Cisco CMTS Router Layer 2 and VPN Features Configuration Guide

First Published: February 14, 2008

Last Modified: July 11, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27608-01

CONTENTS

CHAPTER 1

EtherChannel for the Cisco Cable Modem Termination System

First Published: February 14, 2008

This document describes the features, benefits and configuration of Cisco EtherChannel technology on the Cisco Cable Modem Termination System (CMTS).

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

EtherChannel is a technology by which to configure and aggregate multiple physical Ethernet connections to form a single logical port with higher bandwidth. The first EtherChannel port configured on the Cisco CMTS serves as the EtherChannel bundle master by default, and each slave interface interacts with the network using the MAC address of the EtherChannel bundle master.

EtherChannel ports reside on a routing or bridging end-point. The router or switch uses EtherChannel to increase bandwidth utilization in either half- or full-duplex mode, and load balances the traffic across the multiple physical connections.

EtherChannel on the Cisco CMTS supports inter-VLAN routing with multiple devices and standards, and supports FastEtherChannel (FEC) and Gigabit EtherChannel (GEC) on the Cisco CMTS depending on the router and associated processing modules in the chassis.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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

Contents

Prerequisites for EtherChannel on the Cisco CMTS

The Cisco uBR10012 universal broadband router has the following prerequisites to support GEC and 802.1Q encapsulation for inter-VLAN trunking, also summarized in the table:

- Cisco IOS Release 12.2(9a)BC or a later BC release.
- The Cisco uBR10012 router supports only GEC with PRE2 and PRE4 performance routing engine modules.

The Cisco uBR7246VXR universal broadband router has the following prerequisites to support FEC or GEC and 802.1Q encapsulation for inter-VLAN trunking:

- Cisco IOS Release 12.2(11)BC3 or a later BC release.
- The Cisco uBR7246VXR router supports FEC on Fast Ethernet channels with the Cisco NPE-225 or Cisco NPE-400 network processing engines.
- The Cisco uBR7246VXR router supports GEC on Gigabit Ethernet channels using the Cisco uBR7200-NPE-G1 network processing engine.

Table 1: Supported Interfaces and Encapsulations for EtherChannel on the Cisco CMTS

Cisco CMTS	Full Duplex Supported	Encapsulation Supported	Cisco IOS Release
Cisco uBR7246VXR	Fast Ethernet with the Cisco NPE-225 or Cisco NPE-400	IEEE 802.1Q	12.2(11)BC3
	GigabitEthernet with the Cisco uBR7200-NPE-G1	IEEE 802.1Q	12.2(9a)BC
Cisco uBR10012	Gigabit Ethernet with the PRE2 Module	IEEE 802.1Q	12.2(9a)BC
Cisco uBR10012	Gigabit Ethernet with the PRE4 Module	IEEE 802.1Q	12.2(33)BC

Restrictions for EtherChannel on the Cisco CMTS

The following restrictions apply to both the Cisco uBR10012 and Cisco uBR7246VXR routers with Cisco IOS Release 12.2(9a)BC and earlier supported releases, and Cisco IOS Release 12.2(33)SCA and later releases:

- EtherChannel on the Cisco CMTS is limited to Network Layer 3 functions, and does not support Data-Link Layer 2 EtherChannel functions as with certain other Cisco product platforms.
- The Port Aggregation Protocol (PAgP) is not supported on the Cisco CMTS as with other Cisco product platforms (such as the CatOS switch).
- Only the IEEE 802.1Q trunking protocol is supported on the Cisco CMTS. ATM trunking is not supported on the Cisco uBR10012 or Cisco uBR7246VXR routers as of this release.
- The maximum supported links per bundle is 8.
- EtherChannel on Cisco CMTS supports only physical ports or interfaces that have the same speed.
- Starting Cisco IOS Release 12.2(33)BC, EtherChannel on the Cisco uBR10012 router does not support MQC QOS. You can use Equal Cost Multi Path (ECMP) load balancing instead of EtherChannel.
- Layer 3 configurations on member interfaces of EtherChannel are not supported.
- Port Channel configuration is not supported on Gigabit Ethernet interface of Cisco uBR-MC3GX60 line card.
- MAC Address Accounting feature on port channel is not supported.

Information About EtherChannel on the Cisco CMTS

Several Cisco product platforms currently support EtherChannel, such as the Cisco 7200 Series and Cisco Catalyst Switches. This document describes EtherChannel on the following Cisco CMTS router platforms:

Introduction to EtherChannel on the Cisco CMTS

EtherChannel is based on proven industry-standard technology. The Cisco CMTS supports EtherChannel with several benefits, including the following:

- EtherChannel on the Cisco CMTS supports subsecond convergence times.
- EtherChannel can be used to connect two switch devices together, or to connect a router with a switch.
- A single EtherChannel connection supports a higher bandwidth between the two devices.
- The logical port channels on either Cisco CMTS platform provide fault-tolerant, high-speed links between routers, switches, and servers.
- EtherChannel offers redundancy and high availability on the Cisco CMTS. Failure of one connection causes a switch or router to use load balancing across the other connections in the EtherChannel.
- Load balancing on the Cisco CMTS supports dynamic link addition and removal without traffic interruption.

- EtherChannel supports inter-VLAN trunking. Trunking carries traffic from several VLANs over a point-to-point link between the two devices. The network provides inter-VLAN communication with trunking between the Cisco CMTS router and one or more switches. In a campus network, trunking is configured over an EtherChannel link to carry the multiple VLAN information over a high-bandwidth channel.

Cisco FastEtherChannel (FEC) and GigabitEtherChannel (GEC) on the Cisco uBR7246VXR Router

Cisco's Fast EtherChannel (FEC) technology builds upon standards-based 802.3 full-duplex Fast Ethernet to provide a reliable high-speed solution for network managers who require higher bandwidth between servers, routers, and switches than single-link Ethernet technology can provide.

Fast EtherChannel provides bandwidth scalability within the network backbone by providing increments from 200 Mbps to 800 Mbps with multi-gigabit capacity available on an increasing number of platforms.

Fast EtherChannel technology solves the immediate problem of scaling bandwidth within the network backbone, and can be applied to support Gigabit EtherChannels.

Cisco IOS Release 12.2(11)BC3 introduced support for Cisco EtherChannel technology for the Cisco uBR7246VXR router, and support continues with Cisco IOS Release 12.2(9a)BC. FEC on the Cisco uBR7246VXR router includes the following EtherChannel capabilities:

- Supports a maximum of four physical ports to be combined into one logical FEC or GEC link.
- Supports bandwidth up to 800 Mbps FEC (Fast EtherChannel full duplex) on the Cisco uBR7246VXR router.
- Supports bandwidth up to 4 Gbps GEC (Gigabit EtherChannel—half-duplex) for a combined total of up to 8 Gbps (full-duplex) with the Cisco uBR7200-NPE-G1 processor.

The Cisco uBR7200-NPE-G1 processor includes three onboard Gigabit Ethernet interfaces. If you want to use these interfaces to replace the Fast Ethernet interfaces on the existing I/O controller, you will have to configure the new interfaces before they can be used to access the network. If you are also removing the existing I/O controller, you remove the configuration for its Fast Ethernet interfaces.

The Cisco uBR7200-NPE-G1 contains its own onboard I/O controller, which includes the boot flash memory and NVRAM memory. After you install the Cisco uBR7200-NPE-G1 in a chassis, you can no longer access the boot flash and NVRAM memory on the I/O controller. You must therefore copy the Cisco IOS software image and configuration file to the memory on the Cisco uBR7200-NPE-G1.

Cisco GigabitEtherChannel (GEC) on the Cisco uBR10012 Router

Cisco GigabitEtherChannel (GEC) is high-performance Ethernet technology that provides gigabit-per-second transmission rates. It provides flexible, scalable bandwidth with resiliency and load sharing across links for switches, router interfaces, and servers.

Cisco IOS Release 12.2(9a)BC supports GigabitEtherChannel on the Cisco uBR10012 router with the following EtherChannel capabilities:

- Supports IEEE 802.1Q encapsulation for inter-VLAN networking.
- Supports a maximum of four physical Ethernet ports to be combined as one logical EtherChannel link.

- Supports bandwidth up to 4 Gbps GEC (Gigabit EtherChannel—half duplex) for a combined total of up to 8 Gbps (full duplex) on the Cisco uBR10012 router with PRE2 performance routing engine modules.

How to Configure EtherChannel on the Cisco CMTS

This section contains the following:

Configuring FEC or GEC EtherChannel on the Cisco CMTS

This procedure describes and illustrates the configuration of EtherChannel FEC or GEC on the Cisco uBR7246VXR or Cisco uBR10012 routers, subject to the prerequisites

Before You Begin

- Cisco IOS 12.2(9a)BC is installed or upgraded on either the Cisco uBR10012 or Cisco uBR7246VXR universal broadband router.
- Fast Ethernet or Gigabit Ethernet modules and interfaces are installed on the Cisco uBR7246VXR chassis as described in the "Cisco FastEtherChannel (FEC) and GigabitEtherChannel (GEC) on the Cisco uBR7246VXR Router" section on page 4 .
- PRE2 modules are installed in the Cisco uBR10012 router chassis as described in Cisco GEC on Cisco CMTS.
- Fast Ethernet or Gigabit Ethernet cabling is completed and the ports are operational on the router and network.
- LAN interfaces are configured and operational on the router and network, with IP addresses and subnet masks.

Note

- The Cisco uBR7246VXR and Cisco uBR10012 routers support up to four physical connectors to be configured as one logical FEC or GEC port.

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	**interface port-channel** *n* **Example:** `Router(config)# interface port-channel 1`	Creates an EtherChannel interface. The first EtherChannel interface configured becomes the bundle master for all ports in the EtherChannel group. The MAC address of the first EtherChannel interface is the MAC address for all EtherChannel interfaces in the group. • n—EtherChannel port number for the specified port. The EtherChannel port number may range from 1 to 64. To remove an EtherChannel interface from the EtherChannel group, use the no form of this command. For illustration, the example at left names the interface **Port-channel1**. If the first EtherChannel interface in the group is later removed, the second EtherChannel interface in the group becomes the bundle master by default. Repeat this step on every EtherChannel port to be bundled into a FEC or GEC group. This configuration must be present on all EtherChannel interfaces before the EtherChannel group can be configured.
Step 4	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode for **Port-channel1** and returns to global configuration mode.
Step 5	**interface gigabitethernet** *slot/{subslot}/port* **Example:** `Router# interface gigabitethernet 1/0/0`	(Gigabit Ethernet interface only) Selects the Gigabit Ethernet interface that you wish to add as a member EtherChannel link in the EtherChannel bundle, and enters interface configuration mode. The Cisco CMTS Cisco uBR10012 and Cisco uBR7246VXR routers differ in slot selection as follows: • ◦ slot/subslot/port—Cisco uBR10012 router ◦ slot/port—Cisco uBR7246VXR router **Note** Cisco recommends that the link being added to the Cisco CMTS EtherChannel be shut down prior to configuring it as a member of the EtherChannel. Use the shutdown command in interface configuration mode immediately before completing the following steps in this procedure.
Step 6	**interface fastethernet** *slot/(subslot}port* **Example:** `Router# interface fastethernet 3/0`	(Fast Ethernet interface only) Selects a Fast Ethernet interface and enters interface configuration mode. **Note** The Cisco CMTS Cisco uBR10012 and Cisco uBR7246VXR routers differ in slot selection as follows: • ◦ slot/subslot/port—Cisco uBR10012 router ◦ slot/port—Cisco uBR7246VXR router

	Command or Action	Purpose
Step 7	**shutdown** **Example:** `Router(config-if)# shutdown`	Shuts down the interface selected in Step 5 or Step 6 above prior to configuring it as a member of the EtherChannel. **Note** Cisco recommends that the link being added to the Cisco CMTS EtherChannel be shut down prior to configuring it as a member of the EtherChannel.
Step 8	**channel-group** *number* **Example:** `Router(config-if)# channel-group 1`	Adds the current interface (Gigabit Ethernet or Fast Ethernet) to the EtherChannel Group, associating that interface with an EtherChannel link. • number—The identifying number for the EtherChannel group with which to associate this interface. An EtherChannel group can be identified in the range of 1 to 64, and each group can have up to four interfaces, only one of which is the master. To remove an EtherChannel group and the associated ports from the Cisco CMTS, use the no form of this command.
Step 9	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface on which EtherChannel is configured.
Step 10	**Ctrl-Z** **Example:** `Router(config# Ctrl-z`	Returns to privileged EXEC mode. IP traffic should be visible on the network with completion of the above steps.

Troubleshooting Tips

Once interface operations are confirmed (prior to this procedure), and EtherChannel configurations have been verified (next procedure), any difficulty experienced through the EtherChannel links may pertain to inter-VLAN or IP routing on the network, or perhaps very high bandwidth consumption.

See the “Additional References” section on page 10 for further resources in troubleshooting these and additional configurations.

What to Do Next

Additional IP, access list, inter-VLAN or load balancing configurations may be made to the Cisco CMTS and these changes will be supported in the running EtherChannel configuration without service disruption from EtherChannel.

Refer to the “Additional References” section on page 11 for more information.

Verifying EtherChannel on the Cisco CMTS

Links can be added or removed from an EtherChannel interface without traffic interruption. If an Ethernet link in an EtherChannel interface fails, traffic previously carried over the failed link switches to the remaining links within the EtherChannel. There are a number of events that can cause a link to be added or removed including adding or removing a link using commands and simulating link failure and recovery (as with (no)shutdown links).

Cisco EtherChannel supports online insertion and removal (OIR) of field-replaceable units (FRUs) in the Cisco CMTS chassis. Ports that remain active during OIR of one FRU will take over and support the traffic bandwidth requirements without service disruption. However, OIR is not described in this procedure.

Refer to the "Additional References" section on page 10 for complete OIR procedures and guidelines for the respective FRU.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show interface port-channel** *n* **Example:** `Router# show interface port-channel 1`	Verifies the EtherChannel configuration on the Cisco CMTS for the selected EtherChannel group. • n—The identifying number for the Port Channel group to display.

Configuration Examples for EtherChannel on the Cisco CMTS

The sequential configuration example and commands in Table 2 illustrate the configuration of Etherchannel on a Cisco uBR7246VXR router with a five-port sensor:

The following example illustrates Gigabit EtherChannel (GEC) information for the port-channel interface of 2 as configured on a Cisco uBR10012 router with the PRE2 performance routing engine model.

This configuration is comprised of three GEC port channels as follows:

- Member 0 is the GEC interface bundle master.
- Member 2 is the final slave interface in this GEC group.
- These three port-channel interfaces (members) comprise one GEC group that is set up with a GEC peer on the network.

```
Router# show interface port-channel 2
Port-channel2 is up, line protocol is up
  Hardware is GEChannel, address is 8888.8888.8888 (bia 0000.0000.0000)
```

```
  Internet address is 101.101.101.1/16
  MTU 1500 bytes, BW 3000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 3
    No. of configured  members in this channel: 3
    No. of passive members in this channel: 0
    No. of active members in this channel: 3
        Member 0 : GigabitEthernet1/0/0 , Full-duplex, 1000Mb/s
        Member 1 : GigabitEthernet3/0/0 , Full-duplex, 1000Mb/s
        Member 2 : GigabitEthernet2/0/0 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/225/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/120 (size/max)
  30 second input rate 17292000 bits/sec, 9948 packets/sec
  30 second output rate 17315000 bits/sec, 9935 packets/sec
     866398790 packets input, 3324942446 bytes, 0 no buffer
     Received 2 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     866394055 packets output, 3323914794 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The following example illustrates GEC information for the port-channel interface of 2 as configured on a Cisco uBR7246VXR router.

This configuration is comprised of three port-channel interfaces (members) as follows:

- Member 0 is the GEC interface bundle master.
- Member 2 is the final slave interface in this GEC group.
- These three port-channel interfaces (members) comprise one GEC group that is set up with a GEC peer on the network.

```
Router# show interfaces port-channel 2
Port-channel2 is up, line protocol is up
  Hardware is GEChannel, address is 000b.bf7d.9c01 (bia 000b.bf7d.9c00)
  Internet address is 101.101.101.2/16
  MTU 1500 bytes, BW 3000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 3
    No. of configured  members in this channel: 3
    No. of passive members in this channel: 0
    No. of active members in this channel: 3
        Member 0 : GigabitEthernet0/3 , Full-duplex, 1000Mb/s
        Member 1 : GigabitEthernet0/2 , Full-duplex, 1000Mb/s
        Member 2 : GigabitEthernet0/1 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:13:48, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/225/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/120 (size/max)
  30 second input rate 17358000 bits/sec, 9999 packets/sec
  30 second output rate 17359000 bits/sec, 10000 packets/sec
     868633935 packets input, 3809968911 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     868642883 packets output, 3811242413 bytes, 0 underruns
     2 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     2 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

The following example illustrates FastEtherChannel (FEC) information for the port channel interface of 1 as configured on a Cisco uBR7246VXR router.

