MPLS Pseudowire for Cable L2VPN

The Multiprotocol Label Switching (MPLS) Pseudowire for Cable Layer 2 Virtual Private Network (L2VPN) feature enables service providers to use a single, converged, Internet Protocol (IP)/MPLS network infrastructure to offer Ethernet data link layer (Layer 2) connectivity to two or more VPN customer sites.

- Finding Feature Information, on page 1
- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 1
- Prerequisites for MPLS Pseudowire for Cable L2VPN, on page 3
- Restrictions for MPLS Pseudowire for Cable L2VPN, on page 3
- Information About MPLS Pseudowire for Cable L2VPN, on page 3
- L2VPN Pseudowire Redundancy, on page 7
- MPLS Pseudowire Provisioning Methods, on page 7
- How to Enable MPLS on a Cisco CMTS Router, on page 11
- How to Provision MPLS Pseudowires, on page 16
- How to Configure L2VPN Pseudowire Redundancy, on page 17
- Configuration Examples for MPLS Pseudowire for Cable L2VPN, on page 21
- Verifying the MPLS Pseudowire Configuration, on page 27
- Additional References, on page 30
- Feature Information for MPLS Pseudowire for Cable L2VPN, on page 31

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Note Do not use DPICs (8X10G and 2x100G) to forward IP traffic, as it may cause buffer exhaustion, leading to line card reload.

The only allowed traffic on a DPIC interface is DEPI, UEPI, and GCP traffic from the Cisco cBR-8 router to Remote PHY devices. Other traffic such as DHCP, SSH, and UTSC should flow via another router, since DPICs cannot be used for normal routing.

Prerequisites for MPLS Pseudowire for Cable L2VPN

- Enable Baseline Privacy Interface Plus (BPI+) to provide a simple data encryption scheme to protect data sent to and from cable modems in a data over cable network.
- Enable Cisco Express Forwarding (CEF) to optimize network performance.
- Ensure that the primary and backup pseudowires on the remote provider edge (PE) routers have the same pseudowire type as the Cisco cable modem termination system (CMTS).
- Create the remote pseudowire using a pw-class with VLAN as the interworking for remote PEs, if the CMTS is using VLAN as pseudowire type.

Restrictions for MPLS Pseudowire for Cable L2VPN

The following are the general restrictions for the MPLS Pseudowire for Cable L2VPN feature:

- Supports only Ethernet over MPLS (EoMPLS) pseudowires per RFC 4448.
- Supports only point-to-point forwarding. Ethernet switching is not supported.
- Requires DOCSIS 2.0, 3.0 and 3.1-certified cable modems (CMs). This feature is not supported on DOCSIS 1.0-certified cable modems.
- Supports a maximum of four VPNs per cable modem.
- Supports a maximum of eight upstream service flows and eight downstream classifiers.
- Supports a maximum of 16000 EoMPLS pseudowires per Cisco CMTS router.
- Requires the backup pseudowire to be up on the remote PE for the Cisco CMTS to switchover.
- Requires the backup pseudowire to become active on the Cisco CMTS only after the primary pseudowire fails.
- Supports 2000 Bytes MTU (default value) on remote interface for DOCSIS 3.1 cable modem.

Note The CLI-based (static provisioning) L2VPN supports traffic forwarding to VPN only on primary upstream and downstream service flows. Hence only primary upstream and downstream service flows must be configured in the cable modem configuration file.

Information About MPLS Pseudowire for Cable L2VPN

The MPLS Pseudowire for Cable L2VPN feature enables Ethernet-based Layer 2 VPN service over an MPLS network by encapsulating and transmitting the Layer 2 protocol data units (PDUs) over pseudowires (PWs). This feature enables service providers to offer site-to-site connectivity to their business and enterprise customers.

Layer 2 services emulated over an MPLS network are commonly referred to as MPLS-based L2VPNs or MPLS L2VPNs. Subsequently, Ethernet service emulated over an MPLS network is referred to as Ethernet over MPLS (EoMPLS) service.

The MPLS Pseudowire for Cable L2VPN feature is fully compliant with CableLabs Business Services over DOCSIS (BSOD) L2VPN specification, and is an extension to the existing DOCSIS L2VPN features supported on Cisco CMTS routers.

The MPLS Pseudowire for Cable L2VPN feature provides the following capabilities:

- Supports 2000 Bytes MTU (default value) on remote interface for DOCSIS 3.1 cable modems.
- Transport Ethernet frames over an MPLS network.
- Handle a DOCSIS service flow as an attachment circuit that is mapped to an EoMPLS pseudowire.
- Enable the Cisco CMTS router to be the MPLS provider edge (PE) router.
- Enable forwarding of Ethernet frames over DOCSIS (between a CM and a Cisco CMTS router) to MPLS (towards Metropolitan Area Network or Wide Area Network).
- Provide a common framework to encapsulate and transport supported Layer 2 traffic types over an MPLS network.

The MPLS Pseudowire for Cable L2VPN feature differs from the existing DOCSIS L2VPN features such as 802.1q-based L2VPN (L2VPN Support over Cable). The MPLS Pseudowire for Cable L2VPN feature uses IP/MPLS network to transport layer 2 protocol data units (PDUs), whereas 802.1q-based L2VPN feature uses layer 2 Ethernet network to transport PDUs.

How MPLS Transports Layer 2 Packets

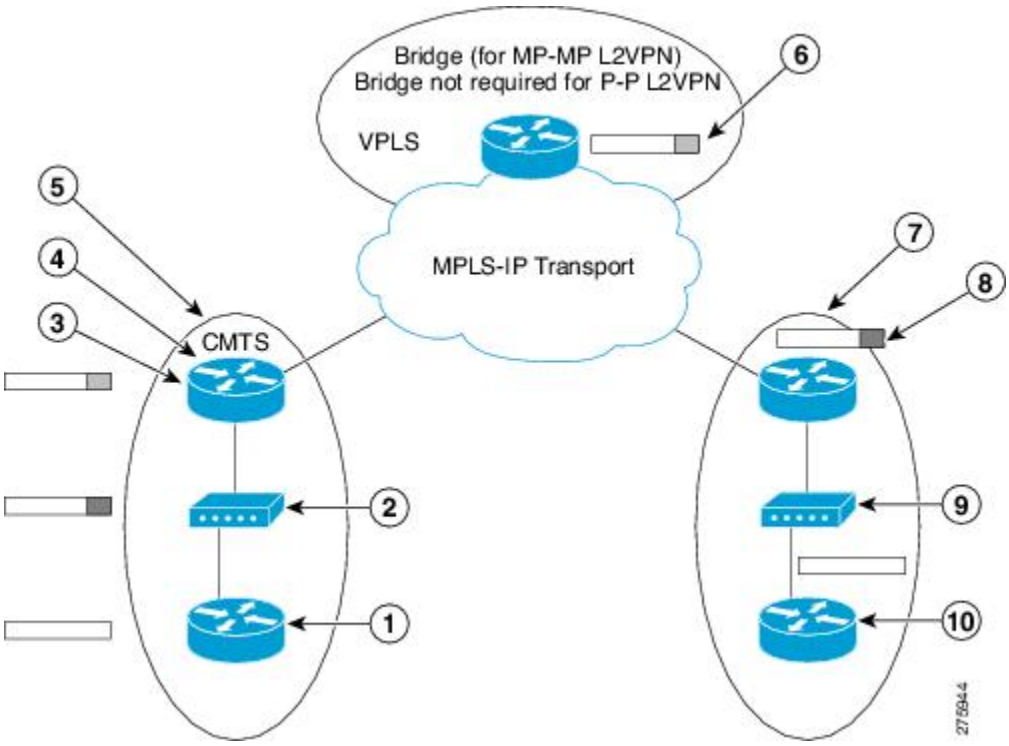
The MPLS subsystem removes DOCSIS encapsulation for Layer 2 Ethernet frames and adds MPLS labels at the ingress provider edge (PE) Cisco CMTS router. Then, the MPLS subsystem sends resulting MPLS packets to the corresponding PE router at the other end of the pseudowire. The PE routers must be configured for successful transmission of IP/MPLS packets between the two PE routers.

