 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 Label Distribution Protocol

Enabling Directly Connected LDP Sessions

This procedure explains how to configure Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) sessions between two directly connected devices.

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls ip** **Example:** `Device(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 device interfaces. You must enable MPLS forwarding on the interfaces as well as for the device.
Step 4	**mpls label protocol** [**ldp** | **tdp** | **both**] **Example:** `Device(config)# mpls label protocol ldp`	Configures the use of LDP on all interfaces. • The keywords that are available depend on the hardware platform. • 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	**interface** *type number* **Example:** `Device(config)# interface fastethernet 0/3/0`	Specifies the interface to be configured and enters interface configuration mode.
Step 6	**mpls ip** **Example:** `Device(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 device.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 8	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
Step 9	**show mpls interfaces** [*interface*] [**detail**] **Example:** `Device# show mpls interfaces`	Verifies that the interfaces have been configured to use LDP.
Step 10	**show mpls ldp discovery** [**all** | **vrf** *vpn-name*] [**detail**] **Example:** `Device# show mpls ldp discovery`	Verifies that the interface is up and is sending Discovery Hello messages.
Step 11	**show mpls ldp neighbor** [[**vrf** *vpn-name*] [*address* | *interface*] [**detail**] | **all**] **Example:** `Device# show mpls ldp neighbor`	Displays the status of LDP sessions.

Examples

The following **show mpls interfaces** command verifies that interfaces FastEthernet 0/3/0 and 0/3/1 have been configured to use LDP:

```
Device# show mpls interfaces
Interface                 IP            Tunnel   BGP Static Operational
FastEthernet0/3/0         Yes (ldp)     No       No  No     Yes
FastEthernet0/3/1         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):

```
Device# show mpls ldp discovery
Local LDP Identifier:
    172.16.12.1:0
    Discovery Sources:
    Interfaces:
        FastEthernet0/3/0 (ldp): xmit
```

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

```
Device# 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:
FastEthernet0/1/0, 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
```

Establishing Nondirectly Connected MPLS LDP Sessions

This section explains how to configure nondirectly connected MPLS Label Distribution Protocol (LDP) sessions, which enable you to establish an LDP session between devices that are not directly connected.

Before You Begin

- Multiprotocol Label Switching (MPLS) requires Cisco Express Forwarding.
- You must configure the devices at both ends of the tunnel to be active or enable one device 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 tunnel** *number*
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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls ip** **Example:** `Device(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 device interfaces. You must enable MPLS forwarding on the interfaces as well as for the device.

	Command or Action	Purpose
Step 4	**mpls label protocol** [**ldp** | **tdp** | **both**] **Example:** `Device(config)# mpls label protocol ldp`	Configures the use of LDP on all interfaces. • The keywords that are available depend on the hardware platform. • 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	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 1`	Configures a tunnel interface and enters interface configuration mode.
Step 6	**tunnel destination** *ip-address* **Example:** `Device(config-if)# tunnel destination 172.16.1.1`	Assigns an IP address to the tunnel interface.
Step 7	**mpls ip** **Example:** `Device(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 device.
Step 8	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 9	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 10	**show mpls ldp discovery** [**all** | **vrf** *vpn-name*] [**detail**] **Example:** `Device# show mpls ldp discovery`	Verifies that the interface is up and is sending Discovery Hello messages.

Examples

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

```
Device# show mpls ldp discovery
Local LDP Identifier:
          172.16.0.0:0
Discovery Sources:
Interfaces:
POS1/2/0 (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 (ldp): passive, xmit/recv
LDP Id: 192.168.0.0:0
```

This command output indicates that:

- The local label switch router (LSR) (172.16.0.0) sent LDP link Hello messages on interface POS1/2/0 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 Tag Distribution Protocol (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.

Saving Configurations MPLS Tag Switching Commands

In releases prior to Cisco IOS Release 12.4(2)T, some Multiprotocol Label Switching (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:

```
Device(config)# interface ATM 3/0
Device(config-if)# ip unnumbered Loopback0
Device(config-if)# tag-switching ip
Device(config-if)# mpls label protocol ldp
```

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

```
interface ATM 3/0
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 device considers all the IP addresses of all operational interfaces.
2. If these addresses include loopback interface addresses, the device selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the device, because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each device 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 device selects the largest interface address.

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

The device 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 Multiprotocol Label Switching (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.

Before You Begin

Make sure the specified interface is operational before assigning it as the Label Distribution Protocol (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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls ip** **Example:** `Device(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 device interfaces. You must enable MPLS forwarding on the interfaces as well as for the device.
Step 4	**mpls label protocol** [**ldp** | **tdp** | **both**] **Example:** `Device(config)# mpls label protocol ldp`	Configures the use of LDP on all interfaces. • The keywords that are available depend on the hardware platform.

	Command or Action	Purpose
		• 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:** `Device(config)# mpls ldp router-id pos 2/0/0`	Specifies the preferred interface for determining the LDP router ID.
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.
Step 7	**show mpls ldp discovery** [**all** | **detail** | **vrf** *vpn-name*] **Example:** `Device# show mpls ldp discovery`	Displays the LDP identifier for the local device.

Example

The following example assigns interface pos 2/0/0 as the LDP router ID:

```
Device> enable
Device# configure terminal
Device(config)# mpls ip
Device(config)# mpls label protocol ldp
Device(config)# mpls ldp router-id pos 2/0/0 force
```

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

```
Device# show mpls ldp discovery
Local LDP Identifier:
    10.15.15.15:0
Discovery Sources:
    Interfaces:
        FastEthernet0/3/0 (ldp): xmit/recv
            LDP Id: 10.14.14.14:0
```

Preserving QoS Settings with MPLS LDP Explicit Null

Normally, the Label Distribution Protocol (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 Multiprotocol Label Switching (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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls ip** **Example:** `Device(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 device interfaces. You must enable MPLS forwarding on the interfaces as well as for the device.

	Command or Action	Purpose
Step 4	**mpls label protocol** [**ldp** | **tdp** | **both**] **Example:** `Device(config)# mpls label protocol ldp`	Configures the use of LDP on all interfaces. • The keywords that are available depend on the hardware platform. • 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	**interface** *type number* **Example:** `Device(config)# interface atm 2/2/0`	Specifies the interface to be configured and enters interface configuration mode.
Step 6	**mpls ip** **Example:** `Device(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 device.
Step 7	**exit** **Example:** `Device(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:** `Device(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:** `Device(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:** `Device# 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 devices.

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

If you issue the **show mpls forwarding-table** command on an adjacent device, 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".

```
Device# 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 devices' 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.

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

If you issue the **show mpls forwarding-table** command on an adjacent device, 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.

```
Device# 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 devices specified in the access-list. To advertise explicit-null to a particular device, you must specify the device'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 device. The device that is configured with explicit null advertises explicit-null labels only to that adjacent device.

```
Device# show mpls ldp discovery

Local LDP Identifier:
    10.15.15.15:0
Discovery Sources:
    Interfaces:
```

```
        FastEthernet2/0/0(ldp): xmit/recv
            TDP Id: 10.14.14.14:0
Device# configure terminal
Device(config)# mpls label protocol ldp
Device(config)# access-list 15 permit host 10.15.15.15
Device(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 device specified in the access list.

```
Device# 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 devices to advertise these explicit-null labels.

```
Device# show access 15

Standard IP access list 15
     permit 10.15.15.15 (7 matches)
Device# show access 24

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

If you issue the **show mpls forwarding-table** command, the output shows that it receives explicit null labels for 10.24.24.24/32.

```
Device# 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          Fe2/0/0        172.16.0.1
20     Pop tag     172.16.0.0/8       0          Fe2/0/0        172.16.0.1
21     20          10.12.12.12/32     0          Fe2/0/0        172.16.0.1
22     16          10.0.0.0/8         0          Fe2/0/0        172.16.0.1
23     21          10.13.13.13/32     0          Fe2/0/0        172.16.0.1
25     Pop tag     10.14.14.14/32     0          Fe2/0/0        172.16.0.1
27     Pop tag     192.168.0.0/8      0          Fe2/0/0        172.16.0.1
28     25          10.16.16.16/32     0          Fe2/0/0        172.16.0.1
29     Pop tag     192.168.34.34/32   0          Fe2/0/0        172.16.0.1
```

Protecting Data Between LDP Peers with MD5 Authentication

You can enable authentication between two Label Distribution Protocol (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 password** command. This causes the device 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 device tears down existing LDP sessions and establishes new sessions with the neighbor.

If a device has a password configured for a neighbor, but the neighboring device does not have a password configured, a message such as the following appears on the console who has a password configured while the two devices 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 device's IP address](646)

Similarly, if the two devices 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 device'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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls ip** **Example:** `Device(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 device interfaces. You must enable MPLS forwarding on the interfaces as well as for the device.

	Command or Action	Purpose
Step 4	**mpls label protocol** [**ldp** | **tdp** | **both**] **Example:** `Device(config)# mpls label protocol ldp`	Configures the use of LDP on all interfaces. • The keywords that are available depend on the hardware platform. • 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 neighbor** [**vrf** *vpn-name*] *ip-address* [**password** [**0-7**] *password-string*] **Example:** `Device(config)# mpls ldp neighbor 172.27.0.15 password onethirty9`	Specifies authentication between two LDP peers.
Step 6	**exit** **Example:** `Device(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:** `Device# 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 device with the password cisco:

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

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

```
Device# 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:
FastEthernet1/0/0, 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 is used for the LDP session.

```
Device# 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:
          FastEthernet1/1/0; 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
```

Configuration Examples for MPLS Label Distribution Protocol

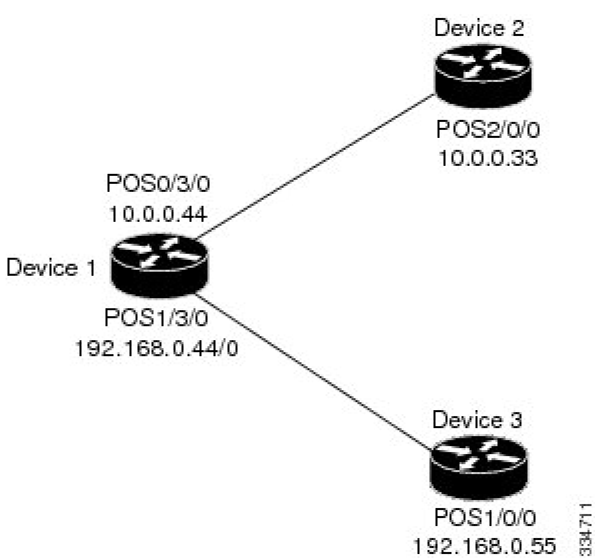
Example: Configuring Directly Connected MPLS LDP Sessions

The figure below shows a sample network for configuring directly connected Label Distribution Protocol (LDP) sessions.

