Any Transport over MPLS

This module describes how to configure Any Transport over MPLS (AToM) transports data link layer (Layer 2) packets over a Multiprotocol Label Switching (MPLS) backbone. AToM enables service providers to connect customer sites with existing Layer 2 networks by using a single, integrated, packet-based network infrastructure--a Cisco MPLS network. Instead of using separate networks with network management environments, service providers can deliver Layer 2 connections over an MPLS backbone. AToM provides a common framework to encapsulate and transport supported Layer 2 traffic types over an MPLS network core.

AToM supports the following like-to-like transport types:

- ATM Adaptation Layer Type-5 (AAL5) over MPLS
- ATM Cell Relay over MPLS
- Ethernet over MPLS (port modes)
- Circuit Emulation (CEM)

Note For information on ATM Cell relay and Circuit Emulation(CEM), see Configuring Pseudowire.

Finding Feature Information

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

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

Prerequisites for Any Transport over MPLS

- IP routing must be configured in the core so that the provider edge (PE) routers can reach each other via IP.
- MPLS must be configured in the core so that a label-switched path (LSP) exists between the PE routers.
- A loopback interface must be configured for originating and terminating Layer 2 traffic. Ensure that 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 traffic engineering (TE) tunnel.

General Restrictions

- Address format--Configure the Label Distribution Protocol (LDP) router ID on all PE routers to be a loopback address with a /32 mask. Otherwise, some configurations might not function properly.
- For PTPoIP configuration with explicit Null MPLS encapsulation, when a Transparent Clock (TC) is placed between a PTP master and a PTP slave, the TC does not update the correction field.
- Ethernet over MPLS (EoMPLS) VC statistics are not supported on the Cisco RSP3 module.
- Virtual Circuit (VC) counters are not supported on the Cisco RSP3 module.

Note VC counters are enabled by default.

- 4000 virtual circuits are supported on the on the Cisco RSP3 module.
- TE-FRR with BGP labels for layer 2 and layer 3 VPNs must terminate on the BGP gateway because of the four-label limitation.
- If an AToM tunnel spans different service providers that exchange MPLS labels using IPv4 Border Gateway Protocol (BGP) (RFC 3107), you add a label to the stack. The maximum MPLS label stack is four (FRR label, TE label, LDP label, VC label).
- BGP PIC Edge with EoMPLS using BGP label Unicast (RFC 3107) requires the **bgp mpls-local-label** command to be explicitly enabled under the Router BGP process. This limitation is applicable only on the Cisco RSP3 module.

- Hot standby pseudowire (HSPW) convergence without pseudowire grouping increments linearly. For example, for a thousand virtual circuits, it requires about 54 seconds of convergence time. This is applicable only for the Cisco RSP3 Module.

  Clear interface is not the recommended way to measure the convergence numbers.

- With two ECMP paths, load sharing on L2VPN traffic occurs based on odd or even MPLS VC labels. If L2VPN circuits have either odd **or** even MPLS VC labels, load sharing is not performed. But if L2VPN circuits have a combination of both odd **and** even MPLS VC labels, then the odd MPLS VC labels circuits will select one link whereas the even MPLS VC labels circuits will select another link.
- Flow-Aware Transport (FAT) Load Balancing over VPLS is not supported.

ATM AAL5 over MPLS Restrictions

- AAL5 over MPLS is supported only in SDU mode.

Ethernet over MPLS (EoMPLS) Restrictions

- The subinterfaces between the CE and PE routers that are running Ethernet over MPLS must be in the same subnet.
- The subinterface on the adjoining CE router must be on the same VLAN as the PE router.
- 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 CE routers.
- The AToM control word is supported. However, if the peer PE does not support a control word, the control word is disabled.
- Ethernet packets with hardware-level cyclic redundancy check (CRC) errors, framing errors, and runt packets are discarded on input.

Tunnel Selection Restrictions

- The selected path should be an LSP destined to the peer PE router.
- The selected tunnel must be an MPLS TE tunnel.
- If you specify an IP address, that address must be the IP address of the loopback interface on the remote PE router. The address must have a /32 mask. There must be an LSP destined to that selected address. The LSP need not be a TE tunnel.

Remote Ethernet Port Shutdown Restrictions

This feature is not symmetrical if the remote PE router is running an older version 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.

Remote Ethernet Port Shutdown is supported only on EFP with encapsulation default.

Information About Any Transport over MPLS

To configure AToM, you must understand the following concepts:

How AToM Transports Layer 2 Packets

AToM encapsulates Layer 2 frames at the ingress PE and sends them to a corresponding PE at the other end of a pseudowire, which is a connection between the two PE routers. The egress PE 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. You specify the following information on each PE router:

- The type of Layer 2 data that will 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

The following example shows the basic configuration steps on a PE router that enable the transport of Layer 2 packets. Each transport type has slightly different steps.

Step 1 defines the interface or subinterface on the PE router:

```
Router# interface
 interface-type interface-number
```

Step 2 configures an ethernet service instance on an interface and enters service instance configuration mode:

```
Router(config-if)#service instance number ethernet WORD
Router(config-if)# service instance 393 ethernet ethernet1
```

Step 3 specifies the encapsulation type for the interface, such as dot1q:

```
Router(config-if-srv)# encapsulation
encapsulation-type
```

Step 4 does the following:

- Makes a connection to the peer PE router by specifying the LDP router ID of the peer PE router.
- Specifies a 32-bit unique identifier, called the VC ID, which is shared between the two PE routers.

The combination of the peer router ID and the VC ID must be unique 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. AToM uses MPLS as the tunneling method.

```
Router(config-if-srv)# xconnect
peer-router-id vcid
encapsulation mpls
```

As an alternative, you can set up a pseudowire class to specify the tunneling method and other characteristics. For more information, see the Configuring the Pseudowire Class, on page 12.

How AToM Transports Layer 2 Packets Using Commands Associated with L2VPN Protocol-Based Feature

AToM encapsulates Layer 2 frames at the ingress PE and sends them to a corresponding PE at the other end of a pseudowire, which is a connection between the two PE routers. The egress PE 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. You specify the following information on each PE router:

- The type of Layer 2 data that will 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

The following example shows the basic configuration steps on a PE router that enable the transport of Layer 2 packets. Each transport type has slightly different steps.

Step 1 defines the interface or subinterface on the PE router:

```
Router# interface
interface-type interface-number

Router(config)# interface gi 0/1/0
```

Step 2 configures an ethernet service instance on an interface and enters service instance configuration mode:

```
Router(config-if)#service instance number ethernet WORD
Router(config-if)# service instance 393 ethernet ethernet1
```

Step 3 specifies the encapsulation type for the interface, such as dot1q:

```
Router(config-if)# encapsulation
encapsulation-type

Router(config-if-srv)# encapsulation dot1q 393
```

Step 3 does the following:

- Makes a connection to the peer PE router by specifying the LDP router ID of the peer PE router.

- Specifies a 32-bit unique identifier, called the VC ID, which is shared between the two PE routers.

The combination of the peer router ID and the VC ID must be unique 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. AToM uses MPLS as the tunneling method.

```
Router(config)# interface pseudowire 100
Router(config-if)# encapsulation mpls
Router(config-if)# neighbor 10.0.0.1 123
Router(config-if)# exit
!
Router(config)# l2vpn xconnect context A
Router(config-xconnect)# member pseudowire 100

Router (config-xconnect)# member gigabitethernet0/1/0 service instance 393

Router(config-xconnect)# exit
```

As an alternative, you can set up a pseudowire class to specify the tunneling method and other characteristics. For more information, see the Configuring the Pseudowire Class, on page 12.

Benefits of AToM

The following list explains some of the benefits of enabling Layer 2 packets to be sent in the MPLS network:

- 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. This benefits the service provider that 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.

MPLS Traffic Engineering Fast Reroute

Note For the supported combinations of MPLS TE FRR on Cisco RSP3 Module, see the *MPLS Traffic Engineering Path Link and Node Protection Configuration Guide*.

AToM can use MPLS traffic engineering (TE) tunnels with fast reroute (FRR) support. AToM VCs can be rerouted around a failed link or node at the same time as MPLS and IP prefixes.

Enabling fast reroute on AToM does not require any special commands; you can use standard fast reroute commands. At the ingress PE, an AToM tunnel is protected by fast reroute when it is routed to an FRR-protected TE tunnel. Both link and node protection are supported for AToM VCs at the ingress PE.

Maximum Transmission Unit Guidelines for Estimating Packet Size

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 * 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. The table below lists the specific sizes of the headers.

Table 1: Header Size of Packets

Transport Type	Packet Size
AAL5	0-32 bytes
Ethernet VLAN	18 bytes
Ethernet Port	14 bytes
Frame Relay DLCI	2 bytes for Cisco encapsulation, 8 bytes for Internet Engineering Task Force (IETF) encapsulation
HDLC	4 bytes
PPP	4 bytes

AToM Header

The AToM header is 4 bytes (control word). The control word is optional for Ethernet, PPP, HDLC, and cell relay transport types. The control word is required for Frame Relay and ATM AAL5 transport types.

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 one for directly connected AToM PEs, 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 two (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 two (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 three (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 four (FRR label, TE label, LDP label, VC label).
- If AToM is used by the customer carrier in an MPLS VPN Carrier Supporting Carrier environment, you add a label to the stack. The maximum MPLS label stack in the provider carrier network is four (FRR label, TE label, LDP label, VC label).
- BGP PIC Edge with EoMPLS using BGP label Unicast (RFC 3107) requires the **bgp mpls-local-label** command to be explicitly enabled under the Router BGP process. This limitation is applicable only on the Cisco RSP3 module.
- If an AToM tunnel spans different service providers that exchange MPLS labels using IPv4 Border Gateway Protocol (BGP) (RFC 3107), you add a label to the stack. The maximum MPLS label stack is four (FRR label, TE label, LDP label, VC label)
- TE-FRR with BGP labels for layer 2 and layer 3 VPNs must terminate on the BGP gateway because of the four-label limitation.

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.

Hot standby pseudowire (HSPW) convergence without pseudowire grouping increments linearly, with a thousand virtual circuits taking 54 seconds of convergence time. This is applicable only on the Cisco RSP3 Module.

Estimating Packet Size Example

The estimated packet size in the following example is 1526 bytes, based on 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 0, because the control word is not used.
- The MPLS label stack is 2, because LDP is used. The MPLS label is 4 bytes.