The cable modem classifies Ethernet frames from the customer premise equipment (CPE) in the upstream direction using upstream classifiers. Then, a DOCSIS header is added to these frames, and they are sent on a given upstream service flow with a different service identifier. On the Cisco CMTS router, the upstream packet is classified as an L2VPN packet based on the cable interface and service identifier. The Cisco CMTS router removes the DOCSIS header and adds an MPLS header. An MPLS header contains two MPLS labels: the outer label corresponding to the remote PE router and the inner label corresponding to the pseudowire label. The Cisco CMTS router forwards the MPLS packet towards the remote PE router, which is the other end of the pseudowire, over the MPLS network.

In the downstream direction, the Cisco CMTS router receives MPLS packets having only one MPLS header that contains the label that the Cisco CMTS router previously allocated for the corresponding EoMPLS pseudowire. The Cisco CMTS router uses the MPLS label to identify one of the L2VPN cable modems. Then, the Cisco CMTS router classifies the MPLS packet using the L2VPN downstream classifiers based on MPLS experimental (MPLS-EXP) bits in the MPLS header of the received MPLS packet, and removes the MPLS header. Then, the Cisco CMTS router sends the packet on the classified downstream service flow by adding the DOCSIS header. The cable modem then removes the DOCSIS header and delivers the Ethernet frame to the CPE.

A unique combination of a cable modem MAC address, VPN ID (if present in the CM configuration file), peer IP address, and a virtual circuit ID (VCID) identifies the MPLS pseudowire on the Cisco CMTS router.

Figure 1: Transporting Layer 2 Packets



The table illustrates how MPLS transports Layer 2 packets in a DOCSIS-based cable communications system.

1	A router sends an untagged Ethernet frame.	6	MPLS packets are label switched.
2	A CM adds a DOCSIS header to the frame.	7	The Cisco CMTS router receives an MPLS packet and looks up the MPLS forwarding table using the label value in the MPLS header.
3	The Cisco CMTS router removes the DOCSIS header from the frame.	8	The Cisco CMTS router replaces the MPLS header with DOCSIS header (containing the right SID value).
4	The Cisco CMTS router looks up the Service ID (SID) database using the SID value from the DOCSIS header and finds the MPLS header.	9	The DOCSIS header is removed.
5	The Cisco CMTS router adds the MPLS header to the frame.	10	The Ethernet frame is delivered untagged.

Supported Ethernet Encapsulation on UNI

The Ethernet User-Network Interface (UNI) is the connection between a cable modem and a customer premise equipment such as a router or a switch. The service provider may or may not use any encapsulation on the UNI.

The MPLS Pseudowire for Cable L2VPN feature supports the following transport types on an Ethernet UNI:

- Port-based UNI (independent of any VLAN)—The port-based UNI provides Metro Ethernet Forum (MEF)-defined Ethernet Private Line (EPL) service. In this transport type, an MPLS pseudowire is mapped to the Ethernet port.
- VLAN-based UNI—Ethernet VLAN using 802.1q encapsulation (including stacked VLANs). The VLAN-based UNI provides MEF-defined Ethernet Virtual Private Line (EVPL) service. In this transport type, the MPLS pseudowire is mapped to the 802.1q VLAN.

Note The Ethernet UNI must be attached to the Ethernet port of a cable modem.

Before configuring this feature, you should understand the following concepts:

MPLS Pseudowire

Pseudowire is a point-to-point Layer 2 connection between two PE routers. The MPLS Pseudowire for Cable L2VPN feature supports the following pseudowire types:

- Type-4 pseudowire—This is used to transport only VLAN tagged Layer 2 Ethernet frames.
- Type-5 pseudowire—This is used to transport VLAN tagged and untagged Layer 2 Ethernet frames. This is the default pseudowire type.

Bundle254 Interface

The bundle254 (Bu254) interface is an internal bundle interface on a Cisco CMTS router that is used as a circuit identifier for all MPLS pseudowires. This internal bundle interface is created automatically on a Cisco CMTS router when you enable the MPLS pseudowire functionality using the **cable l2-vpn-service xconnect** command. Only one Bu254 interface is created to handle all the MPLS pseudowires available on the Cisco CMTS router.

The output of the **show xconnect or show cable l2-vpn xconnect command displays** the circuit identifier created by the Cisco CMTS router for all the MPLS pseudowires**.**

Ingress Process

When an upstream packet received from a cable interface of the Cisco CMTS router is identified as an L2VPN packet based on the cable modem interface and Service ID (SID), the packet goes through the ingress process. The ingress process ensures that the DOCSIS header is removed, and an MPLS label header is added to the packet according to the MPLS pseudowire configuration and the packet is sent out from the Ethernet interface of the Cisco CMTS router. The ingress process is also known as the label imposition process.

Egress Process

When a downstream packet received from an Ethernet interface of the Cisco CMTS router is identified as an L2VPN packet by the innermost MPLS label, the packet goes through the egress process. The egress process ensures that the MPLS label header is deleted from the packet and the DOCSIS header is added to the packet. Then the packet is sent out from the cable interface of the Cisco CMTS router. The egress process is also known as the label disposition process.

MPLS Pseudowire Control Plane Process

When an L2VPN-compliant CM registers with a Cisco CMTS router and conveys the L2VPN related parameters to the router, the router follows the standard Label Distribution Protocol (LDP) procedures to set up an Ethernet over MPLS pseudowire with the remote PE router. When the L2VPN-compliant CM goes offline, the Cisco CMTS router brings down the pseudowire as well. If the Cisco CMTS router has no L2VPN-compliant CM registered, then the router tears down the targeted LDP session with the remote PE router.

L2VPN Pseudowire Redundancy

The L2VPN Pseudowire Redundancy feature enables a PE router to detect a pseudowire failure and reroute the Layer 2 service to a backup pseudowire that can continue to provide the service. The pseudowire redundancy can be implemented with either Cisco CMTS or a generic router as the PE router. When the primary pseudowire recovers from the failure, the L2VPN Pseudowire Redundancy feature provides the option to bring back the Layer 2 service to the primary pseudowire.

