



CHAPTER 20

Configuring L2 Virtual Private Networks

To improve profitability, service providers (SPs) introduce new services to reduce operational expenditures. To reduce the number of managed networks, use network convergence, a multiphase transition of the network. This affects both the core and edge/aggregation side. The technology is predominantly Multiprotocol Label Switching (MPLS) based core networks. However, IP cores are the service of choice in a number of large SPs. Both the IP and the MPLS cores carry multiservice traffic. The edges of the network is constructed with network elements providing a single network element for convergence between Layer 2 and Layer 3 services.

The following Layer 2 virtual private network (L2VPN) solutions enable existing or emerging Layer 2 transport technology to interwork through converged MPLS or IP core networks.

- Virtual Private Wire Services (VPWS)—A point-to-point service consisting of individual point-to-point connections cross-connected to native interfaces.
- Virtual Private LAN Services (VPLS)—A service consisting of a set of point-to-multipoint connections.

L2VPN features are of the VPWS type and are designed for the benefit of the carriers. L2VPN features allow for a transparent use of network resources, and a way of reducing the number of networks that need managing.

Cisco nonstop forwarding (NSF) with stateful switchover (SSO) is effective at increasing availability of network services. Cisco NSF with SSO provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service during a critical failure in the primary processor. SSO synchronizes network state information between the primary and the secondary processor."

Any Transport over MPLS (AToM) uses NSF, SSO, and Graceful Restart to allow a route processor (RP) to recover from a disruption in control plane service without losing the MPLS forwarding state. In Cisco IOS Release 12.2(33) SB, the L2VPN features support NSF/SSO. See the [“NSF and SSO—L2VPN” section on page 20-6](#).

Cisco 10000 series routers also support the following two L2VPN technology solutions:

- Local Switching (LS)—The ordered tuple <AC, AC>. This is the point-to-point interconnection of two attachment circuits within a Cisco 10000 series router chassis. Also, two attachment circuits (ACs) can be of:
 - The same type—Creating a like-to-like LS connection.
 - A distinct type—Creating an any-to-any LS connection.
- AToM—The ordered triple <AC, PW, AC>. This is the point-to-point interconnection of two attachment circuits in separate Cisco 10000 series router chassis through a pseudowire (MPLS). Also, two ACs can be of the same type in which case a like-to-like AToM connection exists. Or, two ACs can be of a distinct type, in which case an any-to-any AToM connection exists.

Using the Label Distribution Protocol (LDP), an AToM circuit session is identified by a unique VC (virtual circuit) between two PE routers. When a Layer 2 frame is received by the imposition PE router, it is encapsulated in an MPLS packet with a VC label, IGP label, and possibly other labels. When the MPLS packet reaches the disposition PE router, the packet is converted back into its Layer 2 encapsulation.

AToM encapsulates Layer 2 frames at the ingress (or imposition) provider edge (PE) router, and sends them to a corresponding PE router at the other end of the connection. The corresponding router is the egress (or disposition) PE router, and it removes the encapsulation and sends out the Layer 2 frame.

The successful transmission of the Layer 2 frames between PE routers is due to the configuration of the PE routers. You set up the connection, called a *pseudowire*, between the routers. An AToM circuit is one type of pseudowire connection.

Benefits of Enabling Layer 2 Packets to Send in an MPLS Network

Some of the benefits of enabling Layer 2 packets to be sent in the MPLS network include:

- The AToM product set accommodates many types of Layer 2 packets, including Ethernet and Frame Relay, across multiple Cisco router platforms. This enables the service provider to transport all types of traffic over the backbone and accommodate all types of customers.
- AToM adheres to the standards developed for transporting Layer 2 packets over MPLS. (See the [“Standards and RFCs” section on page 20-5](#) for the specific standards that AToM follows.) This benefits the service provider who wants to incorporate industry-standard methodologies in the network. Other Layer 2 solutions are proprietary, which can limit the service provider’s ability to expand the network and can force the service provider to use only one vendor’s equipment.
- Upgrading to AToM is transparent to the customer. Because the service provider network is separate from the customer network, the service provider can upgrade to AToM without disruption of service to the customer. The customers assume that they are using a traditional Layer 2 backbone.

A control word (also referred to as a *shim* header) can be added at the imposition router and, if so, this control word is removed at the disposition router.

Cisco 10000 series router supports up to 8000 attachment circuits (ACs). An AToM circuit use one AC and a LS circuit use two ACs. Therefore, Cisco 10000 series router supports 8000 AToM connections or 4000 LS connections or any combination of both AToM and LS connections that sums up to 8000 ACs. Also, Tunnel selection allows you to specify the path that AToM traffic uses. See the [“Any Transport over MPLS—Tunnel Selection” section on page 20-47](#).

This chapter contains the following topics:

- [Feature History for L2VPN, page 20-3](#)
- [Supported L2VPN Transport Types, page 20-3](#)
- [Prerequisites for L2VPN: AToM, page 20-4](#)
- [Restrictions for L2VPN, page 20-5](#)
- [Standards and RFCs, page 20-5](#)
- [MIBs, page 20-6](#)
- [NSF and SSO—L2VPN, page 20-6](#)
- [L2VPN Local Switching—HDLC/PPP, page 20-10](#)
- [Configuration Tasks for L2VPN, page 20-12](#)
- [Monitoring and Maintaining L2VPN, page 20-43](#)
- [Configuration Example—Frame Relay over MPLS, page 20-44](#)

- [Any Transport over MPLS—Tunnel Selection, page 20-47](#)

Feature History for L2VPN

Cisco IOS Release	Description	Required PRE
12.2(28)SB	This feature was introduced on the Cisco 10000 series router.	PRE2
12.2(31)SB2	Support was added for the PRE3.	PRE3
12.2(31)SB2	Ethernet to VLAN over AToM (Bridged) functionality was added.	PRE2/PRE3
12.2(33)SB	<p>The following L2VPN features were added on the Cisco 10000 series router:</p> <ul style="list-style-type: none"> • IEEE 802.1Q Tunneling (QinQ) for AToM • NSF/SSO - Any Transport over MPLS (AToM) • Any Transport over MPLS (AToM): Remote Ethernet Port Shutdown • Any Transport over MPLS: Tunnel Selection • L2VPN Local Switching - HDLC/PPP • Ethernet/VLAN to ATM AAL5 Interworking • Ethernet VLAN to Frame Relay Interworking 	PRE2/PRE3/PRE4

Supported L2VPN Transport Types

In Cisco IOS Release 12.2(28)SB, the Cisco 10000 series router supports the following AToM transport types:

- ATM AAL5 SDU support over MPLS
- Ethernet over MPLS
 - VLAN mode
 - Port mode
- Frame Relay over MPLS
 - DLCI-to-DLCI connections
 - Port-to-port connections
- HDLC over MPLS
- PPP over MPLS



Note Functionally, both HDLC over MPLS and Frame Relay port-to-port connections are the same.

Prerequisites for L2VPN: AToM

Before configuring L2VPN, ensure that the network is configured as follows:

- Configure IP routing in the core so that the PE routers can reach each other using IP.
- Configure the label distribution protocol to be Label Distribution Protocol (LDP).
- Configure label-switched paths (LSPs) between the PE routers. To enable dynamic MPLS labeling on all paths between the imposition and disposition PE routers, use the **mpls ip** command.
- Configure a loopback interface for originating and terminating Layer 2 traffic. Make sure the PE routers can access the other router's loopback interface. Note that the loopback interface is not needed in all cases. For example, tunnel selection does not need a loopback interface when AToM is directly mapped to a TE tunnel.



Note

For L2VPN: LS, it is *not* necessary to configure:

- The label distribution protocol to be Label Distribution Protocol (LDP).
- Label-switched paths (LSPs) between the PE routers using the **mpls ip** command.

Supported Line Cards

Table 20-1 lists line cards supported by the Cisco 10000 series router.

Table 20-1 Cisco 10000 Series Line Cards that Support L2VPN

Transport Type	Supported Line Cards
ATM AAL5 SDU support over MPLS	4-port OC-3/STM-1 ATM 8-port E3/DS3 ATM 1-port OC-12 ATM
Ethernet over MPLS: VLAN mode Port mode	8-port Fast Ethernet Half-Height 1-port Gigabit Ethernet Half-Height 1-port Gigabit Ethernet SIP-600 SPA-1X10GE-L-V2 (10GE) SPA-2X1GE-V2 (2 port GE) SPA-5X1GE-V2 (5 port GE)
Frame Relay over MPLS: DLCI-to-DLCI connections Port-to-port connections HDLC over MPLS PPP over MPLS	24-port Channelized E1/T1 1-port Channelized OC-12/STM-4 4-port Channelized OC-3/STM-1 4-port Channelized T3 6-port Channelized T3 8-port Unchannelized E3/T3 6-port OC-3/STM1 Packet over SONET 1-port OC-12 Packet over SONET 1-port OC-48/STM-16 Packet over SONET

Restrictions for L2VPN

The L2VPN feature has the following restrictions:

- Address format: Configure the LDP router ID on all PE routers to be a loopback address with a /32 mask. Otherwise, some configurations might not function properly.
- The size of maximum transmission unit (MTU) must be the same at both ends of the circuit. To avoid fragmentation of the packets along the way, ensure that the size of MTU at both end of the circuit is smaller than the size of MTU in the core.
- The following L2VPN features are *not* supported:
 - ATM cell switching of any kind
 - ATM AAL5 PDU mode
 - Fragmentation and reassembly, as defined in “PWE3 Fragmentation and Reassembly,” draft-ietf-pwe3-fragmentation-05.txt, February 2004
 - Sequence number support in the control word
 - Tunnel stitching
 - Pseudowire termination

Standards and RFCs

L2VPN conforms to the industry standards and RFCs listed in [Table 20-2](#).

Table 20-2 Standards and RFCs Supported by L2VPN

Standard or RFC	Title
draft-martini-l2circuit-trans-mpls-08.txt	<i>Transport of Layer 2 Frames over MPLS</i>
draft-martini-l2circuit-encap-mpls-04.txt	<i>Encapsulation Methods for Transport of Layer 2 Frames over MPLS</i>
RFC 3032	<i>MPLS Label Stack Encoding</i>
RFC 3036	<i>LDP Specification</i>

MIBs

Table 20-3 lists the MIBs that L2VPN supports.

Table 20-3 *MIBs Supported by L2VPN*

Transport Type	MIB
ATM AAL5 SDU support over MPLS	MPLS LDP MIB (MPLS-LDP-MIB.my) ATM MIB (ATM-MIB.my) CISCO AAL5 MIB (CISCO-AAL5-MIB.my) Cisco Enterprise ATM Extension MIB (CISCO-ATM-EXT-MIB.my) Supplemental ATM Management Objects (CISCO-IETF-ATM2-PVCTRAP-MIB.my) Interfaces MIB (IF-MIB.my)
Ethernet over MPLS: VLAN mode Port mode	CISCO-ETHERLIKE-CAPABILITIES.my Ethernet MIB (ETHERLIKE-MIB.my) Interfaces MIB (IF-MIB.my) MPLS LDP MIB (MPLS-LDP-MIB.my)
Frame Relay over MPLS: DLCI-to-DLCI connections Port-to-port connections	Cisco Frame Relay MIB (CISCO-FRAME-RELAY-MIB.my) Interfaces MIB (IF-MIB.my) MPLS LDP MIB (MPLS-LDP-MIB.my)
HDLC over MPLS	MPLS LDP MIB (MPLS-LDP-MIB.my)
PPP over MPLS	Interface MIB (IF-MIB.my)

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at:

<http://tools.cisco.com/go/mibs>

NSF and SSO—L2VPN

L2VPN NSF improves the availability of a service provider's network that uses AToM to provide Layer 2 VPN services to its customers. High availability (HA) provides the ability to detect failures and manage them with minimal disruption to the service being provided. L2VPN NSF is achieved by SSO and NSF mechanisms. A standby RP provides control-plane redundancy. The control plane state and data plane provisioning information for the attachment circuits (ACs) and AToM pseudowires (PWs) are checkpointed to the standby RP to provide NSF for AToM L2VPNs.

Checkpointing AToM Information

Checkpointing is a function that copies state information from the active RP to the backup RP, thereby ensuring that the backup RP has the latest information. If the active RP fails, the backup RP can take over.