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

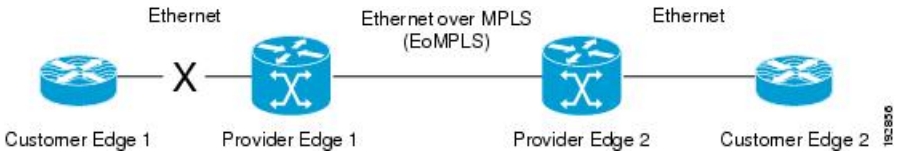
You must configure the P and PE routers in the core to accept packets of 1526 bytes.

Any Transport over MPLS (AToM) Remote Ethernet Port Shutdown

This Cisco IOS XE 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 cause the 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.

The figure below illustrates a condition in an EoMPLS WAN, with a down Layer 2 tunnel link between a CE router (Customer Edge 1) and the PE router (Provider Edge 1). A CE router on the far side of the Layer 2 tunnel (Customer Edge 2), continues to forward traffic to Customer Edge 1 through the L2 tunnel.

Figure 1: Remote Link Outage in EoMPLS WAN



Previous to this feature, the Provider Edge 2 router could not detect a failed remote link. Traffic forwarded from Customer Edge 2 to Customer Edge 1 would be lost until routing or spanning tree protocols detected the down remote link. If the link was configured with static routing, the remote link outage would be even more difficult to detect.

With this feature, the Provider Edge 2 router detects the remote link failure and causes a shutdown of the local Customer Edge 2 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 the figure above, the Remote Ethernet Shutdown sequence is generally described as follows:

1. The remote link between Customer Edge 1 and Provider Edge 1 fails.
2. Provider Edge 2 detects the remote link failure and disables the transmit laser on the line card interface connected to Customer Edge 2.
3. An RX_LOS error alarm is received by Customer Edge 2 causing Customer Edge 2 to bring down the interface.
4. Provider Edge 2 maintains its interface with Customer Edge 2 in an up state.
5. When the remote link and EoMPLS connection is restored, the Provider Edge 2 router enables the transmit laser.
6. The Customer Edge 2 router brings up its downed interface.

This feature is enabled by default for Ethernet over MPLS (EoMPLS). You can also enable this feature by using the **remote link failure notification** command in xconnect configuration mode as shown in the following example:

```
pseudowire-class eompls
 encapsulation mpls
!
interface GigabitEthernet1/0/0
 xconnect 10.13.13.13 1 pw-class eompls
  remote link failure notification
!
```

This feature can be disabled using the **no remote link failure notification** command in xconnect configuration mode. Use the **show ip interface brief** privileged EXEC command to display the status of all remote L2 tunnel links. Use the **show interface** privileged EXEC command to show the status of the L2 tunnel on a specific interface.

Note The **no remote link failure notification** command will not give notification to clients for remote attachment circuit status down.

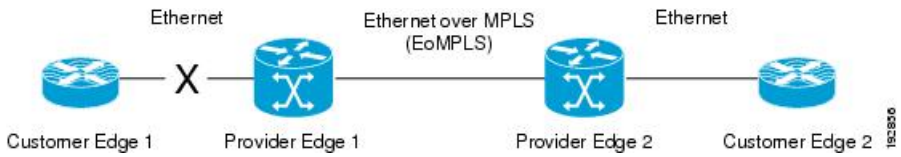
Note Remote Ethernet Port Shutdown is supported only on EFP with encapsulation default.

Any Transport over MPLS (AToM) Remote Ethernet Port Shutdown Using Commands Associated with L2VPN Protocol-Based Feature

This Cisco IOS XE 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 cause the 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.

The figure below illustrates a condition in an EoMPLS WAN, with a down Layer 2 tunnel link between a CE router (Customer Edge 1) and the PE router (Provider Edge 1). A CE router on the far side of the Layer 2 tunnel (Customer Edge 2), continues to forward traffic to Customer Edge 1 through the L2 tunnel.

Figure 2: Remote Link Outage in EoMPLS WAN



Previous to this feature, the Provider Edge 2 router could not detect a failed remote link. Traffic forwarded from Customer Edge 2 to Customer Edge 1 would be lost until routing or spanning tree protocols detected the down remote link. If the link was configured with static routing, the remote link outage would be even more difficult to detect.

With this feature, the Provider Edge 2 router detects the remote link failure and causes a shutdown of the local Customer Edge 2 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 the figure above, the Remote Ethernet Shutdown sequence is generally described as follows:

1. The remote link between Customer Edge 1 and Provider Edge 1 fails.
2. Provider Edge 2 detects the remote link failure and disables the transmit laser on the line card interface connected to Customer Edge 2.
3. An RX_LOS error alarm is received by Customer Edge 2 causing Customer Edge 2 to bring down the interface.
4. Provider Edge 2 maintains its interface with Customer Edge 2 in an up state.
5. When the remote link and EoMPLS connection is restored, the Provider Edge 2 router enables the transmit laser.

6. The Customer Edge 2 router brings up its downed interface.

This feature is enabled by default for Ethernet over MPLS (EoMPLS). You can also enable this feature by using the **remote link failure notification** command in xconnect configuration mode as shown in the following example:

```
l2vpn xconnect context con1
member GigabitEthernet1/0/0 service-instance 300
member Pseudowire 100
remote link failure notification
```

This feature can be disabled using the **no remote link failure notification** command in xconnect configuration mode. Use the **show ip interface brief** privileged EXEC command to display the status of all remote L2 tunnel links. Use the **show interface** privileged EXEC command to show the status of the L2 tunnel on a specific interface.

Note The **no remote link failure notification** command will not give notification to clients for remote attachment circuit status down.

Flow-Aware Transport (FAT) Load Balancing

Note The FAT-PW feature is supported only in the RSP3 module and only with the new CLI.

The Flow-Aware Transport of MPLS Pseudowires feature enables load balancing of packets within the same pseudowire by further classifying the packets into different flows by adding a flow label at the bottom of the MPLS label stack.

Equal Cost Multi-Path

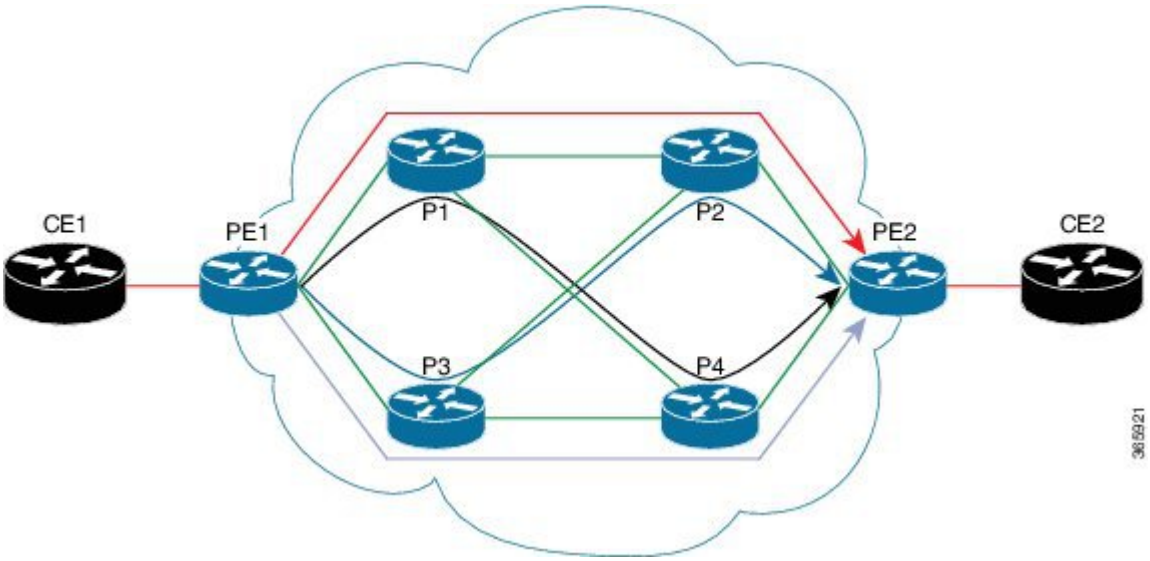
The Flow-Aware Transport Pseudowire (FAT-PW) is used to load-balance traffic in the core when Equal Cost Multiple Paths (ECMP) exist. The existing Load Balance technique does the load balance among multiple pseudowires by choosing different ECMP paths, based on the Virtual Circuit (VC) Label. This does not suffice the load balance of traffic within a pseudowire.

A flow label is a unique identifier to distinguish a flow within the pseudowire and is generated based on source and destination MAC address along with source and destination IP address. The flow label has EOS (End of Label Stack) bit SET and inserted before the VC label and after the control word, if necessary. Calculation and pushing of the flow label is done by an ingress PE, enabled by FAT-PW configuration. Egress PE discards the flow label and no decisions are taken based on that label.

All core routers do a load balance based on the bottom-most label, which is a flow-label in FAT-PW. Hence you get the advantage of distributing flows over ECMP paths.

The figure below shows the various paths through which the data can be transmitted in an ECMP.

Figure 3: Equal Cost Multi-Path



- Without any load-balancing, the pseudowire can use any one path of the four options, for example consider the red path (PE1 > P1 > P2 > PE2)
- If PE1 is able to do load-balancing, then both PE1 and PE2 can be utilized, for example consider the red and gray paths (PE1 > P3 > P4 > PE2)
- With flow labels inserted on PE1, all paths can be utilized, for example red, black, blue, and gray paths

How to Configure Any Transport over MPLS

This section explains how to perform a basic AToM configuration and includes the following procedures:

Configuring the Pseudowire Class

Note In simple configurations, this task is optional. You need not specify a pseudowire class if you specify the tunneling method as part of the **xconnect** command.