Each primary pseudowire can have up to three backup pseudowires, with unique priorities. For example, priority one cannot be given to two different pseudowires in the backup list. When the primary pseudowire goes down, the Cisco CMTS sends the traffic to the backup pseudowire with the highest priority. For a successful service transfer, the remote state of the backup pseudowire should already be ‘up’. Only the local state of the active pseudowire will be 'up' when the modem is BPI online. Similarly, if the backup pseudowire is in use, the local state of only that backup pseudowire will be 'up'.

If the active backup pseudowire goes down, the Cisco CMTS will use the next highest backup pseudowire whose remote state is ‘up’. However, the Cisco CMTS will not switchover from the lower priority pseudowire to the higher priority pseudowire when the backup pseudowire with the highest priority comes ‘up’. This is to prevent unnecessary switchovers between the backup pseudowires.

When the primary pseudowire recovers from the failure, the L2VPN Pseudowire Redundancy feature brings back the service to the primary pseudowire, after waiting for the time period set using the backup delay command. The local state of the active backup pseudowire will be marked as ‘down’ after the primary pseudowire comes up.

MPLS Pseudowire Provisioning Methods

The MPLS Pseudowire for Cable L2VPN feature supports the following provisioning methods for pseudowires:

Note Before performing the static or dynamic provisioning of MPLS pseudowires, you must enable MPLS on a Cisco CMTS router.

Static Provisioning Method for MPLS Pseudowires

The static provisioning method requires the MPLS pseudowire to be statically provisioned on the CMTS using the command line interface (CLI). This type of provisioning does not require the CM configuration file to use BSOD L2VPN-compliant TLVs. For details on how to statically provision MPLS pseudowires, see the *Static Provisioning of MPLS Pseudowires*.

Dynamic Provisioning Method for MPLS Pseudowires

The dynamic provisioning method is a CM configuration file-based provisioning method and is the recommended provisioning method for creating MPLS pseudowires. For details on how to dynamically provision MPLS pseudowires, see the Dynamic Provisioning of MPLS Pseudowires, on page 16.

The following are the benefits of dynamic provisioning of pseudowires:

- Multiple VPNs can be specified in a CM configuration file and a pseudowire can be provisioned for each VPN.
- Multiple upstream service flows and downstream classifiers can be associated with each VPN.
- Each upstream service flow can be tagged to an MPLS experimental (EXP) level for the egress WAN traffic.
- Downstream ingress WAN traffic can be classified based on the downstream MPLS-EXP range specified in each downstream classifier.
- The Cisco CMTS router will have finer control of MPLS quality of service (QoS) over cable and WAN interfaces.

For dynamic provisioning of MPLS pseudowires, you use an L2VPN-compliant CM configuration file that is stored on the Trivial File Transfer Protocol (TFTP) server. You use a common CM configuration file editor such as CableLabs Config File Editor, or a sophisticated provisioning backend system such as Broadband Access Center for Cable (BACC) to create CM configuration files.

This provisioning method requires the usage of CableLabs defined L2VPN encodings such as type, length, value (TLV) objects in the CM configuration file. These L2VPN encodings control L2VPN forwarding of upstream and downstream Ethernet frames.

You can specify the L2VPN encodings in the following ways:

- Per CM
- Per downstream classifier
- Per service flow
- Per upstream classifier

Note The CM L2VPN encoding is mandatory.

The CM L2VPN encoding contains many TLVs, out of which the two most important TLVs are VPN Identifier and NSI Encapsulation. To configure an MPLS pseudowire, you must set the NSI Encapsulation to MPLS. The other TLVs are used to specify the pseudowire identifiers in the form of source attachment individual identifier (SAII), target attachment individual identifier (TAII), and attachment group identifier (AGI).

The L2VPN encoding parameter is encoded as a general extension information (GEI) parameter in the CM configuration file. This indicates that the parameter is encoded as a subtype of the vendor-specific information type parameter using the vendor ID (0xFFFFFF).

The table lists the important CableLabs defined TLVs that are used at the top level of the CM configuration file for the MPLS Pseudowire for Cable L2VPN feature. See the BSOD specification, *Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks,* from CableLabs for *a complete list of CableLabs defined TLVs.*

Table 2: CableLabs Defined L2VPN TLVs

TLV Name	Type	Length	Value and Description
Downstream Unencrypted Traffic (DUT) Control	45.1	1	Bit 0 DUT Filtering DUT Filtering = 0: Disable (default) DUT Filtering = 1: Enable DUT Filtering
Downstream Unencrypted Traffic (DUT) CMIM	45.2	N	DUT CMIM (optional) CM Interface Mask (CMIM) limiting outgoing interfaces of DUT traffic. If the DUT CMIM is omitted, its default value includes the eCM and all implemented eSAFE interfaces, but not any CPE interfaces.
VPN Identifier	43.5.1	1 to N	An opaque octet string that identifies an L2VPN. N is vendor- specific, and the valid range is from 6 to 255.
NSI Encapsulation Subtype	43.5.2	n	A single NSI encapsulation format code/length/value tuple. This TLV uses any of the following values: NSI encapsulation = 0 : Other NSI encapsulation = 1 : IEEE 802.1Q (specify VLAN ID) NSI encapsulation = 2 : IEEE 802.1AD (specify Q-in-Q) NSI encapsulation = 3 : MPLS peer (specify IPv4 or IPv6 address) The value must be set to 3 to ensure MPLS pseudowire usage. The address must identify the remote PE (by its IP address assigned to the loopback interface).
Attachment Group ID	43.5.5	0 to 16	Opaque byte string that identifies the CM or SF as an attachment circuit for IETF Layer 2 VPN signaling protocols.
Source Attachment Individual ID	43.5.6	0 to 16	Opaque byte string signaled as SAII circuit for IETF Layer 2 VPN signaling protocols.
Target Attachment Individual ID	43.5.7	0 to 16	Opaque byte string that identifies the CM or SF as an attachment circuit for IETF Layer 2 VPN signaling protocols.
Ingress User Priority	43.5.8	1	Ingress IEEE 802.1 user priority value in the range of 0 to 7 encoded in the least significant three bits. Higher values indicate higher priority.
User Priority Range	43.5.9	2	The lower user priority value of the user priority range is encoded in the least significant three bits of the first byte, and the higher value of the range is encoded in the least significant three bits of the second byte.

Cisco-Specific L2VPN TLVs

Even though CableLabs defined L2VPN TLVs are sufficient for dynamic provisioning of MPLS pseudowires, CMTS operators can use Cisco-specific TLVs at the top level of the CM configuration file to enable additional functions.

This table lists the new Cisco-specific TLVs that are defined for the MPLS Pseudowire for Cable L2VPN feature.