For the L2VPN NSF feature, the checkpointing function copies the active RP's information bindings to the backup RP. The active RP sends updates to the backup RP when information is modified.

To display checkpointing data, issue the **show acircuit checkpoint** command on the active and backup RPs. The active and backup RPs have identical copies of the information.

Checkpointing Troubleshooting Tips

To help troubleshoot checkpointing errors, enter the following commands:

- **debug acircuit checkpoint** command—To enable checkpointing debug messages for ACs.
- **debug mpls l2transport checkpoint** command—To enable checkpointing debug messages for AToM.
- **show acircuit checkpoint** command—To display the AC checkpoint information.
- **show mpls l2transport checkpoint** command—To display if checkpointing is allowed, the quantity of AToM VCs that were bulk-synced (on the active RP), and the quantity of AToM VCs that have checkpoint data (on the standby RP).
- **show mpls l2transport vc detail** command—To display details of VC checkpointed information.

The NSF/SSO - L2VPN feature is described in the following topics:

- [Prerequisites for NSF/SSO - L2VPN, page 20-7](#)
- [Restrictions for NSF/SSO - L2VPN, page 20-8](#)
- [Configuring NSF/SSO - L2VPN, page 20-8](#)
- [Configuration Examples of NSF/SSO—Layer 2 VPN, page 20-9](#)

Prerequisites for NSF/SSO - L2VPN

This section lists the following prerequisites for the feature:

- [Neighbor Routers in the MPLS HA Environment](#)
- [Stateful Switchover](#)
- [Nonstop Forwarding for Routing Protocols](#)

Neighbor Routers in the MPLS HA Environment

Cisco 10000 routers must be used as the neighboring device.

Stateful Switchover

For information on this topic, see the *Stateful Switchover* section in the *NSF/SSO: Any Transport over MPLS and Graceful Restart* document at:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsatomha.html#wp1098167

Nonstop Forwarding for Routing Protocols

For information on this topic, see the *Nonstop Forwarding for Routing Protocols* section in the *NSF/SSO: Any Transport over MPLS and Graceful Restart* document at:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsatomha.html#wp1098561

Restrictions for NSF/SSO - L2VPN

For information on this topic, see the *Restrictions for AToM NSF* section in the *NSF/SSO: Any Transport over MPLS and Graceful Restart* document at:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsatomha.html#wp1068923

Configuring NSF/SSO - L2VPN

For information on this topic, see the *How to Configure AToM NSF* section in the *NSF/SSO: Any Transport over MPLS and Graceful Restart* document at:

http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsatomha.html#wp1112888

Configuration Examples of NSF/SSO—Layer 2 VPN

[Example 20-1](#) illustrates how to configure AToM NSF on two PE routers:

Example 20-1 Ethernet to VLAN Interworking with AToM NSF

PE1	PE2
<pre> ip cef ! redundancy mode sso ! mpls ldp graceful-restart mpls ip mpls label protocol ldp mpls ldp router-id Loopback0 force mpls ldp advertise-tags ! pseudowire-class atom-eth encapsulation mpls interworking ethernet ! interface Loopback0 ip address 10.8.8.8 255.255.255.255 ! interface FastEthernet1/1/0 xconnect 10.9.9.9 123 encap mpls pw-class atom_eth interface POS6/1/0 ip address 10.1.1.1 255.255.255.0 mpls ip mpls label protocol ldp clock source internal crc 32 ! interface Loopback0 ip address 10.8.8.8 255.255.255.255 no shutdown ! router ospf 10 nsf ietf network 10.8.8.8 0.0.0.0 area 0 network 19.1.1.1 0.0.0.0 area 0 </pre>	<pre> ip cef ! redundancy mode sso ! mpls ldp graceful-restart mpls ip mpls label protocol ldp mpls ldp router-id Loopback0 force mpls ldp advertise-tags ! pseudowire-class atom-eth encapsulation mpls interworking eth ! interface Loopback0 ip address 10.9.9.9 255.255.255.255 ! interface FastEthernet3/0/0 ip route-cache cef ! interface FastEthernet3/0/0.3 encapsulation dot1Q 10 xconnect 10.8.8.8 123 encap mpls pw-class atom_eth interface POS1/0/0 ip address 10.1.1.2 255.255.255.0 mpls ip mpls label protocol ldp clock source internal crc 32 ! interface Loopback0 ip address 10.9.9.9 255.255.255.255 ! router ospf 10 nsf ietf network 10.9.9.9 0.0.0.0 area 0 network 10.1.1.2 0.0.0.0 area 0 </pre>



Note

NSF must be enabled for routing protocols. You can use either the **cisco** or **ietf** option. [Example 20-1](#) has the **ietf** option because it is a standard option, whereas **cisco** is proprietary option.

L2VPN Local Switching—HDLC/PPP

The L2VPN Local Switching - HDLC/PPP feature enables service providers to support different encapsulations over HDLC local switched circuits that function as back-to-back circuits. The provisioned HDLC Local Switched circuits can also be backed by using PWRED.

Prerequisites of L2VPN Local Switching—HDLC/PPP

In Cisco IOS Release 12.2(33)SB, the L2VPN Local Switching - HDLC/PPP, you must ensure that interfaces must be HDLC encapsulated on the PE router. The CE routers can choose any HDLC-based encapsulation, including Frame Relay and PPP.

Restrictions of L2VPN Local Switching—HDLC/PPP

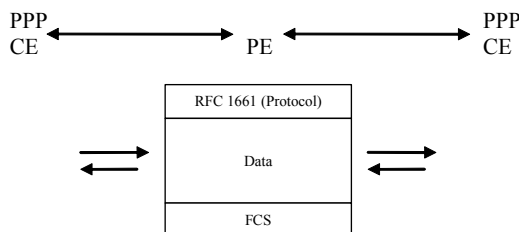
In Cisco IOS Release 12.2(33)SB, the L2VPN Local Switching - HDLC/PPP feature has the following restrictions:

- On the PE HDLC interface, the IP address cannot be configured because it conflicts with the **connect** command.
- Interworking is not supported on HDLC/PPP interfaces.
- Only same-speed interfaces should be connected, to avoid arbitrary packet drops due to a higher speed interface overrunning a lower speed one.
- For some HDLC/PPP applications which are sensitive to time delay, the PE may introduce some network delay, enough to prevent the HDLC/PPP link from coming up because of a protocol timeout (an ISDN Q921 link).

PPP Like-to-Like Local Switching

Some applications, such as transport of compressed voice between the two CEs, require a setup of an end-to-end PPP session between two CE routers that are connected to the same PE router. In such cases, HDLC pass-through mechanism is proposed and the interworking scenario is simplified to PPP transport for like-to-like services. PPP local switching functionality on the PE router provides simple HDLC connectivity between two end-users found on different CE routers as shown in [Figure 20-1](#).

Figure 20-1 PPP Local Switching



The interfaces are HDLC encapsulated on the PE router. The CE routers may use PPP-based encapsulation.

Frames manipulated by the PE router preserve the PPP header as described in RFC-1661.

HDLC Like-to-Like Local Switching

Like PPP, HDLC sessions can be forwarded between two CE routers connected to the same PE router. The microcode implements a HDLC pass-through mechanism for the HDLC traffic. As the service provided is equivalent to a back-to-back serial connection between the two CE routers, the connection should be between same-speed interfaces with the matched Maximum Transmission Unit (MTU) configuration. There are no QoS requirements on the PE router since one interface cannot overrun another.

The interfaces are HDLC encapsulated on the PE router. CE routers may use any HDLC-based encapsulation, including Frame Relay.

Configuration Tasks and Examples

You can configure the L2VPN Local Switching - HDLC/PPP feature on a PE router using the following steps:

1. **config t**
2. **interface serial** slot/subslot/port:channel-id
3. **encapsulation hdlc**
4. **interface serial** slot/subslot/port:channel-id
5. **encapsulation hdlc**
6. **connect** connection-name interface interface

The following example shows you how to configure the L2VPN Local Switching - HDLC/PPP feature on the PE router:

```
config t
interface serial 3/0/20:0
 encapsulation hdlc
interface serial 4/0/11:9
 encapsulation hdlc
connect hdlcls serial3/0/20:0 serial4/0/11:9
```



Note

Because the default encapsulation of a serial interface is HDLC, the **encapsulation** command is optional. However, when you configure the CE router, you must specify the **encapsulation** command because of the difference in configuration.

You can configure PPP on the CE router using the following steps:

1. **config t**
2. **interface serial** slot/subslot/port:channel-id
3. **encapsulation ppp**

You can configure HDLC on the CE router using the following steps:

1. **config t**
2. **interface serial** slot/subslot/port:channel-id
3. **encapsulation hdlc**

Configuration Tasks for L2VPN

To configure L2VPN, you have to configure the following L2VPN features:

- [Setting Up the Pseudowire—AToM Circuit, page 20-12](#)
- [Configuring ATM AAL5 SDU Support over MPLS, page 20-14](#)
- [Configuring ATM-to-ATM PVC Local Switching, page 20-14](#)
- [Configuring OAM Cell Emulation for ATM AAL5 SDU Support over MPLS, page 20-15](#)
- [Configuring Ethernet over MPLS, page 20-19](#)
- [IEEE 802.1Q Tunneling for AToM—QinQ, page 20-22](#)
- [Remote Ethernet Port Shutdown, page 20-25](#)
- [Configuring Frame Relay over MPLS, page 20-28](#)
- [Configuring Frame Relay-to-Frame Relay Local Switching, page 20-31](#)
- [Configuring HDLC and PPP over MPLS, page 20-36](#)
- [Estimating the Size of Packets Traveling Through the Core Network, page 20-37](#)
- [Setting Experimental Bits with AToM, page 20-38](#)
- [Configuring QoS Features, page 20-40](#)

Setting Up the Pseudowire—AToM Circuit

The successful transmission of the Layer 2 frames between PE routers is due to the configuration of a connection called a pseudowire between the routers. You specify the following information on *each* PE router:

- The type of Layer 2 data to be transported across the pseudowire, such as Ethernet, Frame Relay, or ATM
- The IP address of the loopback interface of the peer PE router, which enables the PE routers to communicate
- A unique combination of peer PE IP address and VC ID that identifies the pseudowire

To set up a pseudowire connection or AToM circuit between two PE routers, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# pseudowire-class <i>name</i>	(Optional) Establishes a pseudowire class with a name that you specify and specifies the tunneling encapsulation. It is not necessary to specify a pseudowire class if you specify the tunneling method as part of the xconnect command. The pseudowire-class configuration group specifies the characteristics of the tunneling mechanism, including: <ul style="list-style-type: none"> • Encapsulation type • Control protocol • Payload-specific options
Step 2	Router(config)# interface <i>interface-type interface-number</i>	Defines the interface or subinterface on the PE router.
Step 3	Router(config-if)# encapsulation <i>encapsulation-type</i>	Specifies the encapsulation type for the interface, such as dot1q.
Step 4	Router(config-if)# xconnect <i>peer-router-id vcid encapsulation mpls</i>	Makes a connection to the peer PE router by specifying the LDP router ID of the peer PE router. Identifies a unique identifier that is shared between the two PE routers. The <i>vcid</i> is a 32-bit identifier. Note The combination of the peer-router-id and the VC ID must be a unique combination on the router. Two circuits cannot use the same combination of peer-router-id and VC ID. Specifies the tunneling method used to encapsulate data in the pseudowire. For AToM, the tunneling method used to encapsulate data is mpls .

[Example 20-2](#) shows a sample configuration for the ATM AAL5 SDU over MPLS transport. The PVC on 0/100 is configured for AAL5 transport.

Example 20-2 ATM AAL5 SDU Support over MPLS

```
interface ATM4/0
  pvc 0/100 l2transport
    encapsulation aal5
    xconnect 13.13.13.13 100 encapsulation mpls
```

Configuring ATM AAL5 SDU Support over MPLS

ATM AAL5 SDU support over MPLS encapsulates ATM AAL5 service data units (SDUs) in MPLS packets and forwards them across the MPLS network. Each ATM AAL5 SDU is transported as one packet.