This configuration is comprised of four port channel interfaces (members) as follows:

- Member 0
- Member 0 is the GEC interface bundle master.
- Member 3 is the final slave interface in this FEC group.
- These four port-channel interfaces (members) comprise one FEC group that is set up with an FEC peer on the network.

```
Router# show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is FEChannel, address is 000b.bf7d.9c1c (bia 000b.bf7d.9c00)
  Description: test
  Internet address is 100.100.100.1/24
  MTU 1500 bytes, BW 400000 Kbit, DLY 100 usec,
     reliability 255/255, txload 11/255, rxload 11/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 4
    No. of configured  members in this channel: 4
    No. of passive members in this channel: 0
    No. of active members in this channel: 4
        Member 0 : FastEthernet2/1 , Full-duplex, 100Mb/s
        Member 1 : FastEthernet2/0 , Full-duplex, 100Mb/s
        Member 2 : FastEthernet1/1 , Full-duplex, 100Mb/s
        Member 3 : FastEthernet1/0 , Full-duplex, 100Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:14:48, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/300/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/160 (size/max)
  30 second input rate 17358000 bits/sec, 9998 packets/sec
  30 second output rate 17357000 bits/sec, 9998 packets/sec
     869366601 packets input, 3968956491 bytes
     Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     868944538 packets output, 3876736548 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Additional References

Related Documents

Related Topic	Document Title
EtherChannel for Cisco Products	• Cisco EtherChannel home page http://www.cisco.com/warp/public/cc/techno/lnty/etty/fsetch/index.shtml • Cisco EtherChannel Technology white paper http://www.cisco.com/en/US/tech/tk389/tk213/technologies_white_paper09186a0080092944.shtml
Cisco uBR10012 Universal Broadband Router	• Cisco uBR10012 Universal Broadband Router Hardware Installation Guide http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr10012/installation/guide/hig.html • Cisco uBR10012 Universal Broadband Router Performance Routing Engine Module http://www.cisco.com/c/en/us/td/docs/interfaces_modules/cable/performance_routing_engine/installation/guide/pre5096.html • Cisco uBR10012 OC-48 DPT/POS Interface Module (Installation and Configuration) http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr10012/installation/field_replaceable_units/ub_oc48.html

Related Topic	Document Title
Cisco uBR7246VXR Universal Broadband Router	• Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr7200/installation/guide/ub72khig.html • Cisco uBR7246VXR Universal Broadband Router Performance Routing Engine Module http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr7200/ubr7246vxr/upgrade/guide/15066R.html http://www.cisco.com/en/US/products/hw/modules/ps4917/products_white_paper09186a0080113728.shtml
WAN and Inter-VLAN Routing with the Cisco CMTS	• Configuring LAN Interfaces chapter in the Cisco IOS Interface Configuration Guide , Release 12.2 http://www.cisco.com/c/en/us/td/docs/ios/12_2/interface/configuration/guide/finter_c/icflanin.html • Point-to-Point Protocol over Ethernet Support on the Cisco CMTS http://www.cisco.com/c/en/us/td/docs/cable/cmts/feature/guide/cmtsfg/ufgpppoe.html • ATM Multilink PPP Support on Multiple Virtual Circuits (VCs) http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/atm/configuration/12-2sx/atm-12-2sx-book/atm-ml-ppp-mul-vc.html • Cisco New Virtual Circuit (VC) Configuration Virtual Circuits

Related Topic	Document Title
Configuring Additional Devices for EtherChannel	• *Configuring EtherChannel and 802.1Q Trunking Between a Catalyst 2950 and a Router (inter-VLAN Routing)* http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/24042-158.html • *Configuring EtherChannel and 802.1Q Trunking Between Catalyst 2900XL/3500XL and Catalyst 2940, 2950/2955, and 2970 Switches* http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2900-xl-series-switches/21041-131.html

Standards and RFCs

Standards	Title
IEEE Std 802.1Q, 2003 Edition	IEEE Std 802.1Q, 2003 Edition (Incorporates IEEE Std 802.1Q-1998, IEEE Std 802.1u-2001, IEEE Std 802.1v-2001, and IEEE Std 802.1s-2002) http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=27089

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support

Feature Information for EtherChannel on the Cisco CMTS

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below 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.

Table 2: Feature Information for EtherChannel on the Cisco CMTS

Feature Name	Releases	Feature Information
GEC Support on the Cisco uBR10012 universal broadband router	12.2(9a)BC	GEC support was introduced on the Cisco uBR10012 universal broadband router with the Cisco uBR10012 PRE2 performance routing engine.
FEC and GEC Support on the Cisco uBR7246VXR router	12.2(11)BC3	FEC and GEC support was introduced on the Cisco uBR7246VXR router with the NPE-G1 network processing engine required for GEC. The following commands are introduced or modified in the feature or features documented in this module. • **channel-group** • **interface port-channel** • **show interface port-channel**

CHAPTER 2

Link Aggregation Control Protocol (IEEE 802.3ad) Support for Cisco uBR10012 Routers

This document describes the features, benefits and configuration of Link Aggregation Control Protocol (IEEE 802.3ad) technology on the Cisco uBR10012 Routers.

Currently, adding member interface into a port channel is supported only in a static way. The CMTS port channel interface cannot automatically detect the link status over port channel.

The IEEE 802.3ad is the standard to aggregate physical Ethernet interfaces to form a logical Ethernet link using the Link Aggregation Control Protocol (LACP) that provides greater bandwidth, high availability, and auto reconfiguration.

LACP protocol aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network switches or devices. LACP protocol instance runs on every switch and independently performs aggregations based on the local switch information and the exchanged LACPDUs.

A switch may limit the number of interfaces that can be aggregated together due to system limitations. In such a case, an interface may not be allowed to operate as part of an aggregation it is eligible to join the aggregation from the protocol perspective. LACP provides a mechanism to make such links hot-standby for the aggregation such that they can automatically join the aggregation in case one or more operational members fail.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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

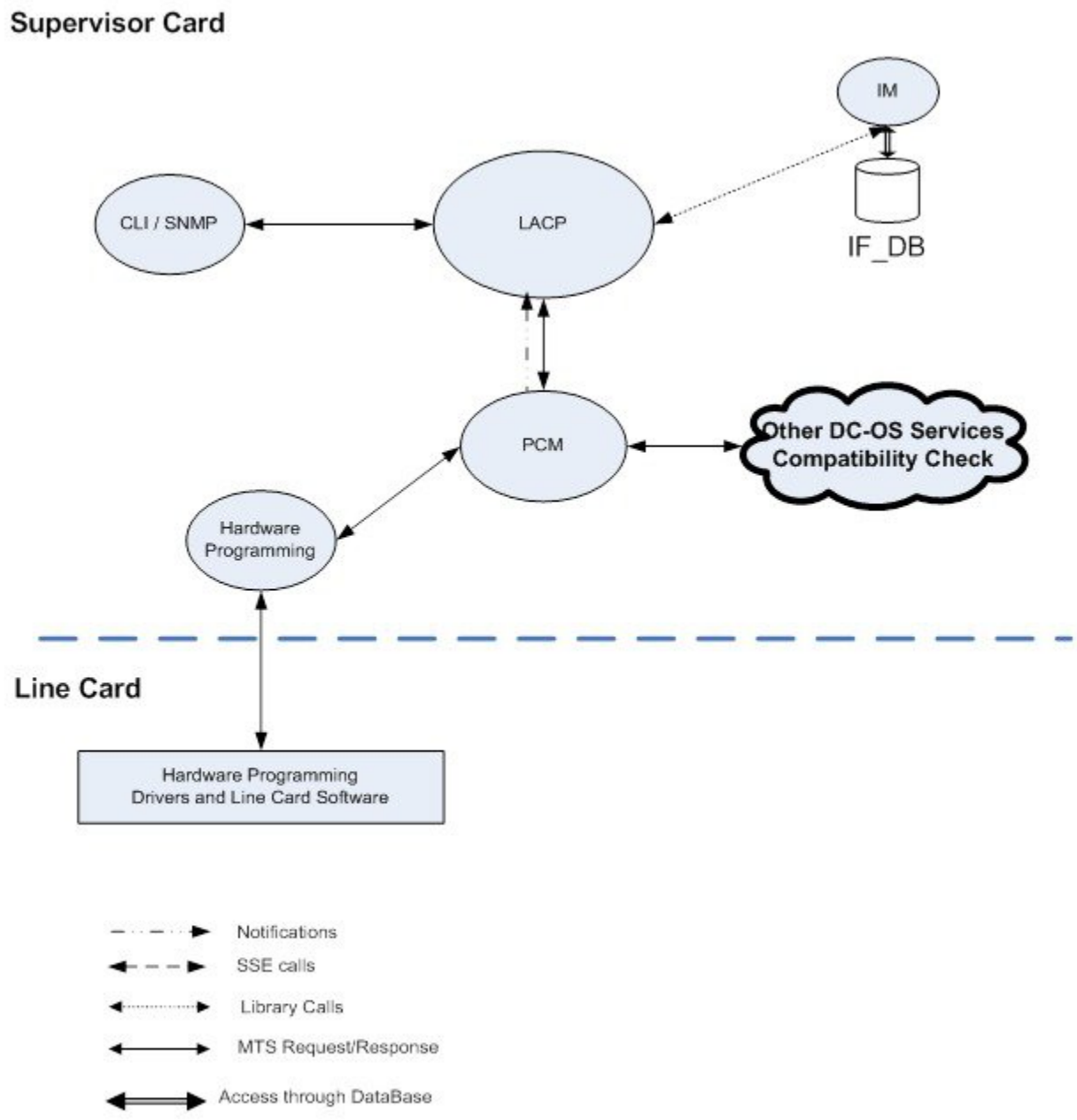
Contents

LACP Feature Advantages

It increases the redundancy and high availability of the aggregation. If a port fails, traffic continues on the remaining ports.

The below figure shows the software interaction for the LACP services.

Figure 1: Software Interaction Diagram for LACP Services



LACP Feature Limitations

The following points list the limitations in enabling the LACP services:

- IOS configuration should be applied seamlessly. If LACP is not running, the VSH and SNMP MIBs are not loaded. You cannot configure the ASCII configuration as the required VHS nodes are not present.
- Channeling mode configuration is maintained by the port channel manager. During the system startup, LACP cannot independently run based on only the configuration present in its binary configuration stored in PSS. If LACP enable or disable is not used, then it requires a special handshake with the Port Channel Manager to know how many ports have LACP configured.
- LACP has some independent global as well as interface level configurations.
- Using enable or disable requires a cleanup of all the existing ports that are using LACP. The current port channel model results in removing these ports from the port channel.

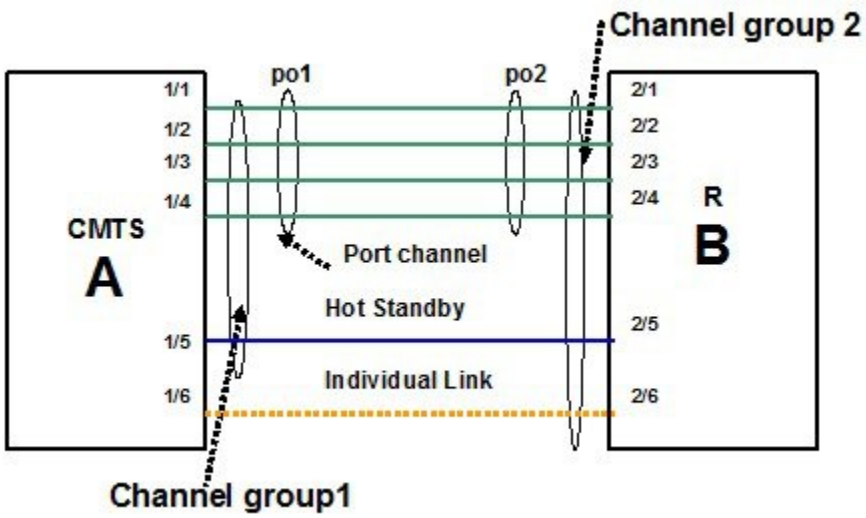
LACP Feature Components

The following are some of the components of LACP services:

- Channel group—It is a group used to aggregate a set of interfaces either explicitly or by using channeling protocols. This group is a container that comprises of all the ports that you have configured. You can add or remove ports from a channel group. In the figure below, Device (CMTS) is configured with channel group 1 with members 1/1-5 and Device (R) is configured with channel group 2 with members 2/1-6.
- Port channel—It is a logical interface representing a set of interfaces that are operationally aggregated into a single logical forwarding interface. The port channel interface aggregation characteristic is determined by the configurational and operational parameters. A port channel interface is always associated with a channel group. Whenever a channel group is created, an associated port channel is also created.
- Suspended link—It is any link that cannot be aggregated due to the misconfiguration of operational or administrative parameters. These links are logically kept down and no data is exchanged till the misconfiguration is resolved.
- Individual link—It is a link that is allowed to participate in aggregation and no other links can be aggregated with this link. Individual links continue to work as a normal 802.3 link. These links are different from the misconfigured links that are kept suspended. Individual links are formed only when channeling protocols run on the port. In the figure below, link between port 1/6 on Device(CMTS) and Device(R) on switch operates as an individual link.
- Hot standby link—It is a link that can be aggregated operationally but is not included in the aggregation due to limitations of the system's aggregation capability. For example, a system can support a maximum of four links in an aggregation but it can allow eight (CMTS currently supports eight member link into one channel group) links to be configured in the channel group. So, any set of four links amongst the configured eight links can be aggregated to form a logical port channel interface within the channel group. The remaining four links become standby links, which can join the port channel interface if one

or more aggregated links fail. In the figure below, link between port fc1/5 on Device(CMTS) and port 2/5 on Device(R) is a standby link for the port channel po1 on Device (CMTS) and po2 on Device(R).

Figure 2: Channel Groups with Multiple Port Channel Interface and Individual Links



Configuring LACP Service Components

This section contains the following topics:

Configuring a Port Channel Virtual Interface

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	**interface port-channel** *channel-number* **Example:** `Router(config)# interface port-channel 1`	Configures the interface port channel number.

The following example shows how to configure interface port channel number 1:

```
Router(config)# enable
Router(config)# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# exit
```

Configuring LACP Port Priority

You can assign a port priority to each port on a device running LACP. You can specify the port priority by using the **lacp port-priority** command or use the default port priority (32768). The port priority is used to decide which ports should be put in the standby mode when a hardware limitation or the **lacp max-bundle** command configuration prevents all compatible ports from aggregating. Priority is supported only on port channels with LACP-enabled physical interfaces.

Note A high priority number means a low priority.

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 port-channel** *channel-number* **Example:** `Router(config)# interface port-channel 10`	Identifies the interface port channel and enters interface configuration mode.
Step 4	**lacp port-priority** *priority* **Example:** `Router(config-if)# lacp port-priority 23700`	Sets the port priority.

The following example shows how to configure port priority of 23700 for an interface:

```
Router> enable
Router# configure terminal
Router(config)# interface port-channel 10
Router(config-if)# lacp port-priority 23700
```

Configuring LACP System Priority

You can assign a system priority to each device running LACP. You can specify the system priority by using the **lacp system-priority** command or use the default system priority (32768). The system priority is used with the MAC address of the device to form the system ID and is used during negotiation with the other systems. The system priority is supported only on port channels with LACP-enabled physical interfaces.

Note A high priority number means a low priority.

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 port-channel** *channel-number* **Example:** `Router(config)# interface port-channel 10`	Identifies the interface port channel and enters interface configuration mode.
Step 4	**lacp system-priority** *priority* **Example:** `Router(config-if)# lacp system-priority 23700`	Sets the system priority.

The following example shows how to configure system priority of 25500 for a device:

```
Router> enable
Router# configure terminal
Router(config)# interface port-channel 10
Router(config-if)# lacp system-priority 25500
```

Configuring LACP 1:1 Link Redundancy

When you enable LACP 1:1 link redundancy based on the system priority and port priority, the port with the higher system priority chooses one link as the active link and the other link as the standby link. When the active link fails, the standby link is selected as the new active link the port channel going down. When the original active link recovers, it reverts to its active link status. During this switchover, the port channel is also up.

Before You Begin

- Make sure that the port channel protocol type is LACP.
- Make sure that **lacp max-bundle** command is configured on the port channel. The **lacp fast-switchover** command does not affect the **lacp max-bundle** command.

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 port-channel** *channel-number* **Example:** `Router(config)# interface port-channel 1`	Identifies the interface port channel and enters the interface configuration mode.
Step 4	**lacp fast-switchover** **Example:** `Router(config-if)# lacp fast-switchover`	Enables the fast switch over feature for this channel group.

The following example shows how to configure the LACP channel group with 1:1 redundancy:

```
Router(config)# enable
Router(config)# configure terminal
Router(config)# interface port-channel 1
Router(config-if)# lacp fast-switchover
```

Configuring Minimum Active Bundled LACP Ports

When the number of active links falls below the minimum threshold, the port channel shuts down.

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 port-channel** *channel-number* **Example:** `Router(config)# interface port-channel 2`	Identifies the interface port channel and enters the interface configuration mode.
Step 4	**lacp min-bundle** *min-bundle-number* **Example:** `Router(config-if)# lacp min-bundle 5`	Sets the minimum threshold of active member links allowed in the LACP bundle. The range is from 1 to 8. The default is 1.

The following example shows how to set a minimum threshold of active member links:

```
Router(config)# enable
Router(config)# configure terminal
Router(config)# interface port-channel 2
Router(config-if)# lacp min-bundle 5
```

Configuring Maximum Active Bundled LACP Ports

The value specified in the max-bundle-number argument determines the number of active links that are bundled in the port channel. The remaining links are in hot-standby mode.

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** `Router(config)# interface port-channel 2`	Identifies the interface port channel and enters the interface configuration mode.
Step 4	**lacp max-bundle** *max-bundle-number* **Example:** `Router(config-if)# lacp max-bundle 3`	Sets the maximum threshold of active member links allowed in the LACP bundle. The range is from 1 to 8. The maximum threshold value must be greater than or equal to the minimum threshold value.

The following example shows how to set a maximum threshold of active member links:

```
Router(config)# enable
Router(config)# configure terminal
Router(config)# interface port-channel 2
Router(config-if)# lacp max-bundle 3
```

Configuring LACP

Before You Begin

- It is recommended to disable the IP address assigned to a physical interface that is part of a channel group.
- You must create a port channel before member links are assigned to it.

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	**interface port-channel** *channel-number* **Example:** `Router(config)# interface port-channel 1`	Identifies the interface port channel.
Step 4	**interface** *type number* **Example:** `Router(config)# interface TenGigabitEthernet 4/1`	Configures a member interface and enters interface configuration mode.
Step 5	**channel-group** *channel-number* **mode {active | passive}** **Example:** `Router(config-if)# channel-group 5 mode active`	Configures the channel group with the LACP.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Returns to privileged EXEC mode.

The following example shows how to configure channel group number 1:

```
Router(config)# enable
Router(config)# configure terminal
Router(config)# interface port-channel 1
Router(config)# interface TenGigabitEthernet 4/1
Router(config-if)# channel-group 1 mode active
Router(config-if)# exit
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

MIBs

MIB	MIBs Link
• IEEE8023-LAG-MIB • CISCO-IEEE8023-LAG-CAPABILITY	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for LACP services

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below 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.

Table 3: Feature Information for LACP Services

Feature Name	Releases	Feature Information
LACP Services	Cisco IOS 12.2(33)SCJ	This feature was introduced on the Cisco uBR Series Universal Broadband Routers.