Table 3: Cisco-Specific L2VPN TLVs

TLV Name	Type	Length	Value	Description
MPLS-PW-TYPE	43.5.43.36	1	• 4 = Type-4 Ethernet VLAN • 5 = Type-5 Ethernet port	The Cisco CMTS router interprets this subtype as MPLS pseudowire type (Type-4 or Type-5). If this TLV value is not specified, then the router accepts the default value (5) for Type-5.
MPLS-VCID	43.5.43.38	4	4 bytes unsigned number = MPLS VCID	This subtype is interpreted as MPLS VCID. This TLV is ignored, and the value of TAII is used as VCID for the pseudowire, if the following conditions are met: • The CableLabs BSOD specification-compliant TLVs, SAII and TAII, are present in the CM configuration file. • Both are of 4 bytes length. • Value of SAII is equal to TAII.
MPLS-PEERNAME	43.5.43.39	N	ASCII encoded data	The Cisco CMTS router interprets this optional subtype as MPLS peer name in ASCII encoded data.

This table lists the new Cisco-specific type, length, values (TLVs) that are defined for the L2VPN Pseudowire Redundancy feature.

Table 4: Cisco-Specific L2VPN TLVs for Pseudowire Redundancy

TLV Name	Type	Length	Value	Description
BACKUP-PW	45.5.43.40	N	Backup pseudowire related parameters	The Cisco CMTS router interprets this subtype as related parameters for the MPLS backup pseudowire. This TLV indicates the start of a new backup pseudowire.
BACKUP-PEERIP	43.5.43.40.1	4	IP address of the backup peer (IPv4)	The Cisco CMTS router interprets this optional subtype as the peer IP address of the MPLS backup pseudowire. This TLV is an IPv4 address.
BACKUP-PEERNAME	43.5.43.40.2	N	ASCII encoded data	The Cisco CMTS router interprets this optional subtype as the MPLS backup peer name in ASCII encoded data. This TLV is resolved to IPv4 address through DNS.

TLV Name	Type	Length	Value	Description
BACKUP-MPLS-VCID	43.5.43.40.3	4	4 bytes unsigned number = MPLS VCID for backup pseudowire	The Cisco CMTS router interprets this subtype as the VCID of the backup pseudowire. This TLV is ignored, and the value of TAII is used as the VCID for the pseudowire, if the following conditions are met: • The CableLabs BSOD specification-compliant TLVs, SAII, and TAII, are present in the CM configuration file. • SAII, and TAII are of 4 bytes length. • Value of SAII is equal to TAII.
BACKUP-MPLS-PRIORITY	43.5.43.40.4	1	1 byte unsigned number = priority for the backup pseudowire	The Cisco CMTS router interprets this subtype as the MPLS priority. Each primary pseudowire can have up to three backup pseudowires, with unique priorities. The priority indicates the order in which the CMTS should switch to the backup peer when the primary peer is down.
BACKUP-ENABLE-DELAY	43.5.43.41	1	1 byte unsigned number = number of seconds	The Cisco CMTS router interprets this subtype as the number of seconds the backup pseudowire should wait to take over after the primary pseudowire goes down. If the TLV value is not specified, then the router uses the default value of 0 seconds.
BACKUP-DISABLE-DELAY	43.5.43.42	1	1 byte unsigned number = number of seconds	The Cisco CMTS router interprets this subtype as the number of seconds the primary pseudowire should wait to take over after the remote state of the primary pseudowire comes up. If the TLV value is not specified, then the router uses the default value of 0 seconds.
BACKUP-DISABLE-NEVER	43.5.43.43	1	1 byte unsigned number = never disable backup pseudowire	The Cisco CMTS router interprets this subtype as a flag indicating that the backup pseudowire should not be disabled even after the primary pseudowire comes up. If this TLV is not present, the router takes the default action of reverting back to the primary pseudowire.

How to Enable MPLS on a Cisco CMTS Router

Perform the following tasks in the same order to enable MPLS on a Cisco CMTS router:

Note Before performing the static or dynamic provisioning of MPLS pseudowires, you must enable MPLS on a Cisco CMTS router.

Configuring an LDP Router ID

The **mpls ldp router-id** command allows you to assign an interface IP address as the LDP router ID.

The normal process to determine the LDP router ID is as follows:

1. The router considers all the IP addresses of all operational interfaces.
2. If these addresses include loopback interface addresses, the router selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the router, because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each router is not required.

The loopback IP address is not considered as the router ID of the local LDP ID under the following circumstances:

1. If the loopback interface has been explicitly shut down.
2. If the **mpls ldp router-id** command specifies that a different interface should be used as the LDP router ID.
3. If you use a loopback interface, make sure that the IP address for the loopback interface is configured with a /32 network mask. In addition, ensure that the routing protocol in use is configured to advertise the corresponding /32 network. Otherwise, the router selects the largest interface address.

The router might select a router ID that is not usable in certain situations. For example, the router might select an IP address that the routing protocol cannot advertise to a neighboring router. The router implements the router ID the next time it is necessary to select an LDP router ID. The effect of the **mpls ldp router-id** command is delayed until it is necessary to select an LDP router ID, which is the next time the interface is shut down or the address is deconfigured.

If you use the **force** keyword with the **mpls ldp router-id** command, the router ID takes effect more quickly. However, implementing the router ID depends on the current state of the specified interface:

- If the interface is up (operational) and its IP address is not currently the LDP router ID, the LDP router ID is forcibly changed to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down, the LDP router ID is forcibly changed to the IP address of the interface when the interface transitions to up. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

Before you begin

Ensure that the specified interface is operational before assigning it as the LDP router ID.

Procedure

	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	**mpls ip** **Example:** `Router(config)# mpls ip`	Enables the dynamic MPLS forwarding function on the specified Gigabit Ethernet interface.
Step 4	**mpls ldp router-id loopback** interface-number [**force**] **Example:** `Router(config)# mpls ldp router-id loopback 2030 force`	Specifies the IP address of the loopback interface as the LDP router ID.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Configuring MPLS on a Gigabit Ethernet Interface

MPLS forwarding and Label Distribution Protocol must be enabled on 1-port or 10-port GE interfaces of the Cisco CMTS router to ensure that the router establishes MPLS label-switched path (LSP) to the remote PE routers. This section explains how to enable MPLS forwarding and LDP on a Gigabit Ethernet interface.

Note Configuration steps are similar for 1-port and 10-port GE interfaces.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** slot/subslot/port **Example:** `Router(config)# interface gigabitethernet 3/0/0`	Enters interface cable configuration mode and specifies the Gigabit Ethernet interface.
Step 4	**mpls ip** **Example:** `Router(config-if)# mpls ip`	Enables the dynamic MPLS forwarding function on the specified Gigabit Ethernet interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface cable configuration mode and enters privileged EXEC mode.

Configuring an MPLS Label Distribution Protocol

The MPLS label distribution protocol (LDP) allows the construction of highly scalable and flexible IP VPNs that support multiple levels of services. This section explains how to configure an MPLS label distribution protocol on a Gigabit Ethernet interface.

MPLS LDP graceful-restart may also be configured for faster L2VPN traffic recovery after a LDP session disruption. For more information see the MPLS LDP Graceful Restart guide.