To configure ATM AAL5 SDU support over MPLS, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface type slot/port	Specifies the interface by type, slot, and port number, and enters interface configuration mode.
Step 2	Router(config-if)# pvc [name] vpi/vci l2transport	Creates or assigns a name to an ATM PVC. The l2transport keyword indicates that the PVC is a switched PVC instead of a terminated PVC. Enters L2transport VC configuration mode.
Step 3	Router(config-if-atm-l2trans-pvc)# encapsulation aal5	Specifies ATM AAL5 encapsulation for the PVC. Make sure you specify the same encapsulation type on the PE and CE routers.
Step 4	Router(config-if-atm-l2trans-pvc)# xconnect peer-router-id vcid encapsulation mpls	Binds the attachment circuit to a pseudowire VC.

[Example 20-3](#) shows how to enable ATM AAL5 SDU support over MPLS on an ATM PVC.

Example 20-3 ATM AAL5 SDU Support over MPLS on an ATM PVC

```
interface atm1/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 13.13.13.13 100 encapsulation mpls
```

Verifying ATM AAL5 SDU Support over MPLS

To verify that ATM AAL5 SDU support over MPLS is configured on a PVC, issue the **show mpls l2transport vc** command. [Example 20-4](#) shows sample output for this command.

Example 20-4 show mpls l2transport vc Command Output

```
Router# show mpls l2transport vc

Local intf   Local circuit   Dest address   VC ID   Status
-----
ATM1/0      ATM AAL5 1/100  4.4.4.4       100     UP
```

Configuring ATM-to-ATM PVC Local Switching

The following ATM line cards are supported for Cisco 10000 series routers:

- 4-port OC-3/STM-1
- 8-port E3/DS3

- 1-port OC-12

To configure ATM-to-ATM PVC local switching, enter the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface atm slot/port	Specifies an ATM interface and enters interface configuration mode.
Step 2	Router(config-if)# pvc vpi/vci l2transport	Assigns a virtual path identifier (VPI) and virtual channel identifier (VCI). The l2transport keyword indicates that the permanent virtual circuit (PVC) is a switched PVC instead of a terminated PVC.
Step 3	Router(cfg-if-atm-l2trans-pvc)# encapsulation layer-type	Specifies the encapsulation type for the PVCs, AAL5 is the only layer type supported. Repeat Steps 1, 2, and 3 for another ATM PVC on the same router.
Step 4	Router(config)# connect connection-name interface pvc interface pvc	Creates a local connection between the two specified PVCs.

[Example 20-5](#) shows how to enable ATM AAL5 SDU mode Layer 2 local switching.

Example 20-5 Enabling ATM AAL5 SDU Mode Layer 2 Local Switching

```
interface atm 1/0/0
  pvc 0/100 l2transport
  encapsulation aal5

interface atm 2/0/0
  pvc 0/50 l2transport
  encapsulation aal5

connect conn1 atm 1/0/0 0/100 atm 2/0/0 0/50
```

Configuring OAM Cell Emulation for ATM AAL5 SDU Support over MPLS

If a PE router does not support the transport of Operation, Administration, and Maintenance (OAM) cells across an LSP, you can use OAM cell emulation to locally terminate or loop back the OAM cells. You configure OAM cell emulation on both PE routers, which emulates a VC by forming two unidirectional LSPs. You use the **oam-ac emulation-enable** and **oam-pvc manage** commands on both PE routers to enable OAM cell emulation.

After you enable OAM cell emulation on a router, you can configure and manage the ATM VC in the same manner as you would a terminated VC. A VC that is configured with OAM cell emulation can send loopback cells at configured intervals toward the local CE router.

The endpoint can be either of the following:

- End-to-end loopback, which sends OAM cells to the local CE router.
- Segment loopback, which responds to OAM cells to a device along the path between the PE and CE routers.

The OAM cells include the following:

- Alarm indication signal (AIS)
- Remote defect indication (RDI)

These cells identify and report defects along a VC. When a physical link or interface failure occurs, intermediate nodes insert OAM AIS cells into all the downstream devices affected by the failure. When a router receives an AIS cell, it marks the ATM VC down and sends an RDI cell to let the remote end know about the failure.



Note

For AAL5 SDU support over MPLS, you can configure the **oam-pvc manage** command only after you issue the **oam-ac emulation-enable** command.

You can configure OAM cell emulation for ATM AAL5 SDU support over MPLS in the following ways:

- [Configuring OAM Cell Emulation for ATM AAL5 SDU Support over MPLS on PVCs, page 20-16](#)
- [Configuring OAM Cell Emulation for ATM AAL5 SDU Support over MPLS in VC Class Configuration Mode, page 20-18](#)

Configuring OAM Cell Emulation for ATM AAL5 SDU Support over MPLS on PVCs

To configure OAM cell emulation for ATM AAL5 SDU support over MPLS on a PVC, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface <i>type slot/port</i>	Specifies the interface by type, slot, and port number, and enters interface configuration mode.
Step 2	Router(config-if)# pvc [<i>name</i>] <i>vpi/vci</i> l2transport	Creates or assigns a name to an ATM PVC. The l2transport keyword indicates that the PVC is a switched PVC instead of a terminated PVC. Enters L2 Transport VC configuration mode.
Step 3	Router(config-if-atm-l2trans-pvc)# encapsulation aal5	Specifies ATM AAL5 encapsulation for the PVC. Make sure you specify the same encapsulation type on the PE and CE routers.
Step 4	Router(config-if-atm-l2trans-pvc)# xconnect <i>peer-router-id vcid</i> encapsulation mpls	Binds the attachment circuit to a pseudowire VC.
Step 5	Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable [<i>ais-rate</i>]	Enables OAM cell emulation for AAL5 over MPLS. The <i>ais-rate</i> variable lets you specify the rate at which AIS cells are sent. The range is 0 to 60 seconds. The default is 1 second, which means that one AIS cell is sent every second.
Step 6	Router(config-if-atm-l2trans-pvc)# oam-pvc manage [<i>frequency</i>]	Enables the PVC to generate end-to-end OAM loopback cells that verify connectivity on the virtual circuit. The optional <i>frequency</i> variable is the interval between transmission of loopback cells and ranges from 0 to 600 seconds. The default value is 10 seconds.

Example 20-6 shows how to enable OAM cell emulation on an ATM PVC.

Example 20-6 OAM Cell Emulation on an ATM PVC

```
interface ATM 1/0/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 13.13.13.13 100 encapsulation mpls
oam-ac emulation-enable
oam-pvc manage
```

Example 20-7 shows how to set the rate at which an AIS cell is sent to every 30 seconds.

Example 20-7 Setting the AIS Send Rate in OAM Cell Emulation on an ATM PVC

```
interface ATM 1/0/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 13.13.13.13 100 encapsulation mpls
oam-ac emulation-enable 30
oam-pvc manage
```

Verifying OAM Cell Emulation on an ATM PVC

In Example 20-8, the **show atm pvc** command shows that OAM cell emulation is enabled on the ATM PVC.

Example 20-8 show atm pvc Command Output

```
Router# show atm pvc 5/500

ATM4/1/0.200: VCD: 6, VPI: 5, VCI: 500
UBR, PeakRate: 1
AAL5-LLC/SNAP, etype:0x0, Flags: 0x34000C20, VCmode: 0x0
OAM Cell Emulation: enabled, F5 End2end AIS Xmit frequency: 1 second(s)
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state: Not ManagedVerified
ILMI VC state: Not Managed
InPkts: 564, OutPkts: 560, InBytes: 19792, OutBytes: 19680
InPRoc: 0, OutPRoc: 0
InFast: 4, OutFast: 0, InAS: 560, OutAS: 560
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0
Out CLP=1 Pkts: 0
OAM cells received: 26
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 26
OAM cells sent: 77
F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutAIS: 77, F5 OutRDI: 0
OAM cell drops: 0
Status: UP
```

Configuring OAM Cell Emulation for ATM AAL5 SDU Support over MPLS in VC Class Configuration Mode

The following steps explain how to configure OAM cell emulation as part of a VC class. You can then apply the VC class to an interface, a subinterface, or a VC. When you configure OAM cell emulation in VC class configuration mode and then apply the VC class to an interface, the settings in the VC class apply to all the VCs on the interface, unless you specify a different OAM cell emulation value at a lower level, such as the subinterface or VC level.

For example, you can create a VC class that specifies OAM cell emulation and sets the rate of AIS cells to every 30 seconds. You can apply the VC class to an interface. Then, for one PVC, you can enable OAM cell emulation and set the rate of AIS cells to every 15 seconds. All the PVCs on the interface use the cell rate of 30 seconds, except for the one PVC that was set to 15 seconds.

To enable OAM cell emulation as part of a VC class and apply it to an interface, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# vc-class atm <i>name</i>	Creates a VC class and enters VC class configuration mode.
Step 2	Router(config-vc-class)# encapsulation <i>layer-type</i>	Configures the ATM adaptation layer (AAL) and encapsulation type.
Step 3	Router(config-vc-class)# oam-ac emulation-enable [<i>ais-rate</i>]	Enables OAM cell emulation for AAL5 over MPLS. The <i>ais-rate</i> variable lets you specify the rate at which AIS cells are sent. The range is 0 to 60 seconds. The default is 1 second, which means that one AIS cell is sent every second.
Step 4	Router(config-vc-class)# oam-pvc manage [<i>frequency</i>]	Enables the PVC to generate end-to-end OAM loopback cells that verify connectivity on the virtual circuit. The optional <i>frequency</i> variable is the interval between transmission of loopback cells and ranges from 0 to 600 seconds. The default value is 10 seconds.
Step 5	Router(config-vc-class)# exit	Returns to global configuration mode.
Step 6	Router(config)# interface <i>type slot/port</i>	Specifies the interface by type, slot, and port number, and enters interface configuration mode.
Step 7	Router(config-if)# class-int <i>vc-class-name</i>	Applies a VC class to the ATM main interface or subinterface. Note You can also apply a VC class to a PVC.
Step 8	Router(config-if)# pvc [<i>name</i>] <i>vpi/vci</i> l2transport	Creates or assigns a name to an ATM PVC. The l2transport keyword indicates that the PVC is a switched PVC instead of a terminated PVC. Enters L2 Transport VC configuration mode.
Step 9	Router(config-if-atm-l2trans-pvc)# xconnect <i>peer-router-id vcid</i> encapsulation mpls	Binds the attachment circuit to a pseudowire VC.

[Example 20-9](#) configures OAM cell emulation for ATM AAL5 SDU support over MPLS in VC class configuration mode. The VC class is then applied to an interface.

Example 20-9 OAM Cell Emulation for ATM AAL5 SDU Support over MPLS in VC Class Configuration Mode—VC Class Applied to an Interface

```
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0
class-int oamclass
pvc 1/200 l2transport
xconnect 13.13.13.13 100 encapsulation mpls
```

[Example 20-10](#) shows how to configure OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to a PVC.

Example 20-10 OAM Cell Emulation for ATM AAL5 SDU Support over MPLS in VC Class Configuration Mode—VC Class Applied to a PVC

```
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0
pvc 1/200 l2transport
class-vc oamclass
xconnect 13.13.13.13 100 encapsulation mpls
```

[Example 20-11](#) shows how to configure OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to an interface. One PVC is configured with OAM cell emulation at an AIS rate of 10. That PVC uses the AIS rate of 10 instead of 30.

Example 20-11 OAM Cell Emulation for ATM AAL5 SDU Support over MPLS in VC Class Configuration Mode—VC Class Applied to an Interface

```
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0
class-int oamclass
pvc 1/200 l2transport
oam-ac emulation-enable 10
xconnect 13.13.13.13 100 encapsulation mpls
```

Configuring Ethernet over MPLS

Ethernet over MPLS works by encapsulating Ethernet protocol data units (PDUs) in MPLS packets and forwarding them across the MPLS network. Each PDU is transported as a single packet. Several methods exist for configuring Ethernet over MPLS:

- **VLAN mode**—Transports Ethernet traffic from a source 802.1Q VLAN to a destination 802.1Q VLAN over a core MPLS network.

- Port mode—Allows a frame coming into an interface to be packed into an MPLS packet and transported over the MPLS backbone to an egress interface. The entire Ethernet frame is transported without the preamble or FCS as a single packet.
- VLAN ID Rewrite—Enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel.