CHAPTER 3

Cisco uBR7200 Series MPLS VPN Cable Enhancements

First Published: February 14, 2008

This feature module describes the Cisco uBR7200 series universal broadband router cable Multiprotocol Label Switching Virtual Private Network (MPLS VPN) and cable interface bundling features. It explains how to create a VPN using MPLS protocol, cable subinterfaces, and interface bundles. VPNs can be created in many ways using different protocols.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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

Contents

Feature Overview

Using MPLS VPN technology, service providers can create scalable and efficient private networks using a shared hybrid fiber coaxial (HFC) network and Internet protocol (IP) infrastructure.

The cable MPLS VPN network consists of:

- The Multiple Service Operator (MSO) or cable company that owns the physical infrastructure and builds VPNs for the Internet Service Providers (ISPs) to move traffic over the cable and IP backbone.
- ISPs that use the HFC network and IP infrastructure to supply Internet service to cable customers.

Each ISP moves traffic to and from a subscriber's PC, through the MSO's physical network infrastructure, to the ISP's network. MPLS VPNs, created in Layer 3, provide privacy and security by constraining the distribution of a VPN's routes only to the routers that belong to its network. Thus, each ISP's VPN is insulated from other ISPs that use the same MSO infrastructure.

An MPLS VPN assigns a unique VPN Routing/Forwarding (VRF) instance to each VPN. A VRF instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine the contents of the forwarding table.

Each PE router maintains one or more VRF tables. It looks up a packet's IP destination address in the appropriate VRF table, only if the packet arrived directly through an interface associated with that table.

MPLS VPNs use a combination of BGP and IP address resolution to ensure security. See *Configuring Multiprotocol Label Switching.*

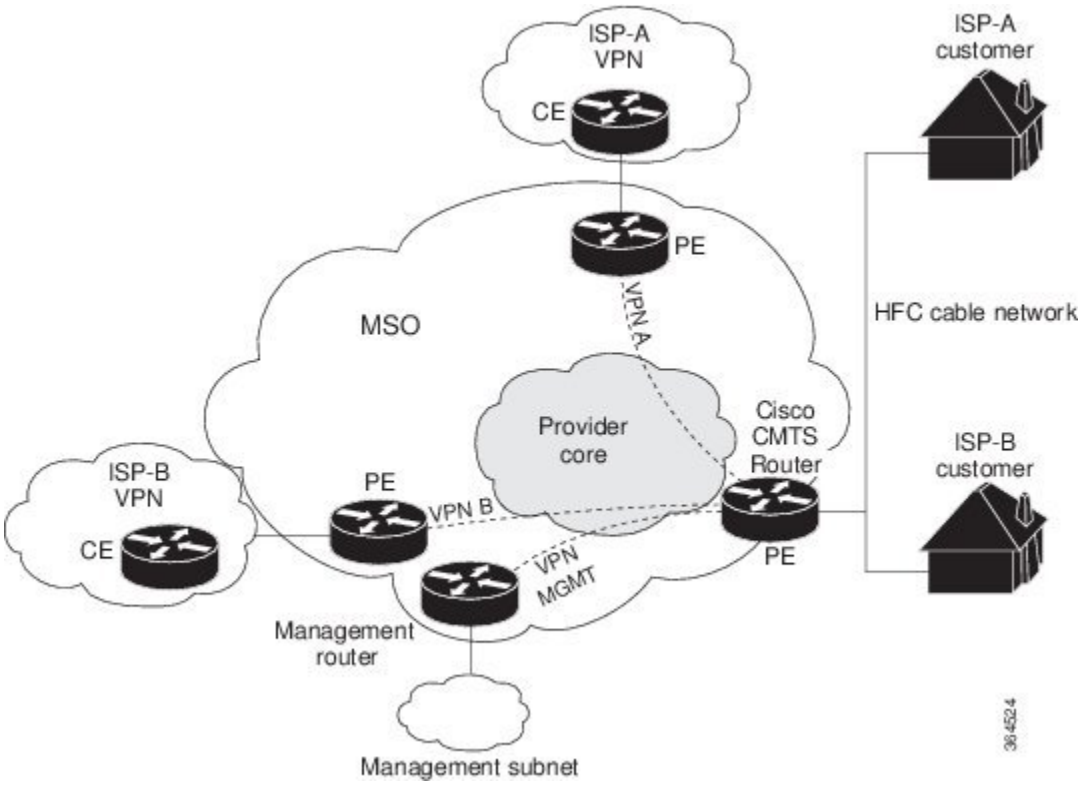
The table shows a cable MPLS VPN network. The routers in the network are:

- Provider (P) router—Routers in the core of the provider network. P routers run MPLS switching, and do not attach VPN labels (MPLS label in each route assigned by the PE router) to routed packets. VPN labels are used to direct data packets to the correct egress router.
- Provider Edge (PE) router— Router that adds the VPN label to incoming packets based on the interface or subinterface on which they are received. A PE router attaches directly to a CE router. In the MPLS-VPN approach, each Cisco CMTS router acts as a PE router.
- Customer (C) router—Router in the ISP or enterprise network.
- Customer Edge (CE) router—Edge router on the ISP's network that connects to the PE router on the MSO's network. A CE router must interface with a PE router.

The MPLS network has a unique VPN that exclusively manages the MSOs devices called the management VPN. It contains servers and devices that other VPNs can access. The management VPN connects the Cisco CMTS router to a PE router, which connects to management servers such as Cisco Network Registrar (CNR) and Time of Day (ToD) servers. A PE router connects to management servers and is a part of the management VPN. Regardless of the ISP they belong to, the management servers serve the Dynamic Host Configuration Protocol (DHCP), DNS (Domain Name System), and TOD requests coming from PCs or cable modems.

Note When configuring MPLS VPNs, you must configure the first subinterface created as a part of the management VPN.

Figure 3: MPLS VPN Network



Cable VPN configuration involves an:

- MSO domain that requires a direct peering link to each enterprise network (ISP), provisioning servers for residential and commercial subscribers, and dynamic DNS for commercial users. The MSO manages cable interface IP addressing, Data-over-Cable Service Interface Specifications (DOCSIS) provisioning, CM hostnames, routing modifications, privilege levels, and usernames and passwords.
- ISP or enterprise domain that includes the DHCP server for subscriber or telecommuter host devices, enterprise gateway within the MSO address space, and static routes back to the telecommuter subnets.

Note Cisco recommends that the MSO assign all addresses to the end user devices and gateway interfaces. The MSO can also use split management to let the ISP configure tunnels and security.

In an MPLS VPN configuration, the MSO must configure the following:

- CMTS
- P routers

- PE routers
- CE routers
- One VPN per ISP DOCSIS servers for all cable modem customers. The MSO must attach DOCSIS servers to the management VPN, and make them visible.

The MSO must configure the Cisco CMTS routers that serve the ISP, and remote PE routers connecting to the ISP, as PE routers in the VPN.

The MSO must determine the primary IP address range for all cable modems.

The ISP must determine the secondary IP address range for subscriber PCs.

To reduce security breaches and differentiate DHCP requests from cable modems in VPNs or under specific ISP management, MSOs can use the **cable helper-address** command in Cisco IOS software. The MSO can specify the host IP address to be accessible only in the ISP's VPN. This lets the ISP use its DHCP server to allocate IP addresses. Cable modem IP address must be accessible from the management VPN.

The MPLS VPN approach of creating VPNs for individual ISPs or customers requires subinterfaces to be configured on the virtual bundle interface. Each ISP requires one subinterface. The subinterfaces are tied to the VPN Routing/Forwarding (VRF) tables for their respective ISPs. The first subinterface must be created on the cable interface bound to the management VPN.

To route a reply from the CNR back to the cable modem, the PE router that connects to the CNR must import the routes of the ISP VPN into the management VPN. Similarly, to forward management requests (such as DHCP renewal to CNR) to the cable modems, the ISP VPN must export and import the appropriate management VPN routes.

You can group all of the cable interfaces on a Cisco CMTS router into a single bundle so that only one subnet is required for each router. When you group cable interfaces, no separate IP subnet or each individual cable interface is required. This grouping avoids the performance, memory, and security problems in using a bridging solution to manage subnets, especially for a large number of subscribers.

Subinterfaces allow traffic to be differentiated on a single physical interface, and assigned to multiple VPNs. You can configure multiple subinterfaces, and associate an MPLS VPN with each subinterface. You can split a single physical interface (the cable plant) into multiple subinterfaces, where each subinterface is associated with a specific VPN. Each ISP requires access on a physical interface and is given its own subinterface. Create a management subinterface to support cable modem initialization from an ISP.

Using each subinterface associated with a specific VPN (and therefore, ISP) subscribers connect to a logical subinterface, which reflects the ISP that provides their subscribed services. When properly configured, subscriber traffic enters the appropriate subinterface and VPN.

Benefits

- MPLS VPNs give cable MSOs and ISPs a manageable way of supporting multiple access to a cable plant. Service providers can create scalable and efficient VPNs across the core of their networks. MPLS VPNs provide systems support scalability in cable transport infrastructure and management.
- Each ISP can support Internet access services from a subscriber's PC through an MSO's physical cable plant to their networks.
- MPLS VPNs allow MSOs to deliver value-added services through an ISP, and thus, deliver connectivity to a wider set of potential customers. MSOs can partner with ISPs to deliver multiple services from multiple ISPs and add value within the MSO's own network using VPN technology.

- Subscribers can select combinations of services from various service providers.
- The MPLS VPN cable features set build on CMTS DOCSIS 1.0 and DOCSIS 1.0 extensions to ensure services are reliably and optimally delivered over the cable plant. MPLS VPN provides systems support domain selection, authentication per subscriber, selection of QoS, policy-based routing, and ability to reach behind the cable modem to subscriber end devices for QoS and billing while preventing session spoofing.
- MPLS VPN technology ensures both secure access across the shared cable infrastructure and service integrity.
- Cable interface bundling eliminates the need for an IP subnet on each cable interface. Instead, an IP subnet is only required for each cable interface bundle. All cable interfaces in a Cisco CMTS router can be added to a single bundle.

Restrictions

- Each subinterface on the CMTS requires an address range from the ISP and from the MSO. These two ranges must not overlap and must be extensible to support an increased number of subscribers for scalability.

Note This document does not address allocation and management of MSO and ISP IP addresses. See *Configuring Multiprotocol Label Switching* for this information.

- The **cable source-verify dhcp** command enables Dynamic Host Control Protocol (DHCP) Lease query protocol from the CMTS to DHCP server to verify IP addresses of upstream traffic, and prevent MSO customers from using unauthorized, spoofed, or stolen IP addresses.
- When using only MPLS VPNs, create subinterfaces on the virtual bundle, assign it an IP address, and provide VRF configuration for each ISP. When you create subinterfaces and configure only MPLS VPNs, the cable interface bundling feature is independent of the MPLS VPN.
- When using cable interface bundling:
  - Define a virtual bundle interface and associate any cable physical interface to the virtual bundle.
  - Specify all generic IP networking information (such as IP address, routing protocols, and switching modes) on the virtual bundle interface. Do not specify generic IP networking information on bundle slave interfaces.
  - An interface that has a subinterface(s) defined over it is not allowed to be a part of the bundle.
  - Specify generic (not downstream or upstream related) cable interface configurations, such as source-verify or ARP handling, on the virtual bundle interface. Do not specify generic configuration on bundle slave interfaces.
- Interface bundles can only be configured using the command line interface (including the CLI-based HTML configuration).

Supported Platforms

- Cisco uBR7223
- Cisco uBR7246
- Cisco uBR7246 VXR

Prerequisites

Before configuring IP-based VPNs, complete the following tasks:

- Ensure your network supports reliable broadband data transmission. Your plant must be swept, balanced, and certified based on National Television Standards Committee (NTSC) or appropriate international cable plant recommendations. Ensure your plant meets all DOCSIS or European Data-over-Cable Service Interface Specifications (EuroDOCSIS) downstream and upstream RF requirements.
- Ensure your Cisco router is installed following instructions in the Hardware Installation Guide and the Regulatory Compliance and Safety Information guide.
- Ensure your Cisco router is configured for basic operations.
- The chassis must contain at least one port adapter to provide backbone connectivity and one Cisco cable modem card to serve as the RF cable TV interface.

Other Important Information

- Ensure all other required headend or distribution hub routing and network interface equipment is installed, configured, and operational based on the services to support. This includes all routers, servers (DHCP, TFTP, and ToD), network management systems, other configuration or billing systems and backbone, and other equipment to support VPN.
- Ensure DHCP and DOCSIS configuration files have been created and pushed to appropriate servers such that each cable modem, when initialized, can transmit a DHCP request, receive an IP address, obtain TFTP and ToD server addresses, and download a DOCSIS configuration file. Configure each subinterface to connect to the ISP's VPN.
- Ensure DOCSIS servers are visible on the management VPN.
- Be familiar with your channel plan to assign appropriate frequencies. Outline your strategies for setting up bundling or VPN solution sets if applicable to your headend or distribution hub. Obtain passwords, IP addresses, subnet masks, and device names as appropriate.
- Create subinterfaces off of a virtual bundle interface. Configure each subinterface to connect to the ISP network.

The MPLS VPN configuration steps assume the following:

- IP addressing has already been determined and there are assigned ranges in the MSO and ISP network for specific subinterfaces.

- The MSO is using CNR and has configured it (using the **cable helper-address** command) to serve appropriate IP addresses to cable modems based on the cable modem MAC address. The CMTS forwards DHCP requests to the CNR based on the **cable helper-address** settings. The CNR server determines the IP address to assign the cable modem using the client-classes feature, which let the CNR assign specific parameters to devices based on MAC addresses.
- ISP CE routers are configured (using the **cable helper-address** command) to appropriately route relevant IP address ranges into the VPN.
- P and PE routers are already running Cisco Express Forwarding (CEF).
- MPLS is configured on the outbound VPN using the **tag switching ip** command in interface configuration mode.

Configuration Tasks

To configure MPLS VPNs, perform the following tasks:

Creating VRFs for each VPN

To create VRFs for each VPN, perform the following steps beginning in the router configuration mode.

Note Since only the CMTS has logical subinterfaces, assignments of VRFs on the other PE devices will be to specific physical interfaces.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **ip vrf** *mgmt-vpn*	Enters VRF configuration mode (config-vrf)# and maps a VRF table to the VPN (specified by *mgmt-vpn*). The management VPN is the first VPN configured.
Step 2	Router(config-vrf)# **rd** *mgmt-rd*	Creates a routing and forwarding table by assigning a route distinguisher to the management VPN.
Step 3	Router(config-vrf)# **route-target** {**export**| **import**| **both**} *mgmt-rd*	Exports and/or imports all routes for the management VPNs route distinguisher. This determines which routes will be shared within VRFs.
Step 4	Router(config-vrf)# **route-target import** isp1-vpn-rd	Imports all routes for the VPNs (*isp1-vpn)* route distinguisher.
Step 5	Router(config-vrf)# **route-target import** isp2-vpn-rd	Imports all routes for the VPNs (*isp2-vpn)* route distinguisher.
Step 6	Router(config-vrf)# **ip vrf** isp1-vpn	Creates a routing and forwarding table by assigning a route distinguisher to *isp1-vpn* .

	Command or Action	Purpose
Step 7	Router(config-vrf)# **rd** *mgmt-rd*	Creates a routing and forwarding table by assigning a route distinguisher (mgmt-rd) to the management VPN (mgmt-vpn).
Step 8	Router(config-vrf)# **route-target export** isp1-vpn-rd	Exports all routes for the VPNs (*isp1-vpn)* route distinguisher.
Step 9	Router(config-vrf)# **route-target import** isp1-vpn-rd	Imports all routes for the VPNs (*isp1-vpn)* route distinguisher.
Step 10	Router(config-vrf)# **route-target import** mgmt-vpn-rd	Exports all routes for the VPNs (*mgmt-vpn)* route distinguisher.
Step 11	Router(config-vrf)# **ip vrf** isp2-vpn	Creates a routing and forwarding table by assigning a route distinguisher to *isp2-vpn* .
Step 12	Router(config-vrf)# **route-target export** isp2-vpn-rd	Exports all routes for the VPNs (*isp2-vpn)* route distinguisher.
Step 13	Router(config-vrf)# **route-target import** isp2-vpn-rd	Imports all routes for the VPNs (*isp2-vpn)* route distinguisher.
Step 14	Router(config-vrf)# **route-target import** mgmt-vpn-rd	Imports all routes for the VPNs (*mgmt-vpn)* route distinguisher.

Defining Subinterfaces on a Virtual Bundle Interface and Assigning VRFs

To create a logical cable subinterface, perform the following steps beginning in the global configuration mode. Create one subinterface for each VPN (one per ISP). The first subinterface created must be configured as part of the management VPN (with the lowest subinterface number).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters configuration mode.
Step 2	Router(config)# **interface bundle n**	Enters virtual bundle interface configuration mode and defines the first (management) subinterface with the lowest subinterface number. Valid range for the bundle number n is from 1 to 255.
Step 3	Router(config-subif)# **description** *string*	Identifies the subinterface as the management subinterface.
Step 4	Router(config-subif)# **ip vrf forwarding** *mgmt-vpn*	Assigns the subinterface to the management VPN (the MPLS VPN used by the MSO to supply service to customers).
Step 5	Router(config-subif)# **ip address** *ipaddress mask*	Assigns the subinterface an IP address and a subnet mask.

