Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

This chapter describes how to configure multiprotocol label switching (MPLS) and Ethernet over MPLS (EoMPLS) on the Cisco ME 3800X and ME 3600X switches. MPLS is a packet-switching technology that integrates link layer (Layer 2) switching with network layer (Layer 3) routing. With MPLS, data is transferred over any combination of Layer 2 technologies, using any Layer 3 protocol, with increased scalability. MPLS supports different routes between a source and destination over a router-based Internet backbone.

- MPLS virtual private networks (VPNs) provides the capability to deploy and administer scalable Layer 3 VPN backbone services to business customers. A VPN is a secure IP-based network that shares resources on one or more physical networks.
- EoMPLS is a tunneling mechanism that transports Layer 2 Ethernet frames over an MPLS network. You can connect two Layer 2 networks that are in different locations, without bridges, routers, or switches at the locations. You enable the MPLS backbone to accept Layer 2 traffic by configuring the label-edge routers (LERs) at both ends of the MPLS backbone.

Note
For more information about MPLS, see the Multiprotocol Label Switching Configuration Guide Library, Cisco IOS Release 15.x.

For complete syntax and usage information for the MPLS commands used in this chapter, see Cisco IOS Multiprotocol Label Switching Command Reference.

This chapter contains these sections:

- General Restrictions, page 54-2
- Understanding MPLS Services, page 54-2
- Understanding MPLS VPNs, page 54-3
- Configuring MPLS VPNs, page 54-7
- Understanding MPLS Traffic Engineering and Fast Reroute, page 54-17
- Configuring MPLS Traffic Engineering and Fast Reroute, page 54-20
- Understanding EoMPLS, page 54-27
- Enabling EoMPLS, page 54-31
- Routed VPLS/EoMPLS, page 54-44
The switch supports hierarchical virtual private LAN service (H-VPLS) architecture to simulate LAN services over the MPLS network. The switch supports H-VPLS using IEEE 802.1Q tunneling or Ethernet over multiprotocol label switching (EoMPLS). For more information, see these software documents:

- For information about EoMPLS, see the “Monitoring and Maintaining MPLS and EoMPLS” section on page 54-85.
- For information about configuring EoMPLS, see the “Enabling EoMPLS” section on page 54-31.
- For information about IEEE 802.1Q tunneling, see the “Configuring Ethernet Virtual Connections (EVCs)” chapter.

The time-to-live (TTL) value is decremented at the penultimate hop popping (PHP) node for all incoming MPLS packets that are in the "no mpls propogate-ttl" mode, before sending them as IP packets. For example, if the TTL value of an incoming MPLS Packet was 255 and that of an incoming IP packet is 10, then the TTL value of the outgoing IP packet is 9.

Understanding MPLS Services

In conventional Layer 3 forwarding, as a packet travels across the network, each router extracts the packet-forwarding information from the Layer 3 header and uses this information as a key for a routing table lookup to determine the packet's next hop. In most cases, the only relevant field in the header is the destination address field, but in some cases other header fields are also relevant. For this reason, each router through which the packet passes must analyze the packet header.

With MPLS, the Layer 3 header is analyzed only once and then is mapped into a fixed-length, unstructured value called a label. Many different headers can map to the same label, as long as those headers always result in the same choice of next hop. In effect, a label represents a forwarding-equivalence class (FEC)—that is, a set of packets that can be very different but that are indistinguishable to the forwarding function.

The initial choice of label can be based exclusively on the contents of the Layer 3 header, or it can be based on policy, allowing forwarding decisions at subsequent hops to be based on policy. After a label is chosen, a short label header is put at the front of the Layer 3 packet and carried across the network as part of the packet. At subsequent hops through each MPLS router in the network, labels are exchanged, and the router uses MPLS forwarding-table lookups for the label to make forwarding decisions. It is not necessary to re-analyze the packet header. Because the label is a fixed length and unstructured, the MPLS forwarding-table lookup process is straightforward and fast.

Each label-switching router (LSR) in the network makes an independent, local decision as to which label value is used to represent which forwarding equivalence class. This association is known as a label binding. Each LSR informs its neighbors of the label bindings that it has made. When a labeled packet is sent from LSR A to neighboring LSR B, the label value carried by the packet is the label value that B assigned to represent the packet’s forwarding equivalence class. Thus, the label value changes as the IP packet travels through the network.
The ME 3800X and ME 3600X switches perform these LSR operations:

- **Swap and forward**
  The switch removes the top label, adds from 1 to 4 labels, then forwards the packet to the specified adjacency with no Layer 2 or Layer 3 lookup.

- **Pop and forward**
  The switch removes the top label in the packet and forwards the packet to the specified adjacency.

- **Pop and lookup**
  The switch removes the top label and performs a lookup based on the exposed packet.
  The type of lookup is determined by the popped label. The lookup could be:
  - IPv4—the label specifies a VRF or global table to be used for an IPv4 lookup.
  - MPLS Label—The switch performs a lookup on the exposed label. The exposed label might specify a Swap or Pop operation. The switch performs up to three recursive MPLS label lookups in the ternary content addressable memory (TCAM).

- **Drop packet**
  The switch drops the packet based on lookup of the top label.

A label represents a forwarding-equivalence class, but it does not represent a particular path through the network. In general, the path through the network continues to be chosen by the existing Layer 3 routing protocols, such as Open Shortest Path First (OSPF), Enhanced Interior Gateway Protocol (EIGRP), Intermediate-System-to-Intermediate-System (IS-IS), and Border Gateway Protocol (BGP). At each hop when a label is looked up, the choice of the next hop is determined by the dynamic routing algorithm.

The ME 3800X and ME 3600X switches support Label Distribution Protocol (LDP) session protection to maintain an LDP session during a link failure. LDP session protection eliminates the need for the link neighbor to relearn the prefix label bindings when the link recovers.

Provider Edge Routers (PE) operate at the edge of the provider network. They perform Label Edge Router (LER) imposition and disposition operations at the edge of an MPLS network. In an MPLS network, the ingress edge router receives the packet and adds a label to the packet. The egress edge router removes the label.

The ME 3800X and ME 3600X switches perform these operations:

- **Push**
  The ingress switch adds one or more labels.

- **Pop**
  The egress switch removes a label and forwards the packet.

### Understanding MPLS VPNs

Using MPLS virtual private networks (VPNs) provides the capability to deploy and administer scalable Layer 3 VPN backbone services to business customers. A VPN is 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.

VPN routes are distributed over the MPLS network by using multiprotocol BGP (MP-BGP), which also distributes the labels associated with each VPN route. MPLS VPN depends on VPN routing and forwarding (VRF) support to isolate the routing domains from each other. When routes are learned over an MPLS VPN, the switch learns the new route as a normal VRF route, except that the destination MAC
address for the next hop is not the real address, but a specially formed address that contains an identifier that is allocated for the route. When an MPLS-VPN packet is received on a port, the switch looks up the labels in the routing table to determine what to do with the packet.

Each VPN is associated with one or more VPN VRF instances. A VRF includes routing and forwarding tables and rules that define the VPN membership of customer devices attached to the customer-edge (CE) device. A customer site can be a member of multiple VPNs; however, a site can associate with only one VRF. A VRF has these elements:

- An IP routing table
- A Cisco Express Forwarding table
- A set of interfaces that use the forwarding table
- A set of rules and routing protocol parameters to control the information in the routing tables

A customer-site VRF contains all the routes available to the site from the VPNs to which it belongs. VPN routing information is stored in the IP routing table and the Cisco Express Forwarding table for each VRF. A separate set of tables is maintained for each VRF, which prevents information from being forwarded outside a VPN and prevents packets that are outside a VPN from being forwarded to a router within the VPN. Based on the routing information stored in the VRF IP routing table and the VRF Cisco Express Forwarding table, packets are forwarded to their destinations.

A provider-edge router binds a label to each customer prefix that is learned from a CE device and includes the label in the network reachability information for the prefix that it advertises to other (PE) routers. When a PE router forwards a packet that is received from a CE device across the provider network, it labels the packet with the label learned from the destination PE router. When the destination PE router receives the labeled packet, it examines the label and uses it to direct the packet to the correct CE device.

A customer data-packet carries two levels of labels when traversing the backbone:

- The top label directs the packet to the correct PE router.
- The second label defines how that PE router should forward the packet to the CE device.

**VPN Benefits**

MPLS VPNs allow service providers to deploy scalable VPNs and build the foundation to deliver value-added services, including:

- Connectionless service—MPLS VPNs are connectionless, which means that no prior action is required to establish communication between hosts. A connectionless VPN does not require tunnels and encryption for network privacy.
- Centralized service—MPLS VPNs are seen as private intranets, which allows delivery of targeted IP services to a group of users represented by a VPN.
- Scalability—MPLS-based VPNs use the peer model and Layer 3 connectionless architecture to leverage a highly scalable solution. The peer model requires a customer site to act as a peer to one PE router as opposed to all other customer PE or CE devices that are members of the VPN. The PE routers maintain VPN routes for those VPNs that are members. Routers in the core network do not maintain any VPN routes.
- Security—MPLS VPNs offer the same level of security as connection-oriented VPNs. Packets from one VPN do not inadvertently go to another VPN. Security provided at the edge of a provider network ensures that packets received from a customer are placed on the correct VPN; security provided at the backbone ensures that VPN traffic is kept separate.
- Easy to create—Because MPLS VPNs are connectionless, no specific point-to-point connection maps or topologies are required, and you can add sites to intranets and extranets to form closed user groups.
- Flexible addressing—Customers can continue to use their present address spaces without network address translation (NAT) because the MPLS VPN provides a public and private view of the address. A NAT is required only if two VPNs with overlapping address spaces want to communicate.
- Straightforward migration—You can build MPLS VPNs over multiple network architectures. Migration for the end customer is simplified because the CE router is not required to support MPLS, so no customer’s intranet modifications are needed.
- MPLS VPN also provides increased BGP functionality.

Figure 54-1 shows an example of a VPN with a service-provider backbone network, provider-edge (PE) and customer leading-edge (CLE) routers and customer-edge (CE) devices.

![Figure 54-1 VPNs with a Service-Provider Backbone](image)

Each VPN contains customer devices attached to the customer-edge (CE) devices. The customer devices use VPNs to exchange information between devices, and the provider routers (P) are not aware of the VPNs.

Figure 54-2 shows five customer sites communicating within three VPNs. The VPNs can communicate with these sites:
- VPN1: Sites 2 and 4
- VPN2: Sites 1, 3, and 4
- VPN3: Sites 1, 3, and 5
Distribution of VPN Routing Information

The distribution of VPN routing information is controlled through the use of VPN route target communities, implemented by BGP extended communities. VPN routing information is distributed in this manner:

- When a VPN route learned from a CE device is added to the BGP process, a list of VPN route target extended community attributes is associated with it. The attribute values are obtained from an export list of route targets associated with the VRF from which the route was learned.

- An import list of route target extended communities is also associated with each VRF. The import list defines route target extended community attributes that a route must have in order for the route to be imported into the VRF. For example, if the import list for a particular VRF includes route target communities A, B, and C, then any VPN route that carries any of those route target extended communities—A, B, or C—is imported into the VRF.

A PE router can learn an IP prefix from a CE device by static configuration, through a BGP session, or through a routing protocol, such as OSPF, EIGRP and Routing Information Protocol (RIP), with the CE device. The IP prefix is a member of the IPv4 address family. After it learns the IP prefix, the PE router converts it into a VPN-IPv4 prefix by combining it with an 8-byte route distinguisher. The generated prefix is a member of the VPN-IPv4 address family and uniquely identifies the customer address, even if the customer site is using globally nonunique (unregistered private) IP addresses.

BGP distributes reachability information for VPN-IPv4 prefixes for each VPN. BGP communication takes place at two levels: within IP domains, known as autonomous systems (internal BGP or IBGP), and between autonomous systems (external BGP or EBGP). The PE-to-PE sessions are IBGP sessions, and PE-to-CE sessions are EBGP sessions.

BGP propagates reachability information for VPN-IPv4 prefixes among provider-edge routers by using the BGP multiprotocol extensions, which define support for address families other than IPv4. It does this in a way that ensures that the routes for a given VPN are learned only by other members of that VPN, which enables members of the VPN to communicate with each other.

Restrictions for MPLS VPNs

6VPE traffic with matching tag as “Ether type IPv6” fails when layer 3 VPN packet is received.
Configuring MPLS VPNs

This section includes this information about configuring MPLS VPNs on a switch used as a PE router:

- Default MPLS Configuration, page 54-7
- MPLS VPN Configuration Guidelines, page 54-7

These sections describe the required tasks:

- Enabling MPLS, page 54-8
- Defining VPNs, page 54-9
- Configuring BGP Routing Sessions, page 54-10
- Configuring Provider-Edge-to-Provider-Edge Routing Sessions, page 54-10

You must also configure a provider-edge-to-customer-edge routing session. These sections provide example configurations:

- Configuring Provider-Edge-to-Customer-Edge Routing Sessions, page 54-12
- BGP Provider-Edge-to-Customer-Edge Configuration, page 54-12
- OSPF Provider-Edge-to-Customer-Edge Configuration, page 54-13
- RIPv2 Provider-Edge-to-Customer-Edge Routing Sessions, page 54-13
- Configuring Static Route Provider-Edge-to-Customer-Edge Routing Sessions, page 54-14
- EIGRP Provider-Edge-to-Customer-Edge Configuration, page 54-15

For an example of packet flow in an MPLS VPN, see the “Packet Flow in an MPLS VPN” section on page 54-15.

Default MPLS Configuration

By default, label switching of IPv4 packets along normally routed paths is globally enabled. MPLS forwarding of IPv4 packets is disabled by default on interfaces.

If no label protocol is explicitly configured for an interface, the default label distribution protocol for the switch is used by the Label Distribution Protocol (LDP). By default, the labels of all destinations are advertised to all LDP neighbors.

No VRFs are defined. The default routing table for an interface is the global routing table.

MPLS VPN Configuration Guidelines

Follow these guidelines when configuring MPLS VPN:

- MPLS requires that CEF is enabled on the switch. CEF is enabled by default. For more information about CEF, see the “Configuring Cisco Express Forwarding” section on page 41-114.
- The switch supports MPLS forwarding on the following interfaces:
  - Routed ports
  - SVIs
  - Routed EtherChannels
### Note

Some MPLS features require specific software licenses.

### SVI Limitations

The following limitations apply when configuring MPLS VPN over SVIs:

1. When MPLS is enabled on SVI, the SVI cannot be part of more than 4 EFP.
2. SVI cannot be part of a switchport trunk, allowing that VLAN and EVC BD.
3. SVI is not supported on port channel interfaces.
4. MPLS-TE is not supported on SVI.
5. When Xconnect is configured on a SVI, `mpls ip` configuration on that SVI is not allowed.

### Enabling MPLS

To use MPLS in a network, such as the one shown in Figure 54-1, MPLS must be globally enabled and explicitly configured on the provider-edge routers.

Beginning in privileged EXEC mode, follow these steps to incrementally deploy MPLS through a network, assuming that packets to all destination prefixes should be label-switched:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>ip routing</code> Enable IP routing on the switch if it is disabled.</td>
</tr>
</tbody>
</table>
| **Step 3** | `mpls label protocol {ldp | tdp | both}` Set the label protocol on the switch  
  - `ldp`—Specifies that the label distribution protocol (LDP) is to be used on the interface. This is the default protocol.  
  - `tdp`—Specifies that the tag distribution protocol (TDP) is to be used on the interface.  
  - `both`—Specifies that both label and tag distribution protocols are to be supported on the interface. |
| **Step 4** | `interface Loopback0` Enter interface configuration mode for a loopback interface.  
**Note** The loopback must be /32. |
| **Step 5** | `ip address ip address` Assign an IP address to the loopback interface.  
The subnet mask value has to be a host mask, /32. |
| **Step 6** | `mpls ldp router-id loopback 0 force` Specify the interface to force the loopback. |
| **Step 7** | `interface interface-id` Enter interface configuration mode, and specify the Layer 3 interface connected to the MPLS network. Valid interfaces include 10GigabitEthernet1/1/1, GigabitEthernet1/1/2, and VLANs. |
| **Step 8** | `ip address ip address` Assign an IP address to the Layer 3 interface connected to the MPLS network. |
| **Step 9** | `mpls ip` Enable MPLS forwarding of IPv4 packets along normally routed paths for the interface. |
Chapter 54  Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Configuring MPLS VPNs

Repeat these steps for every PE router in the network and the appropriate interfaces until all routers and connected interfaces are enabled for MPLS.

Use the `no mpls ip` global configuration command to disable MPLS on the switch. Use the `no mpls label protocol ldp` global configuration command to disable LDP.

Defining VPNs

Before defining VPNs, enable MPLS on the switch (see Enabling MPLS, page 54-8).

Beginning in privileged EXEC mode, follow these steps to define VPN routing instances on the PE router:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2  ip routing</td>
<td>Enable IP routing (required only if routing is disabled).</td>
</tr>
<tr>
<td>Step 3  ip vrf vrf-name</td>
<td>Enter VRF configuration mode, and define the VPN routing instance by assigning a VRF name.</td>
</tr>
<tr>
<td>Step 4  rd route-distinguisher</td>
<td>Create a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y).</td>
</tr>
<tr>
<td>Step 5  route-target { export</td>
<td>import</td>
</tr>
<tr>
<td>Step 6  import map route-map</td>
<td>(Optional) Associate the specified import route map with the VRF.</td>
</tr>
<tr>
<td>Step 7  export map route-map</td>
<td>(Optional) Associate the specified export route map with the VRF.</td>
</tr>
<tr>
<td>Step 8  exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 9  interface interface-id</td>
<td>Enter interface configuration mode, and specify the Layer 3 ES or VLAN interface to be associated with the VRF.</td>
</tr>
<tr>
<td>Step 10 ip vrf forwarding vrf-name</td>
<td>Associate the Layer 3 interface with the VRF.</td>
</tr>
<tr>
<td>Step 11 ip address ip address</td>
<td>Add the VRF route to the VRF routing table.</td>
</tr>
</tbody>
</table>
### Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

#### Chapter 54  Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

#### Configuring BGP Routing Sessions

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure BGP routing sessions in a provider network:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>ip routing</td>
<td>Enable IP routing (required only if routing is disabled).</td>
</tr>
<tr>
<td>3</td>
<td>router bgp autonomous-system-number</td>
<td>Enable a BGP routing process, assign it the AS number passed to the other BGP routers, and enter router configuration mode. The AS number can be from 1 to 65535, with 64512 to 65535 designated as private autonomous numbers.</td>
</tr>
<tr>
<td>4</td>
<td>no bgp default ipv4-unicast</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>neighbor {ip-address</td>
<td>peer-group-name} remote-as as-number</td>
</tr>
<tr>
<td>6</td>
<td>neighbor {ip-address</td>
<td>peer-group-name} update-source interface-id</td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>8</td>
<td>show ip bgp neighbor</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>9</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no ip vrf vrf-name** global configuration command to delete a VRF and remove interfaces from it. Use the **no ip vrf forwarding** interface configuration command to remove an interface from a VRF.

#### Configuring Provider-Edge-to-Provider-Edge Routing Sessions

You can configure provider-edge-to-provider-edge (PE-PE) routing sessions using IBGP or BGP.
IBGP Provider-Edge-to-Provider-Edge Configuration

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure a PE-to-PE routing session in a provider network that uses IBGP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 router bgp autonomous-system-number</td>
<td>Enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3 address-family vpnv4 [unicast]</td>
<td>Enter address family configuration mode to configure routing sessions that use standard VPNv4 address prefixes. (Optional) <strong>unicast</strong>—Specify VPNv4 unicast address prefixes.</td>
</tr>
<tr>
<td>Step 4 neighbor ip-address activate</td>
<td>Activate the advertisement of the IPv4 address family.</td>
</tr>
<tr>
<td>Step 5 neighbor ip address send-community extended</td>
<td></td>
</tr>
<tr>
<td>Step 6 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 7 show ip bgp [ipv4] [neighbors] [vpnv4]</td>
<td>Verify BGP configuration. Display information about all BGP IPv4 prefixes.</td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no router bgp autonomous-system** global configuration command to delete the BGP routing session.