Note Ensure that the loopback interface with the IP address is present on each PE router using the **show ip interface brief** command before configuring an MPLS label distribution protocol. This loopback interface identifies the Cisco CMTS router as the peer IP address of the pseudowire.

Procedure

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

	Command or Action	Purpose
	Example: `Router> enable`	• 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 gigabitethernet 3/0/0`	Enters interface cable configuration mode and specifies the Gigabit Ethernet interface.
Step 4	**mpls label protocol ldp** **Example:** `Router(config-if)# mpls label protocol ldp`	Enables MPLS LDP parameters on the specified Gigabit Ethernet interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface cable configuration mode and enters privileged EXEC mode.

Enabling the Cisco CMTS Support for MPLS Pseudowire for Cable L2VPN

You must enable the MPLS tunnel traffic on the network side of the interface to support configuration of MPLS pseudowires on a Cisco CMTS router.

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**cable l2-vpn-service xconnect nsi mpls** **Example:** `Router(config)# cable l2-vpn-service xconnect nsi mpls`	Enables the MPLS tunnel traffic, where:
Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Customize MTU

You can extend the MTU to a maximum of 2000 B, which is the default value on a remote interface for DOCSIS 3.1 cable modem.

Use the following commands to customize and configure the MTU:

- To configure the MTU globally, run the following command:

```
router(config)#cable l2-vpn-service xconnect extended-mtu ?
  <1500-2000>  Customized MTU
  <cr>
```

- To configure the MTU for each session, run the following command:

```
router(config-ethsrv)#xconnect 2.2.2.2 2000 encapsulation mpls extended-mtu ?
  <1500-2000>  in bytes without L2 overhead
```

How to Provision MPLS Pseudowires

You can provision MPLS pseudowires in the following ways:

Note Before performing the static or dynamic provisioning of MPLS pseudowires, you must enable MPLS on a Cisco CMTS router. See How to Enable MPLS on a Cisco CMTS Router, on page 11.

Dynamic Provisioning of MPLS Pseudowires

The dynamic provisioning method supports the following types of configurations:

- BSOD Specification-Based MPLS Pseudowire Provisioning

- Type-4 MPLS Pseudowire Provisioning Using the CM Configuration File
- Type-5 MPLS Pseudowire Provisioning Using the CM Configuration File

See the Configuration Examples for Dynamic Provisioning of MPLS Pseudowires for details about the dynamic provisioning method using the CM configuration file.

Note We recommend that you use the dynamic provisioning method instead of the static provisioning method for MPLS pseudowires.

Static Provisioning Method for MPLS Pseudowires

The static provisioning method requires the MPLS pseudowire to be statically provisioned on the CMTS using the command line interface (CLI). This type of provisioning does not require the CM configuration file to use BSOD L2VPN-compliant TLVs. For details on how to statically provision MPLS pseudowires, see the *Static Provisioning of MPLS Pseudowires*.

How to Configure L2VPN Pseudowire Redundancy

The L2VPN Pseudowire Redundancy feature enables you to switch to backup pseudowires when the primary pseudowire fails. The feature also allows the Cisco CMTS to resume operation on the primary pseudowire after it comes back up.

Configuring the Backup Pseudowire

You can configure up to three backup pseudowires for a primary pseudowire. The priority of each backup pseudowire has to be unique.

A backup pseudowire is uniquely identified by a combination of IP address or hostname and VCID. Only the IP address or hostname and VCID can be configured for the backup peer, the remaining parameters are the same as the primary pseudowire.

Backup pseudowires can also be configured using the DOCSIS configuration files.

Perform the steps given below to configure a backup pseudowire.

Procedure

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

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**cable l2vpn** *mac-address* **Example:** `Router(config)# cable l2vpn 0011.0011.0011`	Specifies L2VPN MAC address and enters L2VPN *configuration mode.*
Step 4	**service instance** *id service-type* **Example:** `Router(config-l2vpn)# service instance 1 ethernet`	Specifies the service instance ID and enters Ethernet service configuration mode.
Step 5	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** **Example:** `Router(config-ethsrv)# xconnect 10.2.2.2 22 encapsulation mpls`	Specifies the tunneling method to encapsulate the data in the MPLS pseudowire and enters xconnect configuration mode.
Step 6	**backup peer** *peer-ip-address vc-id* [priority value] **Example:** `Router(config-xconn)# backup peer 10.3.3.3 33 priority 2`	Specifies the backup pseudowire and its priority. The priority keyword is optional, if only one backup pseudowire is configured. When multiple backup pseudowires are configured, it is required.
Step 7	**end** **Example:** `Router(config-xconn)# end`	Exits xconnect configuration mode and enters Privileged EXEC mode.

Configuring Backup Delay

Perform the steps given below to configure the period the backup pseudowire should wait to take over after the primary pseudowire goes down. You can also specify how long the primary pseudowire should wait after it becomes active to take over from the backup pseudowire.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable l2vpn** *mac-address* **Example:** `Router(config)# cable l2vpn 0011.0011.0011`	Specifies the L2VPN MAC address and enters L2VPN *configuration mode.* • *mac-address*—MAC address of a CM.
Step 4	**service instance** *id service-type* **Example:** `Router(config-l2vpn)# service instance 1 ethernet`	Specifies the service instance ID and enters Ethernet service configuration mode. • *id*—Service instance ID. • service-type—Service type for the instance.
Step 5	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** **Example:** `Router(config-ethsrv)# xconnect 10.2.2.2 22 encapsulation mpls`	Specifies the tunneling method to encapsulate the data in the MPLS pseudowire and enters xconnect configuration mode. • *peer-ip-address*—IP address of the remote PE router. The remote router ID can be any IP address, as long as it is reachable. • *vc-id*—32-bit identifier of the virtual circuit between the PE routers. • **encapsulation mpls**—Specifies MPLS as the tunneling method.

Step 6	Do one of the following:
	• **backup delay** enable-delay-period {disable-delay-period | never}
	•
	Example:
	`Router(config-xconn)# backup delay 10 10`
	Example:
	`Router(config-xconn)# backup delay 10 never`
		Specifies the period to wait before enabling or disabling the backup pseudowire.
		• *enable-delay-period*—Number of seconds the backup pseudowire should wait to take over after the primary pseudowire goes down. The valid range is from 0 to 180 seconds, with a default value of 0.
		• *disable-delay-period*—Number of seconds the primary pseudowire should wait after it becomes active to take over from the backup pseudowire. The valid range is from 0 to 180 seconds, with a default value of 0.
		• **never**—Specifies the primary pseudowire should not be reactivated after moving to the backup pseudowire.

Step 7	**end** **Example:**	Exits xconnect configuration mode and enters privileged EXEC mode.

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

Performing Manual Switchover

Perform the steps given below to perform a manual switchover to the primary or backup pseudowire. The **xconnect backup force-switchover** command can also be used to forcefully switch to the backup pseudowire for planned outages of the primary remote peer.