- You must specify the **encapsulation mpls** command as part of the pseudowire class or as part of the **xconnect** command for the AToM VCs to work properly. If you omit the **encapsulation mpls** command as part of the **xconnect** command, you receive the following error:

```
% Incomplete command.
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **pseudowire-class** *name*
4. **encapsulation mpls**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pseudowire-class** *name* **Example:** `Router(config)# pseudowire-class atom`	Establishes a pseudowire class with a name that you specify and enters pseudowire class configuration mode.
Step 4	**encapsulation mpls** **Example:** `Router(config-pw)# encapsulation mpls`	Specifies the tunneling encapsulation.

Configuring the Pseudowire Class Using Commands Associated with L2VPN Protocol-Based Feature

Note In simple configurations, this task is optional. You need not specify a pseudowire class if you specify the tunneling method as part of the **l2vpn xconnect context** command.

- You must specify the **encapsulation mpls** command as part of the pseudowire class or as part of the **l2vpn xconnect context** command for the AToM VCs to work properly. If you omit the **encapsulation mpls** command as part of the **l2vpn xconnect context**command, you receive the following error:

```
% Incomplete command.
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface pseudowire** *name*
4. **encapsulation mpls**

5. **neighbor** *peer-address vcid-value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface pseudowire** *name* **Example:** `Router(config)# interface pseudowire atom`	Establishes an interface pseudowire with a name that you specify and enters pseudowire class configuration mode.
Step 4	**encapsulation mpls** **Example:** `Router(config-pw-class)# encapsulation mpls`	Specifies the tunneling encapsulation.
Step 5	**neighbor** *peer-address vcid-value* **Example:** `Router(config-pw-class)#  neighbor 33.33.33.33 1`	Specifies the peer IP address and virtual circuit (VC) ID value of a Layer 2 VPN (L2VPN) pseudowire.

Changing the Encapsulation Type and Removing a Pseudowire

Once you specify the **encapsulation mpls** command, you cannot remove it using the **no encapsulation mpls** command.

Those methods result in the following error message:

```
Encapsulation changes are not allowed on an existing pw-class.
```

To remove the **encapsulation mpls** command, you must delete the pseudowire with the **no pseudowire-class** command.

To change the type of encapsulation, remove the pseudowire using the **no pseudowire-class** command and reconfigure the pseudowire to specify the new encapsulation type.

Changing the Encapsulation Type and Removing a Pseudowire Using Commands Associated with the L2VPN Protocol-Based Feature

Once you specify the **encapsulation mpls** command, you cannot remove it using the **no encapsulation mpls** command.

Those methods result in the following error message:

```
% Cannot remove encapsulation on existing pseudowire
```

To remove the **encapsulation mpls** command, you must delete the pseudowire with the **no interface pseudowire** command.

To change the type of encapsulation, remove the pseudowire using the **no template type pseudowire** command and reconfigure the pseudowire to specify the new encapsulation type.

Configuring ATM AAL5 over MPLS

Configuring ATM AAL5 over MPLS on PVCs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / subslot / port* [**.** *subinterface*]
4. **pvc** [*name*] *vpi / vci* **l2transport**
5. **encapsulation aal5**
6. **xconnect** *peer-router-id vcid* **encapsulation mpls**
7. **end**
8. **show mpls l2transport vc**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot / subslot / port* [**.** *subinterface*] **Example:** `Router(config)# interface atm1/0/0`	Specifies the interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**pvc** [*name*] *vpi* / *vci* **l2transport** **Example:** `Router(config-if)# pvc 1/200 l2transport`	Creates or assigns a name to an ATM PVC and enters L2transport PVC configuration mode. • The **l2transport** keyword indicates that the PVC is a switched PVC instead of a terminated PVC.
Step 5	**encapsulation aal5** **Example:** `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 customer edge (CE) routers.
Step 6	**xconnect** *peer-router-id vcid* **encapsulation mpls** **Example:** `Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls`	Binds the attachment circuit to a pseudowire VC.
Step 7	**end** **Example:** `Router(config-if-atm-l2trans-pvc)# end`	Exits to privileged EXEC mode.
Step 8	**show mpls l2transport vc** **Example:** `Router# show mpls l2transport vc`	Displays output that shows ATM AAL5 over MPLS is configured on a PVC.

Examples

The following is sample output from the **show mpls l2transport vc** command that shows that ATM AAL5 over MPLS is configured on a PVC:

```
Router# show mpls l2transport vc
Local intf   Local circuit          Dest address      VC ID      Status
---------    -------------          ------------      -----      ------
ATM1/0       ATM AAL5 1/100         10.4.4.4           100        UP
```

Configuring ATM AAL5 over MPLS on PVCs using the commands associated with the L2VPN Protocol-Based CLIs feature

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port*[**.** *subinterface*]
4. **pvc** [*name*] *vpi* / *vci* **l2transport**

5. **encapsulation aal5**
6. **end**
7. **interface pseudowire** *number*
8. **encapsulation mpls**
9. **neighbor** *peer-address vcid-value*
10. **exit**
11. **l2vpn xconnect context** *context-name*
12. **member pseudowire** *interface-number*
13. **member atm** *interface-number* **pvc** *vpi* / *vci*
14. **end**
15. **show l2vpn atom vc**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot* / *subslot* / *port*[**.** *subinterface*] **Example:** `Device(config)# interface atm1/0/0`	Specifies the interface type and enters interface configuration mode.
Step 4	**pvc** [*name*] *vpi* / *vci* **l2transport** **Example:** `Device(config-if)# pvc 1/200 l2transport`	Creates or assigns a name to an ATM PVC and enters L2transport PVC configuration mode. • The **l2transport** keyword indicates that the PVC is a switched PVC instead of a terminated PVC.
Step 5	**encapsulation aal5** **Example:** `Device(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 customer edge (CE) routers.
Step 6	**end** **Example:** `Device(config-if-atm-l2trans-pvc)# end`	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 7	**interface pseudowire** *number* **Example:** `Device(config)# interface pseudowire 100`	Specifies the pseudowire interface and enters interface configuration mode.
Step 8	**encapsulation mpls** **Example:** `Device(config-if)# encapsulation mpls`	Specifies that Multiprotocol Label Switching (MPLS) is used as the data encapsulation method.
Step 9	**neighbor** *peer-address vcid-value* **Example:** `Device(config-if)# neighbor 10.13.13.13 100`	Specifies the peer IP address and virtual circuit (VC) ID value of the Layer 2 VPN (L2VPN) pseudowire.
Step 10	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.
Step 11	**l2vpn xconnect context** *context-name* **Example:** `Device(config)# l2vpn xconnect context con1`	Creates a Layer 2 VPN (L2VPN) cross connect context and enters xconnect configuration mode.
Step 12	**member pseudowire** *interface-number* **Example:** `Device(config-xconnect)# member pseudowire 100`	Specifies a member pseudowire to form a Layer 2 VPN (L2VPN) cross connect.
Step 13	**member atm** *interface-number* **pvc** *vpi* / *vci* **Example:** `Device(config-xconnect)# member atm 100 pvc 1/200`	Specifies the location of the ATM member interface.
Step 14	**end** **Example:** `Device(config-xconnect)# end`	Exits to privileged EXEC mode.
Step 15	**show l2vpn atom vc** **Example:** `Device# show l2vpn atom vc`	Displays output that shows ATM AAL5 over MPLS is configured on a PVC.

Examples

The following is sample output from the **show l2vpn atom vc** command that shows that ATM AAL5 over MPLS is configured on a PVC:

```
Device# show l2vpn atom vc
Local intf   Local circuit          Dest address      VC ID      Status
---------    -------------          ------------      -----      ------
ATM1/0       ATM AAL5 1/100         10.4.4.4           100        UP
```

Configuring ATM AAL5 over MPLS in VC Class Configuration Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **encapsulation** *layer-type*
5. **exit**
6. **interface** *type slot* / *subslot* / *port* [**.** *subinterface*]
7. **class-int** *vc-class-name*
8. **pvc** [*name*] *vpi* / *vci* **l2transport**
9. **xconnect** *peer-router-id vcid* **encapsulation mpls**
10. **end**
11. **show atm class-links**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm aal5class`	Creates a VC class and enters VC class configuration mode.
Step 4	**encapsulation** *layer-type* **Example:**	Configures the AAL and encapsulation type.

	Command or Action	Purpose
	`Router(config-vc-class)# encapsulation aal5`	
Step 5	**exit** **Example:** `Router(config-vc-class)# exit`	Exits VC class configuration mode.
Step 6	**interface** *type slot / subslot / port* [**.** *subinterface*] **Example:** `Router(config)# interface atm1/0/0`	Specifies the interface type enters interface configuration mode.
Step 7	**class-int** *vc-class-name* **Example:** `Router(config-if)# class-int aal5class`	Applies a VC class to the ATM main interface or subinterface. **Note** You can also apply a VC class to a PVC.
Step 8	**pvc** [*name*] *vpi / vci* **l2transport** **Example:** `Router(config-if)# pvc 1/200 l2transport`	Creates or assigns a name to an ATM PVC and enters L2transport PVC configuration mode. • The **l2transport** keyword indicates that the PVC is a switched PVC instead of a terminated PVC.
Step 9	**xconnect** *peer-router-id vcid* **encapsulation mpls** **Example:** `Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls`	Binds the attachment circuit to a pseudowire VC.
Step 10	**end** **Example:** `Router(config-if-atm-l2trans-pvc)# end`	Exits to privileged EXEC mode.
Step 11	**show atm class-links** **Example:** `Router# show atm class-links`	Displays the type of encapsulation and that the VC class was applied to an interface.

Examples

In the following example, the command output from the **show atm class-links** command verifies that ATM AAL5 over MPLS is configured as part of a VC class. The command output shows the type of encapsulation and that the VC class was applied to an interface.

```
Router# show atm class-links 1/100
Displaying vc-class inheritance for ATM1/0/0.0, vc 1/100:
```

```
no broadcast - Not configured - using default
encapsulation aal5 - VC-class configured on main interface
```

Configuring ATM AAL5 over MPLS in VC Class Configuration Mode using the commands associated with the L2VPN Protocol-Based CLIs feature

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **encapsulation** *layer-type*
5. **exit**
6. **interface** *type slot* / *subslot* / *port* [**.** *subinterface*]
7. **class-int** *vc-class-name*
8. **pvc** [*name*] *vpi* / *vci* **l2transport**
9. **exit**
10. **interface pseudowire** *number*
11. **encapsulation mpls**
12. **neighbor** *peer-address vcid-value*
13. **exit**
14. **l2vpn xconnect context** *context-name*
15. **member pseudowire** *interface-number*
16. **member atm** *interface-number*
17. **end**
18. **show atm class-links**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vc-class atm** *vc-class-name* **Example:** `Router(config)# vc-class atm aal5class`	Creates a VC class and enters VC class configuration mode.