	Command or Action	Purpose
Step 6	Router(config-subif)# **cable helper-address** *ip-address* **cable-modem**	Forwards DHCP requests from cable modems to the IP address listed.
Step 7	Router(config-subif)# **cable helper-address** *ip-address* **host**	Forwards DHCP requests from hosts to the IP address listed.
Step 8	Router(config-if)# **interface bundle n**	Defines an additional subinterface for the ISP (such as isp1).
Step 9	Router(config-subif)# **description** *string*	Identifies the subinterface (such as subinterface for *isp1-vpn)* .
Step 10	Router(config-subif)# **ip vrf forwarding** *isp1-vpn*	Assigns the subinterface to *isp1-vpn* VPN.
Step 11	Router(config-subif)# **ip address** *ipaddress mask*	Assigns the subinterface an IP address and a subnet mask.
Step 12	Router(config-subif)# **cable helper-address** *ip-address* **cable-modem**	Forwards DHCP requests from cable modems to the IP address listed.
Step 13	Router(config-subif)# **cable helper-address** *ip-address* **host**	Forwards DHCP requests from hosts to the IP address listed.
Step 14	Router(config-if)# **interface cable** *slot/port.n*	Defines an additional subinterface for the ISP (such as isp2).
Step 15	Router(config-subif)# **description** *string*	Identifies the subinterface (such as subinterface for *isp2-vpn)* .
Step 16	Router(config-subif)# **ip vrf forwarding** *isp2-vpn*	Assigns the subinterface to *isp2-vpn* VPN.
Step 17	Router(config-subif)# **ip address** *ipaddress mask*	Assigns the subinterface an IP address and a subnet mask.
Step 18	Router(config-subif)# **cable helper-address** *ip-address* **cable-modem**	Forwards DHCP requests from cable modems to the IP address listed.
Step 19	Router(config-subif)# **cable helper-address** *ip-address* **host**	Forwards DHCP requests from hosts to the IP address listed.
Step 20	Router(config)# **exit**	Returns to configuration mode.

Configuring Cable Interface Bundles

To assign a cable interface to a bundle, perform the following steps beginning in the interface configuration mode.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **interface cable** *slot/port*	Enters the cable interface configuration mode.

	Command or Action	Purpose
		IP addresses are not assigned to this interface. They are assigned to the logical subinterfaces created within this interface.
Step 2	Router(config-if)# **cable bundle** *bundle-number* **[master]**	Defines the interface as the bundle's master interface.
Step 3	Router(config)# **interface cable** *slot/port*	Enters the cable interface configuration mode for another cable interface. IP addresses are not assigned to this interface. They are assigned to the logical subinterfaces created within this interface.
Step 4	Router(config-if)# **cable bundle** *bundle-number*	Adds the interface to the bundle specified by *bundle-number* .

Configuring Subinterfaces and MPLS VPNs on a Virtual Bundle Interface

To configure subinterfaces on a virtual bundle interface and assign each subinterface a Layer 3 configuration:

Configure cable interface bundles.

Define subinterfaces on the virtual bundle interface and assign a Layer 3 configuration to each subinterface.

Create one subinterface for each customer VPN (one per ISP).

Configuring MPLS in the P Routers in the Provider Core

To configure MPLS in the P routers in the provider core, perform the following steps.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **configure terminal**	Enters configuration mode.
Step 2	Router(config)#**ip cef**	Enables Cisco Express Forwarding (CEF) operation. For information about CEF configuration and command syntax, see Cisco Express Forwarding Overview and Configuring Cisco Express Forwarding.
Step 3	Router(config)#**interface FastEthernet** *slot/port*	Enters FastEthernet interface configuration mode.
Step 4	Router(config-if)#**ip address** *ip-address mask*	Defines the primary IP address range for the interface.
Step 5	Router(config-if)#**mpls ip**	Enables the interface to be forwarded to an MPLS packet.

	Command or Action	Purpose
Step 6	Router(config-if)#**exit**	Returns to global configuration mode.
Step 7	Router(config)#**mpls label-protocol ldp**	Enables Label Distribution Protocol (LDP). For information about LDP and MPLS, see Configuring Multiprotocol Label Switching.
Step 8	Router(config)# **exit**	Returns to the configuration mode.

Verifying the MPLS VPN Configuration

Use the following commands to verify MPLS VPN operations on PE routers. For more MPLS VPN verification commands, see Configuring Multiprotocol Label Switching.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **show ip vrf**	Displays the set of VRFs and interfaces.
Step 2	Router# **show ip route vrf [vrf-name]**	Displays the IP routing table for a VRF.
Step 3	Router# **show ip protocols vrf [vrf-name]**	Displays the routing protocol information for a VRF.
Step 4	Router# **show ip route vrf** *vrf-name*	Displays the Local and Remote CE devices that are in the PE routing table.
Step 5	Router# **show mpls forwarding-table**	Displays entries for a VPN Routing/Forwarding instance.

What to Do Next

For more verification instructions, see the MPLS: Layer 3 VPNs Configuration Guide.

Configuration Examples

This section provides the following configuration examples:

Subinterface Configuration Example

The following example shows how to define a subinterface on virtual bundle interface 1.

```
interface cable3/0
! No IP address
```

```
! MAC level configuration only
! first subinterface
interface bundle1.1
description Management Subinterface
ip address 10.255.1.1 255.255.255.0
cable helper-address 10.151.129.2
! second subinterface
interface bundle1.2
ip address 10.279.4.2 255.255.255.0
cable helper-address 10.151.129.2
! third subinterface
interface bundle1.3
ip address 10.254.5.2 255.255.255.0
cable helper-address 10.151.129.2
```

Cable Interface Bundling Example

The following example shows how to bundle a group of physical interfaces.

interface cable 3/0 and interface cable 4/0 are bundled.

```
interface cable 3/0
 cable bundle 1
interface cable 4/0
 cable bundle 1
interface Bundle 1
 ip address 209.165.200.225 255.255.255.0
 ip address 209.165.201.1 255.255.255.0 secondary
```

Subinterface Definition on Virtual Bundle Example

The following example shows how to define subinterfaces on a virtual bundle and define Layer 3 configurations for each subinterface.

interface cable 3/0 and interface cable 4/0 are bundled.

```
interface cable 3/0
! No IP address
! MAC level configuration only
cable bundle 1
interface cable 4/0
! No IP address
! MAC layer configuration
cable bundle 1
! first subinterface
interface bundle1.1
ip address 10.22.64.1 255.255.255.0
cable helper-address 10.4.1.2
! second subinterface
interface bundle1.2
ip address 10.12.39.1 255.255.255.0
cable helper-address 10.4.1.2
! third subinterface
interface bundle1.3
ip address 10.96.3.1 255.255.255.0
cable helper-address 10.4.1.2
```

Cable Interface Bundle Master Configuration Example

The following examples show how to configure cable interface bundles:

```
Displaying the contents of the bundle
Router(config-if)#cable bundle ?
  <1-255>  Bundle number
Router(config-if)#cable bundle 25 master
Router(config-if)#
07:28:17: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to down
07:28:18: %UBR7200-5-UPDOWN: Interface Cable3/0 Port U0, changed state to up
```

PE Router Configuration Example

```
!
! Identifies the version of Cisco IOS software installed.
version 12.0
! Defines the hostname of the Cisco uBR7246
hostname region-1-ubr
!
! Describes where the system is getting the software image it is running. In
! this configuration example, the system is loading a Cisco uBR7246 image named
! AdamSpecial from slot 0.
boot system flash slot0:ubr7200-p-mz.AdamSpecial
!
! Creates the enable secret password.
enable secret xxxx
enable password xxxx
!
! Sets QoS per modem for the cable plant.
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
! Allows the system to use a full range of IP addresses, including subnet zero, for
! interface addresses and routing updates.
ip subnet-zero
!
! Enables Cisco Express Forwarding.
ip cef
!
! Configures a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to insert the
! DHCP relay agent information option in forwarded BOOTREQUEST messages.
ip dhcp relay information option
!
! Enters the virtual routing forwarding (VRF) configuration mode and maps a VRF table to
! the virtual private network (VPN) called MGMT-VPN. The VRF table contains the set of
! routes that points to or gives routes to the CNR device, which provisions the cable
! modem devices. Each VRF table defines a path through the MPLS cloud.
ip vrf MGMT-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:1
!
! Creates a list of import and/or export route target communities for the VPN.
 route-target export 100:2
 route-target export 100:3
!
! Maps a VRF table to the VPN called ISP1-VPN.
ip vrf ISP1-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:2
```

```
!
! Creates a list of import and/or export route target communities for the VPN.
 route-target import 100:1
!
! Maps a VRF table to the VPN called ISP2-VPN.
ip vrf ISP2-VPN
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:3
!
! Creates a list of import and/or export route target communities for the VPN.
 route-target import 100:1
!
! Maps a VRF table to the VPN called MSO-isp. Note: MSO-isp could be considered ISP-3; in
! this case, the MSO is competing with other ISPs for other ISP services.
ip vrf MSO-isp
!
! Creates the route distinguisher and creates the routing and forwarding table of the
! router itself.
 rd 100:4
!
! Creates a list of import and/or export route target communities for the VPN.
  route-target import 100:1
!
! Builds a loopback interface to be used with MPLS and BGP; creating a loopback interface
! eliminates unnecessary updates (caused by physical interfaces going up and down) from
! flooding the network.
interface Loopback0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
!
! Assigns an IP address to this Fast Ethernet interface. MPLS lable protocol must be
! enabled on this interface.
interface FastEthernet0/0
 description Connection to MSO core.
 ip address 10.0.1.1 255.255.255.0
 no ip directed-broadcast
 full-duplex
 mpls ip
 mpls label protocol ldp
!
! Enters cable interface configuration mode and configures the physical aspects of the
! 3/0 cable interface. Please note that no IP addresses are assigned to this interface;
! they will be assigned instead to the logical subinterfaces. All other commands for
! this cable interface should be configured to meet the specific needs of your cable RF
! plant and cable network.
interface Cable3/0
 no ip address
 cable bundle 1
 ip directed-broadcast
 no ip mroute-cache
 load-interval 30
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 855000000
 cable upstream 0 frequency 30000000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 shutdown
 cable upstream 2 shutdown
 cable upstream 3 shutdown
 cable upstream 4 shutdown
 cable upstream 5 shutdown
!
! Configures bundle 1.1 subinterface. If cable modems have
! not been assigned IP addresses, they will automatically come on-line using the settings
! for subinterface bundle1.1.
interface bundle1.1
 description Cable Administration Network
!
```

```
! Associates this interface with the VRF and MPLS VPNs that connect to the MSO cable
! network registrar (CNR). The CNR provides cable modems with IP addresses and other
! initialization parameters.
 ip vrf forwarding MSO
!
! Defines a range of IP addresses and masks to be assigned to cable modems not yet associated
 with an ISP.
 ip address 10.0.0.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PCs that are not yet associated with an ISP.
 cable helper-address 10.4.1.2 host
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
! Configures bundle1.2 subinterface.
interface bundle1.2
 description MSO as ISP Network
!
! Assigns this subinterface to the MPLS VPN used by the MSO to supply service to
! customers——in this case, MSO-isp.
 ip vrf forwarding MSO-isp
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
 ip address 10.1.1.1 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
 ip address 10.1.0.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
 cable helper-address 10.4.1.2 host
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
! Configures bundle1.3 subinterface
interface bundle1.3
 description ISP1's Network
!
! Makes this subinterface a member of the MPLS VPN.
 ip vrf forwarding isp1
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
 ip address 10.1.1.1 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
 ip address 10.0.1.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
```

```
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! cable interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
 cable helper-address 10.4.1.2 host
!
! Configures bundle1.4 subinterface
interface bundle1.4
 description ISP2's Network
!
! Makes this subinterface a member of the MPLS VPN.
 ip vrf forwarding isp2
!
! Defines a range of IP addresses and masks to be assigned to cable modems associated
! with the MSO as ISP network.
 ip address 10.1.2.1 255.255.255.0 secondary
!
! Defines a range of IP addresses and masks to be assigned to host devices associated
! with the MSO as ISP network.
 ip address 10.0.1.1 255.255.255.0
!
! Disables the translation of directed broadcasts to physical broadcasts.
 no ip directed-broadcast
!
! Disables cable proxy Address Resolution Protocol (ARP) and IP multicast echo on this
! interface.
 no cable proxy-arp
 no cable ip-multicast-echo
!
!
 cable dhcp-giaddr policy
!
!! Defines the DHCP server for cable modems whether they are associated with an ISP or
! with the MSO acting as ISP.
 cable helper-address 10.4.1.2 cable-modem
!
! Defines the DHCP server for PC host devices.
 cable helper-address 10.4.1.2 host
!
end
```