Note A manual switchover can be made only to an available member in the redundancy group. If the pseudowire specified in the command is not available, the command will be rejected.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**xconnect backup force-switchover peer 10.10.1.1 123** **Example:** `Router# xconnect backup force-switchover peer 10.10.1.1 123`	Specifies that the router should switch to the backup or to the primary pseudowire.

Troubleshooting Tips

The following commands help you troubleshoot an improper MPLS pseudowire configuration:

- **show ip interface brief**—Helps verify that the loopback interface with the IP address is present on each PE router.
- **show mpls l2transport vc**—Helps verify information about primary and backup pseudowires that have been enabled to route Layer 2 packets on a router.
- **show xconnect all**—Helps verify information about all xconnect attachment circuits and primary and backup pseudowires.
- **show cable l2-vpn xconnect mpls-vc-map**—Helps verify that the primary and backup pseudowires are configured properly.

Configuration Examples for MPLS Pseudowire for Cable L2VPN

The following sections provide MPLS pseudowire configuration examples for the static and dynamic provisioning methods:

Configuration Example for Static Provisioning of MPLS Pseudowires

The following example shows CLI-based provisioning of an MPLS pseudowire:

```
Router> enable
Router# configure terminal
Router(config)# cable l2vpn 0000.396e.6a68 customer2
Router(config-l2vpn)# service instance 2000 ethernet
Router(config-ethsrv)# xconnect 101.1.0.2 221 encapsulation mpls pw-type 4
Router(config-ethsrv)# cable set mpls-experimental 7
```

Configuration Examples for Dynamic Provisioning of MPLS Pseudowires

The following sections provide MPLS pseudowire provisioning examples based on BSOD CableLabs specification, Type-4, and Type-5 TLVs using the CM configuration file:

BSOD Specification-Based MPLS Pseudowire Provisioning: Example

The following example shows an MPLS pseudowire configuration based on BSOD CableLabs specification:

```
03 (Net Access Control) = 1
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN sub-type)
 =
        T01 (VPN Id) = 02 34 56 00 02 # VPNID=0234650002
        T02 (NSI) = 04 05 01 0a 4c 01 01# [04=mpls] [05=len][01=ipv4][IP=10.76.1.1]
        T05 (AGI) = 01 01 07 d1 # AGI = 0x010107d1
        T06 (SAII) = 00 00 07 d1 # SAII = TAII = VCID = 0x7d1 = 2001
        T07 (TAII) = 00 00 07 d1
18 (Maximum Number of CPE) = 16
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)  =
            S01 (VPNID) =   02 34 56 00 02
            S08 (UserPrio) = 01

24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 2
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type) =
            S01 (VPNID) = 02 34 56 00 02
            S08 (UserPrio) = 04
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 3
```

```
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type) =
            S01 (VPNID) =   02 34 56 00 02
            S08 (UserPrio) = 05
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 4
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type) =
            S01 (VPNID) = 02 34 56 00 02
            S08 (UserPrio) = 06
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 2
   S03 (Service Flow Reference) = 2
   S05 (Rule Priority) = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask) = 00 20 ff
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 3
   S03 (Service Flow Reference) = 3
   S05 (Rule Priority) = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask) = 21 40 ff
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 4
   S03 (Service Flow Reference) = 4
   S05 (Rule Priority) = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)  = 41 ff ff
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 11
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 12
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 13
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 14
   S06 (QoS Parameter Set Type) = 7
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 12
   S03 (Service Flow Reference) = 12
   S05 (Rule Priority) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority)   = 00 02
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)

              S01 (VPNID) = 02 34 56 00 02
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 13
   S03 (Service Flow Reference) = 13
   S05 (Rule Priority) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority) = 03 04
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)
```

```
            S01 (VPNID) = 02 34 56 00 02
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 14
   S03 (Service Flow Reference) = 14
   S05 (Rule Priority) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority) = 05 06
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)
              S01 (VPNID) = 02 34 56 00 02
```

Type-4 MPLS Pseudowire Provisioning Using the CM Configuration File: Example

The following example shows a CM configuration file-based provisioning of a Type-4 MPLS pseudowire:

```
03 (Net Access Control) = 1
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 02 # VPN-ID = "0234560002"
T043 (Cisco Vendor Specific) = 2b 16
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 04 # MPLSPWTYPE= Type4 - Ethernet-vlan Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 07 d1 = 2001 VCID
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 03 # VPN-ID = "0234560003"
T043 (Cisco Vendor Specific) =  2b 16
S008 (Vendor ID) = 00 00 0c Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 04 MPLSPWTYPE= Type4 - Ethernet-vlan Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 # MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 0b b9 # = 3001 VCID
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 04 # VPN-ID = "0234560004"
T043 (Cisco Vendor Specific) = 2b 16
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 04 # MPLSPWTYPE= Type4 - Ethernet-vlan Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 # MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 0f a1 # = 4001 VCID
18 (Maximum Number of CPE) = 16
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 2
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 02
       T043 (Cisco Vendor Specific) = 2b 0A
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO

S034 (MPLS-EXP-SET) = 22 05 # MPLSEXP-INGRESS= 5
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 3
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
```

```
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 03
       T043 (Cisco Vendor Specific) =  2b 0A
S008 (Vendor ID) = 00 00 0c
# Vendor ID = "00 00 0C" - CISCO

S034 (MPLS-EXP-SET) = 22 06

# MPLSEXP-INGRESS= 6
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 4
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 04
       T043 (Cisco Vendor Specific) = 2b 0A
S008 (Vendor ID) = 00 00 0c
# Vendor ID = "00 00 0C" - CISCO

S034 (MPLS-EXP-SET) = 22 04

# MPLSEXP-INGRESS= 4
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 2
   S03 (Service Flow Reference) = 2
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = 7d 00
   S05 (Rule Priority) = 2
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 3
   S03 (Service Flow Reference) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = bb 80
   S05 (Rule Priority) = 3
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 4
   S03 (Service Flow Reference) = 4
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = fa 00
   S05 (Rule Priority) = 4
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 11
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 12
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 13
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 14
   S06 (QoS Parameter Set Type) = 7
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 12
   S03 (Service Flow Reference) = 12
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = 7d 00
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 02
       T043 (Cisco Vendor Specific) = 2b 0B
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S035 (MPLS-EXP_RANGE) = 23 02  03 # MPLSEXP-EGRESS_RANGE= 2 - 3
   S05 (Rule Priority) = 2
```

```
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 13
   S03 (Service Flow Reference) = 13
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = bb 80
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) =  02 34 56 00 03
       T043 (Cisco Vendor Specific) = 2b 0B
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO

S035 (MPLS-EXP-RANGE) = 23 04  05 # MPLSEXP-EGRESS_RANGE= 4 - 5
   S05 (Rule Priority = 3
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 14
   S03 (Service Flow Reference) = 14
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = fa 00
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 04
       T043 (Cisco Vendor Specific) = 2b 0B
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO

S035 (MPLS-EXP-RANGE) = 23 00  01 # MPLSEXP-EGRESS_RANGE= 0 - 1
   S05 (Rule Priority) = 4
```