	Command or Action	Purpose
Step 4	**encapsulation** *layer-type* **Example:** `Router(config-vc-class)# encapsulation aal5`	Configures the AAL and encapsulation type.
Step 5	**exit** **Example:** `Router(config-vc-class)# exit`	Exits VC class configuration mode.
Step 6	**interface** *type slot / subslot / port* [**.** *subinterface*] **Example:** `Router(config)# interface atm1/0/0`	Specifies the interface type enters interface configuration mode.
Step 7	**class-int** *vc-class-name* **Example:** `Router(config-if)# class-int aal5class`	Applies a VC class to the ATM main interface or subinterface. **Note** You can also apply a VC class to a PVC.
Step 8	**pvc** [*name*] *vpi / vci* **l2transport** **Example:** `Router(config-if)# pvc 1/200 l2transport`	Creates or assigns a name to an ATM PVC and enters L2transport PVC configuration mode. • The **l2transport** keyword indicates that the PVC is a switched PVC instead of a terminated PVC.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 10	**interface pseudowire** *number* **Example:** `Router(config)# interface pseudowire 100`	Specifies the pseudowire interface and enters interface configuration mode.
Step 11	**encapsulation mpls** **Example:** `Router(config-if)# encapsulation mpls`	Specifies that Multiprotocol Label Switching (MPLS) is used as the data encapsulation method.
Step 12	**neighbor** *peer-address vcid-value* **Example:** `Router(config-if)# neighbor 10.0.0.1 123`	Specifies the peer IP address and virtual circuit (VC) ID value of the Layer 2 VPN (L2VPN) pseudowire.

	Command or Action	Purpose
Step 13	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 14	**l2vpn xconnect context** *context-name* **Example:** `Router(config)# l2vpn xconnect context con1`	Creates a Layer 2 VPN (L2VPN) cross connect context and enters xconnect configuration mode.
Step 15	**member pseudowire** *interface-number* **Example:** `Router(config-xconnect)# member pseudowire 100`	Specifies a member pseudowire to form a Layer 2 VPN (L2VPN) cross connect.
Step 16	**member atm** *interface-number* **Example:** `Device(config-xconnect)# member atm 100`	Specifies the location of the ATM member interface.
Step 17	**end** **Example:** `Router(config-if-atm-l2trans-pvc)# end`	Exits to privileged EXEC mode.
Step 18	**show atm class-links** **Example:** `Router# show atm class-links`	Displays the type of encapsulation and that the VC class was applied to an interface.

Examples

In the following example, the command output from the **show atm class-links** command verifies that ATM AAL5 over MPLS is configured as part of a VC class. The command output shows the type of encapsulation and that the VC class was applied to an interface.

```
Router# show atm class-links 1/100
Displaying vc-class inheritance for ATM1/0/0.0, vc 1/100:
no broadcast - Not configured - using default
encapsulation aal5 - VC-class configured on main interface
```

Configuring Ethernet over MPLS

Configuring Ethernet over MPLS with VLAN ID Rewrite

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot* / *subslot* / *port*
4. **no ip address**
5. **negotiation auto**
6. **service instance** *id* **ethernet**
7. **encapsulation dot1q** *vlan-id*
8. **xconnect** *peer-router-id vcid* **encapsulation mpls**
9. **remote circuit id** *remote-vlan-id*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot* / *subslot* / *port* **Example:** `Router(config)# interface GigabitEthernet0/2/4`	Specifies the Gigabit Ethernet subinterface and enters subinterface configuration mode.
Step 4	**no ip address** **Example:** `Router(config-if)# no ip address`	Specifies that there is no IP address assigned to the interface.
Step 5	**negotiation auto** **Example:** `Router(config-if)# negotiation auto`	Enables the auto negotiation protocol.
Step 6	**service instance** *id* **ethernet** **Example:**	Configures an ethernet service instance on an interface and enters service instance configuration mode.

	Command or Action	Purpose
	`Router(config-if)# service instance 100 ethernet`	
Step 7	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-subif)# encapsulation dot1q 100`	Enables the subinterface to accept 802.1Q VLAN packets.
Step 8	**xconnect** *peer-router-id vcid* **encapsulation mpls** **Example:** `Router(config-subif)# xconnect 10.0.0.1 123 encapsulation mpls`	Binds the attachment circuit to a pseudowire VC and enters xconnect configuration mode.
Step 9	**remote circuit id** *remote-vlan-id* **Example:** `Router(config-subif-xconn)# remote circuit id 101`	(Optional) Enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel.
Step 10	**end** **Example:** `Router(config-subif-xconn)# end`	Exits to privileged EXEC mode.

Configuring Ethernet over MPLS with VLAN ID Rewrite Using Commands Associated with the L2VPN Protocol-Based Feature

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot* / *subslot* / *port*
4. **service instance** *number* **ethernet** *number*
5. **encapsulation dot1q** *vlan-id*
6. **end**
7. **interface pseudowire** *number*
8. **encapsulation mpls**
9. **neighbor** *peer-address vcid-value*
10. **exit**
11. **l2vpn xconnect context** *context-name*
12. **member pseudowire** *interface-number*
13. **member gigabitethernet** *interface-number*
14. **remote circuit id** *remote-vlan-id*
15. **end**
16. **show controllers eompls forwarding-table**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot* / *subslot* / *port* **Example:** `Router(config)# interface gigabitethernet4/0/0`	Specifies the Gigabit Ethernet subinterface and enters subinterface configuration mode.
Step 4	**service instance** *number* **ethernet** *number* **Example:** `Router(config-if)#service instance 393 ethernet`	
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Router(config-subif)# encapsulation dot1q 100`	Enables the subinterface to accept 802.1Q VLAN packets.
Step 6	**end** **Example:** `Router(config-subif)# end`	Exits to privileged EXEC mode.
Step 7	**interface pseudowire** *number* **Example:** `Router(config)# interface pseudowire 100`	Specifies the pseudowire interface and enters interface configuration mode.
Step 8	**encapsulation mpls** **Example:** `Router(config-if)# encapsulation mpls`	Specifies that Multiprotocol Label Switching (MPLS) is used as the data encapsulation method.
Step 9	**neighbor** *peer-address vcid-value* **Example:** `Router(config-if)# neighbor 10.0.0.1 123`	Specifies the peer IP address and virtual circuit (VC) ID value of the Layer 2 VPN (L2VPN) pseudowire.

	Command or Action	Purpose
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 11	**l2vpn xconnect context** *context-name* **Example:** `Router(config)# l2vpn xconnect context con1`	Creates a Layer 2 VPN (L2VPN) cross connect context and enters xconnect configuration mode.
Step 12	**member pseudowire** *interface-number* **Example:** `Router(config-xconnect)# member pseudowire 100`	Specifies a member pseudowire to form a Layer 2 VPN (L2VPN) cross connect.
Step 13	**member gigabitethernet** *interface-number* **Example:** `Router(config-xconnect)# member gigabitethernet4/0/0 service-instance 393`	Specifies the location of the Gigabit Ethernet member interface.
Step 14	**remote circuit id** *remote-vlan-id* **Example:** `Router(config-xconnect)# remote circuit id 101`	(Optional) Enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel.
Step 15	**end** **Example:** `Router(config-xconnect)# end`	Exits to privileged EXEC mode.
Step 16	**show controllers eompls forwarding-table** **Example:** `Router# show controllers eompls forwarding-table`	Displays information about VLAN ID rewrite.

Example

```
RSP3-RT1#show ethernet service instance id HYPERLINK "tel:1002"1002 interface gi 0/1/0 det
Service Instance ID: HYPERLINK "tel:1002"1002
Service Instance Type: Static
Associated Interface: GigabitEthernet0/1/0
Associated EVC:
L2protocol drop
CE-Vlans:
Encapsulation: dot1q HYPERLINK "tel:1002"1002 vlan protocol type 0xHYPERLINK "tel:8100"8100
Rewrite: ingress tag pop 1 symmetric
Interface Dot1q Tunnel Ethertype: 0xHYPERLINK "tel:8100"8100
```

```
State: Up
EFP Statistics:
Pkts In   Bytes In   Pkts Out  Bytes Out
0          0          0          0

RSP3-RT1#
```

Configuring Tunnel Selection

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *name*
4. **encapsulation mpls**
5. **preferred-path** {**interface tunnel** *tunnel-number* | **peer**{*ip-address* | *host-name*}} [**disable-fallback**]
6. **exit**
7. **interface** *type slot* / *subslot* / *port*
8. **encapsulation** *encapsulation-type*
9. **xconnect** *peer-router-id vcid* **pw-class** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pseudowire-class** *name* **Example:** `Router(config)# pseudowire-class ts1`	Establishes a pseudowire class with a name that you specify and enters pseudowire configuration mode.
Step 4	**encapsulation mpls** **Example:** `Router(config-pw)# encapsulation mpls`	Specifies the tunneling encapsulation. For AToM, the encapsulation type is mpls.
Step 5	**preferred-path** {**interface tunnel** *tunnel-number* | **peer**{*ip-address* | *host-name*}} [**disable-fallback**] **Example:**	Specifies the MPLS traffic engineering tunnel or IP address or hostname to be used as the preferred path.

	Command or Action	Purpose
	`Router(config-pw)# preferred path peer 10.18.18.18`	
Step 6	**exit** **Example:** `Router(config-pw)# exit`	Exits from pseudowire configuration mode and enables the Tunnel Selection feature.
Step 7	**interface** *type slot / subslot / port* **Example:** `Router(config)# interface atm1/1/0`	Specifies an interface type and enters interface configuration mode.
Step 8	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation aal5`	Specifies the encapsulation for the interface.
Step 9	**xconnect** *peer-router-id vcid* **pw-class** *name* **Example:** `Router(config-if)# xconnect 10.0.0.1 123 pw-class ts1`	Binds the attachment circuit to a pseudowire VC.

Examples

In the following sample output from the **show mpls l2transport vc** command includes the following information about the VCs:

- VC 101 has been assigned a preferred path called Tunnel1. The default path is disabled, because the preferred path specified that the default path should not be used if the preferred path fails.
- VC 150 has been assigned an IP address of a loopback address on PE2. The default path can be used if the preferred path fails.