This example configures the following:

- Multiprotocol Label Switching (MPLS) hop-by-hop forwarding for the POS links between Device 1 and Device 2 and between Device 1 and Device 3.
- LDP for label distribution between Device 1 and Device 2.
- LDP for label distribution between Device 1 and Device 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 Device 1, Device 2, and Device 3 in the sample network shown in the figure above.

Device 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 POS0/3/0
ip address 10.0.0.44 255.0.0.0
mpls ip                                               !Enable hop-by-hop MPLS forwarding
mpls label protocol ldp
!
interface POS1/3/0
ip address 192.168.0.44 255.0.0.0
mpls ip                                               !Enable hop-by-hop MPLS forwarding
mpls label protocol ldp
```

Device 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
```

Device 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 POS1/0/0
ip address 192.168.0.55 255.0.0.0
mpls ip                                                !Enable hop-by-hop MPLS forwarding
mpls label protocol ldp
```

The LDP configuration for Device 1 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.

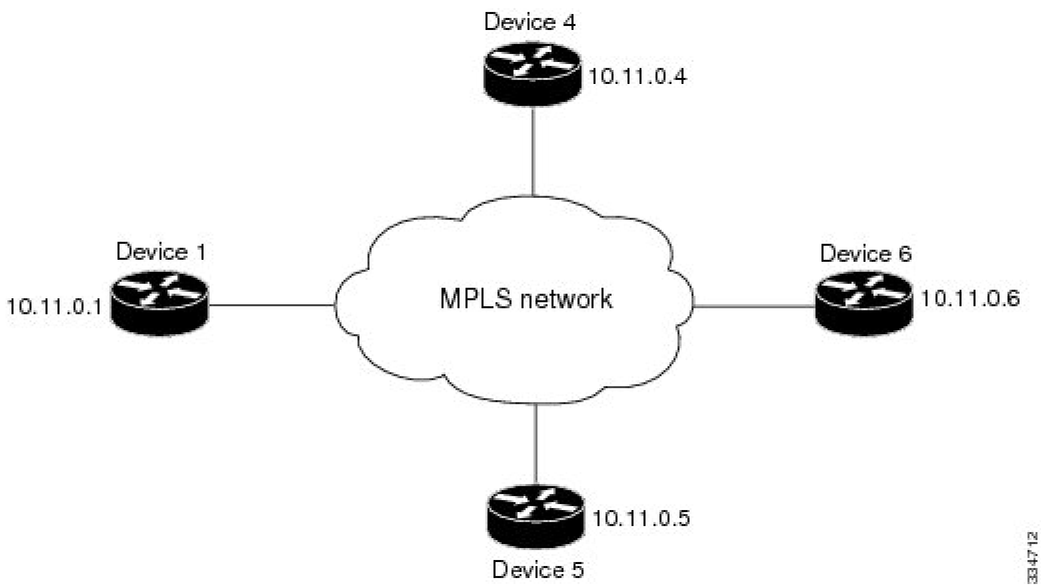
The configuration of Device 2 also uses the **mpls label protocol ldp** command in interface configuration mode. To specify LDP for all interfaces, use the **mpls label protocol ldp** command in global configuration mode without any interface **mpls label protocol** commands.

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

Example: Establishing Nondirectly Connected MPLS LDP Sessions

The following examples illustrate the configuration of platforms for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) nondirectly connected sessions using the sample network shown in the figure below. Note that Devices 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 Devices 1 and 4 use LDP. Devices 1 and 4 are both active.
- Targeted sessions between Devices 1 and 6 use LDP. Device 1 is active and Device 6 is passive.
- Targeted sessions between Devices 1 and 5 use LDP. Device 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.

Device 1 Configuration

Tunnel interfaces Tunnel14 and Tunnel16 specify LDP for targeted sessions associated with these interfaces. The targeted session for Device 5 requires LDP. 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             !Device1 supports distributed CEF
mpls label protocol ldp       !Use LDP for all interfaces
interface Loopback0            !Loopback interface for LDP ID.
ip address 10.25.0.11 255.255.255.255
interface Tunnel14             !Tunnel to Device 4 requiring label distribution
tunnel destination 10.11.0.4  !Tunnel endpoint is Device 4
```

```
mpls ip                        !Enable hop-by-hop forwarding on the interface
interface Tunnel15             !Tunnel to Device 5 requiring label distribution
tunnel destination 10.11.0.5  !Tunnel endpoint is Device 5
mpls label protocol ldp        !Use LDP for session with Device 5
mpls ip                        !Enable hop-by-hop forwarding on the interface
interface Tunnel16             !Tunnel to Device 6 requiring label distribution
tunnel destination 10.11.0.6  !Tunnel endpoint is Device 6
mpls ip                        !Enable hop-by-hop forwarding on the interface
```

Device 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 Device 1.

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

Device 5 Configuration

Device 5 uses LDP for all targeted sessions. Therefore, its configuration includes the **mpls label protocol ldp** command.

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

Device 6 Configuration

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

```
ip cef distributed                       !Device 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 Device 1.
deny any                                 !Deny requests from other sources.
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
Configures LDP on every interface associated with a specified IGP instance.	"MPLS LDP Autoconfiguration" module in the *MPLS Label Distribution Protocol Configuration Guide*
Ensures that LDP is fully established before the IGP path is used for switching.	"MPLS LDP IGP Synchronization" module in the *MPLS Label Distribution Protocol Configuration Guide*
Allows ACLs to control the label bindings that an LSR accepts from its peer LSRs.	"MPLS LDP Inbound Label Binding Filtering" module in the *MPLS Label Distribution Protocol Configuration Guide*
Enables standard, SNMP-based network management of the label switching features.	"MPLS Label Distribution Protocol MIB Version 8 Upgrade" module in the *MPLS Embedded Management and MIBs Configuration Guide*

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mib

RFCs

RFC	Title
RFC 3036	*LDP Specification*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

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

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) Cisco IOS XE Release 2.1	

Feature Name	Releases	Feature Information
		MPLS Label Distribution Protocol (LDP) enables peer label switch routers (LSRs) in an Multiprotocol Label Switching (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. This feature was introduced in Cisco IOS Release 12.0(10)ST, incorporating a new set of MPLS CLI commands implemented for use with Cisco devices. 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 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* keyword and argument in certain existing commands, and other commands were modified to ensure consistent interpretation of associated *prefix-access-list* arguments by Cisco 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** commands were 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**

Feature Name	Releases	Feature Information
		(global configuration), **mpls ldp router-id**

Feature Name	Releases	Feature Information

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. 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 rather than the tag-switching form. Previously,

Feature Name	Releases	Feature Information
		commands were saved by using the tag-switching form of the command, for backward compatibility. In Cisco IOS Release 12.4(5), the **vrf** *vrf-name* keyword and argument was added for the **mpls ldp router-id** command to allow you to associate the LDP router ID with a nondefault VRF. In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Router. The following commands were introduced or modified: **debug mpls atm-ldp failure**, **mpls label protocol** (global configuration), **mpls ldp advertise-labels**, **mpls ldp discovery**, **mpls ldp neighbor implicit-withdraw**, **mpls ldp neighbor targeted-session**, **mpls ldp router-id**.

CHAPTER 2

MPLS LDP Session Protection

The MPLS LDP Session Protection feature provides faster Label Distribution Protocol (LDP) convergence when a link recovers following an outage. MPLS LDP Session Protection protects an LDP session between directly connected neighbors or an LDP session established for a traffic engineering (TE) tunnel.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for MPLS LDP Session Protection

Label switch routers (LSRs) must be able to respond to Label Distribution Protocol (LDP) targeted hellos. Otherwise, the LSRs cannot establish a targeted adjacency. All devices that participate in MPLS LDP Session Protection must be enabled to respond to targeted hellos. Both neighbor devices must be configured for session protection or one device must be configured for session protection and the other device must be configured to respond to targeted hellos.

Restrictions for MPLS LDP Session Protection

The MPLS LDP Session Protection feature is not supported under the following circumstances:

- With extended access lists
- With LC-ATM devices
- With Tag Distribution Protocol (TDP) sessions

Information About MPLS LDP Session Protection

How MPLS LDP Session Protection Works

MPLS LDP Session Protection maintains Label Distribution Protocol (LDP) bindings when a link fails. MPLS LDP sessions are protected through the use of LDP hello messages. When you enable Multiprotocol Label Switching (MPLS) LDP, the label switch 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 devices on the subnet. The hello message is called an LDP Link Hello. A neighboring LSR responds to the hello message, and the two devices begin to establish an LDP session.

If the LSR is more than one hop from its neighbor, it is not directly connected to its neighbor. The LSR sends out a directed hello message as a UDP packet but as a unicast message specifically addressed to that specific LSR. The hello message is called an LDP Targeted Hello. The nondirectly connected LSR responds to the Hello message and the two devices establish an LDP session. (If the path between two LSRs has been traffic engineered and has LDP enabled, the LDP session between them is called a targeted session.)

MPLS LDP Session Protection uses LDP Targeted Hellos to protect LDP sessions. For example, two directly connected devices have LDP enabled and can reach each other through alternate IP routes in the network. An LDP session that exists between two devices 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 devices 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 devices. When the directly connected link recovers, the session does not need to be reestablished, and LDP bindings for prefixes do not need to be relearned.

MPLS LDP Session Protection Customization

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

How Long an LDP Targeted Hello Adjacency Should Be Retained

The default behavior of the **mpls ldp session protection** command allows a Label Distribution Protocol (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 that the LDP Targeted Hello Adjacency is retained after the loss of the LDP Link Hello Adjacency. When the link is lost, a timer starts. If the timer expires, the LDP Targeted Hello Adjacency is removed.

Which Devices Should Have MPLS LDP Session Protection

The default behavior of the **mpls ldp session protection** command allows MPLS LDP Session Protection for all neighbor sessions. You can issue either the **vrf** or **for** keyword to limit the number of neighbor sessions that are protected:

- You can use the **vrf** keyword to select which virtual routing and forwarding (VRF) instance is to be protected if the device is configured with at least one virtual private network (VPN) VRF instance. You cannot specify more than one VRF with the **mpls ldp session protection** command. To specify multiple VRFs, issue the command multiple times.
- You can create an access list that includes several peer devices. You can specify that access list with the **for** keyword to enable LDP Session Protection for the peer devices in the access control list.

How to Configure MPLS LDP Session Protection

Enabling MPLS LDP Session Protection

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip cef** [**distributed**] **Example:** `Device(config)# ip cef distributed`	Configures distributed Cisco Express Forwarding or Cisco Express Forwarding.
Step 4	**interface loopback** *number* **Example:** `Device(config)# interface Loopback 0`	Configures a loopback interface and enters interface configuration mode.
Step 5	**ip address** *prefix mask* **Example:** `Device(config-if)# ip address 10.25.0.11 255.255.255.255`	Assigns an IP address to the loopback interface.
Step 6	**exit** **Example:** `Device(config-if) exit`	Returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface POS 0/3/0`	Specifies the interface to configure and enters interface configuration mode.
Step 8	**mpls ip** **Example:** `Device(config-if)# mpls ip`	Configures MPLS hop-by-hop forwarding for the specified interface.
Step 9	**mpls label protocol** [**ldp** | **tdp** | **both**]	Configures the use of LDP on a specific interface or on all interfaces.

	Command or Action	Purpose
	Example: `Device(config-if)# mpls label protocol ldp`	• The keywords that are available depend on the hardware platform. • 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 10	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 11	**mpls ldp session protection** [**vrf** *vpn-name*] [**for** *acl*] [**duration** {**infinite** | *seconds*}] **Example:** `Device(config)# mpls ldp session protection`	Enables MPLS LDP session protection. • The **vrf** *vpn-name* keyword and argument protects Label Distribution Protocol (LDP) sessions for a specified virtual routing and forwarding (VRF) interface. • The **for** *acl* keyword and argument specifies a standard IP access control list (ACL) of prefixes to be protected. • The **duration** keyword specifies how long the device should retain the LDP Targeted Hello Adjacency following the loss of the LDP Link Hello Adjacency. • The **infinite** keyword specifies that the LDP Targeted Hello Adjacency should be retained forever after a link is lost. • The *seconds* argument specifies the time in seconds that the LDP Targeted Hello Adjacency should be retained after a link is lost. The range is 30 to 2,147,483 seconds. The **mpls ldp session protection** command entered without a keyword protects all LDP sessions.
Step 12	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Troubleshooting Tips

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

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

Verifying MPLS LDP Session Protection

SUMMARY STEPS

1. **enable**
2. **show mpls ldp discovery**
3. **show mpls ldp neighbor**
4. **show mpls ldp neighbor detail**
5. **exit**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password, if prompted.

Example:

```
Device> enable
Device#
```

Step 2 **show mpls ldp discovery**

Verifies that the output contains the term xmit/recv for the peer device.

Example:

```
Device# show mpls ldp discovery

 Local LDP Identifier:
    10.0.0.5:0
    Discovery Sources:
    Interfaces:
        ATM50/1/0.5 (ldp): xmit/recv
            LDP Id: 10.0.0.1:0
    Targeted Hellos:
        10.0.0.5 -> 10.0.0.3 (ldp): active, xmit/recv
            LDP Id: 10.0.0.3:0
```

Step 3 **show mpls ldp neighbor**

Verifies that the targeted hellos are active.

Example:

```
Device# show mpls ldp neighbor

Peer LDP Ident: 10.0.0.3:0; Local LDP Ident 10.0.0.5:0
TCP connection: 10.0.0.3.646 - 10.0.0.5.11005
State: Oper; Msgs sent/rcvd: 1453/1464; Downstream
Up time: 21:09:56
LDP discovery sources:
 Targeted Hello 10.0.0.5 -> 10.0.0.3, active
Addresses bound to peer LDP Ident:
 10.3.104.3       10.0.0.2        10.0.0.3
```

Step 4 **show mpls ldp neighbor detail**

Verifies 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:

```
Device# show mpls ldp neighbor detail

    Peer LDP Ident: 10.16.16.16:0; Local LDP Ident 10.15.15.15:0
        TCP connection: 10.16.16.16.11013 - 10.15.15.15.646
        State: Oper; Msgs sent/rcvd: 53/51; Downstream; Last TIB rev sent 74
        Up time: 00:11:32; UID: 1; Peer Id 0;
        LDP discovery sources:
          Targeted Hello 10.15.15.15 -> 10.16.16.16, active, passive;
            holdtime: infinite, hello interval: 10000 ms
        Addresses bound to peer LDP Ident:
          10.0.0.2        10.16.16.16     10.101.101.101 11.0.0.1
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
        Clients: Dir Adj Client
        LDP Session Protection enabled, state: Protecting
            duration: infinite
```

Step 5 **exit**

Returns to user EXEC mode.

Example:

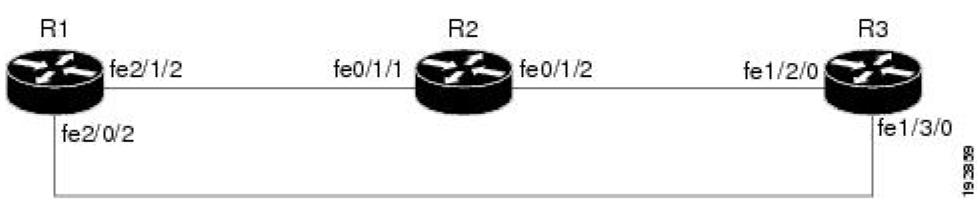
```
Device# exit
Device>
```

Configuration Examples for MPLS LDP Session Protection

Example: Configuring MPLS LDP Session Protection

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

Figure 3: MPLS LDP Session Protection Example



The following configuration examples for R1, R2, and R3 are based on the figure above.

R1

```
redundancy
 no keepalive-enable
```

```
 mode hsa
!
ip cef distributed
no ip domain-lookup
multilink bundle-name both
mpls label protocol ldp
mpls ldp session protection
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Multilink4
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 load-interval 30
 ppp multilink
 multilink-group 4
!
interface FastEthernet1/0/0
 ip address 10.3.123.1 255.255.0.0
 no ip directed-broadcast
!
interface FastEthernet2/0/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface FastEthernet2/0/1
 description --  ip address 10.0.0.2 255.255.255.0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface FastEthernet2/0/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet2/1/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet2/2/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 10.0.0.1 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
ip classless
```

R2

```
redundancy
 no keepalive-enable
```

```
 mode hsa
!
ip subnet-zero
ip cef distributed
mpls label protocol ldp
mpls ldp session protection
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.3 255.255.255.255
 no ip directed-broadcast
!
interface FastEthernet0/1/0
 no ip address
 no ip directed-broadcast
 shutdown
 full-duplex
!
interface FastEthernet0/1/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/1/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 ip load-sharing per-packet
 full-duplex
 mpls label protocol ldp
 mpls ip
!
interface FastEthernet0/2/0
 ip address 10.3.123.112 255.255.0.0
 no ip directed-broadcast
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 10.0.0.3 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
ip classless
```

R3

```
ip cef distributed
no ip domain-lookup
mpls label range 200 100000 static 16 199
mpls label protocol ldp
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.5 255.255.255.255
 no ip directed-broadcast
!
interface FastEthernet1/0/0
 no ip address
 no ip directed-broadcast
 shutdown
 half-duplex
!
interface FastEthernet1/2/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
```

```
 mpls ip
!
interface FastEthernet1/3/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 full-duplex
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 redistribute connected
 network 10.0.0.5 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
ip classless
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
MPLS LDP	"MPLS Label Distribution Protocol" module in the *MPLS Label Distribution Protocol Configuration Guide*
MPLS LDP IGP synchronization	"MPLS LDP IGP Synchronization" module in the *MPLS Label Distribution Protocol Configuration Guide*
MPLS LDP Autoconfiguration	"MPLS LDP Autoconfiguration" module in the *MPLS Label Distribution Protocol Configuration Guide*

MIBs

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

RFCs

RFCs	Title
RFC 3036	LDP Specification
RFC 3037	LDP Applicability

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MPLS LDP Session Protection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 3: Feature Information for MPLS LDP Session Protection

Feature Name	Releases	Feature Information
MPLS LDP Session Protection	12.0(30)S 12.2(27)SBA 12.2(33)SRA 12.2(33)SXH 12.3(14)T Cisco IOS XE Release 2.1	The MPLS LDP Session Protection feature provides faster Label Distribution Protocol (LDP) convergence when a link recovers following an outage. MPLS LDP Session Protection protects an LDP session between directly connected neighbors or an LDP session established for a traffic engineering (TE) tunnel. In Cisco IOS Release 12.0(30)S, this feature was introduced on the Cisco 7200 series routers. In Cisco IOS Release 12.2(27)SBA, this feature was implemented on the Cisco 10000 and 7500 series routers. In Cisco IOS Release 12.2(33)SRA, this feature was implemented on the Cisco 7600 series routers. In Cisco IOS Release 12.2(33)SXH, this feature was implemented on the Cisco 6500 series routers. In Cisco IOS Release 12.3(14)T, this feature was integrated. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified: **debug mpls ldp session protection**, **mpls ldp session protection**, **show mpls ldp neighbor**.

CHAPTER 3

MPLS LDP IGP Synchronization

The MPLS LDP IGP Synchronization feature ensures that the Label Distribution Protocol (LDP) is fully established before the Interior Gateway Protocol (IGP) path is used for switching.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for MPLS LDP IGP Synchronization

- This feature is supported only on interfaces running Open Shortest Path First (OSPF) or Intermediate System-to-System (IS-IS) processes.
- This feature works when LDP is enabled on interfaces with either the **mpls ip** or **mpls ldp autoconfig** command.

Restrictions for MPLS LDP IGP Synchronization

- This feature is not supported on tunnel interfaces or LC-ATM interfaces.
- This feature is not supported with interface-local label space or downstream-on-demand (DoD) requests.
- This feature does not support targeted Label Distribution Protocol (LDP) sessions. Therefore, Any Transport over MPLS (AToM) sessions are not supported.
- The Tag Distribution Protocol (TDP) is not supported. You must specify that the default label distribution protocol is LDP for a device or for an interface.

Information About MPLS LDP IGP Synchronization

How MPLS LDP IGP Synchronization Works

Packet loss can occur because the actions of the Interior Gateway Protocol (IGP) and the Label Distribution Protocol (LDP) are not synchronized. Packet loss can occur in the following situations:

- When an IGP adjacency is established, the device begins forwarding packets using the new adjacency before the LDP label exchange completes between the peers on that link.
- If an LDP session closes, the device continues to forward traffic using the link associated with the LDP peer rather than an alternate pathway with a fully synchronized LDP session.

The MPLS LDP IGP Synchronization feature does the following:

- Provides a means to synchronize LDP and IGPs to minimize Multiprotocol Label Switching (MPLS) packet loss.
- Enables you to globally enable LDP IGP synchronization on each interface associated with an IGP Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS) process.
- Provides a means to disable LDP IGP synchronization on interfaces that you do not want enabled.
- Prevents MPLS packet loss due to synchronization conflicts.
- Works when LDP is enabled on interfaces using either the **mpls ip** or **mpls ldp autoconfig** command.

To enable LDP IGP synchronization on each interface that belongs to an OSPF or IS-IS process, enter the **mpls ldp sync** command. If you do not want some of the interfaces to have LDP IGP synchronization enabled, issue the **no mpls ldp igp sync** command on those interfaces.

If the LDP peer is reachable, the IGP waits indefinitely (by default) for synchronization to be achieved. To limit the length of time the IGP session must wait, enter the **no mpls ldp igp sync holddown** command. If the LDP peer is not reachable, the IGP establishes the adjacency to enable the LDP session to be established.