Type-5 MPLS Pseudowire Provisioning Using the CM Configuration File: Example

The following example shows a CM configuration file-based provisioning of a Type-5 MPLS pseudowire:

```
03 (Net Access Control) = 1
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 02 # VPN-ID = "0234560002"
T043 (Cisco Vendor Specific) = 2b 16
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 05 # MPLSPWTYPE= Type5 - Ethernet-Port Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 # MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 07 d1 # = 2001 VCID
45 (L2VPN CMIM) = 02 04 ff ff ff ff 01 01 01
18 (Maximum Number of CPE) = 16
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 02 # VPN-ID = "0234560002"
       T043 (Cisco Vendor Specific) = 2b 0A
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S034 (MPLS-EXP-SET) = 22 04 # MPLS-EXP-SET at INGRESS= 4
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 12
   S06 (QoS Parameter Set Type) = 7
```

Configuration Examples for L2VPN Pseudowire Redundancy

The following sections provide L2VPN pseudowire redundancy configuration examples using the CM configuration file:

Example: Configuring Backup Pseudowire Peer and VC ID

The following example shows how to provision a file-based backup peer router based on the CM configuration:

PE Router 1

```
cable l2vpn 0025.2e2d.7252
 service instance 1 ethernet
  encapsulation default
  xconnect 10.76.2.1 400 encapsulation mpls
   backup peer 10.76.2.1 600 priority 4
```

PE Router2

```
cable l2vpn 0011.0011.0011
 service instance 1 ethernet
  encapsulation default
  xconnect 10.2.2.2 22 encapsulation mpls
   backup peer 10.3.3.3 33 priority 2
   backup delay 10 10
```

Example: Configuring Backup Delay

The following example shows how to configure a backup delay to determine how much time should elapse before a secondary line status change after a primary line status has been changed.

```
cable l2vpn 0011.0011.0011
 service instance 1 ethernet
  encapsulation default
  xconnect 10.2.2.2 22 encapsulation mpls
   backup delay 10 10
```

Example: L2VPN Backup MPLS Pseudowire Provisioning Using the CM Configuration File

The following example shows how to provision an L2VPN Backup MPLS pseudowire based on the CM configuration file:

```
03 (Net Access Control)          = 1
18 (Maximum Number of CPE)       = 3
43 (Vendor Specific Options)
   S08 (Vendor ID)       = ff ff ff
   S005 (Unknown sub-type)       = 01 04 32 30 32 30 02 07 04 05 01 0a 4c 02 01 2b 15 26 04
 00 00 00 14 28 10 01 05 01 0a 4c 02 01 03 04 00 00 07 08 04 01 05 28 0d 01 05 01 0a 4c 02
 03 03 04 00 00 00 15 28 10 01 05 01 0a 4c 02 01 03 04 00 00 b1 8e 04 01 01 29 01 03 2a 01
 01
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 4
   S06 (QoS Parameter Set Type)          = 7
   S08 (Max Sustained Traffic Rate)      = 2000000
   S09 (Max Traffic Burst)               = 3200
   S15 (Service Flow Sched Type)         = 2
   S43 (Vendor Specific Options)
       T08 (Vendor ID)       = ff ff ff
       T005 (Unknown sub-type)       = 01 04 32 30 32 30
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 2
   S06 (QoS Parameter Set Type)          = 7
```

```
   S08 (Max Sustained Traffic Rate)      = 3000000
   S09 (Max Traffic Burst)               = 250000
29 (Privacy Enable)             = 1
```

Verifying the MPLS Pseudowire Configuration

Use the following **show** commands to verify the MPLS pseudowire configuration:

- **show mpls ldp discovery**
- **show cable l2-vpn xconnect**
- **show xconnect**
- **show mpls l2transport vc**

To verify the mapping between the MPLS pseudowire and virtual circuits for all cable modems, use the **show cable l2-vpn xconnect** command as shown in the following example:

```
Router# show cable l2-vpn xconnect mpls-vc-map
MAC Address     Peer IP Address VCID Type Prio CktID     Cable Intf  SID Customer Name/VPNID
0023.bee1.eb48  123.1.1.1       30   Prim*     Bu254:4101 Cable3/0/0  3
38c8.5cac.4a62  123.1.1.1       20   Prim*     Bu254:4100 Cable3/0/0  4   customer1
602a.d083.2e1c  123.1.1.1       60   Prim*     Bu254:4102 Cable3/0/0  5
```

To verify the mapping between the MPLS pseudowire and virtual circuits for all cable modems when pseudowire redundancy is not configured, use the **show cable l2-vpn xconnect mpls-vc-map** command as shown in the following example:

```
Router# show cable l2-vpn xconnect mpls-vc-map
MAC Address    Peer IP Address VCID Type  Prio CktID      Cable Intf SID Customer Name/VPNID
0025.2e2d.7252 10.76.2.1       400  Prim*      Bu254:400  Cable8/0/3 1
0014.f8c1.fd46 10.2.3.4        1000 Prim*      Bu254:1000 Cable8/0/0 1   2020
0014.f8c1.fd46 10.76.2.1       1800 Prim*      Bu254:1800 Cable8/0/0 1   2021
```

To verify the mapping between the MPLS pseudowire and virtual circuits for all cable modems when pseudowire redundancy is configured, use the **show cable l2-vpn xconnect mpls-vc-map** command as shown in the following example:

```
Router# show cable l2-vpn xconnect mpls-vc-map
MAC Address    Peer IP Address VCID Type  Prio CktID      Cable Intf SID Customer Name/VPNID
602a.d083.2e1c 123.1.1.1       60   Prim*      Bu254:4102 Cable3/0/0 5
38c8.5cac.4a62 123.1.1.1       20   Prim*      Bu254:4103 Cable3/0/0 4   000232303230
               156.1.3.1       30   Bkup  3    Bu254:4103
               123.1.1.1       50   Bkup  8    Bu254:4103
38c8.5cac.4a62 156.1.3.1       56   Prim*      Bu254:4104 Cable3/0/0 4   000232303231
               123.1.1.1       40   Bkup  1    Bu254:4104
```

To obtain the state of all virtual circuits associated with an MPLS pseudowire when pseudowire redundancy is not configured, use the **show cable l2-vpn xconnect mpls-vc-map state** command as shown in the following example:

```
Router# show cable l2-vpn xconnect mpls-vc-map state
MAC Address      Peer IP Address VCID Type Prio State Customer Name/VPNID State
```

```
602a.d083.2e1c   123.1.1.1       60   Prim*     UP                       UP
38c8.5cac.4a62   123.1.1.1       20   Prim*     UP    000232303230       UP
38c8.5cac.4a62   156.1.3.1       56   Prim*     UP    000232303231       UP
```