IBGP Provider-Edge-to-Provider-Edge Configuration

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure a PE-to-PE routing session in a provider network that uses IBGP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 router bgp autonomous-system-number</td>
<td>Enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3 address-family ipv4</td>
<td>Enter routing family configuration mode to configure a routing session using IPv4.</td>
</tr>
<tr>
<td>Step 4 neighbor ip-address activate</td>
<td>Activate the advertisement of the IPv4 address family.</td>
</tr>
<tr>
<td>Step 5 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 6 show ip bgp [ipv4] [neighbors] [vpnv4]</td>
<td>Verify BGP configuration. Display information about all BGP IPv4 prefixes.</td>
</tr>
<tr>
<td>Step 7 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the **no router bgp autonomous-system** global configuration command to delete the BGP routing session.
Configuring Provider-Edge-to-Customer-Edge Routing Sessions

You can configure provider-edge-to-customer-edge (PE-CE) routing sessions using any of these protocols:
- BGP
- OSPF
- RIPv2
- Static Route
- EIGRP

BGP Provider-Edge-to-Customer-Edge Configuration

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure a provider-edge-to-customer-edge (PE-to-CE) routing session in a provider network that uses BGP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>router bgp autonomous-system-number</td>
</tr>
<tr>
<td>Step 3</td>
<td>address-family ipv4 [unicast] vrf vrf-name</td>
</tr>
<tr>
<td>Note</td>
<td>The default is off for auto-summary and synchronization in the VRF address-family configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>redistribute static</td>
</tr>
<tr>
<td>Step 5</td>
<td>redistribute connected</td>
</tr>
<tr>
<td>Step 6</td>
<td>neighbor address remote-as as-number</td>
</tr>
<tr>
<td>Step 7</td>
<td>neighbor address activate</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
</tr>
<tr>
<td>Step 9</td>
<td>show ip bgp [ipv4] [neighbors]</td>
</tr>
<tr>
<td>Step 10</td>
<td>show ip bgp vpnv4 vrf vrf-name</td>
</tr>
<tr>
<td>Step 11</td>
<td>show ip route vrf vrf-name</td>
</tr>
<tr>
<td>Step 12</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no router bgp as-number global configuration command to delete the BGP routing session.
OSPF Provider-Edge-to-Customer-Edge Configuration

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure a PE-to-PE routing session in a provider network that uses OSPF:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router ospf process-id vrf vrf-name Configure per-VRF OSPF.</td>
</tr>
<tr>
<td>Step 3</td>
<td>network ip-address area area-id Associate the interface with an OSPF area.</td>
</tr>
<tr>
<td>Step 4</td>
<td>router-id ip-address (Optional) Configure the OSPF router ID.</td>
</tr>
<tr>
<td>Step 5</td>
<td>domain-id ip-address (Optional) Configure the OSPF domain ID.</td>
</tr>
<tr>
<td>Step 6</td>
<td>router ospf process-id vrf vrf-name Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 7</td>
<td>redistribute bgp as-number subnets [metric metric-value] [metric-type {1</td>
</tr>
<tr>
<td>Step 8</td>
<td>router bgp as-number address-family ipv4 [unicast] vrf vrf-name Redistribute OSPF routes in MBGP.</td>
</tr>
<tr>
<td></td>
<td>redistribute ospf process-id [match {internal</td>
</tr>
<tr>
<td>Step 9</td>
<td>show ip bgp vpnv4 vrf vrf-name Display VPNv4 address information from the BGP table.</td>
</tr>
<tr>
<td>Step 10</td>
<td>show ip route vrf vrf-name Display the IP routing table associated with a VRF instance.</td>
</tr>
</tbody>
</table>

Use the no router bgp as-number global configuration command to delete the BGP routing session.

RIPv2 Provider-Edge-to-Customer-Edge Routing Sessions

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure RIPv2 PE-to-CE routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router rip Enable RIP routing, and enter router configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>version 2 Configure RIPv2.</td>
</tr>
<tr>
<td>Step 4</td>
<td>address-family ipv4 [unicast] vrf vrf-name Define RIPv2 parameters for PE-to-CE routing sessions, and enter VRF address-family configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Note    The default is off for auto-summary and synchronization in the VRF address-family configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>network ip-address Enable RIP on the PE-to-CE link.</td>
</tr>
</tbody>
</table>
Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure static routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ip route vrf vrf-name prefix mask [next-hop-address] [interface [interface-number]] [global] [distance] [permanent] [tag tag]</td>
<td>Configure per-VRF static route on the PE router.</td>
</tr>
<tr>
<td>router bgp as-number address-family ipv4 [unicast] vrf vrf-name</td>
<td>Configure IPv4 address-family.</td>
</tr>
<tr>
<td>redistribute connected</td>
<td>Redistribute the IPV4 address-family in BGP.</td>
</tr>
<tr>
<td>or network network-number [mask network-mask] [route-map map-name]</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show ip bgp vpnv4 vrf vrf-name</td>
<td>Display VPNv4 address information from the BGP table.</td>
</tr>
</tbody>
</table>

Use the no router rip global configuration command to disable RIP routing.

### Configuring Static Route Provider-Edge-to-Customer-Edge Routing Sessions

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure static routing:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>ip route vrf vrf-name prefix mask [next-hop-address] [interface [interface-number]] [global] [distance] [permanent] [tag tag]</td>
<td>Configure per-VRF static route on the PE router.</td>
</tr>
<tr>
<td>router bgp as-number address-family ipv4 [unicast] vrf vrf-name</td>
<td>Configure IPv4 address-family.</td>
</tr>
<tr>
<td>redistribute connected</td>
<td>Redistribute the IPV4 address-family in BGP.</td>
</tr>
<tr>
<td>or network network-number [mask network-mask] [route-map map-name]</td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>show ip bgp vpnv4 vrf vrf-name</td>
<td>Display VPNv4 address information from the BGP table.</td>
</tr>
</tbody>
</table>
Configuring MPLS VPNs

EIGRP Provider-Edge-to-Customer-Edge Configuration

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure a provider-edge-to-customer-edge (PE-to-CE) routing session in a provider network that uses EIGRP:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>router eigrp autonomous-system-number</td>
<td>Configure the EIGRP routing process with the AS number passed to other</td>
</tr>
</tbody>
</table>

EIGRP Provider-Edge-to-Customer-Edge Configuration

Beginning in privileged EXEC mode, follow these steps on the provider-edge router to configure a provider-edge-to-customer-edge (PE-to-CE) routing session in a provider network that uses EIGRP:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode</td>
</tr>
<tr>
<td>Step 2 router eigrp autonomous-system-number</td>
<td>Configure the EIGRP routing process with the AS number passed to other</td>
</tr>
<tr>
<td>Step 3 address-family ipv4 [unicast] vrf vrf-name</td>
<td>Define EIGRP parameters for PE-to-CE routing sessions, and enter VRF</td>
</tr>
<tr>
<td>Step 4 network ip-address wildcard-mask</td>
<td>Specify the network for the VRF.</td>
</tr>
<tr>
<td>Step 5 autonomous-system autonomous-system-number</td>
<td>Specify the autonomous system number of the EIGRP network for the</td>
</tr>
<tr>
<td>Step 6 redistribute bgp autonomous-system-number</td>
<td>Redistribute BGP into the EIGRP.</td>
</tr>
<tr>
<td>Step 7 end</td>
<td>Return to privileged EXEC mode</td>
</tr>
<tr>
<td>Step 8 show ip eigrp vrf neighbors</td>
<td>Display neighbors discovered by EIGRP that carry VRF information.</td>
</tr>
<tr>
<td>Step 9 show ip eigrp vrf topology</td>
<td>Display VRF entries in the EIGRP topology table.</td>
</tr>
<tr>
<td>Step 10 show ip eigrp vrf traffic</td>
<td>Display EIGRP VRF traffic statistics.</td>
</tr>
<tr>
<td>Step 11 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Use the no router eigrp as-number global configuration command to delete the EIGRP routing session.

Packet Flow in an MPLS VPN

Figure 54-3 is an example of packet flow between two customer sites in an MPLS VPN network.
A customer (Fast Ethernet) port on switch PE1 is configured for routed operation in a VPN. The port uses static routing or a routing protocol (RIP, OSPF, EIGRP, or BGP) to forward packets. MP-BGP is configured over the PE1 switch ES port with a route distinguisher that is associated with the customer’s VPN. MP-BGP is configured to redistribute the routes and their associated VPN labels over the ES port that is using this route distinguisher.

The packet flow follows these steps:

**Step 1** Provider-edge switch PE1 (which could be a Metro switch) receives a packet from the customer switch at site 1. The switch determines from the lookup table that the VRF is a VLAN running MPLS and uses the MPLS lookup table to determine what to do with the packet. The MPLS lookup table contains the peer LSR as the destination MAC address and the local interface as the source MAC address.

**Step 2** PE1 finds a BGP route with the appropriate next hop and labels, adds the appropriate labels to the packet, and forwards the packet out of the ES port to the next hop router (P3).

**Step 3** The P3 router receives the packet and forwards it over the MPLS-VPN network, based on the packet’s top label—the interior gateway protocol (IGP) label—and then removes the top label.

**Step 4** PE3 receives the packet, removes the MPLS encapsulation, and forwards the packet by using the VRF interface associated with the VPN label contained in the packet that has the customer-edge switch CE2 as the destination.

### Sample Configurations

This example shows a Layer 3 VPN configured on an EFP:

```
Switch# show run interface g0/24
Building configuration...

Current configuration : 226 bytes
!
interface GigabitEthernet0/24
 port-type nni
```
This example shows a Layer 3 VPN configured on a switched virtual interface (SVI):

Switch# `show run interface vlan 100`
Building configuration...

Current configuration : 82 bytes
!
interface Vlan100
  ip vrf forwarding A
  ip address 100.1.1.1 255.255.255.0
end

This example shows a Layer 3 VPN configured using non-switchport port mode:

Switch# `show run interface g0/24`
interface GigabitEthernet0/24
  port-type nni
  no switchport
  ip vrf forwarding A
  ip address 100.1.1.1 255.255.255.0

This example shows a Layer 3 VPN configured on a switchport and an SVI:

Switch# `show run interface g0/24`
interface GigabitEthernet0/24
  port-type nni
  switchport access vlan 100
end

Switch# `show run interface vlan 100`
interface Vlan100
  ip vrf forwarding A
  ip address 100.1.1.1 255.255.255.0
end

For information about load balancing, see the *Multiprotocol Label Switching Configuration Guide Library, Cisco IOS Release 15.x*.

---

**Understanding MPLS Traffic Engineering and Fast Reroute**

This section describes the switch support of MPLS traffic engineering (TE) and includes these sections:

- **MPLS TE, page 54-18**
- **MPLS TE Fast Reroute, page 54-19**
- **MPLS TE Primary and Backup Autotunnel, page 54-20**
MPLS TE

MPLS traffic engineering (TE) provides control over how traffic is routed through the network. This increases the bandwidth efficiency by preventing over-use of some links while other links are under used. TE overrides the shortest path selected by the Interior Gateway Protocol (IGP) to select the most efficient path for traffic. Network resources are advertised by using a link-state routing protocol, such as Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF). MPLS TE then uses a unidirectional LSP or tunnel to forward traffic, calculating the tunnel paths based on required and available resources.

Regular MPLS traffic engineering automatically establishes and maintains label-switched paths (LSPs) across the backbone using Resource Reservation Protocol (RSVP). The path used by a given LSP is based on the LSP resource requirements and available network resources such as bandwidth. Available resources are flooded via extensions to the link-state based IGP.

For more information on MPLS TE, see Multiprotocol Label Switching Configuration Guide Library, Cisco IOS Release 15.x.

Paths for LSPs are calculated at the LSP headend, the first router in the LSP path. Under failure conditions, the headend determines a new route for the LSP based on destination, bandwidth, link attributes, and priority. RSVP-TE then establishes and maintains the TE tunnel across the MPLS backbone network. Packets are switched inside the tunnel by using MPLS labels. Recovery at the headend provides for the optimal use of resources.

The number of supported tunnels depends upon the installed license. Refer to the licensing document.

The switch supports these MPLS TE features:

- OSPF, IS-IS, and RSVP extensions to support MPLS TE
- TE autotunnel primary and backup
- TE tunnel reoptimization to improve overall efficiency by rerouting some traffic trunks to new paths
- TE load sharing to a destination over paths with unequal costs. The switch supports up to 256 load-shared routes (load-shared routes for up to 256 destinations). Any additional load-balanced routes are forwarded in one path in the hardware.
- TE IP explicit address exclusion to exclude a link or node from the path. You use the `ip explicit-path global configuration mode to enter explicit-path configuration mode and then use the `exclude-address` command to specify addresses to exclude from the path.
- Support for LDP over TE tunnels for Layer 3 VPN traffic by entering the `mpls ip` interface configuration command on the tunnel interface. The switch does not support LDP over TE tunnels for Layer 2 VPN traffic.
- Traffic forwarding to the TE tunnel using static routing
- TE autoroute, which installs the routers announced by the tailend router and the downstream routers into the routing table of the headend router. All traffic directed to prefixes beyond the tunnel end are pushed into the tunnel.
- Prefix-independent fast reroute.

The switch does not support these MPLS TE features:

- Interarea TE support for OSPF and IS-IS
- TE path protection
- Shared risk link group (SRLG)
- Traffic forwarding to the TE tunnel using policy routing
• Traffic forwarding to the TE tunnel using forwarding adjacency
• Auto bandwidth
• Autotunnel mesh group

### MPLS TE Fast Reroute

With MPLS TE, when a link or node failure occurs, the LSP headend determines a new route for the LSP. However, due to messaging delays, the headend cannot recover as quickly as making a repair at the point of failure. Fast reroute (FRR) protects the LSPs from link and node failures by locally repairing the LSP at the point of failure, allowing data to continue to flow while the headend routers establish replacement end-to-end LSPs. Fast reroute locally repairs the protected LSP by rerouting all LSP traffic crossing a failed link over backup tunnels that bypass the failed link or node.

- Link protection is also referred to as next hop (N-Hop) protection because the new route terminates at the next hop beyond the LSP failure.
- Node protection is also referred to as next-next-hop (NN-Hop) protection because the new route bypasses the next hop node and terminates at the node following the next-hop node. Node protection also provides protection from link failures because traffic bypasses the failed link and the failed node.

For more information about MPLS TE fast reroute, see *Multiprotocol Label Switching Configuration Guide Library, Cisco IOS Release 15.x*.

The reroute decision is completely controlled locally by the router interfacing the failed link. The headend of the tunnel is also notified of the link failure through the IGP or through RSVP; the headend then attempts to establish a new LSP that bypasses the failure.

---

**Note**

Local reroute prevents any further packet loss caused by the failed link. If the tunnel is configured to be dynamic, the headend of the tunnel then has time to reestablish the tunnel along a new, optimal route. If the headend still cannot find another path to take, it continues to use the backup tunnel.

Fast link change detection (FLCD) and RSVP hello messages form the failure detection mechanism. FLCD is notified when an interface encounters a link status change and RSVP hello enables the RSVP nodes to detect when a neighboring node is not reachable. You can configure RSVP hello messages by entering the `ip rsvp signalling hello [fast reroute] refresh` global configuration command.

---

**Note**

The `ip rsvp signalling hello [fast reroute] refresh` command is needed only when loss of signal cannot be detected.

Backup tunnels have these characteristics on the switch:

- A backup tunnel can protect multiple LSPs.
- When the primary tunnel restores, traffic changes from the backup tunnel back to the primary tunnel.
- The switch does not support backup tunnel bandwidth protection.
- The switch supports MPLS TE fast reroute over only routed ports and not over SVIs or EtherChannels.
MPLS TE Primary and Backup Autotunnel

The primary and backup autotunnel feature enables a switch to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces configured for MPLS TE.

- Primary autotunnel dynamically creates one-hop primary tunnels on all MPLS TE interfaces. Instead of configuring an MPLS TE tunnel with fast-reroute, you enter the `mpls traffic-eng auto-tunnel primary onehop` global configuration command to dynamically create one-hop tunnels on all MPLS TE interfaces.
- Backup autotunnel enables a router to dynamically build backup tunnels when they are needed so that you do not need to configure them manually. To configure backup autotunnel, enter the `mpls traffic-eng auto-tunnel backup router` configuration command.

Configuring MPLS Traffic Engineering and Fast Reroute

This section includes this information about configuring MPLSTE on a switch:

- Default MPLS TE and Fast Reroute Configuration, page 54-20
- MPLS TE and Fast Reroute Configuration Guidelines, page 54-20

These sections describe the configuration procedures:

- Configuring MPLS TE, page 54-21
- Configuring TE Fast Reroute, page 54-23
- Configuring Primary and Backup Autotunnels, page 54-25

Default MPLS TE and Fast Reroute Configuration

MPLS TE and fast reroute are not configured.
Backup or primary autotunnel is not configured.

MPLS TE and Fast Reroute Configuration Guidelines

Follow these guidelines when configuring MPLS TE:

- Not all of the MPLS TE commands that are visible in the switch command-line interface help are supported. See the “Multiprotocol Label Switching (MPLS) Commands” section on page 67-6 of Appendix 67, “Unsupported Commands.”
- To configure MPLS traffic engineering and fast reroute, the network must be running IP Cisco Express Forwarding (CEF) and MPLS and support at least one of these protocols: OSPF or IS-IS.
- For information on all MPLS commands, see the MPLS command reference at this URL: http://www.cisco.com/en/US/docs/ios-xml/ios/mpls/command/mp-cr-book.html
Configuring MPLS TE

For more information on MPLS TE, see *Multiprotocol Label Switching Configuration Guide Library, Cisco IOS Release 15.x*.

Beginning in privileged EXEC mode, follow these steps to configure MPLS TE and configure an interface to support RSVP-based tunnel signalling and IGP flooding:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mpls traffic-eng tunnels</td>
</tr>
<tr>
<td>Step 3</td>
<td>ip rsvp signalling hello</td>
</tr>
<tr>
<td>Step 4</td>
<td>interface interface-id</td>
</tr>
<tr>
<td>Step 5</td>
<td>mpls traffic-eng tunnels</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip rsvp bandwidth <em>bandwidth</em></td>
</tr>
<tr>
<td>Step 7</td>
<td>ip rsvp signalling hello</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
</tr>
<tr>
<td>Step 9</td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

Enter `no mpls traffic-eng tunnels` to disable MPLS traffic engineering tunnels on the switch or interface. Enter the `no rsvp bandwidth` interface configuration command to return to the default.

Configuring a MPLS TE Tunnel

Beginning in privileged EXEC mode, follow these steps to configure an MPLS traffic engineering tunnel. The configured tunnel has two path setup options—a preferred explicit path and a backup dynamic path:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface tunnel <em>tunnel-id</em></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip unnumbered loopback0</td>
</tr>
<tr>
<td>Step 4</td>
<td>tunnel destination <em>A.B.C.D</em></td>
</tr>
<tr>
<td>Step 5</td>
<td>tunnel mode mpls traffic-eng</td>
</tr>
<tr>
<td>Step 6</td>
<td>tunnel mpls traffic-eng autoroute announce</td>
</tr>
<tr>
<td>Step 7</td>
<td>tunnel mpls traffic-eng priority</td>
</tr>
</tbody>
</table>
Chapter 54  Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Configuring MPLS Traffic Engineering and Fast Reroute

Enter the no forms of the commands to remove the configured MPLS tunnels. Enter the no ip explicit-path name global configuration command to disable IP explicit paths.

Configuring the Routing Protocol for MPLS TE

Beginning in privileged EXEC mode, follow these steps to configure IS-IS or OSPF for MPLS traffic engineering:
To remove the traffic engineering router identifier, use the `no mpls traffic-eng router-id` command.