When an IGP adjacency is established on a link but LDP IGP synchronization is not yet achieved or is lost, the IGP advertises the max-metric on that link.

MPLS LDP IGP Synchronization with Peers

When the MPLS LDP IGP Synchronization feature is enabled on an interface, the Label Distribution Protocol (LDP) determines if any peer connected by the interface is reachable by looking up the peer's transport address in the routing table. If a routing entry (including longest match or default routing entry) for the peer exists, LDP assumes that LDP Interior Gateway Protocol (IGP) synchronization is required for the interface and notifies the IGP to wait for LDP convergence.

LDP IGP synchronization with peers requires that the routing table be accurate for the peer's transport address. If the routing table shows there is a route for the peer's transport address, that route must be able to reach the peer's transport address. However, if the route is a summary route, a default route, or a statically configured route, it may not the correct route for the peer. You must verify that the route in the routing table can reach the peer’s transport address.

When the routing table has an inaccurate route for the peer’s transport address, LDP cannot set up a session with the peer, which causes the IGP to wait for LDP convergence unnecessarily for the sync hold-down time.

MPLS LDP IGP Synchronization Delay Timer

The MPLS LDP IGP Synchronization feature provide the option to configure a delay time for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) and Interior Gateway Protocol (IGP) synchronization on an interface-by-interface basis. If you want to configure a delay time on an interface, use the **mpls ldp igp sync delay** *delay-time* command in interface configuration mode. To remove the delay timer from a specified interface, enter the **no mpls ldp igp sync delay** command. This command sets the delay time to 0 seconds, but leaves MPLS LDP IGP synchronization enabled.

When LDP is fully established and synchronized, LDP checks the delay timer:

- If you configured a delay time, LDP starts the timer. When the timer expires, LDP checks that synchronization is still valid and notifies the Open Shortest Path First (OSPF) process.
- If you did not configure a delay time, if synchronization is disabled or down, or if an interface was removed from an IGP process, LDP stops the timer and immediately notifies the OSPF process.

If you configure a new delay time while a timer is running, LDP saves the new delay time but does not reconfigure the running timer.

MPLS LDP IGP Synchronization Incompatibility with IGP Nonstop Forwarding

The MPLS LDP IGP Synchronization feature is not supported during the startup period if the Interior Gateway Protocol (IGP) nonstop forwarding (NSF) is configured. The MPLS LDP IGP Synchronization feature conflicts with IGP NSF when the IGP is performing NSF during startup. After the NSF startup is complete, the MPLS LDP IGP Synchronization feature is supported.

MPLS LDP IGP Synchronization Compatibility with LDP Graceful Restart

LDP Graceful Restart protects traffic when a Label Distribution Protocol (LDP) session is lost. If an interface that supports a Graceful Restart-enabled LDP session fails, MPLS LDP IGP synchronization is still achieved on the interface while it is protected by Graceful Restart. MPLS LDP IGP synchronization is eventually lost under the following circumstances:

- If LDP fails to restart before the LDP Graceful Restart reconnect timer expires.
- If an LDP session restarts through other interfaces, but the LDP session on the protected interface fails to recover when the LDP Graceful Restart recovery timer expires.

How to Configure MPLS LDP IGP Synchronization

Configuring MPLS LDP IGP Synchronization with OSPF Interfaces

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**mpls ip** **Example:** `Device(config)# mpls ip`	Globally enables hop-by-hop forwarding.
Step 4	**mpls label protocol ldp** **Example:** `Device(config)# mpls label protocol ldp`	Specifies the Label Distribution Protocol (LDP) as the default protocol.
Step 5	**interface** *type number* **Example:** `Device(config)# interface POS 3/0`	Specifies the interface to configure, and enters interface configuration mode.
Step 6	**ip address** *prefix mask* **Example:** `Device(config-if)# ip address 10.0.0.11 255.255.255.255`	Assigns an IP address to the interface.
Step 7	**mpls ip** **Example:** `Device(config-if)# mpls ip`	Enables hop-by-hop forwarding on the interface.
Step 8	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 9	**router ospf** *process-id* **Example:** `Device(config)# router ospf 1`	Enables Open Shortest Path First (OSPF) routing, and enters router configuration mode.
Step 10	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Device(config-router)# network 10.0.0.0 0.0.255.255 area 3`	Specifies the interface on which OSPF runs and defines the area ID for that interface.

	Command or Action	Purpose
Step 11	**mpls ldp sync** **Example:** `Device(config-router)# mpls ldp sync`	Enables the Multiprotocol Label Switching (MPLS) Interior Gateway Protocol (IGP) synchronization for interfaces belonging for an OSPF or an Intermediate System-to-Intermediate System (IS-IS) process.
Step 12	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.

Disabling MPLS LDP IGP Synchronization from Some OSPF Interfaces

When you issue the **mpls ldp sync** command, all of the interfaces that belong to an Open Shortest Path First (OSPF) process are enabled for Label Distribution Protocol (LDP) Interior Gateway Protocol (IGP) synchronization. To remove LDP IGP synchronization from some interfaces, use the **no mpls ldp igp sync** command on those interfaces.

Perform the following task to disable LDP IGP synchronization from some OSPF interfaces after they are configured with LDP IGP synchronization through the **mpls ldp sync** command.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface POS 0/3/0`	Specifies the interface to configure, and enters interface configuration mode.
Step 4	**no mpls ldp igp sync** **Example:** `Device(config-if)# no mpls ldp igp sync`	Disables MPLS LDP IGP synchronization for that interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Verifying MPLS LDP IGP Synchronization with OSPF

After you configure the interfaces for the Label Distribution Protocol (LDP), Open Shortest Path First (OSPF), and LDP Interior Gateway Protocol (IGP) synchronization, verify that the configuration is working correctly by using the **show mpls ldp igp sync** and **show ip ospf mpls ldp interface** commands.

SUMMARY STEPS

1. **enable**
2. **show mpls ldp igp sync**
3. **show ip ospf mpls ldp interface**
4. **exit**

DETAILED STEPS

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

Example:

```
Device> enable
Device#
```

Step 2 **show mpls ldp igp sync**
Shows that the Multiprotocol Label Switching (MPLS) LDP IGP synchronization is configured correctly because LDP is configured and the SYNC status shows that synchronization is enabled.

Example:

```
Device# show mpls ldp igp sync

FastEthernet0/0/0:
 LDP configured;  SYNC enabled.
 SYNC status: sync achieved; peer reachable.
 IGP holddown time: infinite.
 Peer LDP Ident: 10.0.0.1:0
 IGP enabled: OSPF 1
```

If MPLS LDP IGP synchronization is not enabled on an interface, the output appears as follows:

Example:

```
FastEthernet0/3/1:
 LDP configured; LDP-IGP Synchronization not enabled.
```

Step 3 **show ip ospf mpls ldp interface**

Shows that the interfaces are properly configured.

Example:

```
Device# show ip ospf mpls ldp interface

FastEthernet0/3/1
  Process ID 1, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization: Yes
  Holddown timer is not configured
  Timer is not running
FastEthernet0/0/2
  Process ID 1, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization: Yes
  Holddown timer is not configured
  Timer is not running
```

Step 4 **exit**

Returns to user EXEC mode.

Example:

```
Device# exit
Device>
```

Configuring MPLS LDP IGP Synchronization with IS-IS Interfaces

Configuring MPLS LDP IGP Synchronization on All IS-IS Interfaces

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol ldp**
5. **router isis** *process-name*
6. **mpls ldp sync**
7. **interface** *type number*
8. **ip address** *prefix mask*
9. **ip router isis** *process-name*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls ip** **Example:** `Device(config)# mpls ip`	Globally enables hop-by-hop forwarding.
Step 4	**mpls label protocol ldp** **Example:** `Device(config)# mpls label protocol ldp`	Specifies the Label Distribution Protocol (LDP) as the default label distribution protocol.

	Command or Action	Purpose
Step 5	**router isis** *process-name* **Example:** `Device(config)# router isis ISIS`	Enables the Intermediate System-to-Intermediate System (IS-IS) protocol on the device, specifies an IS-IS process, and enters router configuration mode.
Step 6	**mpls ldp sync** **Example:** `Device(config-router)# mpls ldp sync`	Enables Multiprotocol Label Switching (MPLS) LDP Interior Gateway Protocol (IGP) synchronization on interfaces belonging to an IS-IS process.
Step 7	**interface** *type number* **Example:** `Device(config-router)# interface POS 0/3/0`	Specifies the interface to configure, and enters interface configuration mode.
Step 8	**ip address** *prefix mask* **Example:** `Device(config-if)# ip address 10.25.25.11 255.255.255.0`	Assigns an IP address to the interface.
Step 9	**ip router isis** *process-name* **Example:** `Device(config-if)# ip router isis ISIS`	Enables IS-IS.
Step 10	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuring MPLS LDP IGP Synchronization on an IS-IS Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *prefix mask*
5. **ip router isis**
6. **exit**
7. **router isis**
8. **mpls ldp sync**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface POS 0/2/0`	Specifies the interface to configure, and enters interface configuration mode.
Step 4	**ip address** *prefix mask* **Example:** `Device(config-if)# ip address 10.50.72.4 255.0.0.0`	Assigns an IP address to the interface.
Step 5	**ip router isis** **Example:** `Device(config-if)# ip router isis`	Enables the Intermediate System-to-Intermediate System (IS-IS) protocol for IP on the interface.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 7	**router isis** **Example:** `Device(config)# router isis`	Enters router configuration mode, and enables an IS-IS process on the device.
Step 8	**mpls ldp sync** **Example:** `Device(config-router)# mpls ldp sync`	Enables Label Distribution Protocol (LDP) Interior Gateway Protocol (IGP) synchronization for interfaces belonging to an IS-IS process.
Step 9	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.

Disabling MPLS LDP IGP Synchronization from Some IS-IS Interfaces

When you issue the **mpls ldp sync** command, all of the interfaces that belong to an Intermediate System-to-Intermediate System (IS-IS) process are enabled for Label Distribution Protocol (LDP) Interior Gateway Protocol (IGP) synchronization. To remove LDP IGP synchronization from some interfaces, use the **no mpls ldp igp sync** command on those interfaces.

Perform the following task to disable LDP IGP synchronization from some IS-IS interfaces after they are configured with LDP IGP synchronization through the **mpls ldp sync** command.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface POS 0/3/0`	Specifies the interface to configure, and enters interface configuration mode.
Step 4	**no mpls ldp igp sync** **Example:** `Device(config-if)# no mpls ldp igp sync`	Disables Multiprotocol Label Switching (MPLS) LDP IGP synchronization for that interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Troubleshooting Tips

Use the **debug mpls ldp igp sync** command to display events related to MPLS LDP IGP synchronization.