P Router Configuration Example

```
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R7460-7206-02
!
enable password xxxx
!
ip subnet-zero
ip cef
ip host brios 223.255.254.253
!
interface Loopback0
 ip address 10.2.1.3 255.255.255.0
 no ip directed-broadcast
```

```
!
interface Loopback1
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
!
interface FastEthernet0/0
 ip address 1.7.108.2 255.255.255.0
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 full-duplex
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/0
 ip address 10.0.5.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/1
 ip address 10.0.1.17 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/2
 ip address 10.0.2.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/3
 ip address 10.0.3.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/4
 ip address 10.0.4.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip mroute-cache
 mpls ip
 mpls label protocol ldp
 no cdp enable
!
interface Ethernet1/5
 no ip address
 no ip directed-broadcast
 no ip route-cache cef
 shutdown
 no cdp enable
!
interface Ethernet1/6
 no ip address
 no ip directed-broadcast
 no ip route-cache cef
 shutdown
```

```
 no cdp enable
!
interface Ethernet1/7
 no ip address
 no ip directed-broadcast
 no ip route-cache cef
 shutdown
 no cdp enable
!
router ospf 222
 network 10.0.5.0 255.255.255.0 area 0
 network 10.0.2.0 255.255.255.0 area 0
 network 10.0.3.0 255.255.255.0 area 0
 network 10.0.4.0 255.255.255.0 area 0
 network 20.2.1.3 255.255.255.0 area 0
!
ip classless
no ip http server
!
!
map-list test-b
no cdp run
!
tftp-server slot0:master/120/c7200-p-mz.120-1.4
!
line con 0
 exec-timeout 0 0
 password xxxx
 login
 transport input none
line aux 0
line vty 0 4
 password xxxx
 login
!
no scheduler max-task-time
end
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Cable Command Reference* at http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the *Cisco IOS Master Commands List* .

- **cable bundle**
- **cable helper-address**
- **ip dhcp relay information option**
- **show cable bundle**

Additional References

Related Documents

For additional information on the Cisco uBR7200 series and MPLS VPN, see:

- Cisco uBR7200 Series Universal Broadband Router Software Configuration Guide

- Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide
- Cisco uBR7200 Series Software Release Notes and Features
- Cisco uBR7200 Series Configuration Notes
- Cisco Network Registrar for the Cisco uBR7200 Series Universal Broadband Routers
- Regulatory Compliance and Safety Information for the Cisco uBR7200 Series Universal Broadband Router
- Configuring Multiprotocol Label Switching
- MPLS Label Switching on Cisco Routers
- Cisco IOS Release 12.1 Documents

Standards

DOCSIS 1.0.

MIBs

- CISCO-DOCS-REMOTE-QUERY.my

No new or modified MIB objects are supported by the cable interface bundling feature.

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

- RFC 1163, A Border Gateway Protocol
- RFC 1164, Application of the Border Gateway Protocol in the Internet
- RFC 2283, Multiprotocol Extensions for BGP-4
- RFC 2547, BGP/MPLS VPNs
- RFC 2233, DOCSIS OSSI Objects Support
- RFC 2669, Cable Device MIB
- RFC 2665, DOCSIS Ethernet MIB Objects Support

Feature Information for Cisco uBR7200 Series MPLS VPN Cable Enhancements

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below 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.

Feature Name	Releases	Feature Information
Support for Multiprotocol Label Switching Virtual Private Network (MPLS VPN) and Cable Interface Bundling	12.2(33)SCA	Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers

CHAPTER 4

Generic Routing Encapsulation on the Cisco CMTS Routers

First Published: February 14, 2008

This document describes the Generic Routing Encapsulation (GRE) feature. This feature is a tunneling protocol that enables the encapsulation of a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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

Contents

Prerequisites for Generic Routing Encapsulation

- The Cisco uBR7246VXR or Cisco uBR10012 router must be running Cisco IOS 12.3(17a)BC or later release.
- The Cisco uBR10012 router requires the Performance Routing Engine 2 (PRE2) module for use with Generic Routing Encapsulation.
- To use GRE, you must identify the inside interfaces on your devices and specify these in the Router MC Settings configuration area. Inside interfaces are the physical interfaces on the device that connect the device to its internal subnets and networks.
- In Router MC, you must select a routing protocol whenever you enable GRE. The available routing protocols in Router MC are EIGRP and Open Shortest Path First (OSPF):
  - Enhanced Interior Gateway Routing Protocol (EIGRP) allows the exchange of routing information within an autonomous system and addresses some of the more difficult issues associated with routing in large, heterogeneous networks. Compared to other protocols, EIGRP provides superior convergence properties and operating efficiency. EIGRP combines the advantages of several different protocols.
  - OSPF is a link-state, hierarchical protocol that features least-cost routing, multipath routing, and load balancing.

Note Do not configure OSPF on the port channel member interface because the OSPF configuration on this interface might cause abnormal behavior of the port channel.

- In Router MC, you must specify an Interior Gateway Protocol (IGP) process number. This number identifies the IGP. When GRE is implemented, this IGP will be the secured IGP. See How Does Router MC Implement GRE? for more information about IGPs. For secure communication, the inside interfaces on peering devices in your VPN must belong to the same IGP. The IGP process number must be within the range specified in the configuration support settings under the Admin tab. If you have an existing IGP on the device that is within this range, but is different from the IGP process number specified in your GRE settings, Router MC will remove the existing IGP. If the existing IGP process number matches the one specified in your GRE settings, any networks included in the existing IGP process that do not match the specified inside interfaces, will be removed.
- If the inside interfaces on your devices are configured to use an IGP other than the IGP specified in your GRE settings (meaning that the interfaces belong to an unsecured IGP):
  - For spokes: Manually remove the inside interfaces from the unsecured IGP by means of the device CLI before configuring GRE with Router MC.

  - For hubs: If the hub inside interface is used as a network access point for Router MC, then on deployment, the interface will be published in both secured and unsecured IGPs. To ensure that the spoke peers use only the secured IGP, manually add the auto-summary command for the unsecured IGP or remove the unsecured IGP for that inside interface.

- In Router MC, you must provide a subnet that is unique and not globally-routable for loopback. This subnet must only be used to support the implementation of loopback for GRE. The loopback interfaces are created, maintained, and used only by Router MC. You should not use them for any other purpose.
- If you are using static routes instead of unsecured IGP, make sure you configure static routes on the spokes through to the hub inside interfaces

Important Notes about Configuring GRE

- You can define GRE on the Global object or on any device group (with the exception of a High Availability (HA) group).
- You can define different GRE policies for different groups of devices within your hierarchy. If you define GRE on Global, the GRE settings will be inherited by all device groups and devices in the hierarchy. You can override the Global GRE policy by defining a different GRE policy on one or more device groups.
- Peering devices must be configured with the same failover and routing policy. Therefore, if you define a specific GRE policy on a device group, both the hub and the spoke must be descendants of that device group and there must be no overriding policy on a lower level that changes the GRE policy on either the peering hub or spoke.
- Switching from IKE keepalive to GRE—If you previously used IKE keepalive for failover, and you later switch to GRE, everything outside your attached networks will no longer be a part of your VPN. Attached networks include only those networks that are directly connected to the router's inside interfaces.

Restrictions for Generic Routing Encapsulation

- To run GRE configuration, you need to have IP connectivity between the cable modems.
- The Cisco uBR10012 router requires the Performance Routing Engine 2 (PRE2) modules for use with Generic Routing Encapsulation. The GRE feature is not supported for PRE1 modules in the Cisco uBR10012 router.

Information About Generic Routing Encapsulation

To configure the Generic Routing Encapsulation feature, you should understand the following concepts:

Tunneling

Tunneling (also known as port forwarding) is a technique that enables remote access users to connect to a variety of network resources through a public data network. The tunnels established through the public network

are usually point-to-point, though a multipoint tunnel is possible, and is use to link a remote user to a resource at the far end of the tunnel. Major tunneling protocols encapsulate Layer 2 traffic from the remote user and send it across the public network to the far end of the tunnel, where it is de-encapsulated and sent to its destination.

Tunneling requires three different protocols:

- Passenger protocol—The original data (IPX, NetBeui, IP) being carried.
- Encapsulating protocol—The protocol (GRE, IPSec, L2F, PPTP, and L2TP) that is wrapped around the original data.
- Carrier protocol—The protocol used by the network over which the information is traveling.

The original packet (Passenger protocol) is encapsulated inside the encapsulating protocol, which is then put inside the carrier protocol's header (usually IP) for transmission over the public network. Note that the encapsulating protocol also quite often carries out the encryption of the data. As you can see, protocols such as IPX and NetBeui, which would normally not be transferred across the Internet, can safely and securely be transmitted.

For site-to-site virtual private networks (VPNs), the encapsulating protocol is usually IPSec or Generic Routing Encapsulation (GRE). GRE includes information on what type of packet you are encapsulating and information about the connection between the client and server.

For remote-access VPNs, tunneling normally takes place using Point-to-Point Protocol (PPP). Part of the TCP/IP stack, PPP is the carrier for other IP protocols when communicating over the network between the host computer and a remote system. PPP tunneling will use one of PPTP, L2TP or Cisco's Layer 2 Forwarding (L2F).

The most significant benefit of Tunneling is that it allows for the creation of VPNs over public data networks to provide cost savings for both end users, who do not have to create dedicated networks, and for Service Providers, who can leverage their network investments across many VPN customers.

Generic Routing Encapsulation Overview

GRE Tunneling is a protocol for transporting an arbitrary network layer protocol (the payload) over another arbitrary network layer protocol (the delivery). This is achieved by encapsulating the payload packet in a delivery packet, along with a GRE header. By having both protocols encapsulate IP packets within an additional outer IP header, this enables the transport of IP multicast IP packets across a unicast-only backbone.

The following are some of the advantages of GRE tunnels:

- GRE tunnels provide multi-protocol local networks over a single-protocol backbone.
- GRE tunnels provide workarounds for networks that contain protocols with limited hop counts.
- GRE tunnels connect discontinuous sub-networks.
- GRE tunnels allow VPNs across WANs.

How to Configure Generic Routing Encapsulation

Use the following procedures to configure the GRE feature.

Before configuring the GRE feature:

- Please read the following topics:
  - Prerequisites for Generic Routing Encapsulation, on page 48
  - Important Notes about Configuring GRE, on page 49
- If workflow mode is enabled, make sure that you are working within the context of an open activity.

Step 1 Select Configuration > Settings

Step 2 Select General VPN> Failover and Routing in the TOC. The Failover and Routing page appears. the table describes the elements in the Failover and Routing page.

Step 3 Select GRE in the Policy Type list box.The page refreshes to display only the fields that are relevant for GRE configuration.

Step 4 Enter information in the displayed GRE fields, as required. Click Advanced to display additional GRE fields (optional). See the table for a description of each field.

Step 5 Click Apply.

What to Do Next

Table 4: Failover and Routing: GUI Reference

GUI Element	Description
Policy Type list box	Select the type of failover method you want to use. The page will refresh to display only the fields relevant for your selection. • IKE Keepalive • GRE. • GRE Dynamic IP • DMVPN
GRE Elements	
Routing Protocol list box	Select either EIGRP or OSPF as the routing protocol. See Prerequisites for Configuring and Deploying GRE for more information.
Tunnel Interface IP field	Enter a private IP address, including the subnet mask in bits, which defines a subnet in your enterprise to be used to support the implementation of loopback for GRE. For example, 192.10.9.1/255.255.255.0. Router MC creates a loopback interface on the peering devices, with an IP address from this subnet. The loopback interfaces serve as the GRE tunnel endpoints.

GUI Element	Description
Tunnel Source IP field	For GRE Dynamic IP only. Enter a private IP address, including the subnet mask in bits. **Note** To provide robust, stable tunnels, Router MC creates a static IP route using this IP address. If you change this IP address or you change the failover and routing policy, Router MC does not remove the static route from the device configuration. Please consider this if you have a problem with unstable GRE tunnels.
Enable IP Multicast check box	Select this check box to enable multicast transmissions across your GRE tunnels. IP multicast delivers application source traffic to multiple receivers without burdening the source or the receivers, while using a minimum of network bandwidth. When IP Multicast is enabled, you must specify a rendezvous point that acts as the meeting place for sources and receivers of multicast data.
Rendezvous Point field	This field is only editable when the IP Multicast check box is selected. Enter the IP address of the interface that will serve as the rendezvous point (RP) for multicast transmission. Sources send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree.
Allow direct spoke to spoke tunnels check box	For DMVPN only. Select this check box to enable direct communication between spokes, without going through the hub. **Note** Note With direct spoke-to-spoke communication, you must use the Main Mode Address option for preshared key negotiation.
Advanced or Basic button	Click the Advanced button to display additional fields for optional advanced configuration. Router MC provides default values for all the advanced options. You can change these default values if required. When the advanced fields are displayed, click the Basic button to display only the basic configuration fields and hide the advanced fields.

GUI Element	Description
Process Number field	Router MC adds an additional Interior Gateway Protocol (IGP) that is dedicated for IPSec and GRE secured communication. An IGP refers to a group of devices that receive routing updates from one another by means of a routing protocol, either EIGRP or OSPF. Each “routing group” is identified by a logical number, the process number. Enter a routing process number that will be used to identify the secured IGP that Router MC adds when configuring GRE. The number that you provide must be within the range specified next to the field name. The default is the lowest value in the range. This range can be changed in the Configuration Support Settings page in the Admin tab.
Delay	Specify the throughput delay for the interface, in seconds.
Hello Interval EIGRP	Specify the interval between hello packets sent on the interface, from 1 to 65535 seconds. The default is 5 seconds.
Hold Time EIGRP	Specify the number of seconds the router will wait to receive a hello message before invalidating the connection. The default hold time is 15 seconds (three times the hello interval).
Tunnel Key field	For DMVPN only. Enter a number that identifies the tunnel key. The tunnel key differentiates between different multipoint GRE (mGRE) tunnel Non Broadcast Multiple Access (NBMA) networks. All mGRE interfaces in the same NBMA network must use the same tunnel key value. If there are two mGRE interfaces on the same router, they must have different tunnel key values.
Network ID (NHRP) field	For DMVPN only. All NHRP stations within one logical NBMA network must be configured with the same network identifier. Enter a globally unique, 32-bit network identifier within the range of 1 to 4294967295.
Hold Time (NHRP) field	For DMVPN only. Enter the time in seconds that routers will keep information provided in authoritative Next Hop Resolution Protocol (NHRP) responses. The cached IP-to-NBMA (non-broadcast multi-access) address mapping entries are discarded after the hold time expires. The default is 600 seconds.
Authentication (NHRP) field	For DMVPN only. Enter an authentication string that controls whether the source and destination NHRP stations allow intercommunication. All routers within the same network using NHRP must share the same authentication string. The string can be up to eight characters long.
Apply button	Click to apply your definitions.

GUI Element	Description
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

Additional References

The following sections provide references related to the GRE feature.

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco CMTS Cable Command Reference, at the following URL: http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
Configuring GRE Tunnel over Cable	Configuring GRE Tunnel over Cable, at the following URL: http://www.cisco.com/en/US/tech/tk86/tk89/technologies_configuration_example09186a008011520d.shtml

Standards

Standard	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
RFC 1701	Generic Routing Encapsulation (GRE)
RFC 1702	Generic Routing Encapsulation over IPv4 networks
RFC 1853	IP in IP Tunneling
RFC 2003	IP Encapsulation within IP
RFC 2784	Generic Routing Ecapsulation (GRE)
RFC 2890	Key and Sequence Number Extensions to GRE

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Generic Routing Encapsulation

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below 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.

Feature Name	Release	Feature Information
Generic Routing Encapsulation	12.2(33)SCA	Generic Routing Encapsulation (GRE) is a tunneling protocol that enables the encapsulation of a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers.

CHAPTER 5

L2VPN Support over Cable

First Published: February 14, 2008

Last Updated: January 26, 2012

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

In Cisco IOS Release 12.2(33)SCA, the Layer 2 VPN (L2VPN) Support over Cable feature on the Cisco CMTS provides point-to-point Transparent LAN Service (TLS) in support of the Business Services over DOCSIS (BSOD) CableLabs specification.

The L2VPN Support over Cable feature in Cisco IOS Release 12.2(33)SCA differs from prior L2VPN and TLS support for cable in Cisco IOS release 12.3BC in the following ways:

- Both features use an Ethernet trunking interface to transport traffic for multiple L2VPN tunnels in support of different cable modems (CMs) and service flows (SFs) based on IEEE 802.1q VLAN IDs. For the the legacy TLS service, only the primary upstream or downstream SFs are used. With the new L2VPN Support over Cable feature, both primary and secondary SFs can be used.
- The TLS feature uses CLI to provision the service. The L2VPN Support over Cable feature uses the CM configuration file to provision the service, and a single CLI to identify the default Ethernet Network System Interface (NSI).
- Downstream traffic is forwarded on a per-CM basis and upstream traffic is forwarded on a per-SF basis. For L2VPN Support over Cable feature, upstream traffic for the same L2VPN can use multiple upstream service flows and downstream traffic can use different downstream service flows.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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

Contents

Prerequisites for L2VPN Support over Cable

- You should use crypto-supported images. Refer to the Release Notes for Cisco Universal Broadband Routers in Cisco IOS Release 12.2SC for the latest image information.
- Cable modems must be configured to support BPI+.

This table shows the hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 5: L2VPN Support over Cable Feature Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	**Cisco IOS Release 12.2(33)SCB and later** • Cisco uBR10-MC5X20U/H **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V [1]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V [2]
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V

1 Cisco uBR-MC3GX60V cable interface line card is not compatible with PRE2.
2 Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Restrictions for L2VPN Support over Cable

The L2VPN Support over Cable feature has the following general restrictions:

- DOCSIS 1.0 CMs are not supported.
- Load balancing and Dynamic Channel Change (DCC) are not supported for CMs that are enabled for L2VPN support.
- DSx messages (Dynamic Service Add [DSA], Dynamic Service Change [DSC], and Dynamic Service Delete [DSD]) are supported for L2VPN-provisioned CMs from Cisco IOS Release 12.2(33)SCF2 onwards. However, DSx with L2VPN type, length, values (TLVs) are not supported.
- Multipoint L2VPN is not supported, and any Simple Network Management Protocol (SNMP) MIBs for multipoint L2VPN are not supported.
- eSAFE (embedded Service/Application Functional Entities) DHCP snooping is not supported (L2VPN subtype 43.5.3)
- Maximum of 1024 L2VPNs are supported on a single MAC domain.
- Maximum of eight upstream SFs are supported per L2VPN service.
- Maximum of eight downstream classifiers are supported per L2VPN service.

- eSAFE exclusion is supported for only one eSAFE host. If the REG-REQ message for a compliant CM specifies multiple eSAFE hosts, then the eMTA (ifIndex 16) is selected as the eSAFE host to be excluded by the Cisco CMTS router. If the eMTA is not included as part of the capability of the CM, then the first eSAFE host in the capability is selected for exclusion.
- Maximum length of the Cable Modem Interface Mask (CMIM) is 4 bytes.
- Areas of the Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks specification that are not supported are:
  - Vendor-specific L2VPN encodings for the replacement of the required VPN ID and NSI Encapsulation subtype are not supported.
  - Mapping of egress user priority to an NSI port transmission traffic class as specified by IEEE 802.1s is not supported.
  - Forwarding with non-zero default user priority values with vendor-specific configuration is not supported.
  - Accepting multiple Downstream Classifier L2VPN Encoding with the same VPN ID to clasify packets to different service flows is not supported.
  - Assigning multiple SAIDs to the same L2VPN on the same CM is not supported. The primary SAID is used for encrypting all downstream traffic.
  - Assigning of the same group-level L2VPN SAID to different CMs on the same MAC domain attached to the same L2VPN identifier is not supported.
  - Implementing the DOCSIS Spanning Tree Protocol (DSTP) and transmission of DSTP BPDUs on all NSI and RF interfaces configured for L2VPN operation is not supported.
  - Implementing a DSTP SAID specifically for DSTP forwarding to the customer premises equipment (CPE) ports of all L2VPN CMs is not supported.

VPN ID Restrictions

- A maximum of four VPN IDs are supported for each CM.
- A maximum of one VPN ID can be associated with each SF in a CM; although multiple SFs in a CM can belong to the same L2VPN.
- A maximum of 4093 unique VPN IDs are supported per Cisco CMTS router.
- The maximum length of a VPN ID is 16 bytes.
- All L2VPN encodings must contain a VPN ID, except for upstream classifier encodings.

Information About L2VPN Support over Cable

L2VPN Support Over Cable provides the following benefits and functions on a Cisco CMTS router:

- Supports point-to-point L2VPN forwarding mode.
- Supports up to four VPN IDs per CM.

- Supports multiple upstream SFs per CM, with one or more SFs belonging to the same VPN ID.
- Supports a single Ethernet NSI that serves as a trunking port for one or more L2VPN tunnels on the Cisco CMTS router.
- Supports BPI+ encryption using primary SAID of the CM.
- Supports L2VPN encodings in the CM configuration file and CM registration (REG-REQ with L2VPN encoding).
- Supports upstream L2VPN tunnel in support of per-CM and per-SF forwarding.
- Supports synchronization and recovery of the L2VPN database and upstream and downstream SFs during PRE2 NSF/SSO and N+1 line card redundancy switchovers.
- Supports QoS in upstream and downstream.
- Supports stacked IEEE 802.1q tags.
- Supports exclusion of traffic from the L2VPN tunnel for a single Embedded Service/Application Functional Entity (eSAFE) host.
- Supports Layer 2 classifier via CMIM and IEEE 802.1p priority bits.
- Supports detection of provisioning errors, such as duplicate VLAN IDs across CMs or existing VLAN IDs in use, and moves a CM offline with a corresponding error message.
- Supports coexistence of L2VPN and non-L2VPN traffic on the same RF MAC domain, with non-L2VPN traffic isolated from other tunnel traffic.
- Supports voice calls from L2VPN-provisioned CMs. However, voice calls are not part of the L2VPN.
- Supports BSOD VLAN Redundancy feature, which allows users to configure a backup WAN interface in addition to the primary WAN interface. When the primary WAN interface is down, the L2VPN traffic flows through the backup WAN interface.
- Supports manual switchover for VLAN Redundancy feature, which allows users to manually switch active uplink port from the current port to another port when both the uplink ports are up.

Point-to-Point L2VPN Forwarding Mode

The Cisco CMTS routers in Cisco IOS Release 12.2(33)SCA support the point-to-point L2VPN forwarding mode described in the BSOD specification. Each attachment circuit (either SF or CM) on the Cisco CMTS router has a NSI encapsulation value, and is configured with an IEEE 802.1q VLAN ID.

The L2VPN forwarder on the Cisco CMTS router forwards both upstream and downstream traffic between the NSI port on the router and an attachment circuit without using MAC address learning for the forwarding decision. A L2VPN bridge on the backbone network of the cable operator performs the MAC-address learning to bridge packets between VLAN IDs.

shows an example of a point-to-point L2VPN network using IEEE 802.1q NSI encapsulation. In this example, four CMs are associated with four different VLAN IDs: 10, 20, 30, and 40. The L2VPN encoding of the CM includes the logical L2VPN ID (in this case, A or B) with an NSI encapsulation subtype for IEEE 802.1q with the associated VLAN ID.

The logical L2VPN IDs allow creation of separate broadcast domains for certain VLAN IDs. In the diagram, traffic for VLANs 10 and 20 from CM1 and CM2 can be sent to the network of Enterprise A, and traffic for VLAN's 30 and 40 from CM3 and CM4 can be sent to the network of Enterprise B.

Point-to-Point L2VPN Network Diagram 211306.eps

L2VPN Encodings in the CM Configuration File

The CM configuration file contains a set of L2VPN encodings that control how the Cisco CMTS processes L2VPN forwarding of upstream and downstream CPE packets. As per the BSOD specification, the L2VPN encoding is encapsulated using a General Extension Information (GEI) encoding, which uses the type code 43 and subtype of 5 (43.5) with the reserved Vendor ID of 0xFFFFFF.

L2VPN defines the following types of encodings:

- Per-CM L2VPN encodings—An encoding that appears at the top level of the CM configuration file.
- Per-SF L2VPN Encoding—An encoding that appears as a subtype of the Upstream Service Flow Encoding (type 24).
- Upstream Classifier L2VPN Encoding—An encoding that appears in an Upstream Packet Classification Configuration Setting (type 22).
- Downstream Classifier L2VPN Encoding—An encoding that appears in a Downstream Packet Classification Configuration Setting (type 23).

The simplest CM configuration file has a single per-SF L2VPN Encoding within the primary upstream SF definition and a single per-CM L2VPN Encoding with a NSI Encapsulation subtype for that L2VPN.

Note When BSOD (CM configuration file) is used for L2VPN configuration, and QoS policy-map settings are applied to Cisco CMTS WAN interfaces, the packets do not match the QoS policy-map. When CLI mode is used for L2VPN configuration, and QoS policy-map settings are applied to Cisco CMTS WAN interfaces, the packets will match the QoS policy-map first.

Note Starting from Cisco IOS 12.2(33)SCJ release, CMTS supports BSOD VLAN redundancy feature with support for two Ethernet Network Side Interface (NSI) configuration and a backup WAN interface. When the active NSI WAN interface is down, the L2VPN traffic flows through the backup WAN interface.

Supported L2VPN Encodings

This section describes the supported L2VPN encodings in the CM configuration file that are supported by the Cisco CMTS routers.

- The Cisco CMTS routers support the following CM capabilities:
  - L2VPN capability (5.17)
  - eSAFE host capability (5.18)
  - Downstream Unencrypted Traffic (DUT) filtering (5.19)
- The Cisco CMTS routers support the following top-level encodings:
  - VPN identifier (43.5.1)

- CMIM (43.5.4)—When provided, applies to all upstream SFs associated with an L2VPN tunnel; Supports only one eSAFE host.
- NSI encapsulation (43.5.2) with format code 2 for IEEE 802.1q (43.5.2.2)
- DUT filtering encoding

- The Cisco CMTS routers support the following per-SF encodings:
  - VPN identifier (43.5.1)
  - Ingress user priority (43.5.8)
- The Cisco CMTS routers support the following downstream classifier encodings:
  - VPN identifier (43.5.1)
  - CMIM (43.5.4) and (22/23.13)
  - User priority range (43.5.9)

For more information about the CM configuration file and L2VPN Encodings, see the “Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks” specification.

For information about how to use the configuration file generator on the Cisco CMTS, see the “DOCSIS Internal Configuration File Generator for the Cisco CMTS” document.

SNMPv3 Interface

L2VPN Support over Cable in Cisco IOS Release 12.2(33)SCA supports the following MIBs in SNMPv3:

- DOCSIS-L2VPN-MIB

For a link to the Cisco IOS MIB tools, see the http://tools.cisco.com/ITDIT/MIBS/servlet/index.

DOCSIS-L2VPN-MIB

The DOCSIS-L2VPN-MIB contains the SNMP management objects used by the Cisco CMTS router for L2VPN support. The MIB is bundled with the Cisco IOS software images that support the L2VPN Support over Cable feature.

Table 6: DOCSIS-L2VPN-MIB Tables , on page 63 lists the tables in the DOCSIS-L2VPN-MIB supported by the Cisco CMTS routers. For more information, see the MIB documentation.

Table 6: DOCSIS-L2VPN-MIB Tables

Object	Description
docsL2vpnIdToIndexTable	Indexed by the octet string DocsL2vpnIdentifier that provides the local agent's internally assigned docsL2vpnIdx value for that DocsL2vpnIdentifier value.

Object	Description
docsL2vpnIndexToIdTable	Indexed by agent's local docsL2vpnIdx that provides the global L2VPN Identifier.
docsL2vpnCmTable	Describes L2VPN per-CM information that is in common with all L2VPNs for the CM, regardless of forwarding mode.
docsL2vpnVpnCmTable	Describes the operation of L2VPN forwarding on each CM.
docsL2vpnVpnCmStatsTable	Contains statistics for forwarding of packets to and from a CM on each VPN.
docsL2vpnPortStatusTable	Displays summary information for the run-time state of each VPN that is currently operating on each bridge port.
docsL2vpnSfStatusTable	Displays SF-specific L2VPN forwarding status for each upstream service flow configured with a per-SF L2VPN encoding.
docsL2vpnPktClassTable	Provides the L2VPN-specific objects for packet classifiers that apply to only L2VPN traffic. The indices of this table are a subset of the indices of classifiers in the docsQosPktClassTable.
docsL2vpnCmNsiTable	Describes the NSI configuration for a single CM when operating in point-to-point forwarding mode for an L2VPN.

Voice-Call Support on L2VPN CM

Cisco IOS Release 12.2(33)SCF2 introduces the Voice-Call Support on L2VPN CM feature. This feature enables the Cisco CMTS routers to support dynamic service flows on L2VPN-provisioned cable modems to permit voice calls from a non-L2VPN CPE.

To provide voice-call support on a L2VPN CM, you have to configure correct classifiers and create two static service flows (primary and secondary) using the cable modem configuration file. If the eMTA is L2VPN-capable with the embedded CPE configured as an eSAFE host, then only one service flow is required. When correct CMIM bits are configured, the Cisco CMTS does not send packets from the eSAFE host to the L2VPN.

Though the L2VPN can be configured on the primary or secondary service flow, it cannot coexist with eMTAs on the same service flow. The eMTAs should always use a different service flow from that of L2VPN. The classifiers to direct the traffic should also be based on the service flows the L2VPN and eMTAs are using. When the above configuration is in place, the dynamic service flows are created automatically whenever voice calls are initiated.

How to Configure L2VPN Support over Cable

This section contains the following procedures:

Configuring the Ethernet Network System Interface

To configure the L2VPN Support over Cable feature, you need to specify an Ethernet NSI to operate as the trunking interface for the L2VPN traffic. You must configure the NSI using a command on the Cisco CMTS router. It is not configurable through the CM configuration file.

Before You Begin

The following interface types can be configured as an NSI for L2VPN Support over Cable:

- Cisco uBR10012 Universal Broadband Router—Gigabit Ethernet.
- Cisco uBR7246VXR Universal Broadband Router—Fast Ethernet or Gigabit Ethernet

Note The Cisco CMTS routers only support the configuration of a single L2VPN NSI per CMTS.
>

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable l2-vpn-service xconnect nsi dot1q interface***ethernet-intf***[backup-interface ethernet-intf]** **Example:** `Router(config)# cable l2-vpn-service xconnect nsi dot1q interface Te4/1/0 backup-interface Te4/1/4`	Configures WAN interface for DOT1Q L2VPN . (Optional) Backup-interface - If backup-interface is configured it means that BSoD VLAN redundancy feature is enabled.

Preparing the DOCSIS Configuration File for L2VPN Support

To support L2VPN, the DOCSIS configuration file must be configured with the appropriate encodings. For information about the supported encodings by the Cisco CMTS routers, see the L2VPN Encodings in the CM Configuration File, on page 62.

Manual Switchover Command Line Interface

Effective from Cisco IOS 12.2(33)SCJ Release, for BSOD VLAN Redundancy feature, users can manually switch active uplink ports from the active port to another port when both the uplink ports are up through the command line interface. To manually switchover, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **cable l2-vpn dot1q-nsi-redundancy force-switchover from** *active-nsi-interface*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted
Step 2	**cable l2-vpn dot1q-nsi-redundancy force-switchover from** *active-nsi-interface* **Example:** `Router# cable l2-vpn dot1q-nsi-redundancy force-switchover from Te4/0/1`	Switches the active uplink port from the current active port to the specified port.

Verifying L2VPN Support over Cable

To verify L2VPN information on the Cisco CMTS router, use the **show cable l2-vpn dot1q-vc-map** command.

SUMMARY STEPS

1. To display VLAN information for all cable modems, use the **show cable l2-vpn dot1q-vc-map** command as shown in the following example:
2. To display VLAN information for a particular L2VPN ID, use the **show cable l2 dot1q-vc-map vpn** form of the command as shown in the following example:
3. To display information for a particular L2VPN ID on a specific cable modem, use the **show cable l2-vpn dot1q-vc-map vpn** form of the command along with specification of the cable modem MAC address, as shown in the following example:
4. To display detailed information for a particular L2VPN ID on a specific cable modem, use the **show cable l2-vpn dot1q-vc-map vpn verbose** form of the command along with specification of the cable modem MAC address, as shown in the following example:
5. To display detailed information for a particular cable modem, use the the **show cable l2-vpn dot1q-vc-map verbose** form of the command along with specification of the cable modem MAC address, as shown in the following example:
6. To display the current redundancy information of a specific CM, use the **show cable l2-vpn xconnect interface verbose** command as shown in the following example:
7. To display the dot1q L2VPN uplink redundancy information, use the **show cable l2-vpn dot1q-nsi-redundancy** as shown in the following example:

DETAILED STEPS

Step 1 To display VLAN information for all cable modems, use the **show cable l2-vpn dot1q-vc-map** command as shown in the following example:

Example:

```
Router# show cable l2-vpn dot1q-vc-map
MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPN ID
0014.f8c1.fd66 GigabitEthernet4/0/0        68    Cable6/0/0  3    0234560001
```

Step 2 To display VLAN information for a particular L2VPN ID, use the **show cable l2 dot1q-vc-map vpn** form of the command as shown in the following example:

Example:

```
Router# show cable l2-vpn dot1q-vc-map vpn 0234560001

MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPNID
0014.f8c1.fd66 GigabitEthernet4/0/0        68    Cable6/0/0  3    0234560001
```

Step 3 To display information for a particular L2VPN ID on a specific cable modem, use the **show cable l2-vpn dot1q-vc-map vpn** form of the command along with specification of the cable modem MAC address, as shown in the following example:

Example:

```
Router# show cable l2-vpn dot1q-vc-map 0014.f8c1.fd66 vpn 0234560001
```

```
MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPNID
0014.f8c1.fd66 GigabitEthernet4/0/0        68    Cable6/0/0  3    0234560001
```

Step 4 To display detailed information for a particular L2VPN ID on a specific cable modem, use the **show cable l2-vpn dot1q-vc-map vpn verbose** form of the command along with specification of the cable modem MAC address, as shown in the following example:

Example:

```
Router# show cable l2-vpn dot1q-vc-map 0014.f8c1.fd66 vpn 0234560001 verbose
MAC Address                          : 0014.f8c1.fd66
Prim Sid                             : 3
Cable Interface                      : Cable6/0/0
VPN ID                               : 0234560001
L2VPN SAID                           : 12294
Upstream SFID                        : 23
Downstream CFRID[SFID]               : 2[24]
CMIM                                 : 0x60
Ethernet Interface                   : GigabitEthernet4/0/0
DOT1Q VLAN ID                        : 68
Total US pkts                        : 1372
Total US bytes                       : 500226
Total US pkt Discards                : 0
Total US byte Discards               : 0
Total DS pkts                        : 1248
Total DS bytes                       : 415584
Total DS pkt Discards                : 0
Total DS byte Discards               : 0
```

Step 5 To display detailed information for a particular cable modem, use the the **show cable l2-vpn dot1q-vc-map verbose** form of the command along with specification of the cable modem MAC address, as shown in the following example:

Example:

```
Router# show cable l2-vpn dot1q-vc-map 0014.f8c1.fd66 verbose
MAC Address                          : 0014.f8c1.fd66
Prim Sid                             : 3
Cable Interface                      : Cable6/0/0
L2VPNs provisioned                   : 1
DUT Control/CMIM                     : Enable/0xFFFFFFFF
VPN ID                               : 0234560001
L2VPN SAID                           : 12294
Upstream SFID                        : 23
Downstream CFRID[SFID]               : 2[24]
CMIM                                 : 0x60
Ethernet Interface                   : GigabitEthernet4/0/0
DOT1Q VLAN ID                        : 68
Total US pkts                        : 1374
Total US bytes                       : 501012
Total US pkt Discards                : 0
Total US byte Discards               : 0
Total DS pkts                        : 1250
Total DS bytes                       : 416250
Total DS pkt Discards                : 0
Total DS byte Discards               : 0
```

Step 6 To display the current redundancy information of a specific CM, use the **show cable l2-vpn xconnect interface verbose** command as shown in the following example:

Example:

```
Router# show cable l2-vpn xconnect dot1q 0025.2eab.8482 verbose
MAC Address                          : 0025.2eab.8482
Customer Name                        : Topgun
Prim Sid                             : 28
Cable Interface                      : Cable7/1/1
Primary Ethernet Interface           : TenGigabitEthernet4/0/1
Backup  Ethernet Interface           : TenGigabitEthernet4/0/7
```

```
Active  Ethernet Interface          : TenGigabitEthernet4/0/1
DOT1Q VLAN ID                       :207
Total US pkts                       : 151269
Total US bytes                      : 211755224
Total DS pkts                       : 150502
Total DS bytes                      : 210463324
```

Step 7 To display the dot1q L2VPN uplink redundancy information, use the **show cable l2-vpn dot1q-nsi-redundancy** as shown in the following example:

Example:

```
Router# show cable l2-vpn dot1q-nsi-redundancy
Primary-NSI Backup-NSI Active-NSI Elapsed-after-SW
Te4/1/0       Te4/0/4    Te4/1/0    31m9s
Te4/1/2       Te4/0/5    Te4/1/2    59s
```

Enabling Voice-Call on a L2VPN CM

You can enable the Voice-Call Support on a L2VPN CM feature by registering a cable modem with a SID to VPN mapping cable modem configuration file (MPLS or 802.1q).

- If the L2VPN is on the primary service flow, you should use a cable modem configuration file with static secondary service flow and the classifiers should be configured on the secondary service flow for non-L2VPN packets.
- If the L2VPN is on the secondary service flow, then classifiers should be configured for L2VPN packets.

Note The cable modem configuration file based L2VPN configuration provides the flexibility to configure L2VPN on the primary or secondary service flow. However, we recommend that you configure L2VPN on the secondary service flow and the primary service flow is used for the default traffic.

Note In a CLI-based L2VPN configuration, the L2VPN is on the primary service flow; therefore the static secondary service flow should be used for the eMTAs.

Verifying Dynamic Service Flows

To verify dynamically created service flows on the Cisco CMTS router, use the **show interface cable service-flow** command.

Note To verify information about PacketCable operations, use **show packetcable** commands.

```
Router# show interface cable 5/1/0 service-flow
Sfid : 30191
Mac Address : 000a.739e.140a
Type : Secondary(Dynamic)
Direction : Upstream
```

```
Current State : Active
Current QoS Indexes [Prov, Adm, Act] : [0, 24, 24]
Active Time : 00:55
Sid : 7140
Admitted QoS Timeout : 200 seconds
Active QoS Timeout : 0 seconds
Packets : 1824
Bytes : 466944
Rate Limit Delayed Grants : 0
Rate Limit Dropped Grants : 0
Current Throughput : 68356 bits/sec, 32 packets/sec
Classifiers:
Classifier Id : 41
Service Flow Id : 30191
CM Mac Address : 000a.739e.140a
Direction : upstream
Activation State : active
Classifier Matching Priority : 128
PHSI : 1
Number of matches : -
IP Classification Parameters:
IP Source Address : 10.8.230.3
Source IP Address Mask : 255.255.255.255
Destination IP Address : 172.16.2.35
Destination IP Address Mask : 255.255.255.255
IP Protocol Type : 17
Source Port Low : 53456
Source Port High : 53456
Destination Port Low : 7052
Destination Port High : 7052
```

Configuration Examples for L2VPN over Cable

This section provides configuration examples for the L2VPN over Cable feature:

Example: Specifying the Ethernet NSI Interface

You can specify the Ethernet NSI within the CM configuration file, or using the **cable l2-vpn-service xconnect** global configuration command as shown in the following example:

```
cable l2-vpn-service xconnect nsi {dot1q|mpls}
```

Example: Enabling Voice Call Support on MPLS L2VPN

The following is a sample cable modem configuration file that enables voice call support on MPLS L2VPN. In this example the L2VPN is applied to the primary service flow.

```
03 (Net Access Control)         = 1
18 (Maximum Number of CPE)      = 16
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 06 26 04
 00 00 01 90
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 2
   S03 (Service Flow Reference)         = 2
   S09 (IP Packet Encodings)
       T03 (IP Source Address)          = 050 001 005 000
       T04 (IP Source Mask)             = 255 255 255 000
```

```
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 3
   S03 (Service Flow Reference)         = 2
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 e0 f7 5a c9 21
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 21
   S03 (Service Flow Reference)         = 21
   S05 (Rule Priority)                  = 5
   S09 (IP Packet Encodings)
       T05 (IP Destination Address)     = 050 001 005 000
       T06 (IP Destination Mask)        = 255 255 255 000
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 22
   S03 (Service Flow Reference)         = 21
   S05 (Rule Priority)                  = 5
   S10 (Ethernet LLC Packet Classification Encodings)
       T01 (Destination MAC Address)    = 00 e0 f7 5a c9 21 ff ff ff ff ff ff
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 (Unknown sub-type)  = 01 04 32 30 32 30
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 2
   S06 (QoS Parameter Set Type)         = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 20
   S06 (QoS Parameter Set Type)         = 7
   S07 (Traffic Priority)               = 0
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 21
   S06 (QoS Parameter Set Type)         = 7
   S07 (Traffic Priority)               = 1
29 (Privacy Enable)             = 1
```

Example: Enabling Voice Call Support on 802.1q L2VPN

The following is a sample cable modem configuration file that enables voice call support on 802.1q L2VPN. In this example the L2VPN is applied to the secondary service flow.

```
03 (Net Access Control)         = 1
43 (Vendor Specific Options)
   S08 (Vendor ID)      = ff ff ff
   S005 (Unknown sub-type)      = 01 05 02 34 56 00 01 02 04 02 02 00 44
18 (Maximum Number of CPE)      = 16
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 2
   S03 (Service Flow Reference)         = 2
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 e0 14 e3 23 1c
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 4
   S03 (Service Flow Reference)         = 4
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = ff ff ff
       T005 (Unknown sub-type)  = 01 05 02 34 56 00 01
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority)   = 00 07
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
       T005 (Unknown sub-type)  = 01 05 02 34 56 00 01 08 01 01
```

```
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 3
   S06 (QoS Parameter Set Type)         = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 4
   S06 (QoS Parameter Set Type)         = 7
```

Example: Enabling Voice Call Support on CLI-based L2VPN

The following is a sample cable modem configuration file that enables voice call support on L2VPN configured using CLI. L2VPN configured using the CLI is always applied to the primary service flow.