### Configuring TE Fast Reroute

Before or after entering the commands described in these procedures, you must enable the MPLS traffic engineering tunnel capability globally on the tunnel routers by entering the `mpls traffic-eng tunnels` global and interface configuration commands. For information about the commands for MPLS TE fast reroute, see this URL:


Beginning in privileged EXEC mode, follow these steps to enable MPLS traffic engineering fast reroute on an MPLS tunnel and to create a backup tunnel to the next hop or next-next hop:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface tunnel <code>tunnel-number</code></td>
<td>Create a tunnel interface, and enter interface configuration mode for the tunnel interface.</td>
</tr>
<tr>
<td>3</td>
<td><code>ip unnumbered interface-id</code></td>
<td>Configure the tunnel source address. This is usually the IP address of the loopback0 interface. The command is not effective until loopback0 is configured with an IP address.</td>
</tr>
<tr>
<td>4</td>
<td>tunnel destination <code>A.B.C.D</code></td>
<td>Specify the IP address of the device where the tunnel terminates. This should be the router ID of the next-hop or next-next hop of the LSP to be protected.</td>
</tr>
<tr>
<td>5</td>
<td><code>tunnel mode mpls traffic-eng</code></td>
<td>Set the mode of a tunnel to MPLS for traffic engineering.</td>
</tr>
</tbody>
</table>
| 6    | `tunnel mpls traffic-eng path-option number {dynamic | explicit {name path-name | path-number}} [lockdown] [verbatim]` | Configure a path option for an MPLS TE tunnel. Keywords have these meanings:  
  - **number**—When multiple paths are configured, lower-numbered options are preferred.  
  - **dynamic**—Specify that the LSP path is dynamically calculated.  
  - **explicit**—Specify that the LSP path is an explicit IP path.  
  - **name path-name**—Path name of the IP explicit path that the tunnel uses with this option.  
  - **name path-number**—Path number of the IP explicit path that the tunnel uses with this option.  
  - (Optional) **lockdown**—Specify that the LSP cannot be reoptimized.  
  - (Optional) **verbatim**—Specify that the path is send out as is with no checking. |
Configuring MPLS Traffic Engineering and Fast Reroute

Enter the no tunnel mode mpls traffic-eng global configuration command to disable MPLS traffic engineering or the no ip explicit-path global configuration command to remove the IP explicit path configuration.

### Configuring a Protected Link to Use a Backup Tunnel

Beginning in privileged EXEC mode, follow these steps to configure a protected link to use the backup tunnel:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>ip explicit-path name path-name</td>
<td>Specify the path of the tunnel, and enter IP explicit path command mode to set up or modify the explicit path. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.</td>
</tr>
<tr>
<td>Step 8</td>
<td>next-address A.B.C.E</td>
<td>Specify the next IP address in the explicit path.</td>
</tr>
<tr>
<td>Step 9</td>
<td>end</td>
<td>Repeat Step 8 for additional IP addresses in the path.</td>
</tr>
<tr>
<td>Step 10</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 11</td>
<td>show ip explicit-paths</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 12</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

To remove the backup tunnel configuration, enter the no mpls traffic-eng backup-path tunnel interface configuration command.

### Configuring Fast Reroute Failure Detection (Optional)

This configuration is needed only when loss of signal cannot be detected.

Beginning in privileged EXEC mode, follow these steps to configure fast reroute failure detection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Specify the interface ID of the protected link and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>mpls traffic-eng backup-path tunnel tunnel-id</td>
<td>Configure the interface to use a backup tunnel in the event of a detected failure on that interface. You can enter this command multiple times to associate the protected interface with multiple backup tunnels.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show mpls traffic-eng fast-reroute database</td>
<td>Verify the that backup protection is configured. A ready status means that the tunnel is ready to switch to backup; an active status means that tunnel traffic is on backup.</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
### Configure MPLS Traffic Engineering and Fast Reroute

**Step 1**
Configure terminal

- **Purpose**: Enter global configuration mode.

**Step 2**
ip rsvp signalling hello

- **Purpose**: Globally enable Hello signalling on the switch.

**Step 3**
interface interface-id

- **Purpose**: Specify an interface ID, and enter interface configuration mode.

**Step 4**
ip rsvp signalling hello fast-reroute refresh misses number

- **Purpose**: Configure the number of consecutive RSVP TE hello acknowledgments a node can miss before the node communication with its neighbor status is down. Valid values are from 4 to 10. The default is 4.

**Step 5**
ip rsvp signalling hello fast-reroute refresh interval interval-value

- **Purpose**: Configure the frequency, in milliseconds, at which a node sends hello messages to a neighbor. Valid values are from 10 to 30000 (.01 to 30 seconds). The default frequency is 1000 milliseconds (10 seconds).

**Note**: To prevent false detection of a down neighbor and unnecessarily triggering fast reroute, we recommend configuring a minimum frequency of 200 ms.

**Step 6**
ip rsvp signalling hello

- **Purpose**: Enable Hello signalling on the interface.

**Step 7**
end

- **Purpose**: Return to privileged EXEC mode.

**Step 8**
show ip rsvp fast-reroute

- **Purpose**: Verify the configuration.

**Step 9**
copy running-config startup-config

- **Purpose**: (Optional) Save your entries in the configuration file.

Enter the `no ip rsvp signalling hello` global configuration command to disable Hello signalling on the switch. Enter the `no ip rsvp signalling hello fast-reroute refresh misses` or the `no ip rsvp signalling hello fast-reroute refresh interval` interface configuration command to set the misses or refresh interval to the default.

### Configuring Primary and Backup Autotunnels

The Autotunnel Primary and Backup feature enables a router to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces configured for MPLS TE. For information about the commands for MPLS autotunnel, see this URL:


Beginning in privileged EXEC mode, follow these steps to automatically create primary tunnels to all next hop neighbors:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>mpls traffic-eng auto-tunnel primary onehop</td>
</tr>
</tbody>
</table>
Enter the `no` form of each command to delete the tunnel or disable the feature or capability. To remove all primary auto tunnels, enter the `clear mpls traffic-eng auto-tunnel primary` privileged EXEC command.

Beginning in privileged EXEC mode, follow these steps to establish MPLS backup auto tunnels:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>mpls traffic-eng auto-tunnel backup</code></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>mpls traffic-eng auto-tunnel backup nhop-only</code></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>mpls traffic-eng auto-tunnel backup tunnel-num [min num] [max num]</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>mpls traffic-eng auto-tunnel backup timers removal unused sec</code></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>mpls traffic-eng auto-tunnel backup config unnumbered interface interface-id</code></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>mpls traffic-eng auto-tunnel primary config mpls ip</code></td>
</tr>
</tbody>
</table>
Understanding EoMPLS

Any Transport over MPLS (AToM) is a solution for transporting Layer 2 packets over an MPLS network, allowing service providers to use the MPLS network to provide connectivity between customer sites with existing Layer 2 networks. Instead of separate networks with network management environments, service providers can use the MPLS network to transport all types of traffic for different customers. The switch supports EoMPLS, a subset of AToM that uses a tunneling mechanism to carry Layer 2 Ethernet traffic.

EoMPLS encapsulates Ethernet frames in MPLS packets and forwards them across the MPLS network. Each frame is sent as a single packet, and the provider-edge (PE) routers connected to the backbone add and remove labels as appropriate for packet encapsulation:

- The ingress PE router receives an Ethernet frame and encapsulates the packet by removing the preamble, the start of frame delimiter (SFD), and the frame check sequence (FCS). The rest of the packet header is not changed.
- The ingress PE router adds a point-to-point virtual connection label and a label switched path (LSP) tunnel label for normal MPLS routing through the MPLS backbone.
- The network core routers use the LSP tunnel label to move the packet through the MPLS backbone and do not distinguish Ethernet traffic from any other types of packets in the MPLS backbone.
- At the other end of the MPLS backbone, the egress PE router receives the packet and de-encapsulates the packet by removing the LSP tunnel label if one is present. The PE router also removes the virtual-connection label from the packet.
- The provider-edge router updates the header, if necessary, and sends the packet out the appropriate interface to the destination switch.
- The switch supports auto-sense signaling to allow two remote PEs to negotiate VC type signaling.
- The failure of a remote CE-PE link is communicated to the local PE and the local PE shuts down its transmit signal. This results in the local CE link shutdown. The local PE still maintains all the associated interface with local CE in UP state.

The MPLS backbone uses the tunnel labels to send the packet between the PE routers. The egress PE router uses the virtual-connection label to select the outgoing interface for the Ethernet packet. EoMPLS tunnels are unidirectional; for bidirectional EoMPLS, you need to configure one tunnel in each direction.

The point-to-point virtual connection requires you to configure virtual-connection endpoints at the two PE routers. Only the provider-edge routers at the ingress and egress points of the MPLS backbone are aware of the virtual connections dedicated to transporting Layer 2 traffic. Other routers do not have table entries for these virtual connections.

This section includes additional information about these topics:

- Interaction with Other Features, page 54-28
- EoMPLS Limitations, page 54-30
Interaction with Other Features

This section describes how EoMPLS interacts other features. It includes these sections:

- EoMPLS and IEEE 802.1Q Tunneling, page 54-28
- EoMPLS and Layer 2 Tunneling, page 54-29
- EoMPLS and Q in Q, page 54-29
- EoMPLS and QoS, page 54-30

EoMPLS and IEEE 802.1Q Tunneling

IEEE 802.1Q tunneling enables service providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and segregating traffic in different VLANs. For more information about IEEE 802.1Q tunneling, see Chapter 12, “Configuring Ethernet Virtual Connections (EVCs).”

Figure 54-4 is an example configuration where IEEE 802.1Q-tunneled traffic is forwarded using EoMPLS over an MPLS network. To support IEEE 802.1Q tunneling in a topology where a Layer 2 device connects to an MPLS network through a switch functioning as a provider-edge device, the ingress LAN port on the PE that receives the IEEE 802.1Q tunnel-encapsulated traffic (PE1) is configured as a tunnel port that accepts VLAN 100 traffic. On PE1, the interface is configured for port-based EoMPLS forwarding, with PE2 as the destination IP address. When packets from VLANs 10 to 50 arrive from CE1, they are encapsulated in VLAN 100 and sent to the PE1 egress port that is connected to the MPLS network. At the egress port, an MPLS tag is added to the frame header before it is mapped to a virtual connection and forwarded to the next MPLS PE (PE2).

By entering the xconnect interface configuration command on either a VLAN for VLAN-based EoMPLS or an Ethernet port for port-based EoMPLS, you can configure an EoMPLS tunnel to forward traffic based on either the customer VLAN or the Ethernet port.

- To forward IEEE 802.1Q tunnel-encapsulated traffic through the MPLS core to a specific recipient on the other side of the MPLS network, configure port-based EoMPLS.
- To forward IEEE 802.1Q tunnel-encapsulated traffic from an access device to a provider-edge router, configure VLAN-based EoMPLS.
EoMPLS and Layer 2 Tunneling

Layer 2 protocol tunneling over an EoMPLS link allows CDP, STP, and VTP protocol data units (PDUs) to be tunneled through an MPLS network. To support Layer 2 protocol tunneling when the Layer 2 device connects to an MPLS network through a switch functioning as a PE, you configure the ingress port on the provider-edge that receives the Layer 2 protocol traffic as a tunnel port. The Layer 2 protocol traffic is encapsulated before it is forwarded over the MPLS network. For more information about Layer 2 protocol tunneling, see Chapter 12, “Configuring Ethernet Virtual Connections (EVCs).”

This example shows how to configure Layer 2 tunneling:

```bash
Switch(config)# interface Vlan102
Switch(config-if)# no ip address
Switch(config-if)# xconnect 12.12.12.12 102 encapsulation mpls

Switch(config)# interface GigabitEthernet0/24
Switch(config-if)# switchport trunk allowed vlan none
Switch(config-if)# switchport mode trunk
Switch(config-if)# no keepalive
Switch(config-if)# service instance 1 ethernet
Switch(config-if)# encapsulation untagged
Switch(config-if)# l2protocol tunnel cdp
Switch(config-if)# bridge-domain 102
```

EoMPLS and Q in Q

When the remote PE supports Q in Q, but not VC type 4, you can use the `platform rewrite imposition tag push 1 symmetric` interface configuration command to push an additional VLAN tag to make the type 5 PW work like a Q in Q Layer 2 port.

**Note**

The command has no effect on a VC type 4 PW.

This example sends packets with VLAN 11 to EFP 1. When the packets reach the remote PE, the payload Layer 2 packets have two VLAN tags, VLAN 101 and VLAN 11.

```bash
Switch (config)# interface gigabitEthernet 0/15
Switch (config-if)# switchport mode trunk
Switch (config-if)# switchport trunk allowed vlan none
Switch (config-if)# service instance 1 ethernet
Switch (config-if-srv)# encapsulation dot1q 11
Switch (config-if-srv)# bridge-domain 101
Switch (config-if-srv)# exit
Switch (config-if)# exit

Switch (config)# interface Vlan101
Switch (config-if)# platform rewrite imposition tag push 1 symmetric
Switch (config-if)# xconnect 12.12.12.12 300 encapsulation mpls

Switch # show running-config interface gigabitEthernet 0/15
Building configuration...

Current configuration : 188 bytes
Understanding EoMPLS

interface GigabitEthernet0/15
  port-type nni
  switchport trunk allowed vlan none
  switchport mode trunk
  service instance 1 ethernet
  encapsulation dot1q 11
  bridge-domain 101

Switch # show running-config interface vlan 101
Building configuration...

Current configuration : 136 bytes

interface Vlan101
  no ip address
  platform rewrite imposition tag push 1 symmetric
  xconnect 12.12.12.12 300 encapsulation mpls
end

Packets sent from the remote PE have an outer VLAN with any VLAN number and VLAN 11. The outer VLAN number is popped at this PE, and the packets are sent out from EFP 1 with VLAN 11.

EoMPLS and QoS

EoMPLS supports QoS by using three experimental bits in a label to determine the priority of packets. To support QoS between label edge routers (LERs), you set the experimental bits in both the virtual connection and the tunnel labels. EoMPLS QoS classification occurs on ingress, and you can only match on Layer 3 parameters (such as IP or DSCP) and Layer 2 parameters (CoS). See Chapter 35, “Configuring Quality of Service (QoS)” for more information about EoMPLS and QoS.

EoMPLS Limitations

These restrictions apply to EoMPLS:

- You cannot configure MPLS and EoMPLS on the same port.
- MTU—EoMPLS does not support packet fragmentation and reassembly. Therefore, the maximum transmission unit (MTU) of all intermediate links between endpoints must be sufficient to carry the largest Layer 2 VLAN received. The ingress and egress provider-edge routers must have the same MTU value.
- Address Format—All loopback addresses on provider-edge routers must be configured with 32-bit masks to ensure proper operation of MPLS forwarding. OSPF requires the use of loopback addresses.
- Packet Format—EoMPLS supports VLAN packets that conform to the IEEE 802.1Q standard. ISL encapsulation is not supported between provider-edge and customer-edge routers.
- STP—Do not enable per-VLAN spanning-tree (PVST) on the VLAN configured for an EoMPLS session. STP instances are not supported on this VLAN. All PVST bridge protocol data units (BPDUs) coming in on the EoMPLS VLAN from the customer side are tunneled transparently as data packets over to the EoMPLS pseudowire and vice-versa.
- Trunking—The native VLAN of a trunk cannot be an EoMPLS VLAN.
- You can enable EoMPLS on IEEE 802.1Q interfaces by using the xconnect interface configuration command. Use the xconnect command to configure pseudowire redundancy.
Enabling EoMPLS

This section includes this information about configuring EoMPLS on a switch used as a provider-edge router:

- Default EoMPLS Configuration, page 54-31
- EoMPLS Configuration Guidelines, page 54-31
- Configuring EoMPLS, page 54-32
- Configuring the Pseudowire Using Pseudowire Class, page 54-33
- Configuring L2VPN Interworking, page 54-34
- EoMPLS and EVC, page 54-35
- Packet Flow in an EoMPLS Network, page 54-39
- Configuring L2VPN Pseudowire Redundancy, page 54-40
- Routed VPLS/EoMPLS, page 54-44

For more information about EoMPLS commands, see the command reference for this release.

Default EoMPLS Configuration

By default, EoMPLS is not configured.

The `mpls ldp router-id` command is disabled. No virtual connections are configured.

EoMPLS Configuration Guidelines

When you configure EoMPLS, you must follow these guidelines:

- Before enabling EoMPLS, you must enable dynamic MPLS labeling by using the `mpls ip interface` configuration command on all paths between the imposition and disposition LERs. MPLS is globally enabled by default.
- For VLAN-based EoMPLS, you must configure VLANs on the switch.
- EoMPLS operation between two provider-edge routers requires an LDP session between the routers. The IP address used by each router as its LDP router ID must be reachable through IP by the other. Use the optional `mpls ldp router-id` global configuration command to control the selection of the LDP router ID by specifying the interface whose IP address should be used.
  - If the specified interface is up and has an IP address, you can use the command without the optional `force` keyword. When the router ID is selected, that IP address is selected as the router ID.
  - If the specified interface is not up or does not have an IP address, use the `force` keyword with the command to ensure that the IP address of the specified interface is used when that interface is brought up.

- IGMP—Disable IGMP for any bridge domain where pseudowire is configured.
Enabling EoMPLS

Both provider-edge routers require a loopback address that you can use to create a virtual connection between the routers. When you use OSPF as the interior gateway protocol, you must configure all loopback addresses on provider-edge routers with 32-bit masks to ensure proper operation of MPLS forwarding between the provider-edge routers.

Do not configure EoMPLS on an interface configured for VLAN mapping.

You can set the maximum transmission unit (MTU) value on an SVI.

## Configuring EoMPLS

You configure VLAN-based EoMPLS on a VLAN interface. When VLAN-based EoMPLS is enabled, the switch associates the tunnel and virtual-connection labels based on the VLAN ID. You use the same commands to enable port-based EoMPLS.

Beginning in privileged EXEC mode, follow these steps on the provider-edge routers to configure EoMPLS to transport Layer 2 packets between two endpoints:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 mpls label protocol {ldp</td>
<td>tdp</td>
</tr>
<tr>
<td>Step 3 interface loopback0</td>
<td>Enter interface configuration mode for a loopback interface.</td>
</tr>
<tr>
<td>Step 4 ip address ip-address subnet mask</td>
<td>Assign an IP address to the loopback interface.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 6 interface vlan vlan-id or interface interface-id</td>
<td>Enter a VLAN ID (for VLAN-based EoMPLS) to enter SVI configuration mode. or Enter the interface ID of a routed port (for port-based EoMPLS), to enter routed port interface configuration mode.</td>
</tr>
<tr>
<td>Step 7 xconnect destination vc-id encapsulation mpls</td>
<td>Configure the interface to transport the Layer 2 VLAN packets over MPLS.</td>
</tr>
<tr>
<td>Step 8 end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 9 show mpls l2transport vc</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 10 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

Note: Use the `xconnect` command if pseudowire redundancy is required.
Use the `no xconnect destination vc-id encapsulation mpls` interface command to delete the EoMPLS tunnel.

This example shows how to configure an EoMPLS tunnel between switch PE1’s routed port and PE2’s VLAN 4 interface.

PE1 has an IP address 10.0.0.1/32, and PE2 has IP address 20.0.01/32. Both provider-edge routers are configured with an MPLS connection to the MPLS core. The VC ID is 123.

Enter these commands on the PE1 switch:

```
Switch(config)# interface loopback0
Switch(config-if)# ip address 10.10.10.10 255.255.255.255
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# xconnect 20.20.20.20 123 encapsulation mpls
```

Enter these commands on the PE2 switch:

```
Switch(config)# interface loopback0
Switch(config-if)# ip address 20.20.20.20 255.255.255.255
Switch(config-if)# exit
Switch(config)# interface vlan 4
Switch(config-if)# xconnect 10.10.10.10 123 encapsulation mpls
```

This example shows how to set the MTU value on an SVI.

```
Switch(config)# interface vlan 100
Switch(config-if)# xconnect 2.2.2.2 2 encapsulation mpls
Switch(config-if)# mtu 9000
```

### Configuring the Pseudowire Using Pseudowire Class

The pseudowire-class configuration specifies the characteristics of the tunneling mechanism, including encapsulation type and control protocol. You must specify the `encapsulation mpls` command as part of the pseudowire class for the AToM VCAs to work properly.

Beginning in privileged EXEC mode, follow these steps to configure a pseudowire class:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command Sequence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>pseudowire-class name</td>
<td>Create a pseudowire class with the specified name and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td>encapsulation mpls</td>
<td>Specify tunneling encapsulation. For AToM, the encapsulation type is <code>mpls</code>.</td>
</tr>
<tr>
<td>4</td>
<td>preferred-path interface tunnel tunnel-id</td>
<td>(Optional) Specify the path that pseudowire traffic uses to be an MPLS TE tunnel.</td>
</tr>
<tr>
<td>5</td>
<td>end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td>show mpls l2transport vc [detail]</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example configures the pseudowire class test.