You can configure Ethernet over MPLS in the following ways:

- [Configuring Ethernet over MPLS in VLAN Mode, page 20-20](#)
- [Configuring Ethernet over MPLS in Port Mode, page 20-21](#)
- [Configuring Ethernet over MPLS with VLAN ID Rewrite, page 20-27](#)

Ethernet over MPLS Restrictions

The following restrictions pertain to the Ethernet over MPLS transport:

- Packet format: Ethernet over MPLS supports VLAN packets that conform to the IEEE 802.1Q standard. The 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames. The Inter-Switch Link (ISL) protocol is not supported between the PE and customer edge (CE) routers.
- When the first Ethernet over MPLS in VLAN mode circuit is configured, the controller (the entire port) is automatically placed in promiscuous mode. The promiscuous mode is removed only when the last Ethernet over MPLS in VLAN mode circuit associated with that controller is removed.
- The ATOM control word is supported. However, if the peer PE router does not support a control word, the control word is disabled. This negotiation is done by LDP label binding.
- Ethernet packets with hardware-level cyclic redundancy check (CRC) errors, framing errors, and runt packets are discarded on input.

Configuring Ethernet over MPLS in VLAN Mode

A virtual LAN (VLAN) is a switched network that is logically segmented by functions, project teams, or applications regardless of the physical location of users. Ethernet over MPLS allows you to connect two VLAN networks that are in different locations. You configure the PE routers at each end of the MPLS backbone and add a point-to-point virtual circuit (VC). Only the two PE routers at the ingress and egress points of the MPLS backbone know about the VCs dedicated to transporting Layer 2 VLAN traffic. All other routers do not have table entries for those VCs.

For Ethernet over MPLS in VLAN mode, it is possible for VPN circuits to coexist with pseudowire circuits. Because the port is in promiscuous mode, the frames are filtered by the VLAN ID.



Note

You must configure Ethernet over MPLS in VLAN mode on the subinterfaces. However, you cannot configure Ethernet over MPLS (VLAN mode) on a Q-in-Q subinterface.

To configure Ethernet over MPLS in VLAN mode, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface gigabitethernet <i>slot/interface.subinterface</i>	Specifies the Gigabit Ethernet subinterface and enters subinterface configuration mode. Make sure the subinterface on the adjoining CE router is on the same VLAN as this PE router.
Step 2	Router(config-subif)# encapsulation dot1q <i>vlan-id</i>	Enables the subinterface to accept 802.1Q VLAN packets. The subinterfaces between the CE and PE routers that are running Ethernet over MPLS must be in the same subnet. All other subinterfaces and backbone routers do not need to be on the same subnet.
Step 3	Router(config-subif)# xconnect <i>peer-router-id vcid</i> encapsulation mpls	Binds the attachment circuit to a pseudowire VC. The syntax for this command is the same as for all other Layer 2 transports.

Configuring Ethernet over MPLS in Port Mode

Port mode allows a frame coming into an interface to be packed into an MPLS packet and transported over the MPLS backbone to an egress interface. The entire Ethernet frame without the preamble or FCS is transported as one packet. To configure port mode, use the **xconnect** command in main interface mode and specify the destination address and the VC ID. The syntax and semantics of the **xconnect** command are the same as for all other transport types. Each interface is associated with one unique pseudowire VC label.

When configuring Ethernet over MPLS in port mode, use the following guidelines:

- The pseudowire VC type is set to Ethernet.
- Port mode and Ethernet VLAN mode are mutually exclusive. If you enable a main interface for port-to-port transport, you cannot also enter commands on a subinterface.

To configure Ethernet over MPLS in port mode, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface gigabitethernet <i>slot/interface</i>	Specifies the Gigabit Ethernet interface and enters interface configuration mode. Make sure the interface on the adjoining CE router is on the same VLAN as this PE router.
Step 2	Router(config-if)# xconnect <i>peer-router-id vcid</i> encapsulation mpls	Binds the attachment circuit to a pseudowire VC. The syntax for this command is the same as for all other Layer 2 transports.

[Example 20-12](#) shows how to configure VC 123 in Ethernet port mode:

Example 20-12 Ethernet over MPLS in Port Mode

```
pseudowire-class ethernet-port
  encapsulation mpls

interface gigabitethernet1/0
  xconnect 10.0.0.1 123 pw-class ethernet-port
```



Note

Depending on the interface type, you can also use the **interface fastethernet** command.

Verifying Ethernet over MPLS in VLAN Mode and Port Mode

To determine if a VC is set up in VLAN mode or port mode, issue the **show mpls l2transport vc** command.

[Example 20-13](#) shows two VCs set up for Ethernet over MPLS:

- VC 2 is set up in Ethernet VLAN mode.
- VC 8 is set up in Ethernet port mode.

Example 20-13 show mpls l2transport vc Command Output

```
Router# show mpls l2transport vc
```

Local intf	Local circuit	Dest address	VC ID	Status
Gi4/0.1	Eth VLAN 2	11.1.1.1	2	UP
Gi8/0/1	Ethernet	11.1.1.1	8	UP

If you issue the **show mpls l2transport vc detail** command, the output is similar, as shown in [Example 20-14](#).

Example 20-14 show mpls l2transport vc detail Command Output

```
Router# show mpls l2transport vc detail
```

```
Local interface: Gi4/0.1 up, line protocol up, Eth VLAN 2 up
Destination address: 11.1.1.1, VC ID: 2, VC status: up
```

```
...
```

```
Local interface: Gi8/0/1 up, line protocol up, Ethernet up
Destination address: 11.1.1.1, VC ID: 8, VC status: up
```

IEEE 802.1Q Tunneling for AToM—QinQ

The IEEE 802.1Q Tunneling (QinQ) for AToM feature is described in the following topics:

- [Prerequisites for IEEE 802.1Q Tunneling \(QinQ\) for AToM, page 20-23](#)
- [Restrictions for IEEE 802.1Q Tunneling \(QinQ\) for AToM, page 20-23](#)
- [Ethernet VLAN Q-in-Q AToM, page 20-23](#)
- [Configuration Examples, page 20-25](#)
- [Verifying QinQ AToM, page 20-25](#)

Prerequisites for IEEE 802.1Q Tunneling (QinQ) for AToM

In Cisco IOS software Release 12.2(33)SB, the QinQ (short for 802.1Q-in-802.1Q) tunneling and tag rewrite feature is supported on the following Cisco 10000 series engines and line cards:

- PRE-2, PRE-3, and PRE-4 engines
- 8-port Fast Ethernet line card (ESR-HH-8FE-TX)
- 2-port half-height Gigabit Ethernet line card (ESR-HH-1GE)
- 1-port full-height Gigabit Ethernet line card (ESR-1GE)
- SPA line cards

Restrictions for IEEE 802.1Q Tunneling (QinQ) for AToM

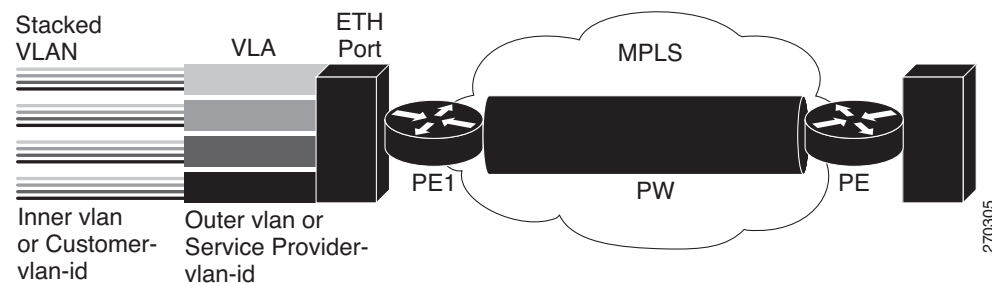
In Cisco IOS Release 12.2(33)SB, the QinQ tunneling and tag rewrite feature has the following restrictions:

- Up to a maximum of 447 outer-VLAN IDs and up to 4095 inner VLAN IDs can be supported for the Ethernet QinQ over AToM feature.
- Only Unambiguous VLAN tagged Ethernet QinQ interfaces are supported in this release. i.e. The Ethernet VLAN QinQ rewrite of both VLAN Tags capability is supported only on ethernet sub-interfaces with a QinQ encapsulation and explicit pair of VLAN IDs defined.

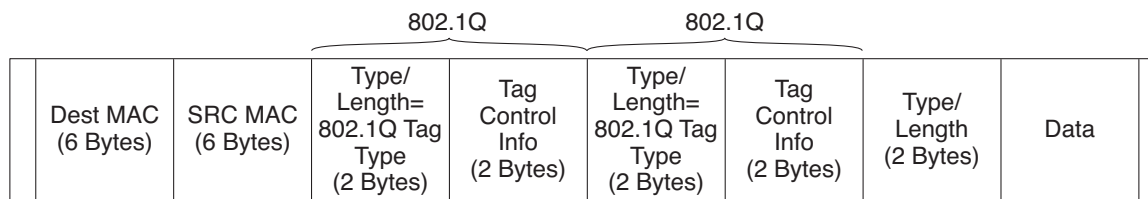
Ethernet VLAN Q-in-Q AToM

In Metro Ethernet deployment, in which CE routers and PE routers are connected through an Ethernet switched access network, packets that arrive at PE routers can contain up to two IEEE 802.1q VLAN tags (one inner VLAN tag which identifies the customer; and another outer VLAN tag which denotes the customer's service provider). This technique of allowing multiple VLAN tagging on the same Ethernet packet and creating a stack of VLAN IDs is known as QinQ (short for 802.1Q-in-802.1Q). [Figure 20-2](#) shows how different edge devices can do L2 switching on the different levels of the VLAN stack.

Figure 20-2 Ethernet VLAN QinQ



When the outer VLAN tag is the service-delimiting VLAN tag, QinQ packets are processed similar to the ones with one VLAN tag (case previously named Ethernet VLAN Q-in-Q modified, which is already supported in the 12.2(31) SB release). However, when a customer must use a combination of the outer and inner VLAN tags to delimit service for customers, the edge device should be able to choose a unique pseudowire based on a combination of the inner and outer VLAN IDs on the packet shown in [Figure 20-3](#). The customer may want to be able to rewrite both the inner and the outer VLAN IDs on the traffic egress side.

Figure 20-3 Ethernet VLAN QinQ Header

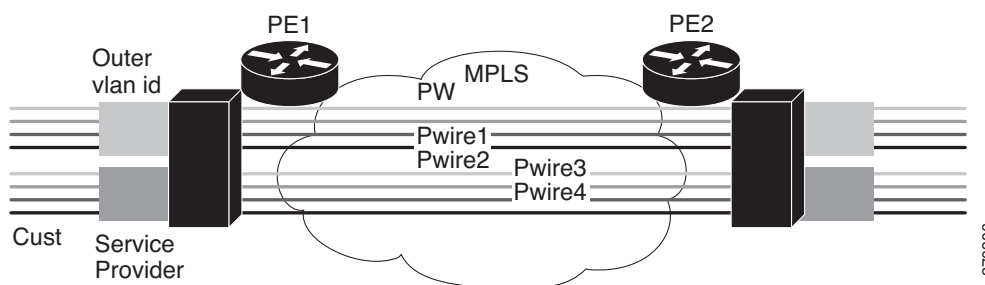
270307

The IEEE 802.1Q Tunneling (QinQ) for AToM can be further explained as follows:

- [QinQ Tunneling Based on Inner and Outer VLAN Tags, page 20-24](#)
- [Rewriting Inner and Outer VLAN Tags on QinQ Frames, page 20-24](#)

QinQ Tunneling Based on Inner and Outer VLAN Tags

When handling incoming QinQ Ethernet traffic, the Cisco 10000 series edge router allows a customer to choose a unique pseudowire endpoint to switch the traffic based on the combination of inner and outer VLAN IDs. For example, [Figure 20-4](#) shows how a unique pseudowire is selected depending upon the combination of inner (customer edge) and outer (service provider) VLAN IDs. Thus, traffic for different customers can be kept separate.

Figure 20-4 QinQ Connection

270306

Rewriting Inner and Outer VLAN Tags on QinQ Frames

When managing incoming AToM Ethernet QinQ traffic, the Cisco 10000 edge router:

1. Strips off the MPLS labels.
2. Allows the customer to rewrite both the inner and outer VLAN IDs before sending the packets to the egress QinQ interface. Note this capability is provided only for AToM like-to-like Ethernet QinQ traffic.

Support for these features is added in Cisco IOS Release 12.2(33). The QinQ AToM feature is a like-to-like interworking case over AToM. This feature requires changes to the microcode to allow it to overwrite two layers of VLAN tags on Ethernet QinQ traffic, transported across AToM pseudowires.