Configuration Examples for MPLS LDP IGP Synchronization

Example: MPLS LDP IGP Synchronization with OSPF

The following task shows how to enable the Label Distribution Protocol (LDP) for Open Shortest Path First (OSPF) process 1. The **mpls ldp sync** and the OSPF **network** commands enable LDP on interfaces POS0/0/0, POS0/1/0, and POS1/1/0, respectively. The **no mpls ldp igp sync** command on interface POS1/0/0 prevents LDP from being enabled on interface POS1/0/0, even though OSPF is enabled for that interface.

```
Device# configure terminal
Device(config)# interface POS0/0/0
Device(config-if)# ip address 10.0.0.1
Device(config-if)# mpls ip
!
Device(config)# interface POS0/1/0
Device(config-if)# ip address 10.0.1.1
Device(config-if)# mpls ip
!
Device(config)# interface POS1/1/0
Device(config-if)# ip address 10.1.1.1
Device(config-if)# mpls ip
!
Device(config)# interface POS1/0/0
Device(config-if)# ip address 10.1.0.1
Device(config-if)# mpls ip
!
Device(config)# router ospf 1
Device(config-router)# network 10.0.0.0 0.0.255.255 area 3
Device(config-router)# network 10.1.0.0 0.0.255.255 area 3
Device(config-router)# mpls ldp sync
Device(config-router)# exit
Device(config)# interface POS1/0/0
Device(config-if)# no mpls ldp igp sync
```

Example: MPLS LDP IGP Synchronization with IS-IS

The following examples show the configuration commands you can use to configure MPLS LDP IGP synchronization on interfaces POS0/2 /0 and POS0/3/0, which are running IS-IS processes:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface POS0/2/0
Device(config-if)# ip router isis
Device(config-if)# exit
Device(config)# router isis
Device(config-router)# mpls ldp sync
Device(config-router)# exit
.
.
.
Device(config)# interface POS0/3/0
Device(config-if)# ip router isis
Device(config-if)# exit
Device(config)# router isis
Device(config-router)# mpls ldp sync
Device(config-router)# exit
Device(config) exit
Device#
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS LDP commands	Cisco IOS Multiprotocol Label Switching Command Reference
LDP autoconfiguration	"MPLS LDP Autoconfiguration" module in the *MPLS Label Distribution Protocol Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 3037	LDP Applicability
RFC 5036	LDP Specification

MIBs

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

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MPLS LDP IGP Synchronization

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 IGP Synchronization

Feature Name	Releases	Feature Information
MPLS LDP IGP Synchronization	12.0(30)S 12.0(32)SY 12.2(33)SB 12.2(33)SRB 15.1(1)SY 15.5(2)SY	The MPLS LDP IGP Synchronization feature ensures that LDP is fully established before the IGP path is used for switching. In 12.0(30)S, this feature was introduced. In 12.0(32)SY, support for enabling synchronization on interfaces running Intermediate System-to-System (IS-IS) processes was added. In 12.2(33)SB, the feature was integrated. MPLS LDP IGP synchronization for IS-IS is not supported in this release. In 12.2(33)SRB, the feature was integrated. MPLS LDP IGP synchronization for IS-IS is not supported in this release. In 15.1(1)SY, support for configuring MPLS LDP IGP synchronization with OSPF and IS-IS interfaces was enabled. The following commands were modified: **debug mpls ldp igp sync**, **mpls ldp igp sync**, **mpls ldp igp sync holddown**, **mpls ldp sync**, **show ip ospf mpls ldp interface**, **show isis mpls ldp**, and **show mpls ldp igp sync**.

CHAPTER 4

MPLS LDP Inbound Label Binding Filtering

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Restrictions for MPLS LDP Inbound Label Binding Filtering

Inbound label binding filtering does not support extended access control lists (ACLs); it only supports standard ACLs.

Information about MPLS LDP Inbound Label Binding Filtering

Overview of MPLS LDP Inbound Label Binding Filtering

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

How to Configure MPLS LDP Inbound Label Binding Filtering

Configuring MPLS LDP Inbound Label Binding Filtering

Perform this task to configure a device for inbound label filtering. The following configuration allows the device to accept only the label for prefix 25.0.0.2 from the Label Distribution Protocol (LDP) neighbor device 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list standard** *access-list-number* **Example:** `Device(config)# ip access-list standard 1`	Defines a standard IP access list with a number.
Step 4	**permit** {*source* [*source-wildcard*] | **any**} [**log**] **Example:** `Device(config-std-nacl)# permit 10.0.0.0`	Specifies one or more prefixes permitted by the access list.
Step 5	**exit** **Example:** `Device(config-std-nacl)# exit`	Returns to global configuration mode.
Step 6	**mpls ldp neighbor** [**vrf** *vpn-name*] *nbr-address* **labels accept** *acl* **Example:** `Device(config)# mpls ldp neighbor 10.12.12.12 labels accept 1`	Specifies the access control list (ACL) to be used to filter label bindings for the specified LDP neighbor.
Step 7	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Verifying that MPLS LDP Inbound Label Bindings are Filtered

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

SUMMARY STEPS

1. **enable**
2. **show mpls ldp neighbor** [**vrf** *vpn-name*] [*address* | *interface*] [**detail**]
3. **show ip access-list** [*access-list-number* | *access-list-name*]
4. **show mpls ldp bindings**
5. **exit**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Device> enable
Device#
```

Step 2 **show mpls ldp neighbor** [**vrf** *vpn-name*] [*address* | *interface*] [**detail**]

Shows the status of the Label Distribution Protocol (LDP) session, including the name or number of the access control list (ACL) configured for inbound filtering.

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

Example:

```
Device# 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:
    Serial1/0/0; Src IP addr: 192.168.1.1
     holdtime: 15000 ms, hello interval: 5000 ms
   Addresses bound to peer LDP Ident:
    10.0.0.129       10.12.12.12     192.168.1.1
   Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
   LDP inbound filtering accept acl: 1
```

Step 3 **show ip access-list** [*access-list-number* | *access-list-name*]

Displays the contents of all current IP access lists or of a specified access list.

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:

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

Step 4 **show mpls ldp bindings**

Verifies that the label switch router (LSR) has remote bindings only from a specified peer for prefixes permitted by the access list.

Example:

```
Device# 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: 10.12.12.12:0, tag: imp-null
 tib entry: 10.0.0.0/8, rev 8
     local binding:  tag: imp-null
```

Step 5 **exit**

Returns to user EXEC mode.

Example:

```
Device# exit
Device>
```

Configuration Examples for MPLS LDP Inbound Label Binding Filtering

Examples: MPLS LDP Inbound Label Binding Filtering Configuration

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.

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

```
Device# 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
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
MPLS Label Distribution Protocol (LDP)	"MPLS Label Distribution Protocol" module in the *MPLS Label Distribution Protocol Configuration Guide*

MIBs

MIB	MIBs Link
LDP Specification, draft-ietf-mpls-ldp-08.txt	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mib

RFCs

RFC	Title
RFC 3036	LDP Specification
RFC 3037	LDP Applicability

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MPLS LDP Inbound Label Binding Filtering

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 5: Feature Information for MPLS LDP Inbound Label Binding Filtering

Feature Name	Releases	Feature Information
MPLS LDP Inbound Label Binding Filtering	12.0(26)S 12.2(25)S 15.2(1)SY	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. In 15.2(1)SY, the feature was integrated into Cisco IOS Release 15.2(2)SY. 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 device—customer edge device. A device that is part of a customer network and that interfaces to a provider edge (PE) device.

inbound label binding filtering—Allows label switch routers (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.

CHAPTER 5

MPLS LDP Local Label Allocation Filtering

The MPLS LDP Local Label Allocation Filtering feature introduces CLI commands to modify the way in which Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) handles local label allocation. This MPLS LDP feature enhancement enables the configuration of filtering policies for selective local label binding assignments by LDP to improve LDP scalability and convergence.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for MPLS LDP Local Label Allocation Filtering

The MPLS LDP Local Label Allocation Filtering feature requires the MPLS Forwarding Infrastructure (MFI).

Restrictions for MPLS LDP Local Label Allocation Filtering

- This feature does not support access lists; it supports prefix lists.
- Label Distribution Protocol (LDP) local label allocation configuration for prefix list or host routes is supported only in the global routing table.
- LDP and Routing Information Base (RIB) restart handling does not apply.
- Wildcard Forwarding Equalence Class (FEC) requests are not supported.
- Remote bindings are retained for LDP table entries that are filtered.

Information About MPLS LDP Local Label Allocation Filtering

MPLS LDP Local Label Allocation Filtering Overview

The Label Distribution Protocol (LDP) allocates a local label for every route learned from the Interior Gateway Protocol (IGP). In the absence of inbound and outbound label filtering, these local labels are advertised to and learned by all peers.

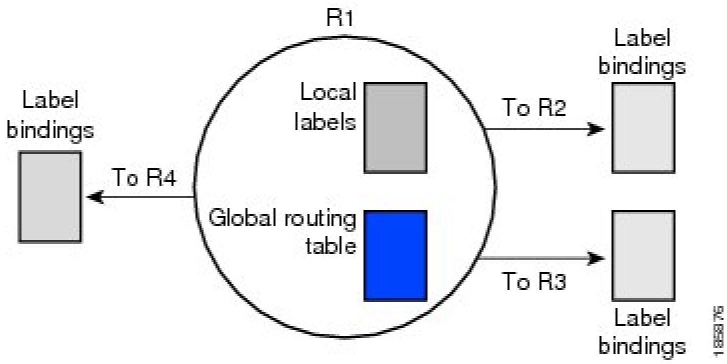
In most Layer 3 Virtual Private Network (VPN) configurations only the label switched paths (LSPs) created to reach the /32 host routes or Border Gateway Protocol (BGP) next hops between the provider edge (PE) devices carry traffic and are relevant to the Layer 3 VPNs. LSPs between the PE devices that are not members of a VPN use more memory and create additional processing in LDP across the core.

With the load increases in the service provider domain in the last decade (1997-2007), scalability has become more important in the service provider networks. Controlling the local label allocation could off-load LDP processing of non-VPN LSPs in the service provider network core devices.

The MPLS LDP Local Label Allocation Filtering feature introduces the **mpls ldp label** and **allocate** commands that allow you to configure LDP to selectively allocate local labels for a subset of the prefixes learned from the IGP. You can select that LDP allocate local labels for prefixes configured in a prefix list in the global table or for host routes in the global table.