Command output that is in boldface font shows the preferred path information.

```
Router# show mpls l2transport vc detail
Local interface: Gi0/0/0.1 up, line protocol up, Eth VLAN 222 up
  Destination address: 10.16.16.16, VC ID: 101, VC status: up
    Preferred path: Tunnel1,  active
    Default path: disabled
    Tunnel label: 3, next hop point2point
    Output interface: Tu1, imposed label stack {17 16}
  Create time: 00:27:31, last status change time: 00:27:31
  Signaling protocol: LDP, peer 10.16.16.16:0 up
    MPLS VC labels: local 25, remote 16
    Group ID: local 0, remote 6
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
```

```
    packet totals: receive 10, send 10
    byte totals:   receive 1260, send 1300
    packet drops:  receive 0, send 0
Local interface: ATM1/0/0 up, line protocol up, ATM AAL5 0/50 up
  Destination address: 10.16.16.16, VC ID: 150, VC status: up
    Preferred path: 10.18.18.18, active
    Default path: ready
    Tunnel label: 3, next hop point2point
    Output interface: Tu2, imposed label stack {18 24}
  Create time: 00:15:08, last status change time: 00:07:37
  Signaling protocol: LDP, peer 10.16.16.16:0 up
    MPLS VC labels: local 26, remote 24
    Group ID: local 2, remote 0
    MTU: local 4470, remote 4470
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 0, send 0
    byte totals:   receive 0, send 0
    packet drops:  receive 0, send 0
```

Troubleshooting Tips

To debug ATM cell packing, issue the **debug atm cell-packing** command.

Configuring Tunnel Selection Using Commands Associated with L2VPN Protocol-Based Feature

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **template type pseudowire** *name*
4. **encapsulation mpls**
5. **preferred-path** {**interface tunnel** *tunnel-number* | **peer** {*ip-address* | *hostname*}} [**disable-fallback**]
6. **exit**
7. **interface** *type slot* / *subslot* / *port*[**.** *subinterface*]
8. **encapsulation** *encapsulation-type*
9. **end**
10. **interface pseudowire** *number*
11. **source template type pseudowire** *name*
12. **neighbor** *peer-address vcid-value*
13. **end**
14. **l2vpn xconnect context** *context-name*
15. **member pseudowire** *interface-number*
16. **member** *ip-address vc-id* **encapsulation mpls**
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**template type pseudowire** *name* **Example:** `Router(config)# template type pseudowire ts1`	Creates a template pseudowire with a name that you specify and enters pseudowire configuration mode.
Step 4	**encapsulation mpls** **Example:** `Router(config-pw)# encapsulation mpls`	Specifies the tunneling encapsulation. For AToM, the encapsulation type is mpls.
Step 5	**preferred-path** {**interface tunnel** *tunnel-number* | **peer** {*ip-address* | *hostname*}} [**disable-fallback**] **Example:** `Router(config-pw)# preferred path peer 10.18.18.18`	Specifies the MPLS traffic engineering tunnel or IP address or hostname to be used as the preferred path.
Step 6	**exit** **Example:** `Router(config-pw)# exit`	Exits from pseudowire configuration mode and enables the Tunnel Selection feature.
Step 7	**interface** *type slot* / *subslot* / *port*[**.** *subinterface*] **Example:** `Router(config)# interface atm1/1/0`	Specifies an interface type and enters interface configuration mode.
Step 8	**encapsulation** *encapsulation-type* **Example:** `Router(config-if)# encapsulation aal5`	Specifies the encapsulation for the interface.
Step 9	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 10	**interface pseudowire** *number* **Example:** `Router(config)# interface pseudowire 100`	Specifies the pseudowire interface and enters interface configuration mode.
Step 11	**source template type pseudowire** *name* **Example:** `Router(config-if)# source template type pseudowire ts1`	Configures the source template of type pseudowire named ts1.
Step 12	**neighbor** *peer-address vcid-value* **Example:** `Router(config-if)#  neighbor 10.0.0.1 123`	Specifies the peer IP address and virtual circuit (VC) ID value of a Layer 2 VPN (L2VPN) pseudowire.
Step 13	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.
Step 14	**l2vpn xconnect context** *context-name* **Example:** `Router(config)# l2vpn xconnect context con1`	Creates a Layer 2 VPN (L2VPN) cross connect context and enters xconnect configuration mode.
Step 15	**member pseudowire** *interface-number* **Example:** `Router(config-xconnect)# member pseudowire 100`	Specifies a member pseudowire to form a Layer 2 VPN (L2VPN) cross connect.
Step 16	**member** *ip-address vc-id* **encapsulation mpls** **Example:** `Router(config-xconnect)# member 10.0.0.1 123 encapsulation mpls`	Creates the VC to transport the Layer 2 packets.
Step 17	**end** **Example:** `Router(config-xconnect)# end`	Exits to privileged EXEC mode.

Troubleshooting Tips using the commands associated with the L2VPN Protocol-Based CLIs feature

You can use the **debug l2vpn atom vc event** command to troubleshoot tunnel selection. For example, if the tunnel interface that is used for the preferred path is shut down, the default path is enabled. The **debug l2vpn atom vc event** command provides the following output:

```
AToM SMGR [10.2.2.2, 101]: Processing imposition update, vc_handle 62091860, update_action
 3, remote_vc_label 16
AToM SMGR [10.2.2.2, 101]: selected route no parent rewrite: tunnel not up
AToM SMGR [10.2.2.2, 101]: Imposition Programmed, Output Interface: Et3/2
```

Setting Experimental Bits with AToM

Note Only EoMPLS and CEM is supported .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-name*
4. **match any**
5. **policy-map** *policy-name*
6. **class** *class-name*
7. **set mpls experimental** *value*
8. **exit**
9. **exit**
10. **interface** *type slot* / *subslot* / *port*
11. **service-policy input** *policy-name*
12. **end**
13. **show policy-map interface** *interface-name* [*vc* [*vpi* /] *vci*] [**dlci** *dlci*] [**input** | **output**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**class-map** *class-name* **Example:** `Router(config)# class-map class1`	Specifies the user-defined name of the traffic class and enters class map configuration mode.

	Command or Action	Purpose
Step 4	**match any** **Example:** `Router(config-cmap)# match any`	Specifies that all packets will be matched. Use only the **any** keyword. Other keywords might cause unexpected results.
Step 5	**policy-map** *policy-name* **Example:** `Router(config-cmap)# policy-map policy1`	Specifies the name of the traffic policy to configure and enters policy-map configuration mode.
Step 6	**class** *class-name* **Example:** `Router(config-pmap)# class class1`	Specifies the name of a predefined traffic class, which was configured with the **class-map** command, used to classify traffic to the traffic policy and enters policy-map class configuration mode.
Step 7	**set mpls experimental** *value* **Example:** `Router(config-pmap-c)# set mpls experimental 7`	Designates the value to which the MPLS bits are set if the packets match the specified policy map.
Step 8	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map class configuration mode.
Step 9	**exit** **Example:** `Router(config-pmap)# exit`	Exits policy-map configuration mode.
Step 10	**interface** *type slot / subslot / port* **Example:** `Router(config)# interface atm1/0/0`	Specifies the interface type and enters interface configuration mode.
Step 11	**service-policy input** *policy-name* **Example:** `Router(config-if)# service-policy input policy1`	Attaches a traffic policy to an interface.
Step 12	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.
Step 13	**show policy-map interface** *interface-name* [*vc* [*vpi* /] *vci*] [**dlci** *dlci*] [**input** | **output**]	Displays the traffic policy attached to an interface.

	Command or Action	Purpose
	Example: `Router# show policy-map interface serial3/0/0`	

Enabling the Control Word

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class cw_enable**
4. **encapsulation mpls**
5. **control-word**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**pseudowire-class cw_enable** **Example:** `Router(config)# pseudowire-class cw_enable`	Enters pseudowire class configuration mode.
Step 4	**encapsulation mpls** **Example:** `Router(config-pw-class)# encapsulation mpls`	Specifies the tunneling encapsulation. • For AToM, the encapsulation type is MPLS.
Step 5	**control-word** **Example:** `Router(config-pw-class)# control-word`	Enables the control word.
Step 6	**end** **Example:**	Exits to privileged EXEC mode.

	Command or Action	Purpose
	`Router(config-pw-class)# end`	

Enabling the Control Word using the commands associated with the L2VPN Protocol-Based CLIs feature

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface pseudowire** *number*
4. **encapsulation mpls**
5. **control-word include**
6. **neighbor** *peer-address vcid-value*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface pseudowire** *number* **Example:** `Router(config)# interface pseudowire 1`	Creates an interface pseudowire with a value that you specify and enters pseudowire configuration mode.
Step 4	**encapsulation mpls** **Example:** `Router(config-pw)# encapsulation mpls`	Specifies the tunneling encapsulation. • For AToM, the encapsulation type is mpls.
Step 5	**control-word include** **Example:** `Router(config-pw)# control-word include`	Enables the control word.

	Command or Action	Purpose
Step 6	**neighbor** *peer-address vcid-value* **Example:** `Router(config-pw)# neighbor 10.0.0.1 123`	Specifies the peer IP address and virtual circuit (VC) ID value of a Layer 2 VPN (L2VPN) pseudowire.
Step 7	**end** **Example:** `Router(config-pw)# end`	Exits to privileged EXEC mode.

Configuring MPLS AToM Remote Ethernet Port Shutdown

Note The Any Transport over MPLS (AToM): Remote Ethernet Port Shutdown feature is automatically enabled by default when an image with the feature supported is loaded on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulation mpls**
5. **exit**
6. **interface** *type slot / subslot / port*
7. **service instance** *number* **ethernet** *number*
8. **encapsulation** *default*
9. **xconnect** *peer-ip-address vc-id pw-class pw-class-name*
10. **no remote link failure notification**
11. **remote link failure notification**
12. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**pseudowire-class** [*pw-class-name*] **Example:** `Router(config)# pseudowire-class eompls`	Specifies the name of a Layer 2 pseudowire class and enters pseudowire class configuration mode.
Step 4	**encapsulation mpls** **Example:** `Router(config-pw)# encapsulation mpls`	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.
Step 5	**exit** **Example:** `Router(config-pw)# exit`	Exits to global configuration mode.
Step 6	**interface** *type slot / subslot / port* **Example:** `Router (config)# interface GigabitEthernet1/0/0`	Configures an interface type and enters interface configuration mode.
Step 7	**service instance** *number* **ethernet** *number* **Example:** `Router(config-if)# service instance 393 ethernet`	Configures an ethernet service instance on an interface and enters service instance configuration mode.
Step 8	**encapsulation** *default* **Example:** `Router(config-if-srv)# encapsulation default`	Specifies the encapsulation type for the interface, such as dot1q. **Note** Remote ethernet port shutdown is supported only with encapsulation default.
Step 9	**xconnect** *peer-ip-address vc-id pw-class pw-class-name* **Example:** `Router(config-if)# xconnect 10.1.1.1 1 pw-class eompls`	Binds an attachment circuit to a pseudowire, and configures an Any Transport over MPLS (AToM) static pseudowire.
Step 10	**no remote link failure notification** **Example:** `Router(config-if-xconn)# remote link failure notification`	Disables MPLS AToM remote link failure notification and shutdown.
Step 11	**remote link failure notification** **Example:** `Router(config-if-xconn)# remote link failure notification`	Enables MPLS AToM remote link failure notification and shutdown.