- On the ingress side—The packets preserve their L2 header with the two VLAN tags, and it is sent across the pseudowire with VC type of 4.

- On the egress side—The MPLS label is stripped, and up to two levels of VLAN tags are rewritten per the configuration.

Only Unambiguous VLAN tagged Ethernet QinQ interfaces are supported in this release. The Ethernet VLAN Q-in-Q rewrite of both VLAN Tags capability is supported only on Ethernet sub-interfaces with a QinQ encapsulation and explicit pair of VLAN IDs defined.

Configuration Examples

[Example 20-15](#) shows an unambiguous QinQ configured on GigE subinterface.

Example 20-15 Unambiguous QinQ

```
interface GigabitEthernet1/0/0.100
encapsulation dot1q 100 second-dot1q 200
xconnect 23.0.0.16 410 encapsulation mpls
```

[Example 20-16](#) shows an ambiguous QinQ configured on a GigE subinterface.

Example 20-16 Ambiguous QinQ

```
interface GigabitEthernet1/0/0.200
encapsulation dot1q 200 second-dot1q 1000-2000,3000,3500-4000
xconnect 23.0.0.16 420 encapsulation mpls
interface GigabitEthernet1/0/0.201
encapsulation dot1q 201 second-dot1q any
xconnect 23.0.0.16 430 encapsulation mpls
```



Note

Ambiguous inner VLAN IDs are not supported in this release.

Verifying QinQ ATOM

[Example 20-17](#) shows the command output of the **show mpls l2transport vc** command, which is used to verify the VC set up in EoMPLS QinQ mode.

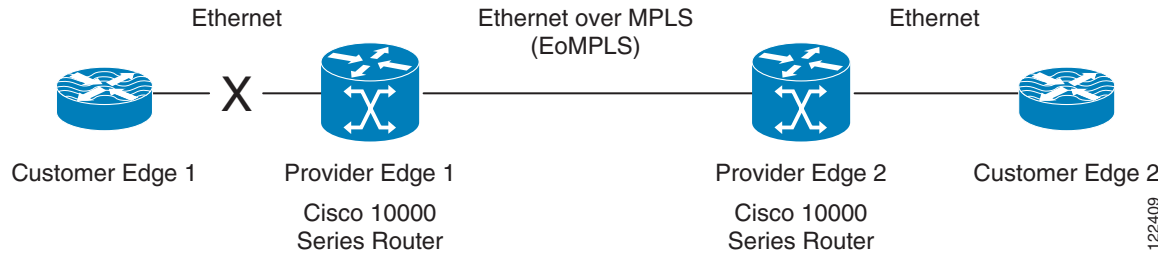
Example 20-17 show mpls l2transport vc Command Output

Local intf	Local circuit	Dest address	VC ID	Status
Gi1/0/0.1	Eth VLAN:100/200	100.1.1.2	1	UP

Remote Ethernet Port Shutdown

This Cisco IOS feature allows a service provider edge (PE) router on the local end of an Ethernet over MPLS (EoMPLS) pseudowire to detect a remote link failure and shutdown of the Ethernet port on the local customer edge (CE) router. Because the Ethernet port on the local CE router is shut down, the router does not lose data by continuously sending traffic to the failed remote link. This is beneficial if the link is configured as a static IP route.

[Figure 20-5](#) illustrates a condition in an EoMPLS wide area network (WAN) with a down Layer 2 tunnel link between a CE1 router and the PE1 router. A CE2 router on the far side of the Layer 2 tunnel, continues to forward traffic to CE1 through the L2 tunnel.

Figure 20-5 Remote Link Outage in EoMPLS Wide Area Network

In earlier releases than Cisco IOS Release 12.2(33)SB, the PE2 router did not detect a failed remote link. Traffic forwarded from CE2 to CE1 is lost until routing or spanning tree protocols detected the down remote link. If the link was configured with static routing, remote link outage can be difficult to detect by the L3 routing protocol.

With Any Transport over MPLS (AToM): Remote Ethernet Port Shutdown, the PE2 router detects the remote link failure and causes a shutdown of the local CE2 Ethernet port. When the remote L2 tunnel link is restored, the local interface is automatically restored as well. The possibility of data loss is thus diminished.

With reference to [Figure 20-5](#), a remote Ethernet shutdown sequence occurs as follows:

1. The remote link between CE1 and PE1 fails.
2. PE2 with remote Ethernet port shutdown enabled detects the remote link failure and disables the transmit laser on the line card interface connected to CE2.
3. CE2 receives an RX_LOS error alarm causing CE2 to bring down the interface.
4. PE2 maintains its interface with CE2 in an up state.
5. When the remote link and EoMPLS connection is restored, the PE2 router enables the transmit laser.
6. The CE2 router brings up its downed interface.

Restrictions for Configuring Remote Ethernet Port Shutdown

The following restrictions pertain to the Remote Ethernet Port Shutdown feature:

- For Cisco IOS Release 12.2(33) SB, this feature is implemented for port mode Ethernet over MPLS connections between Cisco 10000 series Ethernet line cards only.
- This feature is not symmetrical if the remote PE router is running an older version of image or is on another platform that does not support the EoMPLS remote Ethernet port shutdown feature and the local PE is running an image which supports this feature.

Configuring Remote Ethernet Port Shutdown

By default, the Any Transport over MPLS (AToM): Remote Ethernet Port Shutdown feature is automatically enabled when an image with this feature supported is loaded on the Cisco 10000 series router. However, to enable the Remote Ethernet Port Shutdown feature, enter the **remote link failure notification** command, as shown in [Example 20-18](#).

To disable the feature, enter the **no remote link failure notification** command ([Example 20-19](#)).

Example 20-18 Enabling Remote Ethernet Port Shutdown under the Xconnect Configuration

```
pseudowire-class eompls
```

```

encapsulation mpls
!
interface GigabitEthernet1/0/0
  xconnect 1.1.1.1 1 pw-class eompls
  remote link failure notification
!

```

Example 20-19 Disabling Remote Ethernet Port Shutdown under the Xconnect Configuration

```

pseudowire-class eompls
  encapsulation mpls
!
interface GigabitEthernet1/0/0
  xconnect 1.1.1.1 1 pw-class eompls
  no remote link failure notification
!

```

To see the operational status of all remote L2 tunnels by interface, enter **show interface** and **show ip interface brief** commands, as shown in [Example 20-20](#).

Example 20-20 Operational Status for All Remote L2 Tunnels by Interface

```

router# show interface GigabitEthernet1/0/0
GigabitEthernet1/0/0 is L2 Tunnel remote down, line protocol is up
  Hardware is Half-height Gigabit Ethernet MAC Controller, address is 0009.b68f.9b18 (bia
0009.b68f.9b18)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
  .....
  .....

router# sh ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0/0	24.3.8.1	YES	NVRAM	up	up
GigabitEthernet1/0/0	unassigned	YES	NVRAM	L2 Tunnel remote down	up
GigabitEthernet2/0/0	30.1.1.1	YES	manual	up	up

Enter **show controller** and **show controller interface** commands to see the port transceiver state, as shown in [Example 20-21](#).

Example 20-21 Port Transceiver State

```

router# show controller GigabitEthernet1/0/0
Interface GigabitEthernet1/0/0(idb 0x4FB5CA7C)
Hardware is Half-height Gigabit Ethernet MAC Controller, network connection mode is auto
network link is L2 Tunnel remote down
loopback type is none
.....

```

Configuring Ethernet over MPLS with VLAN ID Rewrite

The VLAN ID Rewrite feature enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel. The Cisco 10000 series router automatically performs VLAN ID Rewrite on the disposition PE router. There is no configuration required.

Configuring Frame Relay over MPLS

Frame Relay over MPLS encapsulates Frame Relay protocol data units (PDUs) in MPLS packets and forwards them across the MPLS network. For Frame Relay, you can set up data-link connection identifier (DLCI)-to-DLCI connections or port-to-port connections.

- With DLCI-to-DLCI connections, the PE routers manipulate the packet by removing headers, adding labels, and copying control word elements from the header to the PDU.
- With port-to-port connections, you use HDLC mode to transport the Frame Relay encapsulated packets. In HDLC mode, the entire HDLC packet is transported. Only the HDLC flags and FCS bits are removed. The contents of the packet are not used or changed, including the FECN, BECN, and DE bits.



Note Frame Relay traffic shaping is not supported with AToM-switched VCs.

You can configure Frame Relay over MPLS in the following ways:

- [Configuring Frame Relay over MPLS with DLCI-to-DLCI Connections, page 20-28](#)
- [Configuring Frame Relay over MPLS with Port-to-Port Connections, page 20-29](#)
- [Enabling Other PE Devices to Transport Frame Relay Packets, page 20-30](#)

Configuring Frame Relay over MPLS with DLCI-to-DLCI Connections

To configure Frame Relay over MPLS with DLCI-to-DLCI connections, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# frame-relay switching	Enables permanent virtual circuit (PVC) switching on a Frame Relay device.
Step 2	Router(config)# interface serial slot/port	Specifies a serial interface and enters interface configuration mode.
Step 3	Router(config-if)# encapsulation frame-relay [cisco ietf]	Specifies Frame Relay encapsulation for the interface. You can specify different types of encapsulations. You can set one interface to Cisco encapsulation and the other interface to IETF encapsulation.
Step 4	Router(config-if)# frame-relay intf-type dce	Specifies that the interface is a DCE switch. You can also specify the interface to support NNI and DTE connections.
Step 5	Router(config-if)# exit	Exits from interface configuration mode.

	Command	Purpose
Step 6	Router(config)# connect <i>connection-name</i> <i>interface dlci</i> l2transport	Defines connections between Frame Relay PVCs and enters connect submode. Using the l2transport keyword specifies that the PVC will not be a locally switched PVC, but will be tunneled over the backbone network. The <i>connection-name</i> argument is a text string that you provide. The <i>interface</i> argument is the interface on which a PVC connection is defined. The <i>dlci</i> argument is the DLCI number of the PVC that will be connected.
Step 7	Router(config-fr-pw-switching)# xconnect <i>peer-router-id vcid encapsulation mpls</i>	Creates the VC to transport the Layer 2 packets. In a DLCI-to-DLCI connection type, Frame Relay over MPLS uses the xconnect command in connect submode.

[Example 20-22](#) shows how to enable Frame Relay over MPLS with DLCI-to-DLCI connections.

Example 20-22 Frame Relay over MPLS with DLCI-to-DLCI Connections

```
frame-relay switching
interface Serial3/1
encapsulation frame-relay ietf
frame-relay intf-type dce
exit
connect fr1 Serial 5/0 1000 l2transport
xconnect 10.0.0.1 123 encapsulation mpls
```

Configuring Frame Relay over MPLS with Port-to-Port Connections

When you set up a port-to-port connection between PE routers, you use HDLC mode to transport the Frame Relay encapsulated packets. Perform this task to set up Frame Relay port-to-port connections.

To configure Frame Relay over MPLS with port-to-port connections, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface serial <i>slot/port</i>	Specifies a serial interface and enters interface configuration mode.
Step 2	Router(config-if)# encapsulation hdlc	Specifies that Frame Relay PDUs is encapsulated in HDLC packets.
Step 3	Router(config-if)# xconnect <i>peer-router-id vcid encapsulation mpls</i>	Creates the VC to transport the Layer 2 packets.

[Example 20-23](#) shows how to enable Frame Relay over MPLS with port-to-port connections.

Example 20-23 Frame Relay over MPLS With Port-to-Port Connections

