

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.

- Prerequisites for MPLS Label Distribution Protocol, on page 1
- Information About MPLS Label Distribution Protocol, on page 1
- How to Configure MPLS Label Distribution Protocol, on page 4
- Configuration Examples for MPLS Label Distribution Protocol, on page 19
- Additional References, on page 23

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.

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

Procedure

	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. • 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.

	Command or Action	Purpose
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.
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

Procedure

	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 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.

	Command or Action	Purpose
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

Procedure

	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`	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	**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

Procedure

	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 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.

	Command or Action	Purpose
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

Procedure

	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. • 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:**	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.

	Command or Action	Purpose
	`Device# show mpls ldp neighbor detail`	

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

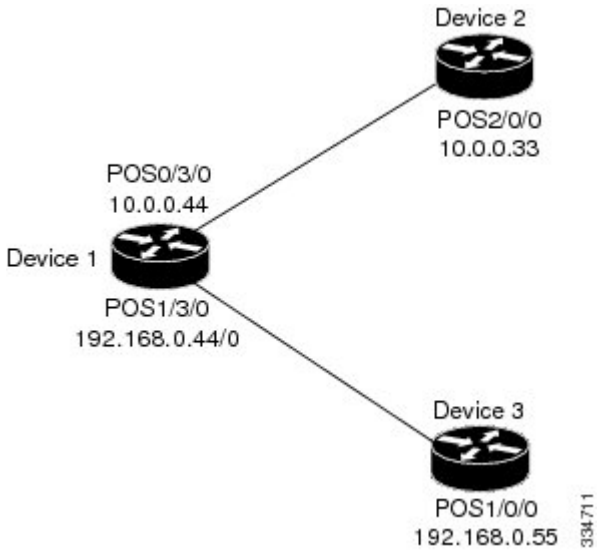
Example: Configuring Directly Connected MPLS LDP Sessions

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.

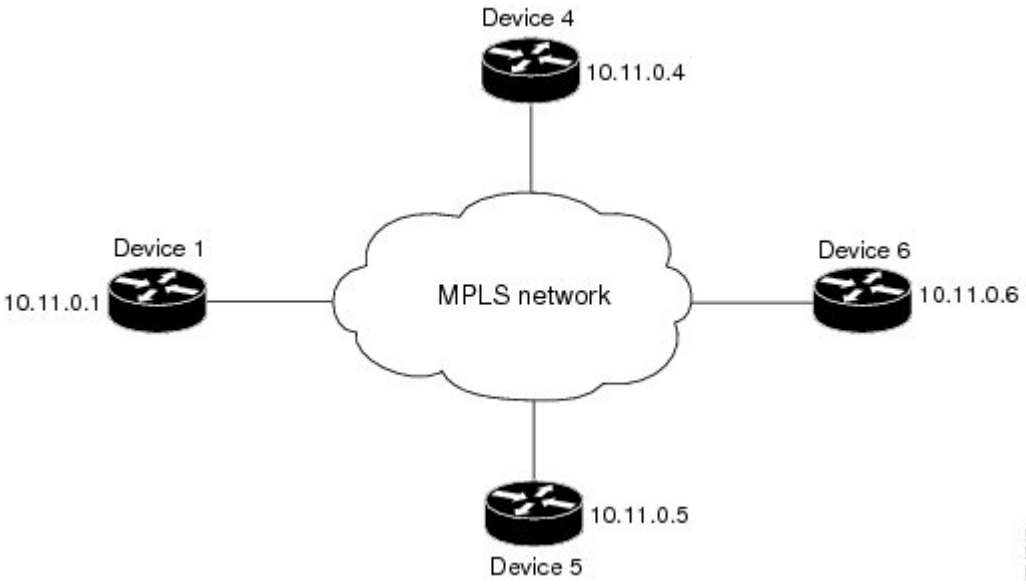
The configuration of Device 2 also uses the **mpls label protocol ldp** command in interface configuration mode. To specify LDP for all interfaces, use the **mpls label protocol ldp** command in global configuration mode without any interface **mpls label protocol** commands.

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
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference

Related Topic	Document Title
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