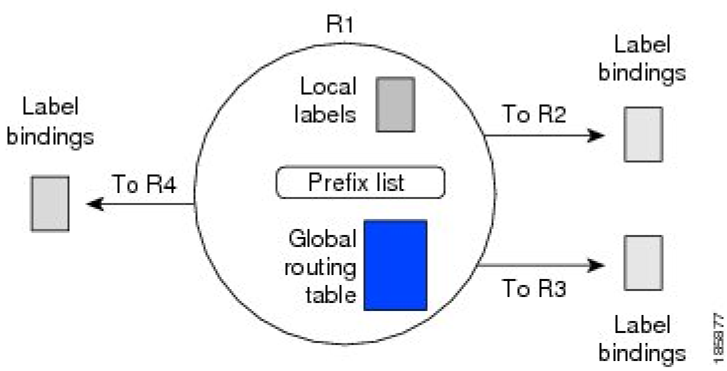
Local label allocation filtering reduces the number of local labels allocated and therefore the number of messages exchanged with peers. This improves LDP scalability and convergence. The two figures below show how controlling local label allocation can reduce local label space size and greatly reduce the number of advertisements to peers. The first figure below shows default LDP label allocation behavior. LDP allocates a local label for every route and advertises a label binding for every route learned from the IGP.

Figure 4: Default LDP Local Label Allocation Behavior



The figure below shows LDP behavior with local label allocation control configured. The size of the local label space and the number of label binding advertisements are reduced with local label allocation filtering through the use of a prefix list. The decrease in the number of local labels and label binding advertisement messages reduces the amount of memory use and improves convergence time for LDP. The MPLS LDP Local Label Allocation Filtering feature also allows for more efficient use of the label space.

Figure 5: LDP Behavior with Local Label Allocation Controls



The figure above shows that device R1 learns a number of routes from its IGP neighbors on devices R2, R3, and R4. A prefix list defined on device R1 specifies the prefixes for which LDP allocates a local label.

Note In general, the number of Label Information Base (LIB) entries remains the same regardless of the kind of label filtering. This is because the remote label bindings for the prefixes that are filtered are kept in the LIB. Memory use is reduced because local label filtering decreases the number of local labels allocated and the number of label bindings advertised to and stored by the peers of a label switch router (LSR).

Prefix Lists for MPLS LDP Local Label Allocation Filtering Benefits and Description

The MPLS LDP Local Label Allocation Filtering feature allows you to configure the Label Distribution Protocol (LDP) to allocate local labels for a subset of the learned prefixes. LDP accepts the prefix and allocates a local label if the prefix is permitted by a prefix list. If the prefix list is not defined, LDP accepts all prefixes and allocates local labels based on its default mode of operation.

The benefits of using prefix lists for LDP local label allocation filtering are as follows:

- Prefix lists provide more flexibility for specifying a subset of prefixes and masks.
- Prefix lists use a tree-based matching technique. This technique is more efficient than evaluating prefixes or host routes sequentially.
- Prefix lists are easy to modify.

You configure a prefix list for the MPLS LDP Local Label Allocation Filtering feature with the **ip prefix-list** command.

Local Label Allocation Changes and LDP Actions

The MPLS LDP Local Label Allocation Filtering enhancement modifies the Label Distribution Protocol's (LDP's) local label allocation handling. The feature supports local label allocation filtering through the specification of a prefix list or host routes.

With the introduction of this feature, LDP needs to determine whether a prefix filter is already configured to control the local label allocation on the local node. If a prefix list exists, the local label allocation is confined to the list of prefixes permitted by the configured prefix list.

LDP also needs to respond to local label allocation configuration changes and to configuration changes that affect the prefix list that LDP is using. Any of the following configuration changes can trigger LDP actions:

- Creating a local label allocation configuration
- Deleting or changing a local label allocation configuration
- Creating a new prefix list for a local label allocation configuration
- Deleting or changing a prefix list for a local label allocation configuration

LDP responds to local label allocation configuration changes by updating the Label Information Database (LIB) and the forwarding table in the global routing table. To update the LIB after a local label filter configuration change without a session reset, LDP keeps all remote bindings.

If you create a local label allocation configuration without defining a prefix list, no LDP action is required. The local label allocation configuration has no effect because the prefix list is created and permits all prefixes.

If you create or change a prefix list and prefixes that were previously allowed are rejected, LDP goes through a label withdraw and release procedure before the local labels for these prefixes are deallocated.

If you delete a prefix, LDP goes through the label withdraw and release procedure for the LIB local label. If the associated prefix is one for which no LIB entry should be allocated, LDP bypasses this procedure.

The LDP default behavior is to allocate local labels for all non-BGP prefixes. This default behavior does not change with the introduction of this feature and the **mpls ldp label** and **allocate** commands.

Note The local label allocation filtering has no impact on inbound label filtering because both provide LDP filtering independently. The LDP Inbound Label Binding Filtering feature controls label bindings that a label switch router (LSR) accepts from its peer LSRs through the use of access control lists (ACLs). The MPLS LDP Local Label Allocation Filtering feature controls the allocation of local labels through the use of prefix lists or host routes.

LDP Local Label Filtering and BGP Routes

The Label Distribution Protocol (LDP) default behavior is to allocate local labels for all non-Border Gateway Protocol (BGP) prefixes.

LDP does not apply the configured local label filter to redistributed BGP routes in the global table for which BGP allocates local label, but LDP does the advertisements (Inter-AS Option C). LDP neither forwards these entries nor releases the local labels allocated by BGP.

How to Configure MPLS LDP Local Label Allocation Filtering

Creating a Prefix List for MPLS LDP Local Label Allocation Filtering

Perform the following task to create a prefix list for the Label Distribution Protocol (LDP) local label allocation filtering. A prefix list allows LDP to selectively allocate local labels for a subset of the routes learned from the Interior Gateway Protocol {IGP). The decrease in the number of local labels in the LDP Label Information Base (LIB) and the number of label mapping advertisements reduces the amount of memory use and improves convergence time for LDP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** {*list-name* | *list-number*} [**seq** *number*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-length*] [**le** *le-length*]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip prefix-list** {*list-name* | *list-number*} [**seq** *number*] {**deny** *network*/*length* | **permit** *network*/*length*} [**ge** *ge-length*] [**le** *le-length*] **Example:** `Device(config)# ip prefix-list list1 permit 192.168.0.0/16 le 20`	Creates a prefix list or adds a prefix-list entry. • The *list-name* argument configures a name to identify the prefix list. • The *list-number* argument configures a number to identify the prefix list. • The **seq** *number* keyword and argument apply a sequence number to a prefix-list entry. The range of sequence numbers is 1 to 4294967294. If a sequence number is not entered when this command is configured, a default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5. • The **deny** keyword denies access for a matching condition. • The **permit** keyword permits access for a matching condition. • The *network*/*length* arguments and keyword configure the network address, and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 0 to 32. • The **ge** *ge-length* keyword and argument specify the lesser value of a range (the "from" portion of the range description) by applying the *ge-length* argument to the range specified. The *ge-length* argument represents the minimum prefix length to be matched. The **ge** keyword represents the greater than or equal to operator. • The **le** *le-length* keyword and argument specify the greater value of a range (the "to" portion of the range description) by applying the *le-length* argument to the range specified. The *le-length* argument represents the maximum prefix length to be matched. The **le** keyword represents the less than or equal to operator.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring MPLS LDP Local Label Allocation Filtering

Perform the following task to configure the Label Distribution Protocol (LDP) local allocation filtering. Configuring filtering policies for selective local label binding assignments by LDP improves LDP scalability and convergence. You can configure either a prefix list or host routes as a filter for local label allocation.

Note The **host-routes** keyword for the **allocate** command makes it convenient for you to specify a commonly used set of prefixes.

Note A maximum of one local label allocation filter is supported for the global table.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp label**
4. **allocate global prefix-list** {*list-name* | *list-number*}
5. **allocate global host-routes**
6. **no allocate global** {**prefix-list** {*list-name* | *list-number*} | **host-routes**}
7. **no mpls ldp label**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls ldp label** **Example:** `Device(config)# mpls ldp label`	Enters MPLS LDP label configuration mode to specify how LDP handles local label allocation.

	Command or Action	Purpose
Step 4	**allocate global prefix-list** {*list-name* | *list-number*} **Example:** `Device(config-ldp-lbl)# allocate global prefix-list list1`	Configures local label allocation filters for learned routes for LDP. • The **global** keyword specifies the global routing. • The **prefix-list** keyword specifies a prefix list to be used as a filter for MPLS LDP local label allocation. • The *list-name* argument indicates a name that identifies the prefix list. • The *list-number* argument indicates a number that identifies the prefix list.
Step 5	**allocate global host-routes** **Example:** `Device(config-ldp-lbl)# allocate global host-routes`	Configures local label allocation filters for learned routes for LDP. • The **global** keyword specifies the global routing. • The **host-routes** keyword specifies that local label allocation be done for host routes only.
Step 6	**no allocate global** {**prefix-list** {*list-name* | *list-number*} | **host-routes**} **Example:** `Device(config-ldp-lbl)# no allocate global host-routes`	Removes the specific MPLS LDP local label allocation filter without resetting the LDP session. • The **global** keyword specifies the global routing. • The **prefix-list** keyword specifies a prefix list to be used as a filter for MPLS LDP local label allocation. • The *list-name* argument indicates a name that identifies the prefix list. • The *list-number* argument indicates a number that identifies the prefix list. • The **host-routes** keyword specifies that host routes be used as a filter for MPLS LDP local label allocation.
Step 7	**no mpls ldp label** **Example:** `Device(config-ldp-lbl)# no mpls ldp label`	Removes all local label allocation filters configured under the MPLS LDP label configuration mode and restores LDP default behavior for local label allocation without a session reset.
Step 8	**end** **Example:** `Device(config-ldp-lbl)# end`	Returns to privileged EXEC mode.

Verifying MPLS LDP Local Label Allocation Filtering Configuration

SUMMARY STEPS

1. **enable**
2. **show mpls ldp bindings detail**
3. **debug mpls ldp binding filter**
4. **exit**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Device> enable
Device#
```

Step 2 **show mpls ldp bindings detail**

Verifies that local label allocation filtering is configured as you expect.

Example:

```
Device# show mpls ldp bindings detail

Advertisement spec:
        Prefix acl = bar
Local label filtering spec: host routes.
  lib entry: 10.1.1.1/32, rev 9
  lib entry: 10.10.7.0/24, rev 10
  lib entry: 10.10.8.0/24, rev 11
  lib entry: 10.10.9.0/24, rev 12
  lib entry: 10.41.41.41/32, rev 17
  lib entry: 10.50.50.50/32, rev 15
  lib entry: 10.60.60.60/32, rev 18
  lib entry: 10.70.70.70/32, rev 16
  lib entry: 10.80.80.80/32, rev 14
```

The output of this command verifies that host routes are configured as the local label allocation filter for the device.

Step 3 **debug mpls ldp binding filter**

Verifies that local label allocation filtering was configured properly and to display how LDP accepts or withdraw labels.

Example:

```
Device# debug mpls ldp binding filter
LDP Local Label Allocation Filtering changes debugging is on
.
.
.
```

Step 4 **exit**

Returns to user EXEC mode.

Example:

```
Device# exit
Device>
```

Configuration Examples for MPLS LDP Local Label Allocation Filtering

Examples: Creating a Prefix List for MPLS LDP Local Label Allocation Filtering

The following examples show how to configure a prefix list for MPLS LDP local label allocation filtering.

In this example, prefix list List1 permits only 192.168.0.0/16 prefixes. The Label Distribution Protocol (LDP) accepts 192.168.0.0/16 prefixes, but does not assign a local label for the following prefixes: 192.168.0.0/24 and 192.168.2.0/24. For example:

```
configure terminal
!
ip prefix-list List1 permit 192.168.0.0/16
end
```

In the following example, prefix list List2 permits a range of prefixes from 192.168.0.0/16 to /20 prefixes. LDP accepts 192.168.0.0/16 prefixes, but does not assign local labels for the following prefixes: 192.168.0.0/24 and 192.168.2.0/24.