```
interface serial5/0
encapsulation hdlc
xconnect 10.0.0.1 123 encapsulation mpls
```

Enabling Other PE Devices to Transport Frame Relay Packets

You can configure an interface as a data terminal equipment (DTE) device or a data circuit-terminating equipment (DCE) switch, or as a switch connected to a switch with network-to-network interface (NNI) connections. Use the following command in interface configuration mode:

frame-relay intf-type [dce | dte | nni]

The following table explains the keywords:

Keyword	Description
dce	Enables the router or access server to function as a switch connected to a router.
dte	Enables the router or access server to function as a DTE device. DTE is the default.
nni	Enables the router or access server to function as a switch connected to a switch.

Local Management Interface and Frame Relay over MPLS

Local Management Interface (LMI) is a protocol that communicates status information about permanent virtual circuits (PVCs). When a PVC is added, deleted, or changed, the LMI notifies the endpoint of the status change. LMI also provides a polling mechanism that verifies that a link is up.

LMI Process

To determine the PVC status, LMI checks that a PVC is available from the reporting device to the Frame Relay end-user device. If a PVC is available, LMI reports that the status is “Active,” which means that all interfaces, line protocols, and core segments are operational between the reporting device and the Frame Relay end-user device. If any of those components is not available, the LMI reports a status of “Inactive.”

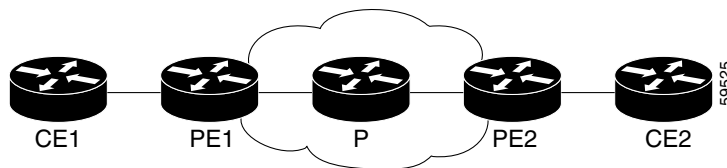


Note

Only the DCE and NNI interface types can report LMI status.

Figure 20-6 is a sample topology that illustrates how LMI works.

Figure 20-6 Sample LMI Topology



In Figure 20-6, note the following:

- CE1 and PE1 and PE2 and CE2 are Frame Relay LMI peers.
- CE1 and CE2 can be Frame Relay switches or end-user devices.
- Each Frame Relay PVC is composed of multiple segments.
- The DLCI value is local to each segment and is changed as traffic is switched from segment to segment. Two Frame Relay PVC segments exist in Figure 20-6; one is between PE1 and CE1 and the other is between PE2 and CE2.

The LMI protocol behavior depends on DLCI-to-DLCI connections versus port-to-port connections.

DLCI-to-DLCI Connections

If DLCI-to-DLCI connections are configured, LMI runs locally on the Frame Relay ports between the PE and CE devices.

- CE1 sends an active status to PE1 if the PVC for CE1 is available. If CE1 is a switch, LMI checks that the PVC is available from CE1 to the user device attached to CE1.
- PE1 sends an active status to CE1 if the following conditions are met:
 - A PVC for PE1 is available.
 - PE1 received an MPLS label from the remote PE router.
 - An MPLS tunnel label exists between PE1 and the remote PE router.

For DTE/DCE configurations, the following LMI behavior exists:

The Frame Relay device accessing the network (DTE) does not report PVC status. Only the network device (DCE) or NNI can report status. Therefore, if a problem exists on the DTE side, the DCE is not aware of the problem.

Port-to-Port Connections

If port-to-port connections are configured, the PE routers do not participate in the LMI status-checking procedures. LMI operates between the CE routers only. The CE routers must be configured as DCE-DTE or NNI-NNI.

For information about LMI, including configuration instructions, see the “Configuring the LMI” section of the *Configuring Frame Relay* document.

Configuring Frame Relay-to-Frame Relay Local Switching

Frame Relay switching is a means of switching packets based upon the data link connection identifier (DLCI), which can be looked upon as the Frame Relay equivalent of a MAC address. You perform the switching by configuring your router or access server as a Frame Relay network. There are two parts to a Frame Relay network: the Frame Relay data terminal equipment (DTE) (the router or access server) and the Frame Relay data communications equipment (DCE) switch.

Local switching allows you to switch Layer 2 data between two interfaces of the same type for example, ATM-to-ATM, or Frame-Relay-to-Frame-Relay.

For background information about Frame-Relay-to-Frame-Relay Local Switching, see the *Distributed Frame Relay Switching* feature guide.

You can switch between virtual circuits on the same port, as detailed in the [“Configuring Frame Relay Same-Port Switching” section on page 20-33](#).

The following channelized line cards are supported for the Cisco 10000 series routers:

- 1-port channelized OC-12/STM-4
- 4-port channelized OC-3/STM-1
- 6-port channelized T3
- 24-port channelized E1/T1

The following packet over SONET line cards are supported for the Cisco 10000 series routers:

- 1-port OC-12 Packet over SONET
- 1-port OC-48/STM-16 Packet over SONET
- 6-port OC-3/STM-1 Packet over SONET

The Frame Relay-to-Frame Relay Local Switching feature is described in the following topics:

- [Configuring Frame Relay for Local Switching, page 20-32](#)
- [Configuring Frame Relay Same-Port Switching, page 20-33](#)
- [Verifying Layer 2 Local Switching for Frame Relay, page 20-34](#)
- [Configuring QoS Features, page 20-34](#)

Configuring Frame Relay for Local Switching

To configure Frame Relay for local switching, enter the following commands, beginning in global configuration mode.

	Command	Purpose
Step 1	Router(config)# frame-relay switching	Enables Permanent Virtual Circuits (PVCs) switching on a Frame Relay DCE device or a Network-to-Network Interface (NNI).
Step 2	Router(config)# interface <i>type number</i>	Specifies an interface and enters interface configuration mode.
Step 3	Router(config-if)# encapsulation frame-relay [cisco ietf]	Enables Frame Relay encapsulation. <ul style="list-style-type: none"> • cisco—Cisco's own encapsulation (default) • ietf—Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to another vendor's equipment across a Frame Relay network.
Step 4	Router(config-if)# frame-relay interface-dlci <i>dlci switched</i>	(Optional) Creates a switched PVC and enters Frame Relay DLCI configuration mode. Repeat Step 1 through Step 4 for each switched PVC. If you do not create a Frame Relay PVC in this step, it is automatically created in Step 6 by the connect command.
Step 5	Router(config-fr-dlci)# exit	Exits Frame Relay DLCI configuration mode and returns to global configuration mode.
Step 6	Router(config)# connect <i>connection-name</i> <i>interface dlci interface dlci</i>	Defines a connection between Frame Relay PVCs.

[Example 20-24](#) configures Frame-Relay-to-Frame-Relay for local switching.

Example 20-24 Configuring Frame Relay-to-Frame Relay for Local Switching

```
frame-relay switching
interface serial 1/0/0.1/1:0
encapsulation frame-relay
frame-relay interface-dlci 100 switched
exit
connect connection1 serial1/0/0.1/1:0 100 serial2/0/0.1/2:0 101
```

Configuring Frame Relay Same-Port Switching

Use the following steps to configure local Frame Relay same-port switching on a single interface, beginning in global configuration mode.

	Command	Purpose
Step 1	Router(config)# frame-relay switching	Enables PVC switching on a Frame Relay DCE device or a NNI.
Step 2	Router(config)# interface <i>type number</i>	Specifies the interface and enters interface configuration mode.
Step 3	Router(config-if)# encapsulation frame-relay [cisco ietf]	Enables Frame Relay encapsulation. <ul style="list-style-type: none"> • cisco—Cisco's own encapsulation (default) • ietf—Internet Engineering Task Force (IETF) standard (RFC 1490). Use this keyword when connecting to another vendor's equipment across a Frame Relay network.
Step 4	Router(config-if)# frame-relay intf-type { dce dte nni }	(Optional) Enables support for a particular type of connection. <ul style="list-style-type: none"> • dce—data communications equipment • dte—data terminal equipment • nni—network-to-network interface
Step 5	Router(config-if)# frame-relay interface-dlci <i>dlci</i> switched	(Optional) Creates a switched PVC and enters Frame Relay DLCI configuration mode. Repeat Step 1 through Step 5 for each switched PVC. If you do not create a Frame Relay PVC in this step, it is automatically created in Step 8 by the connect command.
Step 6	Router(config-fr-dlci)# exit	Exits Frame Relay DLCI configuration mode and returns to interface configuration mode.
Step 7	Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 8	Router(config)# connect <i>connection-name</i> <i>interface dlci interface dlci</i>	Defines a connection between the two data links.

[Example 20-25](#) shows how to configure Frame Relay same-port switching.

Example 20-25 Configuring Frame Relay Same-Port Switching

```
frame-relay switching
interface serial 1/0/0.1/1:0
encapsulation frame-relay
frame-relay intf-type nni
frame-relay interface-dlci 100 switched
exit
exit
connect connection1 serial1/0 100 serial1/0 200
```

Verifying Layer 2 Local Switching for Frame Relay

To verify configuration of the Layer 2 Local Switching feature, use the **show connection frame-relay-to-frame-relay** command and the **show frame-relay pvc** command in privileged EXEC mode.

[Example 20-26](#) shows the output of the **show connection frame-relay-to-frame-relay** command, which displays the local connection between a Frame Relay interface and a Frame Relay local switching interface.

Example 20-26 show connection frame-relay-to-frame-relay Command Output

```
Router# show connection frame-relay-to-frame-relay
ID  Name                Segment 1                Segment 2                State
=====
1   fr2fr                Se3/0/0.1/1:0 100        Se3/0/0.1/2:0 200    UP
```

[Example 20-27](#) shows the output of the **show frame-relay pvc** command, which shows a switched Frame Relay PVC.

Example 20-27 show frame-relay pvc Command Output

```
Router# show frame-relay pvc 16
PVC Statistics for interface POS5/0 (Frame Relay NNI)
DLCI = 16, DLCI USAGE = SWITCHED, PVC STATUS = UP, INTERFACE = POS5/0
LOCAL PVC STATUS = UP, NNI PVC STATUS = ACTIVE
input pkts 0 output pkts 0 in bytes 0
out bytes 0 dropped pkts 100 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
out bcast pkts 0 out bcast bytes 0
switched pkts 0
Detailed packet drop counters:
no out intf 0 out intf down 100 no out PVC 0
in PVC down 0 out PVC down 0 pkt too big 0
pvc create time 00:25:32, last time pvc status changed 00:06:31
```

Configuring QoS Features

For information about configuring QoS features on the Cisco 10000 series router, see the [Cisco 10000 Series Router Quality of Service Configuration Guide](#).

[Table 20-4](#) and [Table 20-5](#) outline the level of support for modular QoS CLI (MQC) commands as they relate to Frame Relay DLCI interfaces.

The values shown in the tables are as follows:

- No—You cannot perform this policy map action
- Yes—You can perform this policy map action
- N/A (not applicable)—You can apply the policy map action but it does not have any effect on packets

Table 20-4 *Frame Relay DLCI Input Policy Map Actions*

Policy Map Actions	Frame Relay DLCI Interface
bandwidth	no
queue-limit	no
priority	no
shape	no
random-detect	no
set ip prec/dscp	N/A
set qos-group	yes
set discard class	yes
set atm-clp	N/A
set fr-de	no
set cos	no
police	yes
set mpls-exp topmost	N/A
set mpls-exp imposition	N/A

Table 20-5 *Frame Relay Output (Disposition Router) Policy Map Actions*

Policy Map Actions	Frame Relay DLCI Interface
bandwidth	yes
queue-limit	yes
priority	yes
shape	yes
random-detect	yes (discard class only)
set ip prec/dscp	N/A
set qos-group	N/A
set discard class	yes
set atm-clp	no
set fr-de	not supported
set cos	no
police	yes
set mpls-exp topmost	N/A

Configuring HDLC and PPP over MPLS

With HDLC over MPLS, the entire HDLC packet is transported. The ingress PE router removes only the HDLC flags and frame check sequence (FCS) bits. The contents of the packet are not used or changed.

With PPP over MPLS, the ingress PE router removes the flags, address, control field, and the FCS.

HDLC over MPLS is described in:

- [Restrictions for HDLC over MPLS, page 20-36](#)
- [Restrictions for PPP over MPLS, page 20-36](#)
- [Configuring HDLC over MPLS or PPP over MPLS, page 20-36](#)

Restrictions for HDLC over MPLS

The following restrictions pertain to the HDLC over MPLS feature:

- Asynchronous interfaces: Asynchronous interfaces are not supported.
- Interface configuration: You must configure HDLC over MPLS on router interfaces only. You cannot configure HDLC over MPLS on subinterfaces.

Restrictions for PPP over MPLS

The following restrictions pertain to the PPP over MPLS feature:

- Asynchronous interfaces—Are not supported. The connections between the CE and PE routers on both ends of the backbone must have similar link layer characteristics. The connections between the CE and PE routers must both be synchronous.
- Multilink PPP (MLP)—Is not supported.
- Interface configuration: You must configure PPP on router interfaces only. You cannot configure PPP on subinterfaces.

Configuring HDLC over MPLS or PPP over MPLS

To configure HDLC over MPLS or PPP over MPLS, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface serial slot/port	Specifies a serial interface and enters interface configuration mode. You must configure HDLC and PPP over MPLS on router interfaces only. You cannot configure HDLC over MPLS on subinterfaces.
Step 2	Router(config-if)# encapsulation encapsulation-type	Specifies HDLC or PPP encapsulation and enters connect submode. <i>encapsulation-type</i> can be HDLC or PPP.
Step 3	Router(config-fr-pw-switching)# xconnect peer-router-id vcid encapsulation mpls	Creates the VC to transport the Layer 2 packets.

Estimating the Size of Packets Traveling Through the Core Network

The following calculation helps you determine the size of the packets traveling through the core network. You set the maximum transmission unit (MTU) on the core-facing interfaces of the P and PE routers to accommodate packets of this size.

The MTU should be greater than or equal to the total bytes of the items in the following equation:

```
Core MTU >= (Edge MTU + Transport header + AToM header + (MPLS label stack size* MPLS label size))
```

The following sections describe the variables used in the equation.

Edge MTU

The edge MTU is the MTU for the customer-facing interfaces.

Transport Header

The transport header depends on the transport type. [Table 20-6](#) lists the specific sizes of the headers.

Table 20-6 Header Size of Packets

Transport Type	Header Size (bytes)
ATM AAL5 SDU support over MPLS	12
Ethernet over MPLS in VLAN mode	18
Ethernet over MPLS in port mode	14
Frame Relay over MPLS with DLCI-to-DLCI connections	4
HDLC over MPLS	4
PPP over MPLS	4

AToM Header

The AToM header is 4 bytes (control word). The Cisco 10000 series router adds the control word for all supported transport types by default.

MPLS Label Stack

The MPLS label stack size depends on the configuration of the core MPLS network.

- AToM uses one MPLS label to identify the AToM VCs (VC label). Therefore, the minimum MPLS label stack is 1 for directly connected AToM PE routers, which are PE routers that do not have a P router between them.
- If LDP is used in the MPLS network, the label stack size is 2 (the LDP label and the VC label).
- If a TE tunnel instead of LDP is used between PE routers in the MPLS network, the label stack size is 2 (the TE label and the VC label).
- If a TE tunnel and LDP are used in the MPLS network (for example, a TE tunnel between P routers or between P and PE routers, with LDP on the tunnel), the label stack is 3 (TE label, LDP label, VC label).
- If you use MPLS Fast Reroute in the MPLS network, you add a label to the stack. The maximum MPLS label stack in this case is 4 (FRR label, TE label, LDP label, VC label).

- If AToM is used by the customer carrier in the MPLS-VPN Carrier Supporting Carrier environment, you add a label to the stack. The maximum MPLS label stack in the provider carrier network is 5 (FRR label, TE label, LDP label, VPN label, VC label).
- If an AToM tunnel spans different service providers that exchange MPLS labels using IPv4 BGP (RFC 3107), you add a label to the stack. The maximum MPLS label stack is 5 (FRR label, TE label, BGP label, LDP label, VC label).

Other circumstances can increase the MPLS label stack size. Therefore, analyze the complete data path between the AToM tunnel endpoints and determine the maximum MPLS label stack size for your network. Then multiply the label stack size by the size of the MPLS label.

Estimating Packet Size—Example

[Example 20-28](#) shows how to estimate the size of packets. The example uses the following assumptions:

- The edge MTU is 1500 bytes.
- The transport type is Ethernet VLAN, which designates 18 bytes for the transport header.
- The AToM header is 4 bytes, because the control word is always used.
- The MPLS label stack size is 2, because LDP is used. The MPLS label size is 4 bytes.

Example 20-28 Estimating the MTU for Packets

```
Core MTU >= (Edge MTU + Transport header + AToM header + (MPLS label stack size* MPLS
label size))
1500      + 18                      + 0      + (2          * 4          ) = 1526
```

You must configure the P and PE routers in the core to accept packets of 1526 bytes. See the following section for setting the MTU size on the P and PE routers.

Changing the MTU Size on P and PE Routers

After you determine the MTU size to set on your P and PE routers, you can issue the **mtu** command on the routers to set the MTU size. The following example specifies an MTU size of 1526 bytes.

```
Router(config-if)# mtu 1526
```

Setting Experimental Bits with AToM

MPLS AToM uses the three experimental (EXP) bits in a label to determine the queue of packets. The EXP bits are set to 0 (zero) by default. [Table 20-7](#) summarizes the commands you can use to override the default values.

Table 20-7 Commands Supported to Change EXP Bits

Transport Type	Supported Commands
ATM AAL5 SDU support over MPLS	set mpls experimental
Ethernet over MPLS: Port mode	match any
Frame Relay over MPLS: DLCI-to-DLCI connections Port-to-port connections	
HDLC over MPLS	
PPP over MPLS	
Ethernet over MPLS: VLAN mode	set mpls experimental match cos

Set the experimental bits in both the VC label and the LSP tunnel label. You set the experimental bits in the VC label, because the LSP tunnel label might be removed at the penultimate router.

To set the experimental bits, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# class-map <i>class-name</i>	Specifies the user-defined name of the traffic class and enters class map configuration mode.
Step 2	For all transport types except Ethernet over MPLS in VLAN mode: Router(config-cmap)# match any For Ethernet over MPLS in VLAN mode only: Router(config-cmap)# match cos <i>cos-value</i>	Specifies that all packets are matched. <i>cos-value</i> is from 0 to 7; up to four CoS values can be specified in one match cos statement.
Step 3	Router(config-cmap)# policy-map <i>policy-name</i>	Specifies the name of the traffic policy to configure and enters policy map configuration mode.
Step 4	Router(config-pmap)# class <i>class-name</i>	Specifies the name of a predefined traffic class, which was configured with the class-map command, used to classify traffic to the traffic policy. Enters policy-map configuration mode.
Step 5	Router(config-pmap-c)# set mpls experimental <i>value</i>	Designates the value to which the MPLS bits are set if the packets match the specified policy map.
Step 6	Router(config-pmap-c)# exit	Exits policy map configuration mode.
Step 7	Router(config-pmap)# exit	Exits policy map mode.
Step 8	Router(config)# interface <i>slot/port</i>	Specifies the interface and enters interface configuration mode.
Step 9	Router(config-if)# service-policy <i>input policy-name</i>	Attaches a traffic policy to an interface.

Displaying the Traffic Policy Assigned to an Interface

To display the traffic policy attached to an interface, use the **show policy-map interface** command.

[Example 20-29](#) uses the **set mpls experimental** command with the **match any** command under a default class. This means that every packet tunneled onto a particular AToM VC carries the same MPLS experimental bit value.

Example 20-29 Setting EXP Bits Using the match any Command

```
class-map match-any default-class
  match any
policy-map atm-default-policy
  class default-class
    set mpls experimental 3
!
!
interface atm4/0
service-policy input atm-default-policy
```

[Example 20-30](#) uses the **set mpls experimental** command with the **match cos** command. This allows packets tunneled onto a particular AToM VC to carry different MPLS experimental bit values. The **match cos** command is only configurable on Ethernet VLAN subinterfaces.

Example 20-30 Setting EXP Bits Using the match cos Command

```
class-map match-any match_cos_low
  match cos 0 1 2 3
class-map match-any match_cos_high
  match cos 4 5 6 7
policy-map ether-clp-policy
  class match_cos_low
    set mpls experimental 1
  class match_cos_high
    set mpls experimental 5
!
!
interface Gi0/0.1
service-policy input ether-clp-policy
```

Configuring QoS Features

For information about configuring QoS features on the Cisco 10000 series router, see the [Cisco 10000 Series Router Quality of Service Configuration Guide](#).

[Table 20-8](#) and [Table 20-9](#) describe the policy map actions supported on various interfaces. The tables indicate the following:

- No—You cannot perform this policy map action or match criteria.
- Yes—You can perform this policy map action or match criteria.
- N/A (Not Applicable)—You can apply the policy map action or match criteria, but it does not have any effect on packets.

Table 20-8 Input (Imposition Router) Policy Map Actions

Policy Map Actions	Interface			
	ATM	Ethernet	Frame Relay	HDLC and PPP
bandwidth	no	no	no	no
queue-limit	no	no	no	no
priority	no	no	no	no
shape	no	no	no	no
random-detect	no	no	no	no
set ip prec/dscp	N/A	N/A	N/A	N/A
set qos-group	yes	yes	yes	yes
set discard class	yes	yes	yes	yes
set atm-clp	N/A	N/A	N/A	N/A
set fr-de	N/A	N/A	N/A	N/A
set cos	N/A	N/A	N/A	N/A
police	yes	yes	yes	yes
set mpls-exp topmost	N/A	N/A	N/A	N/A
set mpls-exp imposition	yes	yes	yes	yes

Table 20-9 Output (Disposition Router) Policy Map Actions

Policy Map Actions	Interface			
	ATM	Ethernet	Frame Relay	HDLC and PPP
bandwidth	yes	yes	yes	yes
queue-limit	yes	yes	yes	yes
priority	yes	yes	yes	yes
shape	yes	yes	yes	yes
random-detect	yes (discard class only)	yes (discard class only)	yes (discard class only)	yes (discard class only)
set ip prec/dscp	no	no	no	no
set qos-group	N/A	N/A	N/A	N/A
set discard class	no	no	no	no
set atm-clp	yes	no	no	no
set fr-de	no	no	no	no
set cos	no	yes	no	no
police	yes	yes	yes	yes
set mpls-exp topmost	no	no	no	no
set mpls-exp imposition	N/A	N/A	N/A	N/A

Table 20-10 and Table 20-11 describe support for class map match criteria on various interfaces. Table 20-10 describes match criteria support for inbound traffic and Table 20-11 describes support for outbound traffic.

Table 20-10 Input (Imposition Router) Class Map Match Criteria

Match Criteria	Interface			
	ATM	Ethernet	Frame Relay	HDLC and PPP
DSCP	no	no	no	no
IP precedence	no	no	no	no
MPLS EXP	no	no	no	no
IEE 802.1P bits	no	yes	no	no
Access-list	no	no	no	no
QoS group	N/A	N/A	N/A	N/A
Discard class	N/A	N/A	N/A	N/A
Input interface	yes	yes	yes	yes
Protocol	no	no	no	no
RTP	no	no	no	no
atm-clp	no	no	no	no
MAC address	no	no	no	no
Frame Relay DLCI	no	no	no	no
VLAN ID	no	no	no	no
Packet length	no	no	no	no
DE bit (Frame Relay)	no	no	no	no

Table 20-11 Output (Disposition Router) Class Map Match Criteria

Match Criteria	Interface			
	ATM	Ethernet	Frame Relay	HDLC and PPP
DSCP	no	no	no	no
IP precedence	no	no	no	no
MPLS EXP	N/A	N/A	N/A	N/A
IEEE 802.1P bits	N/A	N/A	N/A	N/A
Access-list	no	no	no	no
QoS group	yes	yes	yes	yes
Discard class	yes	yes	yes	yes
Input interface	yes	yes	yes	yes
Protocol	no	no	no	no
RTP	no	no	no	no
atm-clp	N/A	N/A	N/A	N/A
MAC address	no	no	no	no

Table 20-11 **Output (Disposition Router) Class Map Match Criteria (continued)**

Match Criteria	Interface			
	ATM	Ethernet	Frame Relay	HDLC and PPP
Frame Relay DLCI	no	no	no	no
VLAN ID	no	no	no	no
Packet Length	no	no	no	no
DE bit (Frame Relay)	N/A	N/A	N/A	N/A

Monitoring and Maintaining L2VPN

To monitor and maintain the configuration of L2VPN features, use the following commands in privileged EXEC mode. Note that with the exception of the **show mpls l2transport** command, these commands can produce output that is meant to be used by Cisco Systems technical support personnel only.

Command	Displays
show mpls l2transport	Information about AToM VCs that have been enabled to route Layer 2 packets on a router, including platform-independent AToM status and the AToM capabilities of a particular interface.
show pxf cpu atom	PXF-specific forwarding AToM and LS information for an interface or VCCI (column 1 forwarding information).
show mpls l2transport vc	Information about AToM virtual circuits (VCs) that have been enabled to route Layer 2 packets on a router.
show pxf cpu mpls label	PXF-specific forwarding information for a label. The output has been extended to indicate AToM disposition labels, specifically, the transport type associated with the label and the set of output features associated with the label, such as control word and sequencing.
show pxf cpu subblocks	Status and PXF-related parameters for the interface and has been extended to display column 0 of AToM status.
show ssm	Platform-specific information about active segments.
debug pxf atom ac	AToM information related to attachment circuit events.
debug pxf atom mpls	AToM information related to MPLS Forwarding Information (MFI)-driven events.



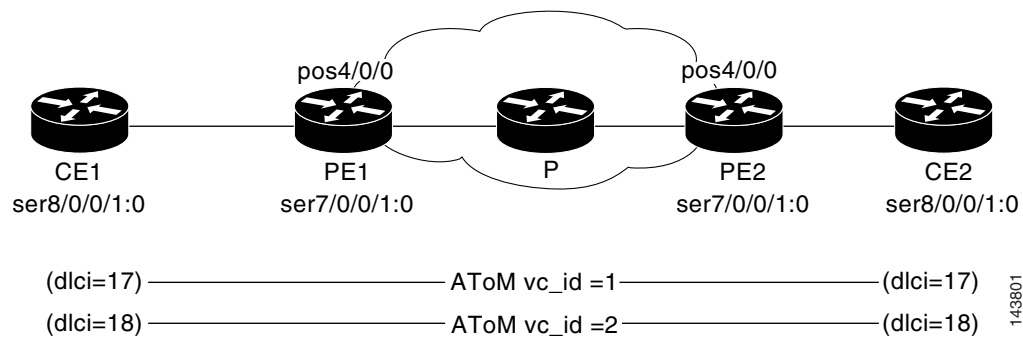
Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use **debug** commands during periods of low network traffic and few users. This decreases the likelihood that increased **debug** command processing overhead will affect system use.

Configuration Example—Frame Relay over MPLS

Example 20-31 shows the configuration of Frame Relay over MPLS on two provider edge routers, PE1 and PE2, and on two customer edge routers, CE1 and CE2. The topology for the example is shown in Figure 20-7.

Figure 20-7 Frame Relay over MPLS Example Topology



For the AToM VCs to come up, MPLS/LDP and a routing protocol need to be run in the core network (PE1---P---PE2). PE1 and PE2 show that they are enabled with the OSPF routing protocol and MPLS/LDP.

Example 20-31 Frame Relay over MPLS Configuration

CE1 Configuration for Frame Relay