	Command or Action	Purpose
Step 12	**end** **Example:** `Router(config-if-xconn)# end`	Exits to privileged EXEC mode.

Configuring MPLS AToM Remote Ethernet Port Shutdown using the commands associated with the L2VPN Protocol-Based CLIs feature

Note The Any Transport over MPLS (AToM): Remote Ethernet Port Shutdown feature is automatically enabled by default when an image with the feature supported is loaded on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **template type pseudowire** [*pseudowire-name*]
4. **encapsulation mpls**
5. **exit**
6. **interface** *type slot / subslot / port*
7. **interface pseudowire** *number*
8. **source template type pseudowire**
9. **neighbor** *peer-address vcid-value*
10. **end**
11. **l2vpn xconnect context** *context-name*
12. **no remote link failure notification**
13. **remote link failure notification**
14. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**template type pseudowire** [*pseudowire-name*] **Example:** `Device(config)# template type pseudowire eompls`	Specifies the name of a Layer 2 pseudowire class and enters pseudowire class configuration mode.
Step 4	**encapsulation mpls** **Example:** `Device(config-pw)# encapsulation mpls`	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.
Step 5	**exit** **Example:** `Device(config-pw)# exit`	Exits to global configuration mode.
Step 6	**interface** *type slot / subslot / port* **Example:** `Device(config)# interface GigabitEthernet1/0/0`	Configures an interface type and enters interface configuration mode.
Step 7	**interface pseudowire** *number* **Example:** `Device(config-if)# interface pseudowire 100`	Specifies the pseudowire interface.
Step 8	**source template type pseudowire** **Example:** `Device(config-if)# source template type pseudowire eompls`	Configures the source template of type pseudowire named eompls.
Step 9	**neighbor** *peer-address vcid-value* **Example:** `Device(config-if)#  neighbor 10.1.1.1 1`	Specifies the peer IP address and virtual circuit (VC) ID value of a Layer 2 VPN (L2VPN) pseudowire.
Step 10	**end** **Example:** `Device(config-if)# end`	Exits to privileged EXEC mode.
Step 11	**l2vpn xconnect context** *context-name* **Example:** `Device(config)# l2vpn xconnect context con1`	Creates a Layer 2 VPN (L2VPN) cross connect context and enters xconnect configuration mode.

	Command or Action	Purpose
Step 12	**no remote link failure notification** **Example:** `Device(config-xconnect)# no remote link failure notification`	Disables MPLS AToM remote link failure notification and shutdown.
Step 13	**remote link failure notification** **Example:** `Device(config-xconnect)# remote link failure notification`	Enables MPLS AToM remote link failure notification and shutdown.
Step 14	**end** **Example:** `Device(config-xconnect)# end`	Exits to privileged EXEC mode.

Configuring Flow-Aware Transport (FAT) Load Balancing

Before you begin

Note that this configuration is applicable only on the NCS 4206 and NCS 4216 systems.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *slot / subslot / port* [**.** *subinterface*]
4. **mtu** *mtu-value*
5. **no ip address** [*ip-address-mask*] [**secondary**]
6. **load-interval** *seconds*
7. **service instance** *id* **ethernet**
8. **encapsulation dot1q** *vlan-id*
9. **rewrite ingress tag pop** *number* [**symmetric**]
10. **enable**
11. **configure terminal**
12. **interface pseudowire** *name*
13. **encapsulation mpls**
14. **neighbor** *peer-address vcid-value*
15. **signaling protocol ldp**
16. **load-balance flow-label both**
17. **l2vpn xconnect context** *context-name*
18. **member pseudowire** *interface-number* **group** *context-name* **priority** *number*
19. **member TenGigabitEthernet** *interface-number* **service-instance** *id*
20. **end**

21. **show l2vpn atom vc detail**
22. **show ssm id**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *slot* / *subslot* / *port* [. *subinterface*] **Example:** `Device(Config)# interface tengigabitethernet0/5/2`	Specifies the interface type and enters interface configuration mode.
Step 4	**mtu** *mtu-value* **Example:** `Device(Config-if)# mtu 9216`	Specifies the MTU value for the interface. The MTU value specified at the interface level can be inherited by a subinterface.
Step 5	**no ip address** [*ip-address-mask*] [**secondary**] **Example:** `Device(Config-if)# no ip address`	Disables IP processing.
Step 6	**load-interval** *seconds* **Example:** `Device(Config-if)# load-interval 30`	Enables the length of time for which data is used to compute load statistics.
Step 7	**service instance** *id* **ethernet** **Example:** `Device(Config-if)# service instance 1 ethernet`	Configures an Ethernet service instance on an interface and enters service instance configuration mode.
Step 8	**encapsulation dot1q** *vlan-id* **Example:** `Device(Config-if-srv)# encapsulation dot1q 1`	Defines the matching criteria to map 802.1Q frames ingress on an interface to the appropriate service instance.

	Command or Action	Purpose
Step 9	**rewrite ingress tag pop** *number* [**symmetric**] **Example:** `Device(Config-if-srv)# rewrite ingress tag pop 1 symmetric`	(Optional) Specifies the encapsulation adjustment to be performed on a frame ingressing a service instance and the tag to be removed from a packet.
Step 10	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 11	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 12	**interface pseudowire** *name* **Example:** `Device(config)# interface pseudowire 1`	Establishes a pseudowire with a name that you specify, and enters pseudowire class configuration mode.
Step 13	**encapsulation mpls** **Example:** `Device(config-pw-class)# encapsulation mpls`	Specifies the tunneling encapsulation. • For AToM, the encapsulation type is mpls.
Step 14	**neighbor** *peer-address vcid-value* **Example:** `Device(config-pw-class)# neighbor 4.4.4.4 1`	Specifies the peer IP address and virtual circuit (VC) ID value of a Layer 2 VPN (L2VPN) pseudowire.
Step 15	**signaling protocol ldp** **Example:** `Device(config-pw-class)# signaling protocol ldp`	Specifies that the Label Distribution Protocol (LDP) is configured for the pseudowire class.
Step 16	**load-balance flow-label both** **Example:** `Device(config-pw-class)# load-balance flow-label both`	Enables the Flow-Aware Transport of MPLS Pseudowire feature and specifies how flow labels are used. We recommended that you use both as the option for flow-label. However, if you choose not to use both, you can either use **load-balance flow-label transmit** or **load-balance flow-label receive** if necessary.
Step 17	**l2vpn xconnect context** *context-name* **Example:** `Device(config-pw-class)# l2vpn xconnect context FAT1`	Creates a Layer 2 VPN (L2VPN) cross connect context and enters xconnect configuration mode.

	Command or Action	Purpose
Step 18	**member pseudowire** *interface-number* **group** *context-name* **priority** *number* **Example:** `Device(config-pw-class)# member pseudowire 1 group FAT1 priority 1`	Specifies a member pseudowire to form a Layer 2 VPN (L2VPN) cross connect.
Step 19	**member TenGigabitEthernet** *interface-number* **service-instance** *id* **Example:** `Device(config-pw-class)# member TenGigabitEthernet0/5/2 service-instance 1`	Specifies the location of the Gigabit Ethernetmember interface.
Step 20	**end** **Example:** `Device(config-pw-class)# end`	Exits to privileged EXEC mode.
Step 21	**show l2vpn atom vc detail** **Example:** `Device# show l2vpn atom vc detail`	Displays detailed output that shows information about the flow labels configured for the pseudowire.
Step 22	**show ssm id** **Example:** `Device# show ssm id`	Displays information for all Segment Switching Manager (SSM) IDs.

Examples

The following is sample output from the **show mpls l2transport vc detail** command that shows information about the VC details:

```
Device# show mpls l2transport vc 1 detail

Local interface: Te0/5/2 up, line protocol up, Eth VLAN 1 up
  Interworking type is Ethernet
  Destination address: 4.4.4.4, VC ID: 1, VC status: up
    Output interface: BD12, imposed label stack {23 16}
    Preferred path: not configured
    Default path: active
    Next hop: 12.0.0.2
  Create time: 23:12:54, last status change time: 23:09:05
    Last label FSM state change time: 23:09:02
  Signaling protocol: LDP, peer 4.4.4.4:0 up
    Targeted Hello: 1.1.1.1(LDP Id) -> 4.4.4.4, LDP is UP
    Graceful restart: configured and enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
```

```
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 27, remote 16
    Group ID: local 8, remote 8
    MTU: local 9216, remote 9216
    Remote interface description:
  Sequencing: receive disabled, send disabled
  Control Word: On
  SSO Descriptor: 4.4.4.4/1, local label: 27
  Dataplane:
    SSM segment/switch IDs: 32870/4116 (used), PWID: 1
  VC statistics:
    transit packet totals: receive 0, send 0
    transit byte totals:   receive 0, send 0
    transit packet drops:  receive 0, seq error 0, send 0
```

The following is sample output from the **show ssm id** command that shows information for all Segment Switching Manager (SSM) IDs:

```
Device# show ssm id

SSM Status: 1 switch
  Switch-ID 4116 State: Open
    Segment-ID: 168039 Type: Vlan[3]
      Switch-ID:                    4116
      Physical intf:                Local
      Allocated By:                 This CPU
      Locked By:                    SIP     [1]
      Circuit status:               UP      [1]
    Class:                        SSS
      State:                        Active
      AC Switching Context:         Te0/5/2
      SSS Info : Switch Handle 2365587479 Ckt 0x458088DC
      Interworking Eth, Encap Len 4, Boardencap Len 0, MTU 9216,
      AC Encap [4 bytes]
        8100 0001
    Class:                        ADJ
      State:                        Active
      AC Adjacency context:
      adjacency = 0x45817160 [complete] RAW TenGigabitEthernet0/5/2:1
      AC Encap [4 bytes]
        8100 0001
      1stMem: 168039 2ndMem: 0 ActMem: 168039

    Segment-ID: 32870 Type: AToM[17]
      Switch-ID:                    4116
      Allocated By:                 This CPU
      Locked By:                    SIP     [1]
    Class:                        SSS
      State:                        Active
    Class:                        ADJ
      State:                        Active
```

Limitations of FAT-PW

- Load balance does not work when flow-aware transport pseudowire is configured with remote loop-free alternate and loop-free alternate configurations with Cisco IOS XE Everest 16.5.1 release version.
- Flow-label generation algorithm is modified if the Port-channel hashing algorithm is modified using command line interface.
- Starting Cisco IOS XE Fuji 16.9.x, Flow aware transport feature (FAT) is supported on VPLS on the RSP3 module.