```
configure terminal
!
ip prefix-list List2 permit 192.168.0.0/16 le 20
end
```

In the following example, prefix list List3 permits a range of prefixes greater than /18. LDP accepts 192.168.17.0/20 and 192.168.2.0/24 prefixes, but does not assign a local label for 192.168.0.0/16.

```
configure terminal
!
ip prefix-list List3 permit 192.168.0.0/16 ge 18
end
```

Examples: Configuring MPLS LDP Local Label Allocation Filtering

This examples shows how to allocate a prefix list to be used as a local label allocation filter:

```
configure terminal
!
ip prefix-list List3 permit 192.168.0.0/16 ge 18
!
mpls ldp label
 allocate global prefix-list List3
 exit
exit
```

Prefix list List3, which permits a range of prefixes greater than /18, is configured as the local label allocation filter for the device. The Label Distribution Protocol (LDP) allows 192.168.17.0/20 and 192.168.2.0/24 prefixes, but withdraws labels for prefixes not in the allowed range.

In the following example, host routes are configured as the local label allocation filter:

```
configure terminal
!
mpls ldp label
 allocate global host-routes
 exit
exit
```

LDP allocates local labels for host routes that are in the global routing table.

In the following example, a specific local label allocation filter is removed:

```
configure terminal
!
mpls ldp label
 no allocate global host-routes
 exit
exit
```

In the following example, all local label allocation filters configured in MPLS LDP label configuration mode are removed and the default LDP local label allocation is restored without a session reset:

```
configure terminal
!
no mpls ldp label
 exit
exit
```

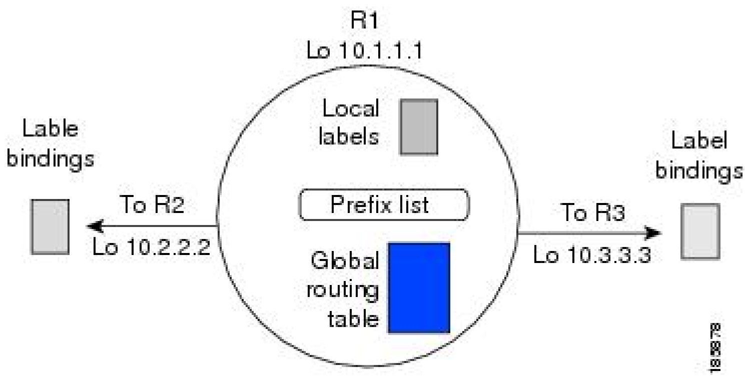
Examples: Sample MPLS LDP Local Label Allocation Filtering Configuration

The figure below is a sample configuration that is used in this section to show how Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) local label allocation filtering works:

- Devices R1, R2, and R3 have loopback addresses 10.1.1.1, 10.2.2.2, and 10.3.3.3 defined and advertised by the Interior Gateway Protocol (IGP), respectively.
- 10.1.1.1 is the router ID of Device R1, 10.2.2.2 is the router ID of Device R2, and 10.3.3.3 is the router ID of Device R3.
- A prefix list is defined on Device R1 to specify the local labels for which LDP allocates a local label.

Device RI learns a number of routes from its IGP neighbors on Devices R2 and R3.

Figure 6: LDP Local Label Allocation Filtering Example



You can use LDP CLI commands to verify the following:

- Device R1 has allocated a local label for the correct subset of the prefixes.
- Devices R2 and R3 did not receive any remote bindings for the prefixes for which Device R1 did not assign a local label.

Routing Table on Device R1

You can enter the **show ip route** command to display the current state of the routing table. The following example shows the routing table on Device R1 based on the figure above:

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/32 is subnetted, 1 subnets
C       10.1.1.1 is directly connected, Loopback0
     10.2.0.0/32 is subnetted, 1 subnets
O       10.2.2.2 [110/11] via 10.10.7.1, 00:00:36, FastEthernet1/0/0
     10.3.0.0/32 is subnetted, 1 subnets
O       10.3.3.3 [110/11] via 10.10.9.1, 00:00:36, FastEthernet3/0/0
     10.0.0.0/24 is subnetted, 3 subnets
C       10.10.7.0 is directly connected, FastEthernet1/0/0
O       10.10.8.0 [110/20] via 10.10.9.1, 00:00:36, FastEthernet3/0/0
                  [110/20] via 10.10.7.1, 00:00:36, FastEthernet1/0/0
C       10.10.9.0 is directly connected, FastEthernet3/0/0
```

Local Label Bindings on Devices R1, R2, and R3

You can enter the **show mpls ldp bindings** command on Devices R1, R2, and R3 to display the contents of the Label Information Base (LIB) on each device. In the following examples, the default Label Distribution Protocol (LDP) allocation behavior is in operation; that is, LDP allocates a local label for every route and advertises a label binding for every route learned from the Interior Gateway Protocol (IGP).

LIB on Device R1

This example shows the contents of the LIB on Device R1 based on the configuration in the figure above:

```
Device# show mpls ldp bindings

  lib entry: 10.1.1.1/32, rev 7
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: 16
        remote binding: lsr: 10.2.2.2:0, label: 17
  lib entry: 10.2.2.2/32, rev 13
        local binding:  label: 1000
        remote binding: lsr: 10.3.3.3:0, label: 18
        remote binding: lsr: 10.2.2.2:0, label: imp-null
  lib entry: 10.3.3.3/32, rev 15
        local binding:  label: 1002
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: 18
  lib entry: 10.10.7.0/24, rev 8
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: 17
        remote binding: lsr: 10.2.2.2:0, label: imp-null
  lib entry: 10.10.8.0/24, rev 11
        local binding:  label: 1001
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: imp-null
  lib entry: 10.10.9.0/24, rev 9
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: 16
```

The local labels assigned to 10.2.2.2 and 10.3.3.3 on Device R1 are advertised to Devices R2 and R3.

LIB on Device R2

This example shows the contents of the LIB on Device R2 based on the configuration in the figure above:

```
Device# show mpls ldp bindings

  lib entry: 10.1.1.1/32, rev 11
        local binding:  label: 17
        remote binding: lsr: 10.3.3.3:0, label: 16
        remote binding: lsr: 10.1.1.1:0, label: imp-null
  lib entry: 10.2.2.2/32, rev 7
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: 18
        remote binding: lsr: 10.1.1.1:0, label: 1000
  lib entry: 10.3.3.3/32, rev 15
        local binding:  label: 18
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: 1002
  lib entry: 10.10.7.0/24, rev 8
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: 17
        remote binding: lsr: 10.1.1.1:0, label: imp-null
  lib entry: 10.10.8.0/24, rev 9
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: 1001
  lib entry: 10.10.9.0/24, rev 13
        local binding:  label: 16
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: imp-null
```

LIB on Device R3

This example shows the contents of the LIB on Device R3 based on the configuration in the figure above:

```
Device # show mpls ldp bindings
```

```
  lib entry: 10.1.1.1/32, rev 13
        local binding:  label: 16
        remote binding: lsr: 10.2.2.2:0, label: 17
        remote binding: lsr: 10.1.1.1:0, label: imp-null
  lib entry: 10.2.2.2/32, rev 15
        local binding:  label: 18
        remote binding: lsr: 10.2.2.2:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: 1000
  lib entry: 10.3.3.3/32, rev 7
        local binding:  label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: 18
        remote binding: lsr: 10.1.1.1:0, label: 1002
  lib entry: 10.10.7.0/24, rev 11
        local binding:  label: 17
        remote binding: lsr: 10.2.2.2:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: imp-null
  lib entry: 10.10.8.0/24, rev 8
        local binding:  label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: 1001
  lib entry: 10.10.9.0/24, rev 9
        local binding:  label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: 16
        remote binding: lsr: 10.1.1.1:0, label: imp-null
```

Local Label Allocation Filtering Configuration on Device R1

You enter the **mpls ldp label** command to configure a local label allocation filter. The following examples show how to configure a local label allocation filter by host routes only and by a prefix list.

Local Label Allocation Filter—Host Routes Only Configuration

This example shows the selection of host routes as the only filter.

The following local label allocation filtering is defined on Device R1 under MPLS LDP label configuration mode:

```
configure terminal
!
mpls ldp label
 allocate global host-routes
 exit
exit
```

Local Label Allocation Filter—Prefix List Configuration

The following example shows how to configure a local label allocation filter that allows or denies prefixes based on a prefix list:

```
configure terminal
!
mpls ldp label
 allocate global prefix-list ListA
 exit
end
```

ListA is a prefix list defined as:

```
configure terminal
!
ip prefix-list ListA permit 0.0.0.0/32 ge 32
```

Local Label Allocation Filtering Changes Label Bindings on Devices R1, R2, and R3

After configuring a local label allocation filter on Device R1, you can enter the **show mpls ldp bindings** command again to see the changes in the local label bindings in the Label Information Base (LIB) on each device. Changes to the output in the LIB entries are highlighted in bold text.

This sample prefix list is used for the examples in the this section:

```
ip prefix-list ListA permit 0.0.0.0/32 ge 32
```

LIB on Device R1 After Local Label Allocation Filtering

This example shows how the configuration of a local label allocation prefix-list filter changes the contents of the LIB on Device R1:

```
Device# show mpls ldp bindings

  lib entry: 10.1.1.1/32, rev 7
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: 16
        remote binding: lsr: 10.2.2.2:0, label: 17
  lib entry: 10.2.2.2/32, rev 13
        local binding:  label: 1000
        remote binding: lsr: 10.3.3.3:0, label: 18
        remote binding: lsr: 10.2.2.2:0, label: imp-null
  lib entry: 10.3.3.3/32, rev 15
        local binding:  label: 1002
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: 18
  lib entry: 10.10.7.0/24, rev 8
        no local binding
        remote binding: lsr: 10.3.3.3:0, label: 17
        remote binding: lsr: 10.2.2.2:0, label: imp-null
  lib entry: 10.10.8.0/24, rev 11
        no local binding
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: imp-null
  lib entry: 10.10.9.0/24, rev 9
        no local binding
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: 16
```

Local label bindings for all but 10.2.2.2 and 10.3.3.3 on Device R1 are advertised as withdrawn.