```
=====
interface Serial8/0/0.1/1:0
no ip address
encapsulation frame-relay
no fair-queue
frame-relay lmi-type q933a
frame-relay intf-type dce
interface Serial8/0/0.1/1:0.1 point-to-point
ip address 192.1.1.1 255.255.255.0
frame-relay interface-dlci 17
!
interface Serial8/0/0.1/1:0.2 point-to-point
ip address 192.1.2.1 255.255.255.0
frame-relay interface-dlci 18
```

PE1 Configuration for LDP and AToM VC

```
=====
!Enabling LDP
mpls ldp graceful-restart timers neighbor-liveness 300
mpls ldp graceful-restart timers max-recovery 600
mpls ldp graceful-restart
mpls ldp router-id Loopback0 force
mpls label protocol ldp
!Define Loopback address for LDP protocol
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!Enable MPLS/LDP on the core interface
interface POS4/0/0
ip address 50.0.0.1 255.0.0.0
mpls label protocol ldp
```

```

mpls ip
crc 32
clock source internal
!
!Enabling OSPF protocol
router ospf 100
log-adjacency-changes
network 1.0.0.0 0.255.255.255 area 100
network 50.0.0.0 0.255.255.255 area 100
!Define pseudowire-class
pseudowire-class pw_atom1
encapsulation mpls
!FR configuration with two subinterfaces
interface Serial8/0/0.1/1:0
no ip address
encapsulation frame-relay
no fair-queue
frame-relay lmi-type q933a
!
interface Serial8/0/0.1/1:0.1 point-to-point
!
interface Serial8/0/0.1/1:0.2 point-to-point
!
!Two AToM VC configuration with vc ids 1 & 2, 2.2.2.2 is LB addr of PE2
connect atom1 Serial8/0/0.1/1:0 17 l2transport
xconnect 2.2.2.2 1 pw-class pw_atom1
!
!
connect atom2 Serial8/0/0.1/1:0 18 l2transport
xconnect 2.2.2.2 2 pw-class pw_atom1

```

PE2 Configuration

```

=====
!Enabling LDP
mpls ldp graceful-restart timers neighbor-liveness 300
mpls ldp graceful-restart timers max-recovery 600
mpls ldp graceful-restart
mpls ldp router-id Loopback0 force
mpls label protocol ldp
!Define Loopback address for LDP protocol
interface Loopback0
ip address 2.2.2.2 255.255.255.255
!Enable MPLS/LDP on the core interface
interface POS4/0/0
ip address 60.0.0.2 255.0.0.0
mpls label protocol ldp
mpls ip
crc 32
clock source internal
!
!Enabling OSPF protocol
router ospf 100
log-adjacency-changes
network 2.0.0.0 0.255.255.255 area 100
network 60.0.0.0 0.255.255.255 area 100
!Define pseudowire-class
pseudowire-class pw_atom1
encapsulation mpls
!FR configuration with two subinterfaces
interface Serial8/0/0.1/1:0
no ip address
encapsulation frame-relay
no fair-queue

```

```

frame-relay lmi-type q933a
interface Serial8/0/0.1/1:0.1 point-to-point
interface Serial8/0/0.1/1:0.2 point-to-point
!Two AToM VC configuration with vc ids 1 & 2
connect atom1 Serial8/0/0.1/1:0 17 l2transport
xconnect 1.1.1.1 1 pw-class pw_atom1
!
!
connect atom2 Serial8/0/0.1/1:0 18 l2transport
xconnect 1.1.1.1 2 pw-class pw_atom1

```

CE2 Configuration

```

=====
interface Serial8/0/0.1/1:0
no ip address
encapsulation frame-relay
no fair-queue
frame-relay lmi-type q933a
frame-relay intf-type dce
!
interface Serial8/0/0.1/1:0.1 point-to-point
ip address 192.1.1.2 255.255.255.0
frame-relay interface-dlci 17
!
interface Serial8/0/0.1/1:0.2 point-to-point
ip address 192.1.2.2 255.255.255.0
frame-relay interface-dlci 18

```

Verifying PE1 Configuration

The PE1 router shows two AToM VCs are up.

```

=====
router# show mpls l2tran vc
Local intf Local circuit Dest address VC ID Status
-----
Se8/0/0.1/1:0 FR DLCI 17 2.2.2.2 1 UP
Se8/0/0.1/1:0 FR DLCI 18 2.2.2.2 2 UP

router# show mpls l2tran vc 1 det
Local interface: Se8/0/0.1/1:0 up, line protocol up, FR DLCI 17 up
Destination address: 2.2.2.2, VC ID: 1, VC status: up
Output interface: PO4/0/0, imposed label stack {93 19}
Preferred path: not configured
Default path: active
Next hop: point2point
Create time: 00:00:49, last status change time: 00:00:06
Signaling protocol: LDP, peer 2.2.2.2:0 up
MPLS VC labels: local 19, remote 93
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
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, seq error 0, send 0

router# sh mpls l2tran vc 2 det
Local interface: Se8/0/0.1/1:0 up, line protocol up, FR DLCI 18 up
Destination address: 2.2.2.2, VC ID: 2, VC status: up
Output interface: PO4/0/0, imposed label stack {98 19}
Preferred path: not configured

```

```

Default path: active
Next hop: point2point
Create time: 00:00:53, last status change time: 00:00:10
Signaling protocol: LDP, peer 2.2.2.2:0 up
MPLS VC labels: local 22, remote 98
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
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, seq error 0, send 0

```

Any Transport over MPLS—Tunnel Selection

Tunnel Selection allows you to specify the path that Any Transport over MPLS (AToM) traffic uses. You can specify either a MPLS traffic engineering tunnel or a destination IP address. If the specified path is unreachable, you can specify that the virtual circuits (VCs) should use the default path, which is the path that MPLS Label Distribution Protocol (LDP) uses for signaling.



Note

By default, the **preferred-path** sub-command has a fallback pseudowire. If the preferred pseudowire goes down, the MPLS/LDP module switch the circuit temporarily to another pseudowire. When the preferred pseudowire is up again, the circuit is switched back to the preferred pseudowire. The **preferred-path** subcommand also has an **disable-fallback** option, so that no random pseudowire is chosen if the preferred path goes down. The circuit is down until the preferred path pseudowire comes back up. However, in the 12.2(33) SB release, by default, the **preferred-path** sub-command has the **disable-fallback** option. There is no fallback pseudowire in this release, even when the option is stated explicitly.

See the [Any Transport over MPLS: Tunnel Selection](#) document for the following information:

- Prerequisites for Any Transport over MPLS: Tunnel Selection
- Restrictions for Any Transport over MPLS: Tunnel Selection
- Configuring Any Transport over MPLS: Tunnel Selection
- The **debug mpls l2transport vc** command for verifying Any Transport over MPLS: Tunnel Selection
- Verifying the Configuration—Example
- Troubleshooting Any Transport over MPLS: Tunnel Selection—Example

Configuration Example—Any Transport over MPLS: Tunnel Selection

The following example sets up two preferred paths for PE1. One preferred path specifies an MPLS traffic engineering tunnel. The other preferred path specifies an IP address of a loopback address on PE2. There is a static route configured on PE1 that uses a TE tunnel to reach the IP address on PE2.

Router PE1

```

mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback0

```

```

pseudowire-class pw1
encapsulation mpls
preferred-path interface Tunnel1 disable-fallback
!
pseudowire-class pw2
encapsulation mpls
preferred-path peer 10.18.18.18
!
interface Loopback0
ip address 10.2.2.2 255.255.255.255
no ip directed-broadcast
no ip mroute-cache
!
interface Tunnel1
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination 10.16.16.16
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng bandwidth 1500
tunnel mpls traffic-eng path-option 1 explicit name path-tu1
!
interface Tunnel2
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination 10.16.16.16
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng bandwidth 1500
tunnel mpls traffic-eng path-option 1 dynamic
!
interface gigabitethernet0/0/0
no ip address
no ip directed-broadcast
no negotiation auto
!
interface gigabitethernet0/0/0.1
encapsulation dot1Q 222
no ip directed-broadcast
xconnect 10.16.16.16 101 pw-class pw1
!
interface ATM1/0/0
no ip address
no ip directed-broadcast
no atm enable-ilmi-trap
no atm ilmi-keepalive
pvc 0/50 l2transport
encapsulation aal5
xconnect 10.16.16.16 150 pw-class pw2
!
interface gigabitEthernet2/0/1
ip address 10.0.0.1 255.255.255.0
no ip directed-broadcast
tag-switching ip
mpls traffic-eng tunnels
ip rsvp bandwidth 15000 15000
!
router ospf 1
log-adjacency-changes
network 10.0.0.0 0.0.0.255 area 0
network 10.2.2.2 0.0.0.0 area 0
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
!

```

```
ip route 10.18.18.18 255.255.255.255 Tunnel2
!
ip explicit-path name path-tu1 enable
next-address 10.0.0.1
index 3 next-address 10.0.0.1
```

Router PE2

```
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback0
interface Loopback0
ip address 10.16.16.16 255.255.255.255
no ip directed-broadcast
no ip mroute-cache
!
interface Loopback2
ip address 10.18.18.18 255.255.255.255
no ip directed-broadcast
!
interface gigabitEthernet3/1
ip address 10.0.0.2 255.255.255.0
no ip directed-broadcast
mpls traffic-eng tunnels
mpls ip
no cdp enable
ip rsvp bandwidth 15000 15000
!
interface gigabitEthernet3/3
no ip address
no ip directed-broadcast
no cdp enable
!
interface gigabitEthernet3/3.1
encapsulation dot1Q 222
no ip directed-broadcast
no cdp enable
mpls l2transport route 10.2.2.2 101
!
interface ATM5/0
no ip address
no ip directed-broadcast
no atm enable-ilmi-trap
no atm ilmi-keepalive
pvc 0/50 l2transport
encapsulation aal5
xconnect 10.2.2.2 150 encapsulation mpls
!
router ospf 1
log-adjacency-changes
network 10.0.0.0 0.0.0.255 area 0
network 10.16.16.16 0.0.0.0 area 0
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
```