```
Switch# config t
Switch(config)# pseudowire-class test
Switch(config-pw-class)# encapsulation mpls
```
This example shows the output of the show mpls l2transport vc command when the primary attachment circuit is up and the backup attachment circuit is available, but not currently selected.

Switch# show mpls l2transport vc
Local intf Local circuit Dest address VC ID Status
-----------------------------------------------
Vl120 Eth VLAN 20 10.1.1.2 20 UP
Vl120 Eth VLAN 20 10.1.1.4 20 DOWN

This example shows how to display the preferred path using the show mpls l2transport vc 2 detail command.

Switch# show mpls l2transport vc 2 detail
Local interface: Gi0/24 up, line protocol up, Ethernet up
Destination address: 2.2.2.2, VC ID: 2, VC status: down
Output interface: none, imposed label stack {}

Preferred path: Tunnel100, no route
Default path:
No adjacency
Create time: 00:00:12, last status change time: 00:00:12
Signaling protocol: LDP, peer unknown
Targeted Hello: 51.51.51.51(LDP Id) -> 2.2.2.2
Status TLV support (local/remote) : enabled/unknown (no remote binding)
Label/status state machine : local standby, AC-ready, LnuRnd
Last local dataplane status rcvd: no fault
Last local SSS circuit status rcvd: no fault
Last local SSS circuit status sent: not sent
Last local LDP TLV status sent: not sent
Last remote LDP TLV status rcvd: unknown (no remote binding)
MPLS VC labels: local 19, remote unassigned
Group ID: local 0, remote unknown
MTU: local 1500, remote unknown
Remote interface description:
Sequencing: receive disabled, send disabled
VC statistics:
  packet totals: receive 0, send 0
  byte totals: receive 0, send 0
  packet drops: receive 0, send 0

Configuring L2VPN Interworking

Layer 2 transport over MPLS and IP exists for like-to-like attachment circuits, such as Ethernet-to-Ethernet. L2VPN interworking builds on this functionality by allowing disparate attachment circuits to be connected. An interworking function facilitates the translation between the different Layer 2 encapsulations.

For information about L2VPN interworking, see the L2VPN Interworking feature module at this URL:


Note that the switch does not support ATM interfaces, Point-to-Point Protocol (PPP), or frame relay as mentioned in this document.

L2VPN interworking on the ME 3800X and ME 3600X switches works in either Ethernet mode (VC type 5) or VLAN mode (VC type 4). You specify the mode by entering the interworking {ethernet | vlan} command in pseudowire-class configuration mode. Although visible in the command-line interface help, the ip keyword is not supported. Entering the interworking command causes the attachment circuits to be terminated locally.
Enabling EoMPLS

The keywords perform these functions:

- The `ethernet` keyword causes Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that are not Ethernet are dropped.

- The `vlan` keyword causes VLAN-tagged packets to be extracted and sent over the pseudowire. Frames that are not VLAN-tagged are dropped.

Beginning in privileged EXEC mode, follow these steps to configure L2VPN VLAN interworking on a PE router:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>pseudowire-class name</code></td>
<td>Create a pseudowire class with the specified name and enter pseudowire class configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td><code>encapsulation mpls</code></td>
<td>Specify tunneling encapsulation. For AToM, the encapsulation type is <code>mpls</code>.</td>
</tr>
<tr>
<td>4</td>
<td>`interworking {ethernet</td>
<td>vlan}`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>ethernet</code>—Send Ethernet packets across the pseudowire.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>vlan</code>—Send VLAN-tagged packets across the pseudowire.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Although visible in the CLI, the <code>ip</code> keyword is not supported.</td>
</tr>
<tr>
<td>5</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>6</td>
<td><code>show mpls l2transport vc [detail]</code></td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>7</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to configure VLAN interworking:

```
Switch# config t
Switch(config)# pseudowire-class test
Switch(config-pw-class)# encapsulation mpls
Switch(config-pw-class)# interworking vlan
Switch(config-pw-class)# exit
```

For a more detailed configuration example, see the configuration example for “Ethernet to VLAN over AToM (Bridged): Example” in the `L2VPN Interworking` feature module.

**EoMPLS and EVC**

When a pseudowire is configured on a VLAN interface, the pseudowire becomes a virtual Layer 2 port in that VLAN or bridge domain. You can configure other types of L2 ports, such as EFP ports and switch ports in the same bridge domain. Switch functions, such as MAC address learning, flooding, and forwarding to learned MAC addresses apply to all the Layer 2 ports, including the pseudowire.

**Note** When EFP and a pseudowire are configured in the same bridge domain, EFP cannot be configured with the `rewrite ingress tag pop 2 symmetric` command. Other restrictions on switching between EFPs or between EFPs and switch ports also apply.
This example shows how to configure a pseudowire on a VLAN interface:

```plaintext
Switch(config)# interface GigabitEthernet0/1
Switch(config-if) switchport access vlan 100

Switch(config)# interface GigabitEthernet0/2
Switch(config-if) switchport mode trunk

Switch(config)# interface GigabitEthernet0/3
Switch(config-if) description all egress efps
Switch(config-if) switchport trunk allowed vlan none
Switch(config-if) switchport mode trunk
Switch(config-if) service instance 1 ethernet
Switch(config-if) encapsulation dot1q 12
Switch(config-if) bridge-domain 100
!
Switch(config-if) service instance 2 ethernet
Switch(config-if) description case 101
Switch(config-if) encapsulation dot1q 13
Switch(config-if) rewrite ingress tag pop 1 symmetric
Switch(config-if) bridge-domain 100

Switch(config)# interface Vlan100
Switch(config-if) no ip address
Switch(config-if) xconnect 12.12.12.12 123 encapsulation mpls
```

To see the MAC addresses learned from a pseudowire, enter the `show mac address-table dynamic` command. The example below shows output from the command.

```plaintext
Switch# show mac address-table dynamic

Mac Address Table

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Mac Address</th>
<th>Type</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>0000.0000.0011</td>
<td>DYNAMIC</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>0000.0000.00bb</td>
<td>DYNAMIC</td>
<td>Gi0/3+Efp1</td>
</tr>
<tr>
<td>100</td>
<td>0000.0101.010b</td>
<td>DYNAMIC</td>
<td>Gi0/1</td>
</tr>
<tr>
<td>100</td>
<td>0000.0101.010a</td>
<td>DYNAMIC</td>
<td>Gi0/2</td>
</tr>
</tbody>
</table>
```

You can disable MAC address learning on a VLAN or a bridge domain.

This command disables MAC address learning on a VLAN.

```plaintext
Switch(config)# no mac address-table learning vlan 100
```

This command disables MAC address learning on a bridge domain.

```plaintext
Switch(config)# no mac address-table learning bridge-domain 100
```

---

**Note**

The output of the `show mac address-table` command does not include the port name for a pseudowire from which a MAC address is learned.

---

**Configuring EVC Xconnect**

Follow these steps to configure EVC xconnect:
### Enabling EoMPLS

**Chapter 54      Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS**

**Enabling EoMPLS**

**Step 1** configure terminal
Enter global configuration mode.

**Step 2** interface [gigabitethernet | tengigabitethernet | port-channel] port-number
Specifies the GigabitEthernet or the Ten Gigabit Ethernet interface to configure.

**Step 3** switchport mode trunk
Configure the port as a trunk port.

**Step 4** switchport trunk allowed vlan none
Configure the trunk port to have no allowed VLANs.

**Step 5** service instance id ethernet [evc]
Configure an EFP (service instance) and enter service instance configuration mode. Creates a service instance on an interface and

**Step 6** encapsulation {dot1q | untagged | priority-tagged | default} {any | vlan-id[vlan-id][-vlan-id]} cos [0-7] second-dot1q {any | vlan-id[vlan-id][-vlan-id]} cos [0-7] etype [ipv4 | ipv6 | pppoe-all | pppoe-discovery | pppoe-session]
Defines the matching criteria to be used in order to map ingress dot1q frames on an interface to the appropriate service instance.

**Step 7** rewrite ingress tag pop {1|2} symmetric
Specifies the tag manipulation that is to be performed on the frame ingress to the service instance.

**Step 8** xconnect peer-id vc-id {encapsulation | pw-class} {mpls} {pw-class name}
Binds the attachment circuit to a pseudowire vc.

**Step 9** backup peer-id vc-id
Specifies a redundant peer for a pseudowire virtual circuit.

---

**Configure Pseudowire-class**

**Step 1** configure terminal
Enter global configuration mode.

**Step 2** pseudowire-class name
Creates a pseudowire class and enters pseudowire class configuration mode.

**Step 3** encapsulation mpls
Specifies the encapsulation type.

**Step 4** interworking {ethernet | vlan | ip}
Enables the L2VPN interworking feature.

This example shows how to configure EVC Xconnect:

```
interface GigabitEthernet0/2
switchport trunk allowed vlan none
switchport mode trunk
service instance 1 ethernet
  encapsulation dot1q 10
  xconnect 1.1.1.1 10 encapsulation mpls
!
service instance 2 ethernet
  encapsulation dot1q 20 cos 5
  xconnect 1.1.1.1 2000 encapsulation mpls
!
service instance 3 ethernet
  encapsulation dot1q 30 cos 2 etype ipv4
  xconnect 1.1.1.1 350 encapsulation mpls
!
service instance 4 ethernet
  encapsulation dot1q 40
  rewrite ingress tag pop 1 symmetric
  xconnect 1.1.1.1 415 encapsulation mpls
```
### Configuring Support for Integrated Routing and Bridging (IRB)

IRB enables a user to route a protocol on one group of interfaces and bridge a protocol on separate group of interfaces within a single router. The protocol can be either routed or bridged on a given interface, but not both.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface [gigabitethernet</td>
<td>tengigabitethernet</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode trunk</td>
<td>Configure the trunk port to have no allowed VLANs.</td>
</tr>
<tr>
<td>Step 4</td>
<td>switchport trunk allowed vlan none</td>
<td>Configure an EFP (service instance) and enter service instance configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>service instance id ethernet [evc] encapsulation [dot1q</td>
<td>untagged</td>
</tr>
</tbody>
</table>

This example shows how to configure IRB:

```plaintext
interface GigabitEthernet0/2
switchport trunk allowed vlan none
switchport mode trunk
service instance 100 ethernet
capsulation dot1q 100
rewrite ingress tag pop 1 symmetric
bridge-domain 100
!
service instance 101 ethernet
capsulation dot1q 101
rewrite ingress tag pop 1 symmetric
```
bridge-domain 100
!
service instance 102 ethernet
  encapsulation dot1q 102
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
!
service instance 103 ethernet
  encapsulation dot1q 103
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
!
service instance 104 ethernet
  encapsulation dot1q 104
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
!
service instance 105 ethernet
  encapsulation dot1q 105
  rewrite ingress tag pop 1 symmetric
  bridge-domain 100
!
end

interface Vlan100
  ip vrf forwarding VRF100
  ip address 12.0.0.1 255.255.255.0
!

Packet Flow in an EoMPLS Network

Figure 54-5 is an example of packet flow in an EoMPLS network. A customer port on PE1 is configured for a per-port EoMPLS tunnel to a remote customer port on PE2. This allows the two physically separated customer switches (A and B) connected to these ports to appear as if they are directly connected on the same physical LAN.

The EoMPLS tunnel is configured with the IP address of Switch B and a VC ID that is associated with the remote customer port. Switch PE1 establishes a tunnel LSP with switch PE2 by using a label advertised with LDP by Router A, which is connected to switch PE1. Switch PE1 then establishes a targeted LDP session to switch PE2 to advertise the virtual-connection label associated with the VC ID. When switch PE2 is configured with the EoMPLS tunnel, it also establishes a targeted LDP session to advertise the virtual-connection label it associated to the VC ID. This establishes an EoMPLS tunnel between switch PE1 and switch PE2.
Assume that Host A is connected to the customer switch on VLAN 3 that has a trunk port connected to PE1 configured for IEEE 802.1Q tagging. Host A sends a packet to Host B, using the specific values of MAC addresses, labels, and VLANs shown in the figure. The customer switch tags the host packet and forwards it over the trunk port to switch PE1.

The tagged packet is received on the customer-edge port that is configured for per-port EoMPLS tunneling. The PE1 switch examines the packet headers and looks at the tables stored in the switch to determine what to do with the packet. Because the port is configured for per-port EoMPLS tunneling, the switch does not remove any VLAN tags that are in the packet, but assigns the packet to an internal VLAN. Only the customer port and the PE1 port are configured with that internal VLAN, which makes the PE1 port the only possible destination for the packet.

The PE1 port encapsulates the packet header with the tunnel label and the virtual-connection label and forwards the packet to the next hop, in this case Router A, to send it across the MPLS network.

The router receives the packet and forwards it over the MPLS network to the remote PE2 switch. PE2 removes the MPLS encapsulation and sends the packet out the port associated with the virtual-connection label. Customer Switch B removes the final VLAN tag and forwards the packet to the remote host B.

VLAN-based EoMPLS packet flow is basically the same as port-based EoMPLS, except that the customer VLAN is used instead of an internal VLAN. The PE1 switch looks up the customer VLAN ID to determine that the packet is forwarded to the designated port, where the packet is again examined and encapsulated with the tunnel label and virtual-connection label based on the EoMPLS for that VLAN.

### Configuring L2VPN Pseudowire Redundancy

Successful transmission of Layer 2 frames between PE routers requires a connection, called a pseudowire, between the routers. You can use the L2VPN pseudowire redundancy feature to configure your network to detect a failure in the network and reroute the Layer 2 service to another endpoint that can continue to provide service. This feature provides the ability to recover from a failure of either the remote provider edge (PE) router or of the link between the PE and customer edge (CE) routers.

For more information see *Wide-Area Networking Configuration Guide Library, Cisco IOS Release 15.x*. L2VPNs also provide pseudowire resiliency through their routing protocols. When connectivity between end-to-end PE routers fails, an alternative path is provided between the directed LDP session and the user data. However, there are some parts of the network where this rerouting mechanism does not protect against interruptions in service. Figure 54-6 shows those parts of the network that are vulnerable to an interruption in service.
Enabling EoMPLS

**Figure 54-6    Points of Potential Failure in an L2 VPN Network**

![Diagram of Points of Potential Failure in an L2 VPN Network]

X1 = End-to-end routing failure  
X2 = PE hardware or software failure  
X3 = Attachment circuit failure from a line break  
X4 = CE hardware or software failure

L2VPN pseudowire redundancy provides the ability to ensure that the CE2 router in Figure 54-6 can always maintain network connectivity, even if one or all of the failures in the figure occur. You can configure a backup pseudowire so that if the primary pseudowire fails, the provider-edge router switches to the backup pseudowire. You can configure the primary pseudowire to resume operation after it restarts. You can also configure the network with redundant pseudowires and redundant network elements (routers).

**Figure 54-7    L2 VPN Network with Redundant Pseudowires and Attachment Circuits**

![Diagram of L2 VPN Network with Redundant Pseudowires and Attachment Circuits]

This section includes this information:

- Configuration Guidelines, page 54-41
- Configuring Pseudowire Redundancy, page 54-42
- Forcing a Manual Switchover to the Backup Pseudowire VC, page 54-43
- Monitoring L2VPN Pseudowire Redundancy, page 54-43

**Configuration Guidelines**

Follow these guidelines when configuring L2 VPN pseudowire redundancy:

- The default Label Distribution Protocol (LDP) session hold-down timer enables the software to detect failures in about 180 seconds. You can use the `mpls ldp holdtime` global configuration command to configure the switch to detect failures more quickly.

- The primary and backup pseudowires must run the same type of transport service. You must configure Any Transport over MPLS (AToM) on both the primary and backup pseudowires.
Enabling EoMPLS

- L2VPN pseudowire redundancy does not support different pseudowire encapsulation types on the MPLS pseudowire.
- L2VPN pseudowire redundancy does support setting the experimental (EXP) bit on the MPLS pseudowire.
- The switch does not support LDP MAC address withdrawal.
- The `mpls l2transport route` command is not supported. Use the `xconnect` command instead.
- The backup pseudowire cannot be operational at the same time that the primary pseudowire is operational. The backup pseudowire becomes active only after the primary pseudowire fails.
- VCCV is supported only on the active pseudowire.
- The switch does not support more than one backup pseudowire.

Configuring Pseudowire Redundancy

When configuring pseudowire redundancy, you use the `xconnect` interface configuration command for each transport type. Beginning in privileged EXEC mode, follow these steps to configure pseudowire redundancy on a PE router:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td><code>interface interface-id</code></td>
<td>Specify an interface and enter interface configuration mode. The interface on the adjoining router must be on the same VLAN as this router.</td>
</tr>
<tr>
<td>3</td>
<td><code>xconnect peer-router-id vcid pw-class name</code></td>
<td>Bind the attachment circuit to a pseudowire virtual circuit (VC) and enter xconnect configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td><code>backup peer peer-router-ip-address vcid [pw-class name]</code></td>
<td>Specify a redundant peer for the pseudowire VC. If you do not specify a <code>pw-class name</code>, the value is inherited from the parent.</td>
</tr>
<tr>
<td>5</td>
<td>`backup delay enable-delay [disable-delay</td>
<td>never]`</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>enable-delay</code>— Specify how long (in seconds) the backup pseudowire VC waits to take over after the primary pseudowire VC goes down. The range is 0 to 180 seconds; the default is 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <code>disable-delay</code>— Specify how long (in seconds) the primary pseudowire waits after it becomes active to take over from the backup pseudowire. The range is 0 to 180 seconds; the default is 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- If you enter <code>never</code>, the switchback to the primary pseudowire never occurs.</td>
</tr>
<tr>
<td>6</td>
<td><code>end</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>7</td>
<td><code>show xconnect all</code></td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>8</td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to configure pseudowire redundancy as a switchover to the peer with the IP address 10.1.1.12 immediately when a failure occurs and to not switch back to the primary VC when it becomes available.

Switch# config t
Switch(config)# interface gigabitethernet1/1/1
Switch (config-if)# xconnect 10.1.1.4 33 encapsulation mpls
Switch(config-if-xconn)# backup peer 10.1.1.2 33
Switch(config-if-xconn)# backup delay 0 never

This example shows the output of the `show mpls l2transport vc` privileged EXEC command when the primary attachment circuit is up and the backup attachment circuit is available, but not currently selected.

Switch# show mpls l2transport vc
Local intf Local circuit Dest address VC ID Status
------------- -------------------------- --------------- ---------- ----------
Vl10 Eth VLAN 10 10.1.1.2 10 UP
Vl10 Eth VLAN 10 10.1.1.4 20 DOWN

**Forcing a Manual Switchover to the Backup Pseudowire VC**

You can manually force the router to switch to the backup or primary pseudowire. You can specify either the interface of the primary attachment circuit or the IP address and VC ID of the peer router. If the specified interface or peer is not available, the switchover does not occur. The backup pseudowire becomes active when you enter the command.

Beginning in privileged EXEC mode, follow these steps to force a pseudowire switchover:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>xconnect backup force-switchover {interface interface-id</td>
<td>peer ip-address voiced}</td>
</tr>
</tbody>
</table>

This command forces a switchover to the peer with the IP address 10.1.1.4 and VCID 33.

Switch# xconnect backup force-switchover peer 10.1.1.4 33

**Monitoring L2VPN Pseudowire Redundancy**

Use the privileged EXEC commands in Table 54-3 to verify or monitor pseudowire redundancy.

<table>
<thead>
<tr>
<th>Table 54-1</th>
<th>Commands for Displaying MPLS and EoMPLS Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>show xconnect {all</td>
<td>interface</td>
</tr>
<tr>
<td>show mpls l2transport vc [detail]</td>
<td>[summary]</td>
</tr>
<tr>
<td>show vfi vfi-name</td>
<td>Display information about a VPLS VFI.</td>
</tr>
</tbody>
</table>

You can also use the `xconnect logging redundancy` global configuration command to track the status of the xconnect redundancy group. The command generates messages during switchover events.

This example shows pseudowire redundancy.

Switch# show mpls l2transport vc 10
Local intf Local circuit Dest address VC ID Status
------------- -------------------------- --------------- ---------- ----------
Vl10 Eth VLAN 10 10.1.1.1 10 UP
Routed VPLS/EoMPLS

Routed VPLS/EoMPLS provides the ability to route or bridge frames to and from pseudowires with MPLS encapsulation. Routed VPLS/EoMPLS accomplishes this by allowing cross-connect and IP addresses to be configured on an SVI.

- Multicast routing is not supported on Routed VPLS

Routed VPLS/EoMPLS supports:

- P2P (SVI based EoMPLS)
- Multi-Point (VPLS)

The following features are supported on routed Routed PW/VPLS:

- SVI based routed pseudowire
- Routed VPLS
- Routed Pseudowire with SVI MPLS in the core (supported from Cisco IOS Release 15.3(2)S2). However, effective with Cisco IOS Release 15.3(3)S, Routed Pseudowire with SVI MPLS in the core being a Trunk interface is unsupported.

Restrictions for Routed VPLS/EoMPLS

- Routed Pseudowire with VC Type 4 is not supported.
- Multihoming is not supported for both BGP or LDP VPLS.

Figure 54-8 shows how Routed VPLS/EoMPLS is connected.
### Configuring Routed Pseudowire

In the privileged EXEC mode, perform these steps to configure routed pseudowire.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip address address mask</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>xconnect peer-router-id vcid pw-class pw-class name</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>end</td>
</tr>
</tbody>
</table>

This is an example of routed pseudowire configuration:

```bash
Router# configure terminal
Router(config)# interface vlan333
Router(config-if)# ip address 2.1.1.1 255.255.255.0
Router(config-if)# xconnect 76.76.76.76 105 encapsulation mpls
Router(config-if-xconn)# end
```

```bash
Router# show ip int br | i Vlan333|Interface
Interface               IP-Address    OK? Method Status      Protocol
Vlan333                2.1.1.1       YES manual up     up
Router#
```
Configuring Routed VPLS

In the privileged EXEC mode, perform these steps to configure routed VPLS.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> l2 vfi vfi_name manual</td>
<td>Create a virtual forwarding infrastructure (VFI) and enter manual VFI configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> vpn id id</td>
<td>Configure the virtual private network (VPN) number for a VFI interface.</td>
</tr>
<tr>
<td><strong>Step 4</strong> neighbor ip-addr encapsulation mpls</td>
<td>Configure the IP address of the remote peer to become a member of the VPLS configured by the VFI and set the MPLS encapsulation type.</td>
</tr>
<tr>
<td><strong>Step 5</strong> interface interface-id</td>
<td>Specify the address of the client that will receive the configuration file.</td>
</tr>
<tr>
<td><strong>Step 6</strong> ip address address mask</td>
<td>Specify the IP address and mask for the interface.</td>
</tr>
<tr>
<td><strong>Step 7</strong> xconnect vfi vfi-name</td>
<td>Bind the attachment circuit to a pseudowire virtual circuit (VC) and enter the Xconnect configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong> end</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

This is an example of basic routed VPLS configuration:

```plaintext
l2 vfi test manual
vpn id 600
neighbor 10.1.255.2 encapsulation mpls
neighbor 10.1.255.10 encapsulation mpls

interface vlan600
ip address 70.1.1.1 255.255.255.0
xconnect vfi test
```

Support for H-VPLS

The Metro 3800X and Metro 3600X switches support hierarchical VPLS (H-VPLS). Layer 2 control packet forwarding is only supported when you use Layer 2 Protocol Tunneling (L2PT) on the tunnel port in H-VPLS scenario. L2PT in the forward mode is not supported in H-VPLS scenario.

Note: This feature requires the ME 3800X Metro Aggregation Access or ME 3800S Scaled Metro Aggregation Access software license.

H-VPLS uses spoke connections, usually between Layer 2 switches acting as the CE and PE devices at the service provider’s point-of-presence (POP). The spoke connections can be either an IEEE 802.1Q tagged connection or an MPLS LSP.
Figure 54-9 shows two Metro 3800X or Metro 3600X customer-located equipment (CLE) switches (PE1 and PE2) configured as neighbors on different sides of an MPLS network. Each switch has multiple customer Ethernet switches connected to it and is connected to a PE device at the service-provider POP. With no direct connections, H-VPLS allows the customer switches from PE1 to connect to customer switches connected to PE2.

**Figure 54-9   H-VPLS Configuration Example**

**Full-Mesh Configuration**

A full-mesh configuration requires a full mesh of tunnel label switched paths (LSPs) between all the PEs that participate in the VPLS. With full mesh, signaling overheads and packet replication requirements for each provisioned VC on a PE can be high.

Set up a VPLS by first creating a virtual forwarding instance (VFI) on each participating PE router. The VFI specifies the VPN ID of a VPLS domain, the addresses of other PE routers in the domain, and the type of tunnel signaling and encapsulation mechanism for each peer PE router.

The set of VFIs formed by the interconnection of the emulated VCs is called a VPLS instance. It is the VPLS instance that forms the logic bridge over a packet-switched network. The VPLS instance is assigned a unique VPN ID.

The PE routers use the VFI to establish a full-mesh LSP of emulated VCs to all the other PE routers in the VPLS instance. PE routers obtain the membership of a VPLS instance through static configuration using the Cisco IOS CLI.

A full-mesh configuration allows the PE router to maintain a single broadcast domain. Thus, when the PE router receives a broadcast, multicast, or unknown unicast packet on an attachment circuit, it sends the packet out through all the other attachment circuits and emulated circuits to all the other CE devices participating in that VPLS instance. The CE devices see the VPLS instance as an emulated LAN.

To avoid the problem of a packet looping in the provider core, the PE devices enforce a split-horizon principle for the emulated VCs. This means that if a packet is received on an emulated VC, it is not forwarded on any other emulated VC.

After the VFI is defined, it must be bound to an attachment circuit, then to the CE device.

The packet forwarding decision is made by looking up the Layer 2 VFI of a particular VPLS domain.
A VPLS instance on a particular PE router receives Ethernet frames that enter on specific physical or logical ports and populate a MAC table that is similar to the way an Ethernet switch works. The PE router can use the MAC address to switch those frames into the appropriate LSP for delivery to the other PE router at a remote site.

If the MAC address is not in the MAC address table, the PE router replicates the Ethernet frame and floods it to all the logical ports associated with that VPLS instance, except the ingress port it just entered. The PE router updates the MAC table as it receives packets on specific ports, and removes the addresses that have not been used for specific periods.

**Hub and Spoke**

In a hub-and-spoke model, the PE router that acts as the hub establishes a point-to-multipoint forwarding relationship with all the PE routers at the spoke sites. An Ethernet or VLAN packet received from the customer network on the hub PE can be forwarded to one or more emulated VCs.

The PE routers that act as spokes establish a point-to-point connection to the PE at the hub site. Ethernet or VLAN packets received from the customer network on the spoke PE are forwarded to the VFI or VPLS instance at the hub. If there are a number of customer sites connecting to the spokes, you can terminate multiple VCs per spoke in the same VFI or VPLS instance at the hub.

**VPLS-Supported Features**

- Imposition VLAN rewrite per pseudowire—This feature connects two L2 domains. VLAN rewrite is usually done at the disposition router. However, some devices do not have this capability.
  
  VLAN rewrite at imposition is supported, but with the following restrictions:
  - The rewritten VLANs must be the same if multiple ACs are attached to the same pseudowire
  - Only two VLANs can be written when combining the outer and inner VLANs.
  - All PW inner headers will have the same EtherType.

- AToM control word per pseudowire—This feature inserts a control word on a per pseudowire basis. The control word is always set to 0 and does not support any sequencing scheme.

- PW QoS—This feature is provided by configuring an input and output policy map on a UNI or PW interface.

- PW statistics—This feature provides statistics on packets, bytes, and drops per PW prior to label imposition for packets entering a tunnel and after MPLS disposition for packets exiting a tunnel.

- UNI to PW mapping for service selection—This feature allows the following UNI attributes to be used for service selection using port mode EoMPLS and EFP-based EoMPLS:
  - Per UNI port
  - Per UNI port, per C-VLAN
  - Per UNI port, per C-VLAN, per C-CoS
  - Per UNI port, per C-VLAN, per C-DSCP

- Auto sense signalling—This feature allows two remote PEs to negotiate VC-type signaling. In earlier software release, two types of VCs were defined, Ethernet VLAN and Ethernet. Only Ethernet is applicable now.

- BGP signaling—This feature enables you to use BGP as both an autodiscovery and a signaling protocol for VPLS, in accordance with RFC 4761.
Support for H-VPLS

- Pseudowire over TE tunnel—This feature allows PW to go over the TE tunnels in which LDP is enabled over the TE tunnel interface and the tunnels are configured end-to-end.
- Pseudowire over FRR path—This feature allows PW to go over the FRR path.
- PW path selection over Equal-cost routes—This feature allows PWs to be routed over different paths in order to distribute the traffic load.
- LDP MAC address withdrawal—To support faster convergence times, remove and relearn the MAC addresses that have been learned over pseudowire. The LDP Address withdrawal Message contains a list of the MAC address entries that have to be relearned. The message is sent on the backup link to the remote PEs in the VPLS domain.

VPLS Services

Transparent LAN Service (TLS) and Ethernet Virtual Connection Service (EVCS) are available for service providers and enterprises.

- TLS—Use when you need transparency with regard to bridging protocols (for example, bridge protocol data units [BPDUs]) and VLAN values. Bridges see this service as an Ethernet segment.
- EVCS—Use when you need routers to reach multiple intranet and extranet locations from a single physical port. Routers see subinterfaces through which they access other routers.

Transparent LAN Service

TLS is an extension of point-to-point port-based EoMPLS. With TLS, the PE router forwards all the Ethernet packets received from the customer-facing interface (including tagged, untagged, and BPDUs) as follows:

- To a local Ethernet interface or an emulated VC if the destination MAC address is found in the Layer 2 forwarding table.
- To all other local Ethernet interfaces and emulated VCs belonging to the same VPLS domain if the destination MAC address is a multicast or broadcast address or if the destination MAC address is not found in the Layer 2 forwarding table.

VPLS BGP Signaling

Before beginning, you should be familiar with the concepts in the "Configuring Virtual Private LAN Services" and the "VPLS Autodiscovery BGP Based" modules of the MPLS Layer 2 VPNs Configuration Guide.

Prerequisites for Configuring VPLS BGP Signaling

Prior to the VPLS BGP Signaling feature, BGP was used for autodiscovery and Label Distribution Protocol (LDP) for signaling in accordance with RFC 6074. The VPLS BGP Signaling feature enables you to use BGP as the control plane protocol for both autodiscovery and signaling in accordance with RFC 4761.

As specified in RFC 4761, internal BGP (iBGP) peers will exchange update messages of the L2VPN AFI/SAFI with L2VPN information to perform both autodiscovery and signaling. The BGP multiprotocol Network Layer Reachability Information (NLRI) consists of the following:

- Route Distinguisher (RD)
- VPLS Endpoint ID (VE ID)
- VE Block Offset (VBO)
- VE Block Size (VBS)
- Label Base (LB)

The figure below shows the format of the NLRI for RFC 4761.

**Figure 54-10  Figure 1 RFC 4761 NLRI**

Additional information, such as next-hop, route target (specified for a VPLS instance), and other Layer 2 data are carried in the BGP extended community attributes. A route target-based import/export mechanism similar to L3VPN is performed by BGP to filter L2VPN NLRIIs of a particular VPLS instance.

Whether you use BGP signaling (RFC 4761) or LDP signaling (RFC 6074) depends on the commands you specify. To enable the VPLS BGP Signaling feature, use the `autodiscovery bgp signaling bgp` command in L2 VFI configuration mode. This command is supported on a per VPLS instance basis.

If a BGP session receives an invalid (that is, not matching the configuration) BGP update advertisement (update or withdraw), it is ignored.

BGP's main task in supporting VPLS is route distribution via the L2VPN address family and interactions with L2VPN. Interactions between BGP and other components remain the same. Basic BGP functionalities like best-path selection, next-hop handling, and update generation, continue to operate in the same manner with VPLS BGP signaling. BGP RT constraint works seamlessly with the BGP VPLS Signaling feature.

**VPLS BGP Signalling Limitations**

The following limitations apply to the VPLS BGP signalling feature for the 3.8 release:

- MAC Flushing is not supported.
- Templates are not supported.
- Traffic Engineering (TE) as core interface is supported but TE as preferred path is not supported because templates are not supported.
- Support for H-VPLS will only be available for the hierarchical route reflector (RR) model.
- The maximum number of supported BGP Signaling neighbors per VFI is 32.
- BGP signaling Inter-AS option A is supported. BGP signaling Inter-AS option B and Option C are not supported.

- When the route designator (RD) is explicitly configured within the same VPLS domain, the virtual forwarding interface (VFI) with the same VPN ID on different PE’s must have the same RD configured. This is as the auto-generated RD is same for Intra AS. All the PE’s within a VPLS domain must have the same RD. See example “Configuring VPLS BGP Signaling with Explicit RD Configurations” on page -54.

- Multihoming is not supported for both BGP and LDP VPLS.

## Configuring VPLS BGP Signaling

### Summary Steps

1. enable
2. configure terminal
3. l2vpn vfi context name
4. vpn id vpn-id
5. autodiscovery bgp signaling {bgp | ldp} [template template-name]
6. ve id ve-id
7. ve range ve-range
8. exit
9. exit
10. router bgp autonomous-system-number
11. bgp graceful-restart
12. neighbor ip-address remote-as autonomous-system-number
13. address-family l2vpn [vpls]
14. neighbor ip-address activate
15. neighbor ip-address send-community [both | standard | extended]
16. neighbor ip-address suppress-signaling-protocol ldp
17. end
18. show bgp l2vpn vpls {all | rd route-distinguisher}

### Detailed Steps

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Device &gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Support for H-VPLS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command Description</th>
<th>Command Syntax</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>l2vpn vfi context name</td>
<td>Device(config)# l2vpn vfi context vfi1</td>
<td>Establishes a L2VPN virtual forwarding interface (VFI) between two or more separate networks and enters Layer 2 VFI configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td>vpn id vpn-id</td>
<td>Device(config-vfi)# vpn id 100</td>
<td>Configures a VPN ID for the VPLS domain.</td>
</tr>
<tr>
<td>5</td>
<td>autodiscovery bgp signaling {bgp</td>
<td>ldp} [template template-name]</td>
<td>Device(config-vfi)# autodiscovery bgp signaling bgp</td>
</tr>
<tr>
<td>6</td>
<td>ve id ve-id</td>
<td>Device(config-vfiautodiscovery)# ve id 1001</td>
<td>Specifies the VPLS endpoint (VE) device ID value. The VE ID identifies a VFI within a VPLS service. The VE device ID value is from 1 to 16384.</td>
</tr>
<tr>
<td>7</td>
<td>ve range ve-range</td>
<td>Device(config-vfiautodiscovery)# ve range 12</td>
<td>Specifies the VE device ID range value. The VE range overrides the minimum size of VE blocks. The default minimum size is 10. Any configured VE range must be higher than 10.</td>
</tr>
<tr>
<td>8</td>
<td>exit</td>
<td>Device(config-vfiautodiscovery)# exit</td>
<td>Enters L2VPN VFI configuration mode.</td>
</tr>
<tr>
<td>9</td>
<td>exit</td>
<td>Device(config-vfi)# exit</td>
<td>Exits L2VPN VFI configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td>10</td>
<td>router bgp autonomous-system-number</td>
<td>Device(config)# router bgp 100</td>
<td>Enters router configuration mode to create or configure a BGP routing process.</td>
</tr>
<tr>
<td>11</td>
<td>bgp graceful-restart</td>
<td>Device(config-router)# bgp graceful-restart</td>
<td>Enables the BGP graceful restart capability and BGP nonstop forwarding (NSF) awareness.</td>
</tr>
<tr>
<td>12</td>
<td>neighbor ip-address remote-as autonomous-system-number</td>
<td>Device(config-router)# neighbor 10.10.10.1 remote-as 100</td>
<td>Configures peering with a BGP neighbor in the specified autonomous system.</td>
</tr>
<tr>
<td>13</td>
<td>address-family l2vpn [vpls]</td>
<td>Device(config-router)# address-family l2vpn vpls</td>
<td>Specifies the L2VPN address family and enters address family configuration mode. The optional vpls keyword specifies that VPLS endpoint provisioning information is to be distributed to BGP peers. In this example, an L2VPN VPLS address family session is created.</td>
</tr>
<tr>
<td>14</td>
<td>neighbor ip-address activate</td>
<td>Device(config-routeraf)# neighbor 10.10.10.1 activate</td>
<td>Enables the neighbor to exchange information for the L2VPN VPLS address family with the local device.</td>
</tr>
<tr>
<td>15</td>
<td>neighbor ip-address send-community [both</td>
<td>standard</td>
<td>extended]</td>
</tr>
</tbody>
</table>
Chapter 54  Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Support for H-VPLS

Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Configuration Examples for VPLS BGP Signaling

The following example configures and verifies VPLS BGP Signaling:

```
l2vpn vfi context vfi1
  vpn id 100
    autodiscovery bgp signaling bgp
    ve id 1001
    ve range 10
  !
router bgp 100
  bgp graceful-restart
  neighbor 80.0.0.2 remote-as 200200
  !
  address-family l2vpn vpls
    neighbor 80.0.0.2 activate
    neighbor 80.0.0.2 send-community extended
    neighbor 80.0.0.2 suppress-signaling-protocol ldp
  end
  !
show bgp l2vpn vpls all
```

For access side configurations, the following example assumes that you have switchport trunk configurations on the interface:

```
l2vpn vfi context vfi1
  vpn id 100
    autodiscovery bgp signaling bgp
    ve id 1001
    ve range 10
  !
  int gi 0/1
  switchport mode trunk allowed vlan 100
  switchport mode trunk

  int vlan 100
  member vfi vfi1
```

### Command Summary

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 16</td>
<td><code>neighbor ip-address suppress-signaling-protocol ldp</code></td>
<td>Suppresses LDP signaling and enables BGP signaling. In this example, LDP signaling is suppressed (and BGP signaling enabled) for the neighbor at 192.0.2.1.</td>
</tr>
<tr>
<td>Step 17</td>
<td><code>end</code></td>
<td>Exits address family configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 18</td>
<td>`show bgp l2vpn vpls {all</td>
<td>rd route-distinguisher}`</td>
</tr>
</tbody>
</table>
For access side configurations, the following example assumes that instead of switchport trunk configurations, you are configuring EFP on the access interface:

```
12vpn vfi context vfi1
    vpn id 100
    autodiscovery bgp signaling bgp
    ve id 1001
    ve range 10

int gi 0/1
switchport mode trunk allowed vlan none
switchport mode trunk
service instance 100 ethernet
encap dot1q 100
rewrite ingress tag pop 1 symmetric (optional)

int vlan 100
member vfi vfi1
bridge-domain 100
member gigabitEthernet 0/1 service-instance 100
```

### Configuring VPLS BGP Signaling with Explicit RD Configurations