LIB on Device R2 After Local Label Allocation Filtering

This example shows how the configuration of a local label allocation prefix-list filter on Device R1 changes the contents of the LIB on Device R2:

```
Device# show mpls ldp bindings
  lib entry: 10.1.1.1/32, rev 11
        local binding:  label: 17
        remote binding: lsr: 10.3.3.3:0, label: 16
  lib entry: 10.2.2.2/32, rev 7
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: 18
        remote binding: lsr: 10.1.1.1:0, label: 1000
  lib entry: 10.3.3.3/32, rev 15
        local binding:  label: 18
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: 1002
lib entry: 10.10.7.0/24, rev 8
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: 17
  lib entry: 10.10.8.0/24, rev 9
```

```
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: imp-null
  lib entry: 10.10.9.0/24, rev 13
        local binding:  label: 16
        remote binding: lsr: 10.3.3.3:0, label: imp-null
```

The 10.10.7.0/24, 10.10.8.0/24, and 10.10.9.0/24 prefixes are no longer assigned local labels. Therefore, Device R1 sends no label advertisement for these prefixes.

LIB on Device R3 After Local Label Allocation Filtering

This example shows how the configuration of a local label allocation prefix-list filter on Device R1 changes the contents of the LIB on Device R3:

```
Device# show mpls ldp bindings
  lib entry: 10.1.1.1/32, rev 13
        local binding:  label: 16
        remote binding: lsr: 10.2.2.2:0, label: 17
        remote binding: lsr: 10.1.1.1:0, label: imp-null
  lib entry: 10.2.2.2/32, rev 15
        local binding:  label: 18
        remote binding: lsr: 10.2.2.2:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: 1000
  lib entry: 10.3.3.3/32, rev 7
        local binding:  label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: 18
        remote binding: lsr: 10.1.1.1:0, label: 1002
  lib entry: 10.10.7.0/24, rev 11
        local binding:  label: 17
        remote binding: lsr: 10.2.2.2:0, label: imp-null
  lib entry: 10.10.8.0/24, rev 8
        local binding:  label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: imp-null
  lib entry: 10.10.9.0/24, rev 9
        local binding:  label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: 16
```

The 10.10.7.0/24, 10.10.8.0/24, and 10.10.9.0/24 prefixes are no longer assigned local labels. Again, Device R1 sends no label advertisement for these prefixes.

Command to Display the Local Label Allocation Filter

You can enter the **show mpls ldp detail** command to display the filter used for local label allocation. For example:

```
Device# show mpls ldp bindings detail

Advertisement spec:
        Prefix acl = List1
Local label filtering spec: host routes. ! <--- Local local label filtering spec

  lib entry: 10.1.1.1/32, rev 9
  lib entry: 10.10.7.0/24, rev 10
  lib entry: 10.10.8.0/24, rev 11
  lib entry: 10.10.9.0/24, rev 12
  lib entry: 10.41.41.41/32, rev 17
  lib entry: 10.50.50.50/32, rev 15
  lib entry: 10.60.60.60/32, rev 18
  lib entry: 10.70.70.70/32, rev 16
  lib entry: 10.80.80.80/32, rev 14
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
Configuration tasks for MPLS LDP	"MPLS Label Distribution Protocol" module in the *MPLS Label Distribution Protocol Configuration Guide*
Configuration tasks for inbound label binding filtering for MPLS LDP	"MPLS LDP Inbound Label Binding Filtering" module in the *MPLS Label Distribution Protocol Configuration Guide*

RFCs

RFC	Title
RFC 3037	LDP Applicability
RFC 3815	Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
RFC 5036	LDP Specification

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MPLS LDP Local Label Allocation Filtering

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 6: Feature Information for MPLS LDP Local Label Allocation Filtering

Feature Name	Releases	Feature Information
MPLS LDP Local Label Allocation Filtering	12.2(33)SRC 12.2(33)SB Cisco IOS 15.2(1)SY	The MPLS LDP Local Label Allocation Filtering feature introduces CLI commands to modify the way in which Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) handles local label allocation. This MPLS LDP feature enhancement enables the configuration of filtering policies for selective local label binding assignments by LDP to improve LDP scalability and convergence. In 12.2(33)SRC, the feature was introduced on a Cisco IOS 12.2SR release. In 12.2(33)SB, the feature was integrated into a Cisco IOS 12.2SB release. In 15.2(1)SY, the feature was integrated into Cisco IOS Release 15.2(2)SY.
		The following commands were introduced or modified: **allocate**, **debug mpls ldp bindings**, **mpls ldp label**, **show mpls ldp bindings**.

Glossary

BGP—Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. It is defined by RFC 1163.

CE device—customer edge device. A device that is part of a customer network and that interfaces to a provider edge (PE) device. CE devices do not have routes to associated Virtual Private Networks (VPNs) in their routing tables.

FEC—Forwarding Equivalence Class. A set of packets that can be handled equivalently for the purpose of forwarding and thus is suitable for binding to a single label. The set of packets destined for an address prefix is one example of an FEC.

IGP—Interior Gateway Protocol. Internet protocol used to exchange routing information within a single autonomous system. Examples of common Internet IGP protocols include Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Routing Information protocol (RIP).

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

LDP—Label Distribution Protocol. A standard protocol between Multiprotocol Label Switching (MPLS)-enabled devices that is used for the negotiation of the labels (addresses) used to forward packets.

LIB—Label Information Base. A database used by a label switch router (LSR) to store labels learned from other LSRs, and labels assigned by the local LSR.

LSP—label switched path. A sequence of hops in which a packet travels from one device to another device by means of label switching mechanisms. A label switched path can be established dynamically, based on normal routing mechanisms, or through configuration.

LSR—label switch router. A device that forwards Multiprotocol Label Switching (MPLS) packets based on the value of a fixed-length label encapsulated in each packet.

MPLS—Multiprotocol Label Switching. A switching method that forwards IP traffic using a label. This label instructs the devices and the switches in the network where to forward the packets. The forwarding of MPLS packets is based on preestablished IP routing information

PE device—provider edge device. A device that is part of a service provider's network connected to a customer edge (CE) device. All Virtual Private Network (VPN) processing occurs in the PE device.

VPN—Virtual Private Network. A secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.

CHAPTER 6

MPLS LDP VRF-Aware Static Labels

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Information About MPLS LDP VRF-Aware Static Labels

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 Multiprotocol Label Switching (MPLS) virtual private networks (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 devices 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 devices do not implement the LDP or RSVP label distribution, but do implement an MPLS forwarding path.
- To statically bind a virtual routing and forwarding (VRF)-aware label on a provider edge (PE) device 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 devices 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) devices 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.

How to Configure MPLS LDP VRF-Aware Static Labels

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

To reserve the labels that are to be statically assigned so that the labels are not dynamically assigned, perform the following task.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls label range** *minimum-value maximum-value* [**static** *minimum-static-value maximum-static-value*] **Example:** `Device(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 device for the range of labels you reserve to take effect.
Step 4	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show mpls label range** **Example:** `Device# 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

To configure MPLS static labels in the MPLS virtual private network (VPN) provider core, perform the following task.

MPLS static labels allow you to configure entries in the MPLS forwarding table and assign label values to forwarding equivalence classes (FECs) learned by the Label Distribution Protocol (LDP). You can manually configure a label switched path (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.

Before You Begin

- Globally enable Multiprotocol Label Switching (MPLS) on each label switch router (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. **exit**
5. **show mpls static binding ipv4**
6. **show mpls forwarding-table**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls static binding ipv4** *prefix mask* {*label* | **input** *label* | **output** *nexthop* {**explicit-null** | **implicit-null** | *label*}} **Example:** `Device(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	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	**show mpls static binding ipv4** **Example:** `Device# show mpls static binding ipv4`	Displays the configured static labels.
Step 6	**show mpls forwarding-table** **Example:** `Device# 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 devices do not implement either the Label Distribution Protocol (LDP) or Resource Reservation Protocol (RSVP) label distribution, but do implement an MPLS forwarding path.

Before You Begin

- Globally enable Multiprotocol Label Switching (MPLS) on each label switch router (LSR).
- Enable Cisco Express Forwarding on each LSR.

Note

- MPLS static cross-connect labels remain in the Label Forwarding Information Base (LFIB) even if the device 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls static crossconnect** *inlabel out-interface nexthop* {*outlabel* | **explicit-null** | **implicit-null**} **Example:** `Device(config)# mpls static crossconnect 45 pos5/0 45 explicit-null`	Specifies static cross connects. **Note** The *nexthop* argument is required for multiaccess interfaces.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**show mpls static crossconnect** **Example:** `Device# 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 virtual routing and forwarding (VRF)-aware label on a provider edge (PE) device 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.

Before You Begin

- Globally enable Multiprotocol Label Switching (MPLS) on each label switch router (LSR).
- Enable Cisco Express Forwarding on each LSR.
- Ensure the MPLS virtual private network (VPN) is configured.
- Ensure that the provider network has the MPLS Label Distribution Protocol (LDP) installed and running.

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. **exit**
5. **show mpls static binding ipv4 vrf** *vpn-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**mpls static binding ipv4 vrf** *vpn-name prefix mask* {**input** *label* | *label*} **Example:** `Device(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	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.
Step 5	**show mpls static binding ipv4 vrf** *vpn-name* **Example:** `Device(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

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

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:

```
Device(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:

```
Device# 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:

```
Device# show mpls label range

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

Example: Configuring MPLS Static Labels in the MPLS VPN Provider Core

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

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

```
Device# 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
```

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

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

```
Device(config)# mpls static binding ipv4 vrf vpn100 10.0.0.0 10.0.0.0 55
Device(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:

```
Device# 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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
MPLS VPN CSC with LDP and IGP	"MPLS VPN Carrier Supporting Carrier Using LDP and IGP" module in the *MPLS Layer 3 VPNs Inter-AS and CSC Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

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 7: 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 12.2(33)SRA 12.2(33)SXH 12.2(33)SB 12.3(14)T Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	

Feature Name	Releases	Feature Information
		The MPLS LDP VRF-Aware Static Labels feature explains how to configure the MPLS LDP VRF-Aware Static Labels feature and MPLS static labels. VRF-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. The MPLS static cross connect functionality is supported in Cisco IOS Releases 12.0(23)S, 12.3(14)T, and later releases. It is not supported in Cisco IOS Release 12.4(20)T. 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. In Cisco IOS XE Release 2.1, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router. The following commands were introduced or modified: **debug mpls static binding**, **mpls label range**, **mpls static binding ipv4**, **mpls static binding ipv4 vrf**, **show mpls label range**, **show**

Feature Name	Releases	Feature Information
		mpls static binding ipv4, **show mpls static binding ipv4 vrf**.