Configuration Examples for Any Transport over MPLS

Example: ATM over MPLS

The table below shows the configuration of ATM over MPLS on two PE routers.

Table 2: ATM over MPLS Configuration Example

PE1	PE2
mpls label protocol ldp mpls ldp router-id Loopback0 force ! interface Loopback0 ip address 10.16.12.12 255.255.255.255 ! interface ATM4/0/0 pvc 0/100 l2transport encapsulation aal0 xconnect 10.13.13.13 100 encapsulation mpls ! interface ATM4/0/0.300 point-to-point no ip directed-broadcast no atm enable-ilmi-trap pvc 0/300 l2transport encapsulation aal0 xconnect 10.13.13.13 300 encapsulation mpls	mpls label protocol ldp mpls ldp router-id Loopback0 force ! interface Loopback0 ip address 10.13.13.13 255.255.255.255 interface ATM4/0/0 pvc 0/100 l2transport encapsulation aal0 xconnect 10.16.12.12 100 encapsulation mpls ! interface ATM4/0/0.300 point-to-point no ip directed-broadcast no atm enable-ilmi-trap pvc 0/300 l2transport encapsulation aal0 xconnect 10.16.12.12 300 encapsulation mpls

Example: Ethernet over MPLS with MPLS Traffic Engineering Fast Reroute

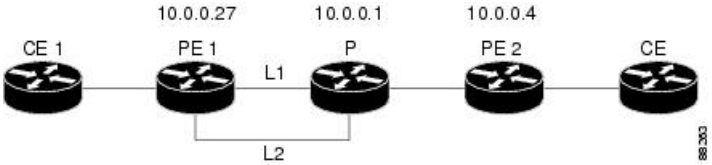
The following configuration example and the figure show the configuration of Ethernet over MPLS with fast reroute on AToM PE routers.

Routers PE1 and PE2 have the following characteristics:

- A TE tunnel called Tunnel41 is configured between PE1and PE2, using an explicit path through a link called L1. AToM VCs are configured to travel through the FRR-protected tunnel Tunnel41.
- The link L1 is protected by FRR, the backup tunnel is Tunnel1.

- PE2 is configured to forward the AToM traffic back to PE1 through the L2 link.

Figure 4: Fast Reroute Configuration



PE1 Configuration

```
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
pseudowire-class T41
 encapsulation mpls
 preferred-path interface Tunnel41 disable-fallback
!
pseudowire-class IP1
 encapsulation mpls
 preferred-path peer 10.4.0.1 disable-fallback
!
interface Loopback1
 ip address 10.0.0.27 255.255.255.255
!
interface Tunnel1
 ip unnumbered Loopback1
 tunnel destination 10.0.0.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 10000
 tunnel mpls traffic-eng path-option 1 explicit name FRR
!
interface Tunnel41
 ip unnumbered Loopback1
 tunnel destination 10.0.0.4
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name name-1
 tunnel mpls traffic-eng fast-reroute
!
interface POS0/0/0
 description pe1name POS8/0/0
 ip address 10.1.0.2 255.255.255.252
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel1
 crc 16
 clock source internal
 pos ais-shut
 pos report lrdi
 ip rsvp bandwidth 155000 155000
!
interface POS0/3/0
 description pe1name POS10/1/0
 ip address 10.1.0.14 255.255.255.252
 mpls traffic-eng tunnels
 crc 16
 clock source internal
```

```
 ip rsvp bandwidth 155000 155000
!
interface gigabitethernet3/0/0.1
 encapsulation dot1Q 203
 xconnect 10.0.0.4 2 pw-class IP1
!
interface gigabitethernet3/0/0.2
 encapsulation dot1Q 204
 xconnect 10.0.0.4 4 pw-class T41
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
!
ip classless
ip route 10.4.0.1 255.255.255.255 Tunnel41
!
ip explicit-path name xxxx-1 enable
 next-address 10.4.1.2
 next-address 10.1.0.10
```

P Configuration

```
ip cef
mpls traffic-eng tunnels
!
interface Loopback1
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet1/0/0
 ip address 10.4.1.2 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 10000 10000
!
interface POS8/0/0
 description xxxx POS0/0
 ip address 10.1.0.1 255.255.255.252
 mpls traffic-eng tunnels
 pos ais-shut
 pos report lrdi
 ip rsvp bandwidth 155000 155000
!
interface POS10/1/0
 description xxxx POS0/3
 ip address 10.1.0.13 255.255.255.252
 mpls traffic-eng tunnels
 ip rsvp bandwidth 155000 155000
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
```

PE2 Configuration

```
ip cef
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
```

```
interface Loopback1
 ip address 10.0.0.4 255.255.255.255
!
interface loopback 2
ip address 10.4.0.1 255.255.255.255
!
interface Tunnel27
 ip unnumbered Loopback1
 tunnel destination 10.0.0.27
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name xxxx-1
!
interface FastEthernet0/0/0.2
 encapsulation dot1Q 203
 xconnect 10.0.0.27 2 encapsulation mpls
!
interface FastEthernet0/0/0.3
 encapsulation dot1Q 204
 xconnect 10.0.0.27 4 encapsulation mpls
!
interface FastEthernet1/1/0
 ip address 10.4.1.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 10000 10000
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
!
ip explicit-path name xxxx-1 enable
 next-address 10.4.1.2
 next-address 10.1.0.10
```

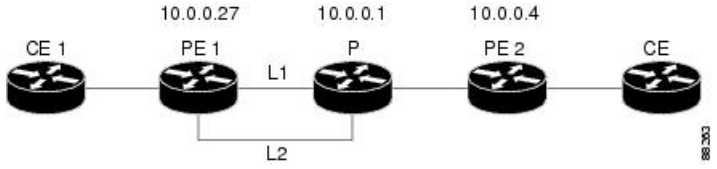
Example: Ethernet over MPLS with MPLS Traffic Engineering Fast Reroute Using Commands Associated with L2VPN Protocol-Based Feature

The following configuration example and the figure show the configuration of Ethernet over MPLS with fast reroute on AToM PE routers.

Routers PE1 and PE2 have the following characteristics:

- A TE tunnel called Tunnel41 is configured between PE1and PE2, using an explicit path through a link called L1. AToM VCs are configured to travel through the FRR-protected tunnel Tunnel41.
- The link L1 is protected by FRR, the backup tunnel is Tunnel1.
- PE2 is configured to forward the AToM traffic back to PE1 through the L2 link.

Figure 5: Fast Reroute Configuration



PE1 Configuration

```
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
template type pseudowire T41
 encapsulation mpls
 preferred-path interface Tunnel41 disable-fallback
!
template type pseudowire IP1
 encapsulation mpls
 preferred-path peer 10.4.0.1 disable-fallback
!
interface Loopback1
 ip address 10.0.0.27 255.255.255.255
!
interface Tunnel1
 ip unnumbered Loopback1
 tunnel destination 10.0.0.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 10000
 tunnel mpls traffic-eng path-option 1 explicit name FRR
!
interface Tunnel41
 ip unnumbered Loopback1
 tunnel destination 10.0.0.4
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name name-1
 tunnel mpls traffic-eng fast-reroute
!
interface POS0/0/0
 description pe1name POS8/0/0
 ip address 10.1.0.2 255.255.255.252
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel1
 crc 16
 clock source internal
 pos ais-shut
 pos report lrdi
 ip rsvp bandwidth 155000 155000
!
interface POS0/3/0
 description pe1name POS10/1/0
 ip address 10.1.0.14 255.255.255.252
 mpls traffic-eng tunnels
 crc 16
 clock source internal
 ip rsvp bandwidth 155000 155000
!
interface gigabitethernet3/0/0.1
 encapsulation dot1Q 203
 interface pseudowire 100
 source template type pseudowire T41
 neighbor 10.0.0.4 2
!
l2vpn xconnect context con1
!
interface gigabitethernet3/0/0.2
 encapsulation dot1Q 204
```

```
 interface pseudowire 100
 source template type pseudowire IP1
 neighbor 10.0.0.4 4
!
l2vpn xconnect context con2
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
!
ip classless
ip route 10.4.0.1 255.255.255.255 Tunnel41
!
ip explicit-path name xxxx-1 enable
 next-address 10.4.1.2
 next-address 10.1.0.10
```

P Configuration

```
ip cef
mpls traffic-eng tunnels
!
interface Loopback1
 ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet1/0/0
 ip address 10.4.1.2 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 10000 10000
!
interface POS8/0/0
 description xxxx POS0/0
 ip address 10.1.0.1 255.255.255.252
 mpls traffic-eng tunnels
 pos ais-shut
 pos report lrdi
 ip rsvp bandwidth 155000 155000
!
interface POS10/1/0
 description xxxx POS0/3
 ip address 10.1.0.13 255.255.255.252
 mpls traffic-eng tunnels
 ip rsvp bandwidth 155000 155000
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
```

PE2 Configuration

```
ip cef
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
interface Loopback1
 ip address 10.0.0.4 255.255.255.255
!
interface loopback 2
```

```
ip address 10.4.0.1 255.255.255.255
!
interface Tunnel27
 ip unnumbered Loopback1
 tunnel destination 10.0.0.27
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name xxxx-1
!
interface FastEthernet0/0/0.2
 encapsulation dot1Q 203
 interface pseudowire 100
 encapsulation mpls
 neighbor 10.0.0.1 123
!
l2vpn xconnect context A
 member pseudowire 100
 member gigabitethernet 0/0/0.1
!
interface FastEthernet0/0/0.3
 encapsulation dot1Q 204
 interface pseudowire 100
 encapsulation mpls
 neighbor 10.0.0.1 123
!
l2vpn xconnect context A
 member pseudowire 100
 member gigabitethernet 0/0/0.1
!
interface FastEthernet1/1/0
 ip address 10.4.1.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 10000 10000
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback1
 mpls traffic-eng area 0
!
ip explicit-path name xxxx-1 enable
 next-address 10.4.1.2
 next-address 10.1.0.10
```

Example: Configuring Tunnel Selection

The following example shows how to set 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.