To obtain the state of all virtual circuits associated with an MPLS pseudowire when pseudowire redundancy is configured, use the **show cable l2-vpn xconnect mpls-vc-map state** command as shown in the following example:

```
Router# show cable l2-vpn xconnect mpls-vc-map state
MAC Address      Peer IP Address VCID Type   Prio State Customer Name/VPNID State
602a.d083.2e1c   123.1.1.1       60   Prim*       UP                       UP
38c8.5cac.4a62   123.1.1.1       20   Prim*       UP    000232303230       UP
                 156.1.3.1       30   Bkup   3    UP    000232303230       STDBY
                 123.1.1.1       50   Bkup   8    DOWN  000232303230       STDBY
38c8.5cac.4a62   156.1.3.1       56   Prim*       UP    000232303231       UP
                 123.1.1.1       40   Bkup   1    UP    000232303230       STDBY

When the local state of the modem is DOWN, the L2VPN is not configured on the WAN interface
 and the remote state of the L2VPN will be shown as OFF.

Router#show cable l2-vpn xconnect mpls-vc-map state
MAC Address     Peer IP Address VCID Type   Prio State Customer Name/VPNID State
602a.d083.2e1c  123.1.1.1       60   Prim*       OFF               DOWN
38c8.5cac.4a62  123.1.1.1       20   Prim*       UP    000232303230 UP
38c8.5cac.4a62  156.1.3.1       56   Prim*       UP    000232303231 UP
```

To verify information about the MPLS pseudowire mapping for a particular MAC address of a CM when pseudowire redundancy is configured, use the **show cable l2-vpn xconnect mpls-vc-map** command as shown in the following example:

```
Router# show cable l2-vpn xconnect mpls-vc-map 0025.2e2d.7252
MAC Address    Peer IP Address VCID Type  Prio CktID     Cable Intf SID Customer Name/VPNID
0025.2e2d.7252 10.76.2.1       400  Prim*      Bu254:400 Cable8/0/3 1
               10.76.2.1       600  Bkup  4    Bu254:600
```

To verify the detailed information about the MPLS pseudowire mapping for a CM when pseudowire redundancy is configured, use the **show mpls l2-vpn xconnect mpls-vc-map verbose** command as shown in the following examples.

The following example shows the information for a modem for which pseudowires were configured using backup peer command:

```
Router# show cable l2-vpn xconnect mpls-vc-map 0025.2e2d.7252 verbose
MAC Address                    : 0025.2e2d.7252
Customer Name                  :
Prim Sid                       : 1
Cable Interface                : Cable8/0/3
MPLS-EXP                       : 0
PW TYPE                        : Ethernet
Backup enable delay            : 0 seconds
Backup disable delay           : 0 seconds
Primary peer
Peer IP Address (Active)       : 10.76.2.1
XConnect VCID                  : 400
Circuit  ID                    : Bu254:400
Local State                    : UP
Remote State                   : UP
Backup peers
Peer IP Address                : 10.76.2.1
```

```
XConnect VCID                       : 600
Circuit  ID                         : Bu254:600
Local State                         : STDBY
Remote State                        : UP
Priority                            : 4
Total US pkts                       : 0
Total US bytes                      : 0
Total US pkts   discards            : 0
Total US bytes  discards            : 0
Total DS pkts                       : 0
Total DS bytes                      : 0
Total DS pkts   discards            : 0
Total DS bytes  discards            : 0
```

The following example shows the information for a modem for which pseudowires were created using the modem configuration file:

```
Router# show cable l2-vpn xconnect mpls-vc-map 0014.f8c1.fd46 verbose
MAC Address                         : 0014.f8c1.fd46
Prim Sid                            : 3
Cable Interface                     : Cable8/0/0
L2VPNs provisioned                  : 1
DUT Control/CMIM                    : Disable/0x8000FFFF
VPN ID                              : 2020
L2VPN SAID                          : 12289
Upstream SFID Summary               : 15
Downstream CFRID[SFID] Summary      : Primary SF
CMIM                                : 0x60
PW TYPE                             : Ethernet
MPLS-EXP                            : 0
Backup enable delay                 : 3 seconds
Backup disable delay                : 1 seconds
Primary peer
Peer IP Address (Active)            : 10.2.3.4
XConnect VCID                       : 1000
Circuit  ID                         : Bu254:1000
Local State                         : UP
Remote State                        : UP

Backup peers
Peer IP Address                     : 10.2.3.4
XConnect VCID                       : 21
Circuit  ID                         : Bu254:21
Local State                         : STDBY
Remote State                        : DOWN
Priority                            : 2
Peer IP Address                     : 10.76.2.1
XConnect VCID                       : 1800
Circuit  ID                         : Bu254:1800
Local State                         : STDBY
Remote State                        : DOWN
Priority                            : 5
Peer IP Address                     : 10.76.2.1
XConnect VCID                       : 45454
Circuit  ID                         : Bu254:45454
Local State                         : STDBY
Remote State                        : DOWN
```

To verify information about all attachment circuits and pseudowires for online modems, use the **show xconnect** command as shown in the following example:

```
Router# show xconnect all
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering      NH=No Hardware
XC ST  Segment 1                        S1 Segment 2                        S2
------+---------------------------------+--+---------------------------------+--
UP     ac   Bu254:2001(DOCSIS)           UP mpls 10.76.1.1:2001              UP
UP     ac   Bu254:2002(DOCSIS)           UP mpls 10.76.1.1:2002              UP
UP     ac   Bu254:2004(DOCSIS)           UP mpls 10.76.1.1:2004              UP
DN     ac   Bu254:22(DOCSIS)             UP mpls 101.1.0.2:22                DN
```

To verify information about MPLS virtual circuits and static pseudowires that have been enabled to route Layer 2 packets on a Cisco CMTS router, use the **show mpls l2transport vc** command as shown in the following example:

```
Router# show mpls l2transport vc
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Bu254          DOCSIS 2002                10.76.1.1       2002       UP
Bu254          DOCSIS 2003                10.76.1.1       2003       UP
Bu254          DOCSIS 2004                10.76.1.1       2004       DOWN
Bu254          DOCSIS 2017                10.76.1.1       2017       UP
Bu254          DOCSIS 2018                10.76.1.1       2018       UP
Bu254          DOCSIS 2019                10.76.1.1       2019       UP
```

Additional References

Standards

Standard	Title
CM-SP-L2VPN-I08-080522	*Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks*
L2VPN-N-10.0918-2	*L2VPN MPLS Update*

MIBs

MIB	MIBs Link
• DOCS-L2VPN-MIB • CISCO-IETF-PW-MIB • CISCO-CABLE-L2VPN-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: https://cfnng.cisco.com/mibs

RFCs

RFC	Title
RFC 3985	*Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*
RFC 4385	*Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*

RFC	Title
RFC 4446	*IANA Allocations for Pseudowire Edge-to-Edge Emulation (PWE3)*
RFC 4447	*Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*
RFC 4448	*Encapsulation Methods for Transport of Ethernet over MPLS Networks*
RFC 5085	*Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires*

Technical Assistance

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

Feature Information for MPLS Pseudowire for Cable L2VPN

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 5: Feature Information for MPLS Pseudowire for Cable L2VPN

Feature Name	Releases	Feature Information
MPLS Pseudowire for Cable L2VPN	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on theCisco cBR Series Converged Broadband Routers.