```
12vpn vfi context TEST1
    vpn id 1
    autodiscovery bgp signaling bgp
    ve id 1
    ve range 100
    rd 2:1 ---> RD must be same for all the VFI's in all the PE's
    route-target export 2:1
    route-target import 2:1
    no auto-route-target
router bgp 100
bgp graceful-restart
neighbor 209.165.200.224 remote-as 100
neighbor 209.165.200.224 update-source Loopback1
!
address-family l2vpn vpls
    neighbor 209.165.200.224 activate
    neighbor 209.165.200.224 send-community extended
    neighbor 209.165.200.224 suppress-signaling-protocol ldp
exit-address-family
```

### Configuring the VPLS Pseudowire

To configure a VPLS pseudowire tunnel between two PE routers, use either of the following procedures:

- **Configuring a VPLS Pseudowire Using VFI**, page 54-55
- **Configuring the Pseudowire Using Pseudowire Class**, page 54-33
Configuring a VPLS Pseudowire Using VFI

Create a virtual circuit (VC) using VC Type 5 signaling on each provider edge (PE) router. The interface must be a routed interface or a switched virtual interface (SVI). To establish a bidirectional label-switched protocol (LSP), perform the configuration on both the PE routers. The VC ID is used by both the PE routers to identify a VC.

In the global configuration mode, perform these steps to create a virtual forwarding infrastructure (VFI).

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter the global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>l2 vfi name manual Enables the Layer 2 VFI manual configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>vpn id vc-id Configures a VC ID for a VPLS domain. The emulated VCs that are bound to this Layer 2 VRF use this VC ID for signaling.</td>
</tr>
<tr>
<td>Step 4</td>
<td>neighbor remote router id [vc-id-value] {encapsulation mpls} [no-split-horizon] Specifies the remote peering router ID and the tunnel encapsulation type or the pseudowire property to be used to set up the emulated VC.</td>
</tr>
<tr>
<td>Note</td>
<td>Split horizon is the default configuration to avoid broadcast packet looping and to isolate Layer 2 traffic. Use the no-split-horizon keyword to disable split horizon and to configure multiple VCs per spoke on the same VFI.</td>
</tr>
<tr>
<td>Note</td>
<td>The optional VC ID value identifies the emulated VC between a pair of peering PE routers.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end Return to the privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Configuring a P2P Pseudowire Using pw-class

In the privileged EXEC mode, perform these steps to configure a P2P pseudowire using pw-class:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal Enter the global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>pseudowire-class pw-class-name manual Specify the name of a Layer 2 pseudowire class and enter the pseudowire class configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>encapsulation [mpls] Specify that Multiprotocol Label Switching (MPLS) is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.</td>
</tr>
<tr>
<td>Step 4</td>
<td>interworking {ethernet</td>
</tr>
<tr>
<td>Note</td>
<td>The ip keyword is not supported.</td>
</tr>
<tr>
<td>Step 5</td>
<td>end Return to the privileged EXEC mode.</td>
</tr>
</tbody>
</table>

VPLS Autodiscovery: BGP Based

VPLS Autodiscovery enables each Virtual Private LAN Service (VPLS) provider edge (PE) router to discover which other PE routers are part of the same VPLS domain. VPLS Autodiscovery also automatically detects when PE routers are added to or removed from the VPLS domain. You no longer
need to manually configure the VPLS and maintain the configuration when a PE router is added or deleted. VPLS Autodiscovery uses the Border Gateway Protocol (BGP) to discover the VPLS members and to set up and tear down pseudowires in the VPLS.

Information About VPLS Autodiscovery: BGP Based

To understand VPLS Autodiscovery, you should understand the following concepts:

- How the VPLS Feature Works, page 54-56
- How the VPLS Autodiscovery: BGP Based Feature Works, page 54-56
- How Enabling VPLS Autodiscovery Differs from Manually Configuring VPLS, page 54-56
- Show Commands Affected by VPLS Autodiscovery: BGP Based, page 54-57

How the VPLS Feature Works

VPLS allows Multiprotocol Label Switching (MPLS) networks to provide multipoint Ethernet LAN services, also known as Transparent LAN Services (TLS). All customer sites in a VPLS appear to be on the same LAN, even though those sites might be in different geographic locations.

How the VPLS Autodiscovery: BGP Based Feature Works

VPLS Autodiscovery enables each VPLS PE router to discover the other PE routers that are part of the same VPLS domain. VPLS Autodiscovery also tracks when PE routers are added to or removed from the VPLS domain. The autodiscovery and signaling functions use BGP to find and track the PE routers.

BGP uses the L2VPN Routing Information Base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 VFI is configured. Prefix and path information is stored in the L2VPN database, allowing BGP to make decisions on the best path. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to configure a pseudowire mesh to support L2VPN-based services.

The BGP autodiscovery mechanism facilitates the configuration of L2VPN services, which are an integral part of the Cisco IOS Virtual Private LAN Service (VPLS) feature. VPLS enables flexibility in deploying services by connecting geographically dispersed sites as a large LAN over high-speed Ethernet in a robust and scalable IP MPLS network. For more information about BGP and the L2VPN address family in relation to VPLS Autodiscovery, see the following documents:

- The section called “L2VPN Address Family” in the Cisco BGP Overview.
- The document called BGP Support for the L2VPN Address Family

How Enabling VPLS Autodiscovery Differs from Manually Configuring VPLS

With VPLS Autodiscovery, you no longer need to manually set up the VPLS. The commands you use to set up VPLS Autodiscovery are similar to those you use to manually configure a VPLS, as shown in Table 2. VPLS Autodiscovery uses neighbor commands in L2VPN address family mode to distribute endpoint information to configure a pseudowire.
When you configure VPLS Autodiscovery, you enter the `l2vfi autodiscovery` command. This command allows the VFI to learn and advertise the pseudowire endpoints. As a result, you no longer need to enter the `neighbor (VPLS)` command in L2 VFI configuration mode.

However, the `neighbor (VPLS)` command is still supported with VPLS Autodiscovery in L2 VFI command mode. You can use the `neighbor (VPLS)` command to allow PE routers that do not participate in the autodiscovery process to join the VPLS. You can also use the `neighbor (VPLS)` command with PE routers that have been configured using the Tunnel Selection feature. You can also use the `neighbor (VPLS)` command in hierarchical VPLS configurations that have U-PE routers that do not participate in the autodiscovery process and have split-horizon forwarding disabled.

### Show Commands Affected by VPLS Autodiscovery: BGP Based

VPLS Autodiscovery changes the following show commands:

- The `show mpls l2transport vc` command with the `detail` keyword has been updated to include FEC 129 signaling information for the autodiscovered VPLS pseudowires.
- The `show vfi` command now displays information related to autodiscovered VFIs. The new information includes the VPLS ID, the route distinguisher (RD), the RT, and the router IDs of the discovered peers.
- The `show xconnect` command has been updated with the `rib` keyword to provide RIB information about the pseudowires.

### How to Configure VPLS Autodiscovery: BGP Based

To configure VPLS Autodiscovery, perform the following tasks:

- **Enabling VPLS Autodiscovery: BGP Based, page 54-58** (required)
- **Configuring BGP to Enable VPLS Autodiscovery, page 54-58** (required)
- **Customizing the VPLS Autodiscovery Settings, page 54-60** (optional)
Enabling VPLS Autodiscovery: BGP Based

Perform the following task to enable each VPLS PE router to discover the other PE routers that are part of the same VPLS domain.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 l2 vfi vfi-name autodiscovery</td>
<td>Enables VPLS Autodiscovery on the PE router and enters L2 VFI configuration mode.</td>
</tr>
<tr>
<td>Step 4 vpn id vpn-id</td>
<td>Configures a VPN ID for the VPLS domain.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Exits L2 VFI configuration mode. Commands take effect after the router exits L2 VFI configuration mode.</td>
</tr>
</tbody>
</table>

Configuring BGP to Enable VPLS Autodiscovery

BGP learns the endpoint provisioning information from the L2VPN database which is updated each time a Layer 2 virtual forwarding instance (VFI) is configured. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to configure a pseudowire mesh to support aL2VPN-based services.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 router bgp autonomous-system-number</td>
<td>Enters router configuration mode for the specified routing process.</td>
</tr>
<tr>
<td>Step 4 no bgp default ipv4-unicast</td>
<td>Disables the IPv4 unicast address family for the BGP routing process.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Routing information for the IPv4 unicast address family is advertised by default for each BGP routing session configured with the neighbor remote-as router configuration command unless you configure the no bgp default ipv4-unicast router configuration command before configuring the neighbor remote-as command. Existing neighbor configurations are not affected.</td>
</tr>
<tr>
<td>Step 5 bgp log-neighbor-changes</td>
<td>Enables logging of BGP neighbor resets.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 6    | `neighbor (ip-address | peer-group-name)` <br>`remote-as autonomous-system-number` | Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.  
   - If the `autonomous-system-number` argument matches the autonomous system number specified in the `router bgp` command, the neighbor is an internal neighbor.  
   - If the `autonomous-system-number` argument does not match the autonomous system number specified in the `router bgp` command, the neighbor is an external neighbor.  
   - In this example, the neighbor at 10.10.10.1 is an internal BGP neighbor. |
| 7    | `neighbor (ip-address | peer-group-name)` <br>`update-source interface-type interface-number` | (Optional) Configures a router to select a specific source or interface to receive routing table updates.  
   - This example uses a loopback interface. The advantage to this configuration is that the loopback interface is not affected by the effects of a flapping interface. |
| 8    | Repeat Step 6 and Step 7 to configure other BGP neighbors | — |
| 9    | `address-family l2vpn [vpls]` | Specifies the L2VPN address family and enters address family configuration mode.  
   - The optional `vpls` keyword specifies that VPLS endpoint provisioning information is to be distributed to BGP peers.  
   - In this example, an L2VPN VPLS address family session is created. |
| 10   | `neighbor (ip-address | peer-group-name)` <br>`activate` | Enables the neighbor to exchange information for the L2VPN VPLS address family with the local router. |
| 11   | `neighbor (ip-address | peer-group-name)` <br>`send-community (both | standard | extended)` | Specifies that a communities attribute should be sent to a BGP neighbor.  
   - In this example, an extended communities attribute is sent to the neighbor at 10.10.10.1. |
| 12   | Repeat Step 10 and Step 11 to activate other BGP neighbors under an L2VPN address family. | — |
| 13   | `exit-address-family` | Exits address family configuration mode and returns to router configuration mode. |
| 14   | `exit` | Exits router configuration mode. |
| 15   | `exit` | Exits privileged EXEC mode. |
| 16   | `show vfi` | (Optional) Displays information about the configured VFI instances. |
| 17   | `show ip bgp l2vpn vpls (all | rd vpn-rd)` | (Optional) Displays information about the Layer2 VPN VPLS address family. |
Customizing the VPLS Autodiscovery Settings

Several commands allow you to customize the VPLS environment. You can specify identifiers for the VPLS domain, the route distinguisher, the route target, and the PE router. Perform the following steps to customize these settings.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 l2 vfi vfi-name autodiscovery</td>
<td>Enables VPLS Autodiscovery on the PE router and enters L2 VFI configuration mode.</td>
</tr>
<tr>
<td>Step 4 vpn id vpn-id</td>
<td>Configures a VPN ID for the VPLS domain.</td>
</tr>
<tr>
<td>Step 5 vpls-id {autonomous-system-number:nn</td>
<td>(Optional) Specifies the VPLS domain. This command is optional, because VPLS Autodiscovery automatically generates a VPLS ID using the BGP autonomous system number and the configured VFI VPN ID. You can use this command to change the automatically generated VPLS ID. There are two formats for configuring the VPLS ID argument. It can be configured in the autonomous-system-number:network number (ASN:nn) format, as shown in the example, or it can be configured in the IP-address:network number format (IP-address:nn).</td>
</tr>
<tr>
<td>Step 6 rd {autonomous-system-number:nn</td>
<td>(Optional) Specifies the RD to distribute endpoint information. This command is optional, because VPLS Autodiscovery automatically generates an RD using the BGP autonomous system number and the configured VFI VPN ID. You can use this command to change the automatically generated route distinguisher. There are two formats for configuring the route distinguisher argument. It can be configured in the autonomous-system-number:network number (ASN:nn) format, as shown in the example, or it can be configured in the IP-address:network number format (IP-address:nn).</td>
</tr>
<tr>
<td>Step 7 route-target [import</td>
<td>export</td>
</tr>
</tbody>
</table>
Configuration Examples for VPLS Autodiscovery: BGP Based

The following examples show the configuration of a network using VPLS Autodiscovery and VPLS Autodiscovery supported on a route reflector:

- VPLS Autodiscovery: BGP Based: Basic Example, page 54-61
- Understanding MPLS OAM, page 54-64

VPLS Autodiscovery: BGP Based: Basic Example

Figure 11 show a basic configuration of VPLS Autodiscovery.

![Figure 11 Basic VPLS Autodiscovery Configuration]

**PE1**

```
l2 router-id 10.1.1.1
l2 vfi auto autodiscovery
    vpn id 100
! pseudowire-class mpls
    encapsulation mpls
! interface Loopback1
    ip address 10.1.1.1 255.255.255.255
! interface Ethernet0/0
```
description Backbone interface
ip address 192.168.0.1 255.255.255.0
mls ip
!
router ospf 1
log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0
network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp update-delay 1
neighbor 10.1.1.2 remote-as 1
neighbor 10.1.1.2 update-source Loopback1
neighbor 10.1.1.3 remote-as 1
neighbor 10.1.1.3 update-source Loopback1
!
address-family ipv4
no synchronization
no auto-summary
exit-address-family
!
address-family l2vpn vpls
neighbor 10.1.1.2 activate
neighbor 10.1.1.2 send-community extended
neighbor 10.1.1.3 activate
neighbor 10.1.1.3 send-community extended
exit-address-family

PE2

12 router-id 10.1.1.2
12 vfi auto autodiscovery
vpn id 100
!
pseudowire-class mpls
encapsulation mpls
!
interface Loopback1
ip address 10.1.1.2 255.255.255.255
!
interface Ethernet0/0
description Backbone interface
ip address 192.168.0.2 255.255.255.0
mls ip
!
router ospf 1
log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0
network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp update-delay 1
neighbor 10.1.1.1 remote-as 1
neighbor 10.1.1.1 update-source Loopback1
neighbor 10.1.1.3 remote-as 1
neighbor 10.1.1.3 update-source Loopback1
!
address-family ipv4
no synchronization
no auto-summary
exit-address-family

address-family l2vpn vpls
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 send-community extended
neighbor 10.1.1.3 activate
neighbor 10.1.1.3 send-community extended
exit-address-family

PE3

12 router-id 10.1.1.3
12 vfi auto autodiscovery
vpn id 100
! pseudowire-class mpls
encapsulation mpls
!
interface Loopback1
ip address 10.1.1.3 255.255.255.255
!
interface Ethernet0/0
description Backbone interface
ip address 192.168.0.3 255.255.255.0
mpls ip
!
router ospf 1
log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0
network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp update-delay 1
neighbor 10.1.1.1 remote-as 1
neighbor 10.1.1.1 update-source Loopback1
neighbor 10.1.1.2 remote-as 1
neighbor 10.1.1.2 update-source Loopback1
!
address-family ipv4
no synchronization
no auto-summary
exit-address-family
!
address-family l2vpn vpls
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 send-community extended
neighbor 10.1.1.2 activate
neighbor 10.1.1.2 send-community extended
exit-address-family

Sample configuration for VPLS BGP Signalling

l2vpn vfi context vfi1
vpn id 1
autodiscovery bgp signaling bgp
ve id 1001
ve range 10
!
!
Understanding MPLS OAM

MPLS OAM helps service providers monitor label-switched paths (LSPs) and quickly isolate MPLS forwarding problems to assist with fault detection and troubleshooting in an MPLS network. The switch supports these MPLS OAM features:

- LSP ping/traceroute LDP IPv4 version 3
- Any Transport over MPLS (AToM) Virtual Circuit Connection Verification (VCCV) to use MPLS LSP Ping to test the pseudowire section of an AToM virtual circuit (VC).
- IP Service Level Agreements (IP SLAs) to monitor MPLS LSP networks and IP SLAs Health Monitor to automatically generate LSP ping and traceroute to BGP VPN neighbors.

Note

In Cisco IOS Release 12.2(37)SE, IP SLAs support implemented nonstandard IP SLAs command-line interface commands, using the rtr global configuration command to put the switch into response time reporter (RTR) configuration mode. Beginning with Cisco IOS Release 12.2(40)SE, the switch uses the standard IP SLAs configuration commands, using the ip sla global configuration command to put the switch into IP SLAs configuration mode. See Chapter 46, “Configuring Cisco IOS IP SLAs Operations,” for more information on configuring IP SLAs.

For more information about MPLS OAM, see Multiprotocol Label Switching Configuration Guide Library, Cisco IOS Release 15.x.

Note

The switch does not support all of the commands referenced in the MPLS LSP Ping/Traceroute feature module. For a list of commands that are visible in the CLI help, but not supported on the switch, see Appendix 67, “Unsupported Commands.”

Beginning with Cisco IOS Release 12.2(40)SE, the switch supports these additional keywords for the ping mpls and traceroute mpls privileged EXEC commands to support RFC4379:

- Entering the dsmap keyword with the ttl keyword to the ping command allows you configure a MPLS echo request from the source router to expire at a transit router with a wildcard downstream map to obtain downstream information from the transit router.
- Entering the flags fec keyword configures the source router to force the transit router to validate the target forwarding equivalence class (FEC).
- Entering the force-explicit-null keyword adds a Null label to the end of the label stack to allow the destination provider-edge device to distinguish between traffic that has been rejected by the destination provider router and traffic that arrives untagged.
- Entering the interval keyword allows you to specify the echo request packet send interval.
- Entering the output interface interface-id keywords provides path information as input to the LDP IPv4 ping and traceroute configuration to force echo packets through the same paths for more detailed analysis for LSP debugging.
- Entering the repeat keyword specifies the number of retries attempted if an echo request times out before an echo reply is received.
- To allow interoperability between these IETF RFC 4379 drafts, the revision keyword was added to enable Cisco IOS releases to support the existing draft changes and any changes from future versions of the IETF LSP Ping draft. The switch supports revision 2 and RFC 4329 Compliant.

In addition, these other features have been added:
Understanding MPLS OAM

- Echo request return codes have been enhanced for better fault isolation.
- You can use the `no mpls oam` global configuration command to disable the MPLS OAM subsystem when MPLS is running.
- You can configure the maximum number of labels in a label stack for load balancing.
- The switch supports IP load balancing, up to a total of four next-hop paths. With the IP license, the switch supports up to sixteen next-hop paths. Each path supports up to four Equal Cost Routing (ECR) multipaths.
- The switch now supports LSP tree trace, using the `trace mpls multipath` privileged EXEC command to trace all possible paths of an LSP network between the ingress and egress routers by using downstream mapping.

Enhancements to the IP SLAs MPLS LSP Health Monitor include:

- Entering the `auto ip sla mpls-lsp-monitor` global configuration command automatically configures ping and traceroute boundaries
- Entering the `path-discover` command in auto IP SLA MPLS parameter configuration mode configures equal cost multipath (ECMP) tree trace. VPN end points are automatically discovered and ping or traceroute actions are automatically generated for each provider edge router.
- For more information on configuring the LSP Health Monitor, go to this URL: http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_lsp_mon_autodisc.html

LSP Ping

MPLS LSP ping uses MPLS echo request and reply packets, similar to Internet Control Message Protocol (ICMP) echo request and reply messages, to validate an LSP. ICMP echo request and reply messages validate IP networks; MPLS OAM echo and reply messages validate MPLS LDP networks. The LSP ping and trace functions use IPv4 UDP packets with UDP port number 3503. You can use MPLS LSP ping to validate IPv4 LDP or Forwarding Equivalence Classes (FECs) by using the `ping mpls` privileged EXEC command. The MPLS echo request packet is sent to a target router by using the label stack associated with the FEC to be validated.

The source address of the LSP echo request is the IP address of the LDP router generating the LSP request. The destination IP address is a 127.x.y.z/8 address, which prevents the IP packet from being switched to its destination if the LSP is broken. The 127.0.0.x destination address range prevents the OAM packets from exiting the egress provider-edge router, which keeps them from leaking from the service-provider network to the customer network.

In response to an MPLS echo request, an MPLS echo reply is forwarded as an IP packet by using IP, MPLS, or a combination of both. The source address of the MPLS echo-reply packet is an address obtained from the router generating the echo reply. The destination address is the source address of the router that originated the MPLS echo-request packet. The MPLS echo-reply destination port is the echo-request source port.

LSP Traceroute

MPLS LSP traceroute also uses MPLS echo request and reply packets to validate an LSP. You can use MPLS LSP traceroute to validate LDP IPv4 by using the `trace mpls` privileged EXEC command. The traceroute time-to-live (TTL) settings force expiration of the TTL along an LSP. MPLS LSP traceroute incrementally increases the TTL value in its MPLS echo requests (TTL = 1, 2, 3, 4) to discover the
downstream mapping of each successive hop. The transit router processing the MPLS echo request returns an MPLS echo reply containing information about the transit hop in response to the TTL-expired MPLS packet. The MPLS echo reply destination port is sent to the echo request source port.

**AToM VCCV (LSP Ping over Pseudowire)**

You can use AToM VCCV control words to send control packets inband of an AToM pseudowire from the originating provider edge router or out-of-band by using router alert. The switch supports out-of-band VCCV. You configure this by using the `ping mpls pseudowire` privileged EXEC command. The transmission is intercepted at the destination provider-edge router, instead of being forwarded to the customer-edge router. You can use AToM VCCV and MPLS LSP ping to test the pseudowire section of AToM virtual circuits.

AToM VCCV consists of these components:

- A signaled component in which the AToM VCCV capabilities are advertised during virtual-circuit label signaling
- A switching component that causes the AToM VC payload to be treated as a control packet

An LSP ping through a Layer 2 pseudowire requires that the originating router first validate the pseudowire control channel capability during the exchange of virtual-circuit labels. In the switch, this is done by using a router alert label, which sends the LSP ping or traceroute packet to the egress PE router processor instead forwarding it to the CE devices. This is type 2 AToM VCCV.

The switch also supports inband VCCV validation using a control word (type 1).

**IP SLAs Interworking with MPLS OAM**

IP SLAs provides a way to generate MPLS LSPs and measure statistics between provider-edge routers participating in the MPLS network. It uses LSP ping and traceroute to determine network availability or measure network connectivity and performance between the provider-edge routers. You can manually configure IP SLAs LSP ping or traceroute, or you can configure it using the IP SLAs Health Monitor.

- When you manually configure LSP ping or traceroute, you explicitly specify the FEC you want to validate, for example, a VPN end point.
- When you use the MPLS LSP Health Monitor, you specify a VRF, and the monitor automatically discovers the VPN end points. When configured, the LSP Health Monitor automatically creates and deletes IP SLAs LSP ping or LSP traceroute operations based on network topology. It automatically discovers all adjacent BGP next-hop provider-edge routers and creates individual IP SLAs LSP ping operations for each applicable BGP next-hop neighbor.

For more information on configuring the LSP Health Monitor, go to this URL:


**LSP Tree Trace and IP SLAs ECMP Tree Trace**

As the number of MPLS deployments increases, the number of traffic types the MPLS networks carry could increase. In addition, load balancing in the MPLS network provides alternate paths for carrying MPLS traffic to a target router, making troubleshooting forwarding problems between PEs difficult. The MPLS LSP multipath tree trace feature provides the means to discover all possible routing paths of an
LSP network between an egress and ingress router by using downstream mapping. Once discovered, you can retest these paths periodically by using MPLS LSP ping or traceroute. This feature is an extension to the MPLS LSP tracerouter functionality for the tracing of LDP IPv4 LSPs.

With equal cost multipath (ECMP) tree trace, the source router tries to force the request down each ECMP path so that the targeted FEC crosses all possible ECMP paths. The source LSR starts path discovery by sending a transit router a bitmap in an MPLS echo request. The transit router returns information that contains subsets of the bitmap in a downstream map in an echo reply. The source router uses the information in the echo reply to interrogate the next router. It interrogates each successive router until it finds one bitmap setting that is common to all routers along the path.

You can manually configure tree trace by using downstream mapping Type Length Values (TLVs). You can also use the ECMP tree trace feature in the IP SLAs LSP Health Monitor. When you enter the `path-discover` command in auto IP SLA MPLS parameter configuration mode, VPN end points are automatically discovered and ping or traceroute actions are automatically generated for each provider edge router. You can also use the LSP Health Monitor to configure multioperation scheduling.

For more information about LSP multipath tree trace, see this URL:

### Configuring MPLS OAM and IP SLAs MPLS

This section includes this information about configuring MPLS OAMs on a switch:

- Default MPLS OAM Configuration, page 54-67
- MPLS OAM Configuration Guidelines, page 54-67

These sections describe the optional or required tasks:

- Using LSP Ping for LDP IPv4 FEC, page 54-68
- Using LSP Ping to Specify a MPLS TE Tunnel, page 54-70
- Using LSP Traceroute, page 54-71
- Using LSP Ping for Pseudowire (AToM VCCV), page 54-73
- Configuring IP SLAs MPLS Ping and Traceroute, page 54-75
- Using LSP Tree Trace, page 54-81

### Default MPLS OAM Configuration

MPLS OAM LSP ping and traceroute are not configured.

The IP SLAs MPLS LSP Health Monitor is not configured.

The `mpls oam` global configuration command is enabled.

### MPLS OAM Configuration Guidelines

Follow these guidelines when configuring MPLS OAM:
### Note

The switch does not support traffic engineering FEC in this release.

- Because MPLS OAM detects problems in the MPLS LSP network, it is a useful tool when there is a discrepancy between the MPLS LSP and IP networks or between the MPLS control plane and data plane.
- When the switch is used as a provider router in the core and ECMP tree trace is configured, the switch can force the LSP packet down only one path, the actual data path.

## Using LSP Ping for LDP IPv4 FEC

When you enter the `ping mpls` privileged EXEC command to begin an LSP ping operation, the keyword that follows specifies the Forwarding Equivalence Class (FEC) that is the target of the LCP ping to which you want to verify connectivity.

Beginning in privileged EXEC mode, follow these steps to configure LSP LDP IPv4 ping:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**  
`ping mpls ipv4` 
destination-address 
destination-mask [destination address-start address-end increment] [exp exp-bits] [interval ms] [pad pattern] [repeat count] [reply dscp dscp-value] [reply mode {ipv4 | router-alert}] [revision {1 | 2 | 3}] [size packet-size | sweep minimum maximum size-increment] [source source-address] [timeout seconds] [ttl time-to-live] [verbose] [revision tlv-revision-number] [force-explicit-null] [output interface interface-id [nexthop ip-address]] [dmap [hashkey [none | ipv4 bitmap bitmap-size]] [flags fec]] | Configure LSP IPv4 ping. The keywords have these meanings:
- `destination-address destination-mask`—Specify the address and network mask of the target FEC.
- (Optional) `destination address-start address-end increment` —Enter the destination 127 network address range.
- (Optional) `exp exp-bits`—Specify the MPLS experimental-field value in the MPLS header for an echo reply. The range is from 0 to 7. The default is 0.
- (Optional) `interval ms`—Specify the time in milliseconds between successive MPLS echo requests. The range is 0 to 3600000 ms; the default is 0 (no interval is configured).
- (Optional) `pad pattern`—Specify to use the pad TLV to fill the datagram so that the MPLS echo request is the specified size.
- (Optional) `repeat count`—Specify the number of times to resend the packet. The range is from 1 to 2147483647. If you do not enter the `repeat` keyword, the packet is sent 5 times.
- (Optional) `reply dscp dscp-value`—Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.
Configuring MPLS OAM and IP SLAs MPLS

This is an example of an LSP IPv4 ping:

Switch# ping mpls ipv4 10.131.159.251/32 destination 127.0.0.1 127.0.0.2 0.0.0.1 repeat 2 sweep 1450 1475 25

This is an example of an LSP IPv4 ping:

Switch# ping mpls ipv4 10.131.159.251/32 destination 127.0.0.1 127.0.0.2 0.0.0.1 repeat 2 sweep 1450 1475 25
# Using LSP Ping to Specify a MPLS TE Tunnel

To specify the destination type as an MPLS traffic engineering (TE) tunnel and tunnel interface, use the `ping mpls traffic-eng` privileged EXEC command.

Beginning in privileged EXEC mode, follow these steps to specify the destination type as an MPLS TE tunnel and interface:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| ping mpls traffic-eng {tunnel intf num} [dmap] [exp exp bits in MPLS header] [force-explicit-null] [interval send interval between requests in msec] [pad pad TLV pattern] [repeat repeat count] [reply dscp differentiated services codepoint value] [reply mode {ipv4 | router-alert | no-reply | reply pad-tlv}] [revision echo packet tlv versioning] [source source specified as an IP address] [sweep {min value} {max value} {increment}] [timeout send interval between requests in msec] [ttl time-to-live] [verbose] | Specify the destination type as an MPLS TE tunnel and interface. The keywords have these meanings:  
- **tunnel intf num**—Specifies the destination type as an MPLS traffic engineering (TE) tunnel and the tunnel interface number. The range for the tunnel interface number is from 0 to 65535.  
- **dmap**—Indicates that a downstream mapping (DSMAP) type length and value should be included in the LSP echo request.  
- **exp exp bits in MPLS header**—Specifies the MPLS experimental field value in the MPLS header for echo replies. Range is 0 to 7. Default is 0.  
- **force-explicit-null**—Forces an unsolicited explicit null label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.  
- **interval send interval between requests in msec**—Specifies a send interval between requests in milliseconds. The range is 0 to 3600000 ms; the default is 0 (no interval is configured).  
- **pad pad TLV pattern**—Specifies the pad pattern for an echo request.  
- **repeat repeat count**—Specifies the number of times to resend the packet. The range is from 1 to 2147483647. If you do not enter the repeat keyword, the packet is sent 5 times. |
This is an example of an LSP traffic-eng ping:

```
Switch# ping mpls traffic-eng tunnel 100
```

## Using LSP Traceroute

To learn the routes that packets follow when travelling to their destinations, use the **traceroute mpls** command in EXEC mode.

The LSP traceroute originator sends incremental MPLS echo requests to discover the downstream mapping of each successive hop. When the originating provider edge router receives the reply from the intermediate router, it forms another MPLS echo request with the same target FEC and the time-to-live is incremented by one.
Beginning in privileged EXEC mode, follow these steps to configure LSP traceroute:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Configure LSP traceroute. The keywords have these meanings:</strong></td>
</tr>
<tr>
<td>`traceroute mpls { (ipv4 addr/mask)</td>
<td>(traffic-eng tunnel tunnel intf num) } [destination { start address } { end address } { address increment }]</td>
</tr>
<tr>
<td><strong>Command</strong></td>
<td><strong>Purpose</strong></td>
</tr>
</tbody>
</table>
| `traceroute mpls` | - `ipv4 addr/mask`—Specifies the destination type as a LDP prefix. Enter the address prefix of the target and number of bits in the target address network mask.  
- `traffic-eng tunnel tunnel intf num`—Specifies the destination type as an MPLS traffic engineering (TE) tunnel and tunnel interface.  
- `{start address} {end address} {address increment}`—Specifies a network 127 address to be used as the destination address in the echo request packet.  
- `exp exp bits in MPLS header`—Specifies the MPLS experimental field value in the MPLS header for echo replies. The range is from 0 to 7. The default is 0.  
- `flags fec`—Specifies that forwarding equivalent class (FEC) stack checking is to be performed at transit routers.  
- `force-explicit-null`—Forces an unsolicited explicit NULL label to be added to the MPLS label stack and allows LSP ping to be used to detect LSP breakages at the penultimate hop.  
- `output interface echo request output interface`—Specifies the output interface where echo request packets are sent.  
- `reply dscp differentiated services codepoint value`—Specifies the differentiated service codepoint value for an MPLS echo reply.  
- `reply mode ipv4 | router-alert | no-reply`—Specifies the reply mode for the echo request packet. Enter `ipv4` to reply with an IPv4 UDP packet (the default) or `router-alert` to reply with an IPv4 UDP packet with router alert.  
- `revision echo packet tlv versioning`—Specifies the Cisco extension TLV versioning field:  
  - 1 draft-ietf-mpls-lsp-ping-03 (initial)  
  - 2 draft-ietf-mpls-lsp-ping-03 (rev 1)  
  - 3 draft-ietf-mpls-lsp-ping-03 (rev 2)  
  - 4 draft-ietf-mpls-lsp-ping-09 (initial)  
- `source source specified as an IP address`—Specifies the source address used in the echo request packet.  
- `timeout timeout in seconds`—Specifies the timeout interval in seconds. Range is from 0 to 3600. Default is 2 seconds.  
- `ttl time to live`—Specifies the maximum number of hops. The range is from 1 to 255.  
- `verbose`—Enables verbose output information, including MPLS echo reply, sender address of the packet, and return codes. |
Here are some examples of configuring an LSP traceroute:

```
Switch# traceroute mpls ipv4 10.131.159.251/32 destination 127.0.0.1 127.0.0.2 1 ttl5
```

```
Switch# traceroute mpls traffic-eng tunnel 4
```

### Using LSP Ping for Pseudowire (AToM VCCV)

Entering the `ping mpls pseudowire` privileged EXEC command invokes the functionality of MPLS VCCV, which is the ability to inject traffic control into an AToM virtual circuit and have it intercepted by the remote provider edge router instead of being passed to the attachment circuits for switching. The command requires you to enter the egress provider edge IP address and a virtual-circuit identifier.
Beginning in privileged EXEC mode, follow these steps to configure LSP ping over pseudowire:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping mpls pseudowire ipv4-address vc-id [destination start-address [end-address [address-increment]]] [exp exp-bits] [interval ms] [pad pattern] [repeat count] [reply dscp dscp-value] [reply mode {ipv4</td>
<td>router-alert}] [revision {1</td>
</tr>
</tbody>
</table>

Configure LSP ping over pseudowire. The keywords have these meanings:

- **ipv4-address**—Specify the IPv4 address of the peer.
- **vc-id**—Specify virtual-circuit identification number. The range is from 1 to 4294967295.
- **destination**—Enter the destination 127 network address or address range with increment.
- **exp exp-bits**—Specify the MPLS experimental-field value in the MPLS header. The range is from 0 to 7. The default is 0.
- **interval ms**—Specify the time in milliseconds between successive MPLS echo requests. The range is from 0 to 3600000; the default is 0.
- **pad pattern**—Specify that the pad TLV is used to fill the datagram so that the MPLS echo request is the specified size.
- **repeat count**—Specify the number of times to resend the packet. The range is from 1 to 2147483647. The default is 1. If you do not enter the repeat keyword, the same packet is sent 5 times.
- **reply dscp dscp-value**—Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.
- **reply mode {ipv4 | router-alert}**—Specify the reply mode for the echo request packet. Enter ipv4 to reply with an IPv4 packet (the default) or router-alert to reply with an IPv4 UPD packet with router alert. Router alert is type 2 AToM VCCV.
- **revision**—Enter the IETF MPLS ping draft revision number as 1, 2, or 3.
- **source source-address**—Specify the source IPv4 address of the echo request. The default is the source IPv4 address of the router.
- **size packet-size**—Specify the size of the packet with the label stack imposed as the number of bytes in each ping. The range is from 40 to 18024. The default is 100.
- **sweep minimum maximum size-increment** —Send a number of packets of different sizes.
### Configuring MPLS OAM and IP SLAs MPLS

This is an example of an LSP ping over pseudowire:

Switch# ping mpls pseudowire 10.131.159.251 22 127.0.0.1 127.0.0.2 1 exp 5

### Configuring IP SLAs MPLS Ping and Traceroute

To use IP SLAs for monitoring MPLS LSP ping or traceroute operations to monitor Layer 3 MPLS VPNs, you can manually configure the IP SLAs ping or trace operation or you can configure the IP SLAs LSP Health Monitor. When configured, the LSP Health Monitor automatically discovers VPN endpoints and creates and deletes IP SLAs ping or traceroute operations based on network topology.

As with any IP SLAs operation, you can schedule the start time and end time for MPLS IP SLAs ping or trace, as well as whether it is an ongoing or recurring operation. Multioperation scheduling support for the LSP Health Monitor feature provides the capability to easily schedule the automatically created operations to begin at intervals equally distributed over a specified duration of time (schedule period) and to restart at a specified frequency. Multioperation scheduling is particularly useful in cases where the LSP Health Monitor is enabled on a source PE router that has a large number of PE neighbors and, therefore, a large number of IP SLAs operations running at the same time.

This section includes these configuration procedures:

- Configuring the IP SLAs LSP Health Monitor, page 54-76
- Manually Configuring IP SLAs MPLS LSP Ping or Traceroute, page 54-79

For more details about LSP Health Monitor and MPLS IP SLAs ping or traceroute, see the IP SLAs- LSP Health Monitor configuration guide at this URL:


For more details about IP SLAs operations, see Chapter 54, “Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS.” For detailed information about IP SLAs commands, see the command reference at this URL:


<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | • (Optional) **timeout seconds**—Specify the timeout interval for an MPLS request packet. The range is from 0 to 3600 seconds. The default is 2 seconds.  
• (Optional) **verbose**—Display the MPLS echo reply sender address of the packet and return codes.  
• (Optional) **flags fec**—Request FEC stack checking at the transit router.  
• (Optional) **dmap**—Request downstream mapping information from the replying router.  
• (Optional) **hashkey**—Specify downstream map multipath settings as either none or ipv4 bitmap size (0 to 256). |

---

This is an example of an LSP ping over pseudowire:
Configuring the IP SLAs LSP Health Monitor

You can configure the MPLS LSP Health Monitor to discover BGP VPN next hops and automatically create IP SLAs LSP ping or traceroute operations. You can specify an LSP ping or traceroute operation and VRF tables to be used. By default the LSP Health Monitor discovers all BGP next-hop neighbors by using all VRFs associated with the source provider edge router.

When you configure an LSP Health Monitor operation, you enter auto IP SLAs MPLS parameters configuration mode where you can configure the optional parameters shown in the Steps 4 through 17. See the IP SLAs-LSP Health Monitor feature module for more information about the parameters.

You must configure the MPLS LSP Health Monitor on a provider-edge router. The IP SLAs measurement statistics are stored on the source PE router.

Beginning in privileged EXEC mode, follow these steps to configure the operation parameters, reaction conditions, and scheduling options for a MPLS LSP monitor ping or traceroute.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> auto ip sla mpls-lsp-monitor operation-number</td>
<td>Specify an LSP Health Monitor operation number and enter auto IP SLA MPLS configuration mode. The operation number range is from 1 to 2147483647.</td>
</tr>
<tr>
<td><strong>Step 3</strong> type {echo</td>
<td>pathEcho} {ipsla-vrf-all</td>
</tr>
<tr>
<td>- echo—Select an LSP monitor ping operation.</td>
<td></td>
</tr>
<tr>
<td>- pathEcho—Select an LSP monitor traceroute operation.</td>
<td></td>
</tr>
<tr>
<td>- ipsla-vrf-all—Configure IP SLAs MPLS LSP monitor for all VPNs.</td>
<td></td>
</tr>
<tr>
<td>- vrf vpn-name—Configure the IP SLAs LSP monitor for the specified VPN.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> access-list access-list-number</td>
<td>(Optional) Specify an access list to apply to LSP Health Monitor operation.</td>
</tr>
<tr>
<td><strong>Step 5</strong> delete-scan-factor factor</td>
<td>(Optional) Specify the number of times the LSP Health Monitor checks the scan queue before automatically deleting IP SLAs operations for BGP next-hop neighbors that are no longer valid. The factor range is 0 to 2147483647. The default scan factor is 1.</td>
</tr>
<tr>
<td>Note</td>
<td>You must use the scan-interval command with this command.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exp exp-bits</td>
<td>(Optional) Specify the experimental field value in the echo request packet header. The range is 0 to 7; the default value is 0.</td>
</tr>
<tr>
<td><strong>Step 7</strong> force-explicit-null</td>
<td>(Optional) Add an explicit null label to all echo request packets of an IP SLAs operation.</td>
</tr>
<tr>
<td><strong>Step 8</strong> lsp-selector ip-address</td>
<td>(Optional) Specify the local host IP address used to select the IP SLAs operation LSP. The default is 127.0.0.1.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>9</td>
<td>reply-dscp-bits <code>dscp-value</code></td>
</tr>
<tr>
<td>10</td>
<td>reply-mode `{ipv4</td>
</tr>
<tr>
<td>11</td>
<td>request-data-size <code>bytes</code></td>
</tr>
<tr>
<td>12</td>
<td>scan-interval <code>minutes</code></td>
</tr>
<tr>
<td>13</td>
<td>secondary-frequency `{connection-loss</td>
</tr>
<tr>
<td>14</td>
<td>tag <code>text</code></td>
</tr>
<tr>
<td>15</td>
<td>threshold <code>milliseconds</code></td>
</tr>
<tr>
<td>16</td>
<td>timeout <code>milliseconds</code></td>
</tr>
<tr>
<td>17</td>
<td>ttl <code>time-to-live</code></td>
</tr>
<tr>
<td>18</td>
<td>exit</td>
</tr>
<tr>
<td>19</td>
<td>exit</td>
</tr>
</tbody>
</table>
Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Chapter 54 Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 20</strong></td>
<td>(Optional) Configure other LSP Health Monitor actions:</td>
</tr>
<tr>
<td><code>auto ip sla mpls-lsp-monitor</code>&lt;br&gt;<code>reaction-configuration operation-number react</code>&lt;br&gt;<code>monitored-element [action-type option]</code>&lt;br&gt; `[threshold-type {consecutive [occurrences]</td>
<td>immediate</td>
</tr>
<tr>
<td>- <code>react monitored-element</code>—Specify the element to be monitored for violations. For example, enter <code>connectionLoss</code> to configure a reaction to a 1-way connection loss for the operation.</td>
<td></td>
</tr>
<tr>
<td>- (Optional) <code>action-type option</code>—Specify the action to take when the threshold event occurs. For example, enter <code>none</code> for no action or <code>trapOnly</code> to send an SMNP logging trap.</td>
<td></td>
</tr>
<tr>
<td>- (Optional) <code>threshold-type</code>—Specify when the action-type occurs. These are the options:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <code>consecutive [occurrences]</code>—When reaction conditions are met consecutively for a specified number of times. The valid range is from 1 to 16; the default is 5.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) <code>threshold-type immediate</code>—When the reaction conditions are met.</td>
</tr>
<tr>
<td></td>
<td>- (Optional) <code>threshold-type never</code>—Never. This is the default threshold type.</td>
</tr>
<tr>
<td><strong>Step 21</strong></td>
<td>Schedule time parameters for the LSP Health Monitor.</td>
</tr>
<tr>
<td><code>auto ip sla mpls-lsp-monitor schedule</code>&lt;br&gt;<code>operation-number schedule-period seconds</code>&lt;br&gt;`[frequency seconds] [start-time {hh:mm [:ss] [month day</td>
<td>day month]</td>
</tr>
<tr>
<td>- <code>schedule-period</code> seconds—Enter the schedule period in seconds. The range is 1 to 604800 seconds.</td>
<td></td>
</tr>
<tr>
<td>- (Optional) <code>frequency seconds</code>—Enter the frequency for LSP monitoring in seconds. The range is 1 to 604800 seconds.</td>
<td></td>
</tr>
<tr>
<td>- (Optional) <code>start-time</code>—Enter the time for the operation to begin collecting information:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- To start at a specific time, enter the hour, minute, second (in 24-hour notation) and day of the month. If no month is entered, the default is the current month.</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>pending</code> to select no information being collected until a start time is selected.</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>now</code> to start the operation immediately.</td>
</tr>
<tr>
<td></td>
<td>- Enter <code>after hh:mm:ss</code> to indicate that the operation should start after the entered time has elapsed.</td>
</tr>
<tr>
<td><strong>Step 22</strong></td>
<td>(Optional) Reset LDP monitor group statistics.</td>
</tr>
<tr>
<td><code>auto ip sla mpls-lsp-monitor reset</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 23</strong></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 24</strong></td>
<td>Show the configured LSP monitoring operations.</td>
</tr>
<tr>
<td><code>show ip sla mpls-lsp-monitor configuration</code>&lt;br&gt;<code>[operation-number]</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 25</strong></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 26</strong></td>
<td>Display a summary of IP SLAs LSP MPLS status.</td>
</tr>
<tr>
<td><code>show ip sla mpls-lsp-monitor summary</code></td>
<td></td>
</tr>
</tbody>
</table>
Enter the `no auto ip sla mpls-lsp-monitor operation-number` global configuration command to delete the operation.

This is an example of configuring the MPLS LSP Health Monitor for all VPNs:

```plaintext
Switch# config t
Switch(config)# auto ip sla mpls-lsp-monitor 1
Switch(config-auto-ip-sla-mpls)# type echo ipsla-vrf-all
Switch(config-auto-ip-sla-mpls-params)# timeout 1000
Switch(config-auto-ip-sla-mpls-params)# scan-interval 1
Switch(config-auto-ip-sla-mpls-params)# secondary-frequency connection-loss 10
Switch(config-auto-ip-sla-mpls-params)# secondary-frequency timeout 10
Switch(config-auto-ip-sla-mpls-params)# exit
Switch(config)# auto ip sla mpls-lsp-monitor reaction-configuration 1 react connectionLoss threshold-type consecutive 3 action-type trapOnly
Switch(config)# auto ip sla mpls-lsp-monitor schedule 1 schedule-period 60 start-time now
Switch(config)# end
```

### Manually Configuring IP SLAs MPLS LSP Ping or Traceroute

Beginning in privileged EXEC mode, follow these steps to manually configure the IP SLAs LSP ping or traceroute:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enter an IP SLAs operation number and enter IP SLAs configuration mode.</td>
</tr>
<tr>
<td><code>ip sla operation-number</code></td>
<td>The range is from 1 to 2147483647.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Manually configure the IP SLAs LSP monitor and enter IP SLAs monitor</td>
</tr>
<tr>
<td>`mpls lsp {ping</td>
<td>trace} ipv4 destination_address destination_mask [force-explicit-null] [lsp-selector ip_address] [reply dscp] [reply mode {ipv4</td>
</tr>
<tr>
<td></td>
<td>trace—Select an LSP monitor traceroute operation.</td>
</tr>
<tr>
<td></td>
<td>destination_address destination_mask—Enter the address and network mask of the target.</td>
</tr>
<tr>
<td></td>
<td>(Optional) force-explicit-null—Add an explicit NULL label to the end of the label stack.</td>
</tr>
<tr>
<td></td>
<td>(Optional) lsp-selector ip_address—Specify the local host address used to select the LSP.</td>
</tr>
<tr>
<td></td>
<td>(Optional) reply dscp dscp-value—Specify a specific class of service (CoS) in an echo reply by providing a differentiated services code point (DSCP) value.</td>
</tr>
<tr>
<td></td>
<td>(Optional) reply mode {ipv4</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Specify the experimental field value in the echo request packet header. The range is 0 to 7; the default value is 0.</td>
</tr>
<tr>
<td><code>exp exp-bits</code></td>
<td></td>
</tr>
</tbody>
</table>
### Step 5
```
request-data-size bytes
```
(Optional) Specify the protocol data size for an IP SLAs request packet. The range is 100 to 1500; the default is 100 bytes.

### Step 6
```
secondary-frequency \{connection-loss \| timeout\} frequency
```
(Optional) Set the secondary frequency (faster measurement frequency) to which an IP SLAs operation should change when a reaction condition occurs. The frequency range is 1 to 604800.

### Step 7
```
tag text
```
(Optional) Create a user-specified identifier for an IP SLAs operation.

### Step 8
```
threshold milliseconds
```
(Optional) Specify the rising threshold (hysteresis) that generates a reaction event and stores history information for an IP SLAs operation. The range is 0 to 2147483647; the default is 5000 ms.

### Step 9
```
timeout milliseconds
```
(Optional) Specify the amount of time that the IP SLAs operation waits for a response from its request packet. The range is 0 to 604800000; the default value is 5000 ms.

### Step 10
```
ttl time-to-live
```
(Optional) Specify the maximum hop count for an IP SLAs echo request packet. The range is 1 to 255.

### Step 11
```
exit
```
Return to global configuration mode.

### Step 12
```
ip sla schedule operation-number \[ageout seconds\] \[life \{forever \| seconds\} \] \[recurring\] \[start-time \{hh:mm [:ss] \| month day \| day month\] \| pending \| now \| after hh:mm:ss\]
```
Schedule the time parameters for MPLS LSP monitoring.
- **operation-number**—Enter the IP SLAs operation number.
- (Optional) **ageout seconds**—Enter the number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 seconds (never ages out). The range is 0 to 2073600 seconds.
- (Optional) **life**—Set the operation to run indefinitely (**forever**) or for a specific number of **seconds**. The range is from 0 to 2147483647. The default is 3600 seconds (1 hour)
- (Optional) **recurring**—Set the probe to be automatically scheduled every day.
- (Optional) **start-time**—Enter the time for the operation to begin collecting information:
  - To start at a specific time, enter the hour, minute, second (in 24-hour notation) and day of the month. If no month is entered, the default is the current month.
  - Enter **pending** to select no information being collected until a start time is selected.
  - Enter **now** to start the operation immediately.
  - Enter **after hh:mm:ss** to indicate that the operation should start after the entered time has elapsed.

### Step 13
```
end
```
Return to privileged EXEC mode.

### Step 14
```
show ip sla configuration \[operation-number\]
```
Show the configured LSP monitoring operations.
To remove an IP SLAs operation, enter the no ip sla operation-number global configuration command.

This is an example of manually configuring an MPLS LSP ping operation:

```
Switch# config t
Switch(config)# ip sla 1
Switch(config-ip-sla)# mpls lsp ping ipv4 192.168.1.4 255.255.255.255 lsp-selector 127.1.1.1
Switch(config-ip-sla-lspPing)# secondary-frequency connection-loss 30
Switch(config-ip-sla-lspPing)# secondary-frequency timeout 30
Switch(config-ip-sla-lspPing)# exit
Switch(config)# ip sla schedule 1 start-time now life forever
Switch(config)# exit
```

Using LSP Tree Trace

LSP tree trace is the capability to trace through all possible paths of an LSP network between the ingress and egress routers by using downstream mapping. You can manually configure tree trace using the `trace mpls multipath` privileged EXEC command. You can use IP SLAs Health Monitor for (ECMP tree trace by entering the `path-discover` command in auto IP SLA MPLS parameter configuration mode. VPN end points are automatically discovered and ping or traceroute actions are automatically generated for each provider edge router.

This section includes these configuration procedures:

- Manually Setting LSP Tree Trace, page 54-81
- Configuring ECMP IP SLAs Tree Trace, page 54-82

Manually Setting LSP Tree Trace

Beginning in privileged EXEC mode, follow these steps to manually set LSP tree trace:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>traceroute mpls multipath ipv4 destination-address destination-mask [destination address-start address-end increment] [exp exp-bits] [reply dscp dscp-value] [reply mode ipv4</td>
</tr>
<tr>
<td></td>
<td>[source source-address] [timeout seconds] [ttl time-to-live] [verbose] [revision tlv-revision-number] [force-explicit-null] [output interface interface-id [nexthop ip-address]] [flags fec]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 54  Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

Configuring MPLS, MPLS VPN, MPLS OAM, and EoMPLS

### Configuring MPLS OAM and IP SLAs MPLS

Beginning in privileged EXEC mode, follow these steps to use the LSP Health Monitor to configure IP SLAs ECMP tree trace:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) reply mode ( \textbf{ipv4}</td>
<td>\textbf{router-alert} )—Specify the reply mode for the echo request packet. Enter \textbf{ipv4} to reply with an IPv4 UDP packet (the default) or \textbf{router-alert} to reply with an IPv4 UDP packet with router alert.</td>
</tr>
<tr>
<td>(Optional) revision —Enter the draft revision number as ( 1, 2, ) or ( 3. )</td>
<td></td>
</tr>
<tr>
<td>(Optional) source source-address—Specify the source address or the name. This is the destination address in the MPLS echo response. The default address is loopback0.</td>
<td></td>
</tr>
<tr>
<td>(Optional) timeout seconds—Specify the timeout interval for an MPLS request packet. The range is from 0 to 3600 seconds. The default is 2 seconds.</td>
<td></td>
</tr>
<tr>
<td>(Optional) ttl time-to-live—Specify a time-to-live value. The range is from 1 to 255.</td>
<td></td>
</tr>
<tr>
<td>(Optional) verbose—Display the MPLS echo reply sender address of the packet and return codes.</td>
<td></td>
</tr>
<tr>
<td>(Optional) revision number—Enter a Cisco-TLV-revision-number, 1 through 4.</td>
<td></td>
</tr>
<tr>
<td>(Optional) force-explicit-null—Add an explicit NULL label to the end of the label stack.</td>
<td></td>
</tr>
<tr>
<td>(Optional) output interface interface-id—Specify the output interface for the echo request.</td>
<td></td>
</tr>
<tr>
<td>(Optional) nexthop ip-address—Force packets to go through the specified next-hop address.</td>
<td></td>
</tr>
<tr>
<td>(Optional) flags fec—Request FEC stack checking at the transit router.</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring ECMP IP SLAs Tree Trace

Beginning in privileged EXEC mode, follow these steps to use the LSP Health Monitor to configure IP SLAs ECMP tree trace:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 auto ip sla mpls-lsp-monitor operation-number</td>
<td>Specify an LSP Health Monitor operation number and enter auto IP SLAs MPLS configuration mode. The operation number range is from 1 to 2147483647.</td>
</tr>
<tr>
<td>Step 3 path-discover</td>
<td>Enter IP SLAs MPLS LSP monitor path discover configuration mode to configure sending MPLS trace down all multiple paths (tree trace).</td>
</tr>
<tr>
<td>Step 4 force-explicit-null</td>
<td>(Optional) Add an explicit null label to all echo request packets of an IP SLAs Health Monitor operation.</td>
</tr>
<tr>
<td>Step 5 hours-or-statistics kept ( \text{hours} )</td>
<td>(Optional) Set the number of hours for which LSP discovery group statistics are maintained for an LSP Health Monitor operation.</td>
</tr>
</tbody>
</table>
### Configuring MPLS OAM and IP SLAs MPLS

**Step 6**  
`interval milliseconds`  
(Optional) Specify the time interval between MPLS echo requests that are sent as part of the LSP discovery process for an LSP Health Monitor operation.

**Step 7**  
`lsp-selector-base ip-address`  
(Optional) Specifies the base IP address used to select the LSPs belonging to the LSP discovery groups of an LSP Health Monitor operation.

**Step 8**  
`maximum-sessions`  
(Optional) Set the number of concurrent active tree trace request to be submitted. This is the maximum number of BGP next hop neighbors that can be concurrently undergoing LSP discovery for a single LSP Health Monitor operation.  
**Note** Use careful consideration when configuring this parameter to avoid a negative impact on the switch CPU.

**Step 9**  
`scan-period minutes`  
(Optional) Set a time period in minutes for completing tree trace discovery. This is the amount of time after which the LSP discovery process can restart for an LSP Health Monitor operation.

**Step 10**  
`session timeout seconds`  
(Optional) Set a timeout value in seconds for tree trace requests. This is the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its LSP discovery request for a particular BGP next hop neighbor.

**Step 11**  
`timeout seconds`  
(Optional) Set the amount of time the LSP discovery process for an LSP Health Monitor operation waits for a response to its echo request packets.  
**Note** Use careful consideration when configuring this parameter to avoid a negative impact on the switch CPU.

**Step 12**  
`exit`  
Exit IP SLAs MPLS LSP monitor path discover configuration mode and return to auto IP SLA MPLS parameter configuration mode.

**Step 13**  
`exit`  
Exit auto IP SLA MPLS parameter configuration mode and returns to global configuration mode.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 14   | auto ip sla mpls-lsp-monitor reaction-configuration operation-number react lpd {lpd-group [retry number] | (Optional) Configure LSP Health Monitor tree trace actions:  
|      |         |         |  
|      |         |   | • operation-number—Enter the Health Monitor tree-trace operation number.  
|      |         |         | • react lpd—Specify LPD as the element to be monitored for violations.  
|      |         |         | • lpd-group—Enable monitoring of LSP discovery group status changes.  
|      |         |         | • retry number—Specify the number of times the equal-cost multipaths belonging to an LSP discovery group are retested when a failure is detected. The value of the number argument is zero by default.  
|      |         |         | • tree-trace—Enable monitoring of situations where LSP discovery to a BGP next hop neighbor fails.  
|      |         |         | • (Optional) action-type trapOnly—Specify the action to take when the threshold event occurs as trapOnly to send an SMNP logging trap.  
| 15   | ip sla monitor logging traps | (Optional) Enable the generation of SNMP system logging messages specific to IP SLAs trap notifications.  
| 16   | auto ip sla mpls-lsp-monitor schedule operation-number schedule-period seconds [frequency seconds] [start-time {hh:mm [:ss]} [month day | Schedule the time parameters for the LSP Health Monitor.  
|      |         |         |  
|      |         |         |   | • operation number—Enter the IP SLAs MPLS LSP monitor operation number.  
|      |         |         |   | • schedule-period seconds—Enter the schedule period in seconds. The range is 1 to 604800 seconds.  
|      |         |         |   | • (Optional) frequency seconds—Enter the frequency for LSP monitoring. The range is 1 to 604800 seconds.  
|      |         |         |   | • (Optional) start-time—Enter the time for the operation to begin collecting information:  
|      |         |         |     | – To start at a specific time, enter the hour, minute, second and day of the month. If no month is entered, the default is the current month.  
|      |         |         |     | – Enter pending to select no information being collected until a start time is selected.  
|      |         |         |     | – Enter now to start the operation immediately.  
|      |         |         |     | – Enter after hh:mm:ss to indicate that the operation should start after the entered time has elapsed.  
| 17   | end     | Return to privileged EXEC mode.  
| 18   | show ip sla mpls-lsp-monitor configuration [operation-number] | Show the configured LSP monitoring operations.  

**Command Purpose**
## Monitoring and Maintaining MPLS and EoMPLS

To clear MPLS counters or display MPLS and EoMPLS information, use the privileged EXEC commands in Table 54-3.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
<tr>
<td>show ip sla monitor mpls-lsp-monitor collection-statistics [group-id]</td>
<td>(Optional) Displays the statistics for IP SLAs operations belonging to an LSP discovery group of an LSP Health Monitor operation.</td>
</tr>
<tr>
<td>show ip sla mpls-lsp-monitor lpd operational-state</td>
<td>Optional) Displays the operational status of the LSP discovery groups belonging to an LSP Health Monitor operation.</td>
</tr>
<tr>
<td>Note</td>
<td>These commands are applicable only if the LSP discovery option is enabled.</td>
</tr>
</tbody>
</table>

### Table 54-3 Commands for Displaying MPLS and EoMPLS Information

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mpls counters</td>
<td>Clear MPLS forwarding counters.</td>
</tr>
<tr>
<td>clear mpls traffic-eng autotunnel primary</td>
<td>Remove all primary auto tunnels and recreate them.</td>
</tr>
<tr>
<td>show interface tunnel tunnel-number</td>
<td>Display information about the specified tunnel interface.</td>
</tr>
<tr>
<td>show ip explicit paths</td>
<td>Display the configured IP explicit paths.</td>
</tr>
<tr>
<td>show ip rsvp fast reroute [detail]</td>
<td>Display specific information for RSVP categories, including fast reroute.</td>
</tr>
<tr>
<td>show ip rsvp host</td>
<td>Display RSVP terminal point information for receivers or senders</td>
</tr>
<tr>
<td>show isis database verbose</td>
<td>Display information about the IS-IS database.</td>
</tr>
<tr>
<td>show isis mpls traffic-eng</td>
<td>Display information about IS-IS MPLS traffic engineering.</td>
</tr>
<tr>
<td>show mpls forwarding-table</td>
<td>Display the contents of the MPLS label forwarding information base (LFIB).</td>
</tr>
<tr>
<td>show mpls interfaces</td>
<td>Display information about interfaces that have been configured for label switching.</td>
</tr>
<tr>
<td>show mpls ip binding</td>
<td>Display specified information about label bindings learned by LDP.</td>
</tr>
<tr>
<td>show mpls l2transport vc [detail] [summary]</td>
<td>Display detailed or summary information about the EoMPLS virtual connections that have been enabled to route Layer 2 packets on a provider-edge device.</td>
</tr>
<tr>
<td>show mpls l2transport vc [vc-id] [vc-id-min - vc-id-max]</td>
<td>Display information about the specified virtual connection or range of virtual-connections. The range is from 1 to 4294967295.</td>
</tr>
<tr>
<td>show mpls label range</td>
<td>Display the range of local labels available for use on packet interfaces.</td>
</tr>
<tr>
<td>show mpls ldp backoff</td>
<td>Display information about the configured session setup backoff parameters and any potential LDP peers with which session setup attempts are being throttled.</td>
</tr>
<tr>
<td>show mpls ldp bindings</td>
<td>Display the contents of the label information base (LIB).</td>
</tr>
<tr>
<td>show mpls ldp discovery</td>
<td>Display the status of the LDP discovery process.</td>
</tr>
</tbody>
</table>
### Table 54-3 Commands for Displaying MPLS and EoMPLS Information (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mpls ldp neighbor</td>
<td>Display the status of LDP sessions.</td>
</tr>
<tr>
<td>show mpls ldp parameters</td>
<td>Display current LDP parameters.</td>
</tr>
<tr>
<td>show mpls prefix-map</td>
<td>Show the prefix map used to assign a QoS map to network prefixes that</td>
</tr>
<tr>
<td></td>
<td>match a standard IP access list.</td>
</tr>
<tr>
<td>show mpls traffic-eng autoroute</td>
<td>Display tunnels announced to the IGP, including interface, destination,</td>
</tr>
<tr>
<td></td>
<td>and bandwidth.</td>
</tr>
<tr>
<td>show mpls traffic-eng fast-reroute database</td>
<td>Display the contents of the Fast Reroute (FRR) database.</td>
</tr>
<tr>
<td>show mpls traffic-eng link-management</td>
<td>Display link information about MPLS traffic engineering link</td>
</tr>
<tr>
<td>show mpls traffic-eng topology</td>
<td>Display the MPLS traffic engineering global topology as currently known</td>
</tr>
<tr>
<td></td>
<td>at a node.</td>
</tr>
<tr>
<td>show mpls traffic-eng tunnel</td>
<td>Display information about MPLS traffic-engineering tunnels.</td>
</tr>
</tbody>
</table>