PE1 Configuration

```
mpls label protocol ldp
mpls traffic-eng tunnels
tag-switching tdp 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 FastEthernet2/0/1
 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
```

PE2 Configuration

```
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 FastEthernet1/1/0
 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 FastEthernet1/1/1
 no ip address
 no ip directed-broadcast
 no cdp enable
!
interface FastEthernet1/1/1.1
 encapsulation dot1Q 222
 no ip directed-broadcast
 no cdp enable
 mpls l2transport route 10.2.2.2 101
!
interface ATM5/0/0
 no ip address
 no ip directed-broadcast
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 pvc 0/50 l2transport
  encapsulation aal5
  xconnect 10.2.2.2 150 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
```

Example: Configuring Tunnel Selection Using Commands Associated with L2VPN Protocol-Based Feature

The following example shows how to set 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.

PE1 Configuration

```
mpls label protocol ldp
```

```
mpls traffic-eng tunnels
tag-switching tdp router-id Loopback0
template type pseudowire pw1
 encapsulation mpls
 preferred-path interface Tunnel1 disable-fallback
!
template type pseudowire 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
 interface pseudowire 100
 source template type pseudowire pw1
  neighbor 10.16.16.16 101
!
l2vpn xconnect context con1
!
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
 interface pseudowire 100
 source template type pseudowire pw2
 neighbor 10.16.16.16 150
!
l2vpn xconnect context con1
!
interface FastEthernet2/0/1
 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
```

PE2 Configuration

```
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 FastEthernet1/1/0
 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 FastEthernet1/1/1
 no ip address
 no ip directed-broadcast
 no cdp enable
!
interface FastEthernet1/1/1.1
 encapsulation dot1Q 222
 no ip directed-broadcast
 no cdp enable
 mpls l2transport route 10.2.2.2 101
!
interface ATM5/0/0
 no ip address
 no ip directed-broadcast
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 pvc 0/50 l2transport
  encapsulation aal5
  interface pseudowire 100
   encapsulation mpls
   neighbor 10.2.2.2 150
!
l2vpn xconnect context A
  member pseudowire 100
  member GigabitEthernet0/0/0.1
```

```
!
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
```

Example: Configuring MTU Values in xconnect Configuration Mode for L2VPN Interworking

The following example shows an L2VPN Interworking example. The PE1 router has a serial interface configured with an MTU value of 1492 bytes. The PE2 router uses xconnect configuration mode to set a matching MTU of 1492 bytes, which allows the two routers to form an interworking VC. If the PE2 router did not set the MTU value in xconnect configuration mode, the interface would be set to 1500 bytes by default and the VC would not come up.

Note L2VPN interworking is not supported on Cisco ASR 900 RSP3 Module.

PE1 Configuration

```
pseudowire-class atom-ipiw
 encapsulation mpls
 interworking ip
!
interface Loopback0
 ip address 10.1.1.151 255.255.255.255
!
interface Serial2/0/0
 mtu 1492
 no ip address
 encapsulation ppp
 no fair-queue
 serial restart-delay 0
 xconnect 10.1.1.152 123 pw-class atom-ipiw
!
interface Serial4/0/0
 ip address 10.151.100.1 255.255.255.252
 encapsulation ppp
 mpls ip
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.151 0.0.0.0 area 0
 network 10.151.100.0 0.0.0.3 area 0
!
mpls ldp router-id Loopback0
```

PE2 Configuration

```
pseudowire-class atom-ipiw
 encapsulation mpls
 interworking ip
```

```
!
interface Loopback0
 ip address 10.1.1.152 255.255.255.255
!
interface FastEthernet0/0/0
 no ip address
 xconnect 10.1.1.151 123 pw-class atom-ipiw
  mtu 1492
!
interface Serial4/0/0
 ip address 10.100.152.2 255.255.255.252
 encapsulation ppp
 mpls ip
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.152 0.0.0.0 area 0
 network 10.100.152.0 0.0.0.3 area 0
!
mpls ldp router-id Loopback0
```

The **show mpls l2transport binding** command shows that the MTU value for the local and remote routers is 1492 bytes.

PE1

```
Router# show mpls l2transport binding
Destination Address: 10.1.1.152,  VC ID: 123
    Local Label: 105
        Cbit: 1,    VC Type: PPP,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
    Remote Label: 205
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
Router# show mpls l2transport vc detail
Local interface: Serial2/0/0 up, line protocol up, PPP up
  MPLS VC type is PPP, interworking type is IP
  Destination address: 10.1.1.152, VC ID: 123, VC status: up
    Output interface: Serial4/0/0, imposed label stack {1003 205}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:25:29, last status change time: 00:24:54
  Signaling protocol: LDP, peer 10.1.1.152:0 up
    Targeted Hello: 10.1.1.151(LDP Id) -> 10.1.1.152
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 105, remote 205
    Group ID: local n/a, remote 0
    MTU: local 1492, remote 1492
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
```

```
    packet totals: receive 30, send 29
    byte totals:   receive 2946, send 3364
    packet drops:  receive 0, send 0
```

PE2

```
Router# show mpls l2transport binding
Destination Address: 10.1.1.151,  VC ID: 123
    Local Label: 205
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
    Remote Label: 105
        Cbit: 1,    VC Type: FastEthernet,    GroupID: 0
        MTU: 1492,   Interface Desc: n/a
        VCCV: CC Type: CW [1], RA [2]
              CV Type: LSPV [2]
Router# show mpls l2transport vc detail
Local interface: Fe0/0/0 up, line protocol up, FastEthernet up
  MPLS VC type is FastEthernet, interworking type is IP
  Destination address: 10.1.1.151, VC ID: 123, VC status: up
    Output interface: Se4/0/0, imposed label stack {1002 105}
    Preferred path: not configured
    Default path: active
    Next hop: point2point
  Create time: 00:25:19, last status change time: 00:25:19
  Signaling protocol: LDP, peer 10.1.1.151:0 up
    Targeted Hello: 10.1.1.152(LDP Id) -> 10.1.1.151
    Status TLV support (local/remote)   : enabled/supported
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: no fault
      Last local SSS circuit status rcvd: no fault
      Last local SSS circuit status sent: no fault
      Last local  LDP TLV    status sent: no fault
      Last remote LDP TLV    status rcvd: no fault
    MPLS VC labels: local 205, remote 105
    Group ID: local n/a, remote 0
    MTU: local 1492, remote 1492
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 29, send 30
    byte totals:   receive 2900, send 3426
    packet drops:  receive 0, send 0
```

Examples: Configuring Any Transport over MPLS (AToM) Remote Ethernet Port Shutdown

The following example shows how to enable remote Ethernet port shutdown:

```
configure terminal
!
pseudowire-class eompls
 encapsulation mpls
!
interface GigabitEthernet1/0/0
 xconnect 10.1.1.1 1 pw-class eompls
  remote link failure notification
```

The following example shows how to disable remote Ethernet port shutdown:

```
configure terminal
!
pseudowire-class eompls
 encapsulation mpls
!
interface GigabitEthernet1/0/0
 xconnect 10.1.1.1 1 pw-class eompls
  no remote link failure notification
```

The related **show** command output reports operational status for all remote L2 Tunnels by interface.

```
Router# show interface G1/0/0
GigabitEthernet1/0/0 is L2 Tunnel remote down, line protocol is up
Hardware is GigMac 4 Port GigabitEthernet, address is 0003.ff4e.12a8 (bia 0003.ff4e.12a8)
  Internet address is 10.9.9.2/16
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec, rely 255/255, load 1/255
Router# show ip interface brief
Interface              IP-Address      OK? Method Status Protocol
GigabitEthernet2/0/0 unassigned      YES NVRAM  L2 Tunnel remote down up
GigabitEthernet2/1/0 unassigned      YES NVRAM  administratively down down
```

Note Remote Ethernet port shutdown is enabled by default when EVC "default encapsulation" is configured.

Examples: Configuring Any Transport over MPLS (AToM) Remote Ethernet Port Shutdown Using Commands Associated with L2VPN Protocol-Based Feature

The following example shows how to enable remote Ethernet port shutdown:

```
configure terminal
!
template type pseudowire eompls
 encapsulation mpls
!
interface GigabitEthernet1/0/0
interface pseudowire 100
 source template type pseudowire eompls
 neighbor 10.1.1.1 1
!
l2vpn xconnect context con1
 remote link failure notification
```

The following example shows how to disable remote Ethernet port shutdown:

```
configure terminal
!
template type pseudowire eompls
 encapsulation mpls
!
interface GigabitEthernet1/0/0
 interface pseudowire 100
 source template type pseudowire eompls
 neighbor 10.1.1.1 1
!
```

```
l2vpn xconnect context con1
 no remote link failure notification
```

The related **show** command output reports operational status for all remote L2 Tunnels by interface.

```
Router# show interface G1/0/0
GigabitEthernet1/0/0 is L2 Tunnel remote down, line protocol is up
Hardware is GigMac 4 Port GigabitEthernet, address is 0003.ff4e.12a8 (bia 0003.ff4e.12a8)
  Internet address is 10.9.9.2/16
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec, rely 255/255, load 1/255
Router# show ip interface brief
Interface              IP-Address      OK? Method Status Protocol
GigabitEthernet2/0/0 unassigned      YES NVRAM  L2 Tunnel remote down up
GigabitEthernet2/1/0 unassigned      YES NVRAM  administratively down down
```

Additional References for Any Transport over MPLS

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference

Technical Assistance

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

Feature Information for Any Transport over MPLS

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

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

Table 3: Feature Information for Any Transport over MPLS

Feature Name	Releases	Feature Information
Any Transport over MPLS (AToM)	Cisco IOS XE Release 3.18SP	This feature was introduced on the NCS 4200 Series.