```
03 (Net Access Control)         = 1
18 (Maximum Number of CPE)      = 16
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 2
   S03 (Service Flow Reference)         = 2
   S09 (IP Packet Encodings)
       T03 (IP Source Address)          = 050 001 005 000
       T04 (IP Source Mask)             = 255 255 255 000
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 3
   S03 (Service Flow Reference)         = 2
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 e0 f7 5a c9 21
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 21
   S03 (Service Flow Reference)         = 21
   S05 (Rule Priority)                  = 5
   S09 (IP Packet Encodings)
       T05 (IP Destination Address)     = 050 001 005 000
       T06 (IP Destination Mask)        = 255 255 255 000
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 22
   S03 (Service Flow Reference)         = 21
   S05 (Rule Priority)                  = 5
   S10 (Ethernet LLC Packet Classification Encodings)
       T01 (Destination MAC Address)    = 00 e0 f7 5a c9 21 ff ff ff ff ff ff
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)         = 77
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 20
   S06 (QoS Parameter Set Type)         = 7
   S07 (Traffic Priority)               = 0
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 21
   S06 (QoS Parameter Set Type)         = 7
   S07 (Traffic Priority)               = 1
29 (Privacy Enable)             = 1
```

Additional References

The following sections provide references related to the L2VPN Support over Cable feature.

Related Documents

Related Topic	Document Title
SNMP configuration information	*Cisco IOS Configuration Fundamentals Configuration Guide,* Part 3: Cisco IOS System Management, "Configuring SNMP Support" section http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf014.html
SNMP command information	*Cisco IOS Network Management Command Reference , Release 12.2SB* http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/command/reference/nm_book.html

Standards

Standard	Title
CM-SP-BPI+-I12-050812	*Baseline Privacy Plus Interface Specification* http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-BPI+-C01-081104.pdf
CM-SP-L2VPN-I03-061222	*Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks* http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-L2VPN-I12-131120.pdf
CM-SP-RFIv2.0-I11-060602	*Radio Frequency Interface Specification* http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-RFIv2.0-C02-090422.pdf
IEEE 802.1ad	*IEEE 802.1ad-2005 IEEE Standards for Local and metropolitan area networks*— Virtual Bridged Local Area Networks http://www.ieee.org
IEEE 802.1q	*IEEE Std 802.1Q Virtual Bridged Local Area Networks* http://www.ieee.org

MIBs

MIB	MIBs Link
DOCS-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: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
RFC 2685	Virtual Private Networks Identifier http://www.ietf.org/rfc/rfc2685.txt
RFC 4364	*BGP/MPLS IP Virtual Private Networks (VPNs)* http://www.ietf.org/rfc/rfc4364.txt

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 L2VPN Support over Cable

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below 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.

Table 7: Feature Information for L2VPN Support Over Cable

Feature Name	Releases	Feature Information
L2VPN Support over Cable	12.2(33)SCA	This feature was introduced and provides point-to-point Transparent LAN Service (TLS) in support of the Business Services over DOCSIS (BSOD) CableLabs specification. The **cable l2-vpn-service default-nsi** command is introduced.
L2VPN Support over Cable	12.2(33)SCC	The **cable l2-vpn-service default-nsi** command is replaced with **cable l2-vpn-service xconnect nsi** {**dot1q** | **mpls**} command.
Voice-Call Support on L2VPN CM	12.2(33)SCF2	This feature allows you to enable voice calls on L2VPN-provisioned cable modem.

CHAPTER 6

MPLS Pseudowire for Cable L2VPN

First Published: November 16, 2009

Last Updated: June 20, 2011

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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

Contents

• Feature Information for MPLS Pseudowire for Cable L2VPN, page 112

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 like the c7600, if the CMTS is using VLAN as pseudowire type.

The table shows the CMTS hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 8: Hardware Compatibility Matrix for MPLS Pseudowire for Cable L2VPN Feature

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • PRE2 Cisco IOS Release 12.2(33)SCB and later • PRE4 Cisco IOS Release 12.2(33)SCH and later • PRE5	**Cisco IOS Release 12.2(33)SCB and later** • Cisco uBR10-MC5X20U/H **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V Cisco IOS Release 12.2(33)SCE and later • Cisco uBR-MC3GX60V [3]
Cisco uBR7246VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V [4]

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR7225VXR Universal Broadband Router	Cisco IOS Release 12.2(33)SCA and later • NPE-G1 Cisco IOS Release 12.2(33)SCB and later • NPE-G2	Cisco IOS Release 12.2(33)SCA and later • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X Cisco IOS Release 12.2(33)SCD and later • Cisco uBR-MC88V

[3] The Cisco uBR-3GX60V cable interface line card is not compatible with PRE2.
[4] The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

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 and 3.0-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.

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:

- 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

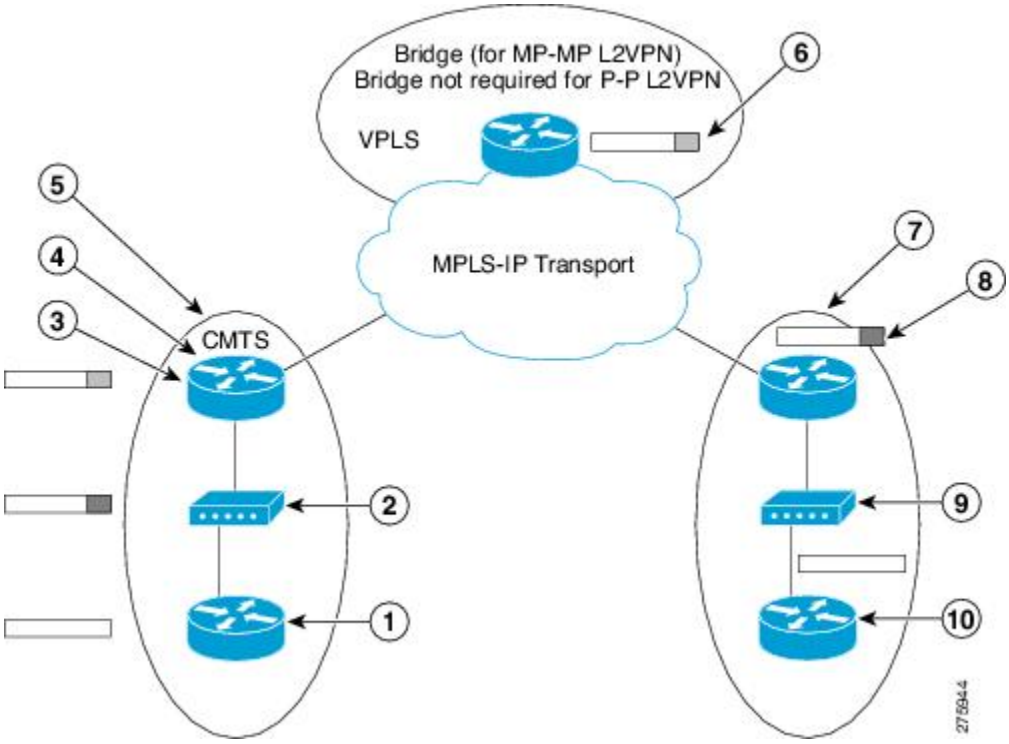
The MPLS subsystem removes DOCSIS encapsulation for Layer 2 Ethernet frames and adds MPLS labels at the ingress provider edge (PE) Cisco CMTS router. Then, the MPLS subsystem sends resulting MPLS packets to the corresponding PE router at the other end of the pseudowire. The PE routers must be configured 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 4: 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. For details on the tasks required to enable MPLS, see the How to 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, on page 96.

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 95.

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 9: 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.

TLV Name	Type	Length	Value and Description
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.

TLV Name	Type	Length	Value and Description
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 10: 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.

TLV Name	Type	Length	Value	Description
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 11: 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.

TLV Name	Type	Length	Value	Description
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.
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.

TLV Name	Type	Length	Value	Description
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.

TLV Name	Type	Length	Value	Description
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.

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	**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.

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 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.

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.

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 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.

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	**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.

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.

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 of MPLS Pseudowires

Static provisioning of MPLS pseudowires is not required if you have already provisioned MPLS pseudowires using the dynamic provisioning method.

Note
- You can provision only one MPLS pseudowire per L2VPN.
- Only one Ethernet service instance can exist per MPLS pseudowire configuration.

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	**cable l2vpn** *mac-address [customer-name]* **Example:** `Router(config)# cable l2vpn 0000.396e.6a68 customer1`	Specifies L2VPN MAC address and enters L2VPN *configuration mode.*

	Command or Action	Purpose
Step 4	**service instance** *id service-type* **Example:** `Router(config-l2vpn)# service instance 2000 ethernet`	Specifies the service instance ID and enters Ethernet service configuration mode.
Step 5	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** [*pw-type*] **Example:** `Router(config-ethsrv)# xconnect 101.1.0.2 221 encapsulation mpls pw-type 4`	Specifies the tunneling method to encapsulate the data in the MPLS pseudowire.
Step 6	**cable set mpls-experimental** *value* **Example:** `Router(config-ethsrv)# cable set mpls-experimental 7`	Specifies the experimental bit on the MPLS pseudowire. The valid range is from 0 to 7.
Step 7	**end** **Example:** `Router(config-ethsrv)# end`	Exits Ethernet service configuration mode and enters global configuration mode.

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. Cisco Specific L2VPN TLVs lists Cisco-specific TLVs introduced in Cisco IOS Release 12.2(33)SCF to support the L2VPN Pseudowire Redundancy feature.

Perform the steps given below to configure a backup pseudowire.

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	**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.

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	**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} •	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.

	Command or Action	Purpose

	Example:
	`Router(config-xconn)# backup delay 10 10`
	
	Example:
	`Router(config-xconn)# backup delay 10 never`
		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:** `Router(config-xconn)# end`	Exits xconnect configuration mode and enters privileged EXEC mode.

Performing Manual Switchover

Perform the steps given below to perform a manual switchover to the primary or backup pseudowire. The **cable l2vpn 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.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**cable l2vpn xconnect backup force-switchover peer 10.10.1.1 123** **Example:** `Router# cable l2vpn 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 LDP router ID and the status of the LDP discovery process, use the **show mpls ldp discovery command** as **shown in the following example:**

```
Router# show mpls ldp discovery
 Local LDP Identifier:
    10.10.1.1:0
    Discovery Sources:
    Targeted Hellos:
        10.10.1.1 -> 10.76.1.1 (ldp): active/passive, xmit/recv
            LDP Id: 10.76.1.1:0
```

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       CktID      Cable Intf  SID  Customer
Name/VPNID
0000.396e.6a68  101.1.0.2       221        Bu254:221    Cable7/0/0  1    customer1
0014.f8c1.fd66  10.76.1.1       2004       Bu254:5121   Cable7/0/0  8
0019.474a.d566  10.76.1.1       2001       Bu254:5122   Cable7/0/0  4    0234560002
0019.474a.d42e  10.76.1.1       2002       Bu254:2003   Cable7/0/0  5    0234560003
```

To verify the mapping between the MPLS pseudowire and virtual circuits for all cable modems (when pseudowire redundancy is not configured in Cisco IOS Release 12.2(33)SCF and later releases), 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 in Cisco IOS Release 12.2(33)SCF and later releases), 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
                10.76.2.1      600    Bkup    4  Bu254:600
0014.f8c1.fd46  10.2.3.4       1000   Prim*      Bu254:1000   Cable8/0/0  1   2020
                10.76.2.1      45454  Bkup    1  Bu254:45454
```

```
0014.f8c1.fd46  10.76.2.1      1800   Prim*      Bu254:1800   Cable8/0/0  1   2021
                10.2.3.4       55     Bkup    1  Bu254:55
```

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

```
Router# show cable l2-vpn xconnect mpls-vc-map state
Peer IP Address  VCID       STATE MAC Address    Customer Name/VPNID  STATE
101.1.0.2        22         DOWN  0000.396e.6a68  customer1            UP
10.76.1.1        2004       UP    0014.f8c1.fd66                       UP
10.76.1.1        2001       UP    0019.474a.d566  0234560002           UP
10.76.1.1        2002       UP    0019.474a.d42e  0234560003           UP
```

To obtain the state of all virtual circuits associated with an MPLS pseudowire (when pseudowire redundancy is not configured in Cisco IOS Release 12.2(33)SCF and later releases), 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
0025.2e2d.7252  10.76.2.1       400    Prim*        UP                        UP
0014.f8c1.fd46  10.2.3.4        1000   Prim*        UP    2020                UP
0014.f8c1.fd46  10.76.2.1       1800   Prim*        UP    2021                UP
```

To obtain the state of all virtual circuits associated with an MPLS pseudowire (when pseudowire redundancy is configured in Cisco IOS Release 12.2(33)SCF and later releases), 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
0025.2e2d.7252  10.76.2.1       400    Prim*        UP                        UP
                10.76.2.1       600    Bkup    4    UP                        STDBY
0014.f8c1.fd46  10.2.3.4        1000   Prim*        UP    2020                UP
                10.76.2.1       45454  Bkup    1    UP    2020                STDBY
0014.f8c1.fd46  10.76.2.1       1800   Prim*        UP    2021                UP
                10.2.3.4        55     Bkup    1   DOWN   2021                STDBY
```

To verify information about the MPLS pseudowire mapping for a particular MAC address of a CM (when pseudowire redundancy is configured in Cisco IOS Release 12.2(33)SCF and later releases), 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 in Cisco IOS Release 12.2(33)SCF and later releases), 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, 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

The following sections provide references related to the MPLS pseudowire functionality.

Related Documents

Related Topic	Document Title
Cisco IOS CMTS Cable Command Reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
L2VPN Support Over Cable	*Cisco IOS CMTS Cable Software Configuration Guide, Release 12.2SC* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_l2vpn.html
Any Transport over MPLS	*Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.4T* http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-1mt/mp-any-transport.html

Related Topic	Document Title
Label Distribution Protocol	MPLS Label Distribution Protocol http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/ftldp41.html

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: http://tools.cisco.com/ITDIT/MIBS/servlet/index

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 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

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below 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.

Table 12: Feature Information for MPLS Pseudowire for Cable L2VPN

Feature Name	Releases	Feature Information
MPLS Pseudowire for Cable L2VPN	12.2(33)SCC	The MPLS Pseudowire for Cable L2VPN feature is an extension to the existing DOCSIS L2VPN functionality using an Ethernet VLAN on Cisco uBR10012 routers and Cisco uBR7200 Series routers. The following commands were introduced or modified: • **cable l2vpn** • **cable l2-vpn-service xconnect** • **cable set mpls-experimental** • **service instance** • **show cable l2-vpn xconnect** • **show mpls l2transport vc** • **show xconnect** • **xconnect**
L2VPN Pseudowire Redundancy	12.2(33)SCF	The L2VPN Pseudowire Redundancy feature enables you to configure a backup pseudowire in case the primary pseudowire fails. The following sections provide information about this feature: The following commands were introduced or modified: • **backup delay** • **backup peer** • **cable l2-vpn xconnect backup force-switchover** • **show cable l2vpn xconnect** • **show mpls l2transport vc** • **show xconnect**

CHAPTER 7

Point-to-PointProtocoloverEthernetTermination on the Cisco CMTS

First Published: February 14, 2008

Last Updated: December 18, 2008

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco uBR7246VXR and Cisco uBR7225VXR CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS BC releases.

This chapter describes the PPPoE Termination feature, which allows service providers to extend their existing PPP dial-up provisioning systems to users on cable networks by encapsulating the PPP packets within Ethernet MAC frames.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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

Contents

Prerequisites for PPPoE Termination

The PPPoE Termination feature has the following prerequisites:

- The PPPoE Termination feature is supported only on the Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers.
- The Cisco CMTS router must be running Cisco IOS Release 12.2(4)BC1a or later release. In addition, to support the PPPoE Termination feature, the software image name must include the IP+ feature set (the letters “i” and “s” must appear in the software image name).
- To support PPPoE Termination on bundled cable interfaces, the Cisco CMTS router must be running Cisco IOS Release 12.2(8)BC2 or later release.
- Client software must support the PPPoE Termination protocol. If the computer operating system does not include such support, the user can use client software such as WinPoet.
- If planning on a large number of PPPoE sessions and traffic, increase the size of the packet hold queues on the WAN interfaces (ATM, DPT, Gigabit Ethernet, etc.), using the **hold-queue** *packet-size* {**in** | **out**} command. For example:

```
Router(config)# interface gigabitethernet 1/0
Router(config-if)# hold-queue 4096 in
Router(config-if)# hold-queue 4096 out
Router(config-if)#
```

Restrictions for PPPoE Termination

The PPPoE Termination feature has the following restrictions and limitations:

- The PPPoE Termination feature is only supported on the Cisco uBR7100 series routers and Cisco uBR7246VXR router, using Cisco IOS Release 12.2(4)BC1a or later. It is not supported on the Cisco uBR10012 router.
- The PPPoE Termination feature is not supported on any Cisco CMTS router when using Cisco IOS Release 12.1 EC.
- Effective with Cisco IOS Release 12.2(33)SCD, the PPPoE Termination feature is not supported on the Cisco uBR7200 router.
- PPPoE Forwarding is not supported on any Cisco CMTS.

- Table 13: Absolute Maximum Number of PPPoE Sessions, on page 117 shows the absolute maximum number of PPPoE sessions supported on the Cisco uBR7100 series routers, and on the Cisco uBR7246VXR router when using different processor cards.

Table 13: Absolute Maximum Number of PPPoE Sessions

Processor	Absolute Maximum Number of PPPoE Sessions
Cisco uBR7100 series	4000
NPE-225	4000
NPE-300[5]	4000
NPE-400	8000
NPE-G1	10000

5 The NPE-300 processor reached its end-of-life milestone on August 15, 2001.

Note The maximum number of active, simultaneous PPPoE sessions is much less (approximately 600 to 800), depending on the number of amount of memory onboard the processor card, the type of cable interface cards being used, the bandwidth being consumed by each user, and the router's configuration.

Information About PPPoE Termination

This section describes the PPPoE Termination feature:

Feature Overview

The Point-to-Point Protocol over Ethernet (PPPoE) feature supports PPPoE on cable interfaces, allowing service providers to extend their existing PPP dial-up provisioning systems to users on cable networks. When PPPoE Termination is enabled, the Cisco CMTS encapsulates PPP packets in Ethernet frames within PPPoE sessions.

When the Cisco CMTS receives PPPoE traffic from PPPoE sessions that are initiated by the user's PC, the Cisco CMTS either terminates the PPPoE sessions on the cable interface or transmits the PPPoE traffic through a secure tunnel connection, depending on the Cisco CMTS configuration. The following are the most typical configurations:

- Internet access—For residential customers and other users who want only basic Internet access, traffic is sent out on the WAN interface as standard IP packets. The service provider can use the same provisioning systems as they use for their dial-up users and other broadband users. The PPPoE session exists only between the cable modem and Cisco CMTS, simplifying network management and configuration.

- Secure corporate access—For businesses or telecommuters, traffic is forwarded over a Layer 2 point-to-point Tunneling Protocol (L2TP) tunnel to a L2TP network server (LNS) to create secure corporate intranet access. Cable modem users can access company resources as if they were directly connected to the corporate network, without compromising network security. This tunnel can be built over whatever interface is being used with the corporate site (Ethernet, ATM, and so forth).

When using the L2TP tunnel configuration, the Cisco CMTS acts as the L2TP Access Concentrator (LAC), or Network Access Server (NAS). The endpoint of the tunnel is the LNS, which can be a router such as a Cisco 6400 Carrier-Class Broadband Aggregator.

When the cable modem, acting as a bridge, receives its PPPoE session traffic, it forwards the traffic on to the hosts and other customer premises equipment (CPE) devices that are connected behind it. Users at these hosts or CPE devices can use standard PPP to log on to the cable network and obtain their IP addresses and other network information. Users can automate this procedure by using a router that supports PPPoE or by using standard PPPoE software, such as WinPoet.

User names and passwords can be included in the Cisco CMTS configuration, or the service provider can use the same Remote Authentication Dial-In User Service (RADIUS) authentication servers as they use for their dial-up and digital subscriber line (DSL) users. For example, the Cisco Subscriber Registration Center (CSRC) provides an Access Registrar that provides RADIUS server authentication.

The PPPoE Termination feature supports simultaneous use of PPPoE clients and Dynamic Host Configuration Protocol (DHCP) clients behind the same cable modems. Subscribers can use PPPoE for their initial log on to the cable network, and then use DHCP to allow their other PCs and other hosts to obtain IP addresses for network access.

Note The Cisco CMTS routers do not support PPPoE Forwarding, which receives PPPoE packets from an incoming interface and forwards them out on an outgoing interface. The Cisco uBR7100 series routers do automatically forward PPPoE traffic when configured for MxU bridging mode (which is supported only on Cisco IOS Release 12.1 EC), but this is a consequence of the bridging configuration and not due to any PPPoE support.

Benefits

The PPPoE Termination feature provides the following benefits to cable service providers and their partners and customers:

- PPPoE complements and does not interfere with the standard DOCSIS registration and authentication procedures that are used for cable modems.
- PPPoE can be used on existing customer premise equipment, by extending the PPP session over the bridged Ethernet LAN to the PC (host).
- PPPoE preserves the point-to-point session used by ISPs in a dial-up model, without requiring an intermediate set of IP communications protocols.
- Service providers can use their existing dial-up PPP provisioning and authentication systems for users on the cable network.
- PPPoE supports the security features, such as Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP), that are built into PPP systems.
- Service providers can support both PPPoE clients and DHCP-based hosts behind the same cable modem.

How to Configure the PPPoE Termination Feature

Note For Point-to-Point over Ethernet (PPPoE) configuration on the Cisco uBR7200 series routers beginning in Cisco IOS Release 12.2(33)SCA, the **bba-group** command replaces the **vpdn-group** command. The software will automatically convert an existing **vpdn-group** configuration to **bba-group** global configuration. After the configuration of **bba-group**, you cannot configure PPPoE at the VPDN level. You need to use the **bba-group** configuration.

This section describes the following tasks that are needed to implement the PPPoE Termination feature. All procedures are required, depending on the router's configuration.

Enabling VPDN Operations on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to enable virtual private dialup network (VPDN) operations on the Cisco CMTS router that is acting an L2TP access concentrator (LAC). This procedure must be done before performing any of the other configuration procedures.

Note This procedure also must be performed on the Cisco router that is acting as the L2TP network server (LNS).

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	
	Example:
	`Router(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 3	**buffers small {initial | max-free | permanent} 1024**
	
	Example:
	`Router(config)# buffers small initial 1024`
	
	Example:
	`Router(config)# buffers small max-free 1024`
	
	Example:
	`Router(config)# buffers small permanent 1024`
	
	Example:
	`Router(config)#`
		(Optional) Increases the size of the buffers on the router that are used for small packets to account for the larger number of keepalive packets that are sent during PPPoE sessions.
		
		Note Repeat this command for each type of small packet buffers.

Step 4	**vpdn enable**
	
	Example:
	`Router(config)# vpdn enable`
	
	Example:
	`Router(config)#`
		Enables virtual private dial-up networking (VPDN).

Step 5	**vpdn logging**
	
	Example:
	`Router(config)# vpdn logging`
	
	Example:
	`Router(config)#`
		(Optional) Enable logging for VPDN operations. Logging is automatically disabled by default (**no vpdn logging**) when you enable VPDN. Use this command to enable logging.

Step 6	**username** *user-name* **password** [*level*] *password*
	
	Example:
	`Router(config)# username pppoe-user1@client.com password 0 pppoepassword`
	
	Example:
	`Router(config)#`
		Specifies a username and password for each user to be granted PPPoE access:
		
		• *user-name* = Username that the user uses to log in.
		• *level* = (Optional) Encryption level for the password. The valid values are 0 (default, the following password is not encrypted) and 7 (the following password is encrypted—this option is typically used only when cutting and pasting configurations from other routers).
		• *password* = Password that the above user must use to log in and create a PPPoE user session.

	Command or Action	Purpose
		Note This step is not required if you are using an external server, such as a RADIUS server, to perform user authentication.

Step 7	**exit**
	
	Example:
	`Router(config)# exit`
	
	Example:
	`Router#`
		Exits global configuration mode.

Configuring a Virtual Template on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to create and configure a virtual template on the Cisco CMTS router when it is acting as a LAC. This procedure is required because the Cisco CMTS uses the virtual template to configure the virtual interfaces it creates for each individual PPPoE session.

Note At least one virtual template must be created on the router to support PPPoE sessions from cable modem users.

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	
	Example:
	`Router(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 3	**interface virtual-template** *number*
	
	Example:
	`Router(config)# interface virtual-template 1`
	
	Example:
	`Router(config-if)#`
		Select the number of the virtual-template interface to be configured and enters interface configuration mode.
		
		Note You can create up to 200 virtual interfaces on each router.

Step 4	**ip unnumbered** *interface*
	
	Example:
	`Router(config-if)# ip unnumbered Ethernet2/0`
	
	Example:
	`Router(config-if)#`
		Enables the virtual template interfaces to process IP packets by using the IP address of the specified interface, as opposed to assigning a unique IP address to each virtual interface.

Step 5	**ip mtu 1492**
	
	Example:
	`Router(config-if)# ip mtu 1492`
	
	Example:
	`Router(config-if)#`
		Configures the maximum transmission unit (MTU) size to 1492 bytes to allow for the eight additional header bytes used by the PPP and PPPoE encapsulation.

Step 6	**keepalive** *period* [*retries*]
	
	Example:
	`Router(config-if)# keepalive 60 10`
	
	Example:
	`Router(config-if)#`
		(Optional) Specifies how often and how many times the router should send keepalive messages on the virtual interface without receiving a response before bringing down the tunnel protocol and ending that particular PPPoE session.
		• *period* = Specifies how long, in seconds, the router should send a keepalive message and wait for a response. The valid range is 0 to 32767 seconds, with a default of 10.
		• *retries* = (Optional) Specifies the number of times the router will resend a keepalive packet without receiving a response. The valid range is 1 to 255, with a default of 5.
		
		Note Increasing the keepalive period and number of retries might be necessary when supporting a large number of PPPoE sessions.

Step 7	**peer default ip address pool** *name* [*name2* ...] **Example:** `Router(config-if)# peer default ip address pool local`	(Optional) Defines one or more pools of addresses to be used when assigning IP addresses to the PPPoE clients.

	Command or Action	Purpose
	Example: `Router(config-if)#`	

Step 8	**ppp authentication** {**chap** | **ms-chap** | **pap**}
	Example:
	`Router(config-if)# ppp authentication chap`
	Example:
	`Router(config-if)#`
		Defines the authentication method to be used for PPPoE sessions:
		• **chap** = Challenge Handshake Authentication Protocol
		• **ms-chap** = Microsoft's version of CHAP
		• **pap** = Password Authentication Protocol

Step 9	**ppp timeout authentication** *response-time*
	Example:
	`Router(config-if)# ppp timeout authentication 10`
	Example:
	`Router(config-if)#`
		(Optional) Specifies the maximum time, in seconds, that the router should wait for a response to a PPP authentication packet. The valid range is 0 to 255 seconds, with a default of 10 seconds.
		Note Increase this timeout if PPPoE sessions begin failing due to timeout errors.

Step 10	**ppp timeout retry** *timeout*
	Example:
	`Router(config-if)# ppp timeout retry 5`
	Example:
	`Router(config-if)#`
		(Optional) Specifies the maximum time, in seconds, that the router should wait for a response during PPP negotiation. The valid range is 1 to 255 seconds, with a default of 2 seconds.
		Note Increase this timeout if PPPoE sessions begin failing due to timeout errors.

Step 11	**no logging event link-status**
	Example:
	`Router(config-if)# no logging event link-status`
	Example:
	`Router(config-if)#`
		(Optional) Disables sending unnecessary link up and link down event messages to the router's event log. These messages would otherwise be sent each time a PPPoE session begins and ends.

Step 12	**no cdp enable** **Example:** `Router(config-if)# no cdp enable`	(Optional) Disables the use of the Cisco Discovery Protocol (CDP) on the virtual interface. This protocol is unnecessary on a virtual interface for PPPoE sessions.

	Command or Action	Purpose
	Example: `Router(config-if)#`	

Step 13	**exit**
	Example:
	`Router(config-if)# exit`
	Example:
	`Router(config)#`
		Exits interface configuration mode.

Step 14	**exit**
	Example:
	`Router(config)# exit`
	Example:
	`Router#`
		Exits global configuration mode.

Configuring a VPDN Group for PPPoE Sessions

Use the following commands, starting in user EXEC mode, to create and configure a virtual private dialup network (VPDN) group on the Cisco CMTS router that is acting an L2TP access concentrator (LAC). The router uses the VPDN group to configure the PPPoE sessions it creates for cable modem users. This step is required on the Cisco CMTS.

Note You can create only one VPDN group to support PPPoE sessions.

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	Example:
	`Router> enable`
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	
	Example:
	`Router(config)#`
		Enters global configuration mode.

Step 3	**vpdn-group** *name*
	
	Example:
	`Router(config)# vpdn-group 1`
	
	Example:
	`Router(config-vpdn)#`
		Creates a VPDN group with the specified name or number and enters VPDN-group configuration mode.

Step 4	Router(config-vpdn)# **accept-dialin**
	
	Example:
	`Router(config-vpdn)# accept-dialin`
	
	Example:
	`Router(config-vpdn-acc-in)#`
		Configures the router to accept tunneled PPP/PPPoE connections from the LAC and enters VPDN accept dialin configuration mode.

Step 5	Router(config-vpdn)# **protocol pppoe**
	
	Example:
	`Router(config-vpdn)# protocol pppoe`
	
	Example:
	`Router(config-vpdn-acc-in)#`
		Configures the VPDN group to use the PPPoE protocol.

Step 6	**virtual-template** *number*
	
	Example:
	`Router(config-vpdn-acc-in)# virtual-template 1`
	
	Example:
	`Router(config-vpdn-acc-in)#`
		Specifies the number of the virtual-interface template to be used when configuring a PPPoE session.
		
		Note This should be the same virtual-interface template defined in Configuring a Virtual Template on the Cisco CMTS, on page 121.

	Command or Action	Purpose

Step 7	**exit**
	
	Example:
	`Router(config-vpdn-acc-in)# exit`
	
	Example:
	`Router(config-vpdn)#`
		Exits VPDN accept dialin configuration mode.

Step 8	**lcp renegotiation** {**always** | **on-mismatch**}
	
	Example:
	`Router(config-vpdn)# lcp renegotiation always`
	
	Example:
	`Router(config-vpdn)#`
		(Optional) Specifies whether the Cisco CMTS, acting as the LNS, can renegotiate the PPP Link Control Protocol (LCP) with the router acting as the LAC:
		• **always** = Always allows the Cisco CMTS to renegotiate the connection.
		• **on-mismatch** = The Cisco CMTS can renegotiate the connection only when a configuration mismatch is discovered between the LNS and LAC.
		
		The default is that the LNS should not be able to renegotiate the connection.

Step 9	**pppoe limit per-mac** *number*
	
	Example:
	`Router(config-vpdn)# pppoe limit per-mac 1`
	
	Example:
	`Router(config-vpdn)#`
		(Optional) Specifies the maximum number of PPPoE sessions that can originate from each MAC address. The valid range is 1 to 5000, with a default of 100. For cable users, Cisco recommends a maximum of 1 PPPoE session per MAC address.
		Note This command is not available until after you have configured the group for the PPPoE protocol in Step 5.

Step 10	**pppoe limit max-sessions** *number-of-sessions* [**threshold-sessions** *number*]
	
	Example:
	`Router(config-vpdn)# pppoe limit max-sessions 1000 threshold-sessions 750`
	
	Example:
	`Router(config-vpdn)#`
		(Optional) Specifies the number of PPPoE sessions supported on the router:
		• *number* = Specifies the maximum number of PPPoE sessions that can be established at any one time on the router. The valid range is 1 to 5000, with a default of 100.
		• **threshold-sessions** *number* = (Optional) Specifies the threshold for active PPPoE sessions. If the number of sessions exceeds this value, an SNMP trap can be sent. The valid range is 1 to 5000, and the default equals the *number-of-sessions* value.
		
		Note This command is not available until after you have configured the group for the PPPoE protocol in Step 5 .

	Command or Action	Purpose

Step 11	**exit**
	
	Example:
	`Router(config-vpdn)# exit`
	
	Example:
	`Router(config)#`
		Exits VPDN-group configuration mode.

Step 12	**exit**
	
	Example:
	`Router(config)# exit`
	
	Example:
	`Router#`
		Exits global configuration mode.

Configuring a VPDN Group for L2TP Tunnel Initiation on the Cisco CMTS

Use the following commands, starting in user EXEC mode, to create and configure a virtual private dialup network (VPDN) group on the Cisco CMTS router that is acting as a when it is acting an L2TP access concentrator (LAC), so that it can create an L2TP tunnel with the L2TP network server (LNS).

Note This step is required when you are using L2TP tunneling with PPPoE sessions. In this configuration, you must create at least one VPDN group to support the PPPoE sessions and at least one other VPDN group to support the L2TP tunnel.

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	
	Example:
	`Router(config)#`
		Enters global configuration mode.

Step 3	**vpdn-group** *number*
	
	Example:
	`Router(config)# vpdn-group 2`
	
	Example:
	`Router(config-vpdn)#`
		Creates the VPDN group with the specified number and enters VPDN-group configuration mode.

Step 4	Router(config-vpdn)# **request-dialin**
	
	Example:
	`Router(config-vpdn)# request-dialin`
	
	Example:
	`Router(config-vpdn-req-in)#`
		Configures the router to initiate L2TP tunnel requests and enters VPDN request dialin configuration mode.

Step 5	**protocol l2tp**
	
	Example:
	`Router(config-vpdn-req-in)# protocol l2tp`
	
	Example:
	`Router(config-vpdn-req-in)#`
		Configures the VPDN group for the L2TP protocol.

Step 6	**domain** *domain-name*
	
	Example:
	`Router(config-vpdn-req-in)# domain client.com`
	
	Example:
	`Router(config-vpdn-req-in)#`
		Specifies that this VPDN group should be used to create PPPoE sessions for clients requesting access from the specified domain name.

Step 7	**exit** **Example:** `Router(config-vpdn-req-in)# exit`	Exits VPDN request dialin configuration mode.

	Command or Action	Purpose
	Example: `Router(config-vpdn)#`	

Step 8	**initiate-to ip** *ip-address*
	Example:
	`Router(config-vpdn)# initiate-to ip 10.10.10.2`
	Example:
	`Router(config-vpdn)#`
		Establishes the IP address for the termination point of the L2TP tunnel that is used by PPPoE clients using this VPDN group.

Step 9	**local name** *pppoe-username*
	Example:
	`Router(config-vpdn)# local name PpPoE-UsER`
	Example:
	`Router(config-vpdn)#`
		Specifies the username to be used for authentication on the VPDN group.

Step 10	**no l2tp tunnel authentication**
	Example:
	`Router(config-vpdn)# no l2tp tunnel authentication`
	Example:
	`Router(config-vpdn)#`
		Disables authentication for the creation of the L2TP tunnel (but continues to authenticate individual user sessions).

Step 11	**exit**
	Example:
	`Router(config-vpdn)# exit`
	Example:
	`Router(config)#`
		Exits VPDN-group configuration mode.

Step 12	**exit**
	Example:
	`Router(config)# exit`
	Example:
	`Router#`
		Exits global configuration mode.

Enabling PPPoE on a Cable Interface

Use the following commands, starting in user EXEC mode, to enable PPPoE on a specific cable interface on the Cisco CMTS router when it is acting an L2TP access concentrator (LAC).

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	
	Example:
	`Router(config)#`
		Enters global configuration mode.

Step 3	**interface cable** *x/y*
	
	Example:
	`Router(config)# interface cable 4/0`
	
	Example:
	`Router(config-if)#`
		Enters cable interface configuration mode for the specified cable interface:

Step 4	**pppoe enable**
	
	Example:
	`Router(config-if)# pppoe enable`
	
	Example:
	`Router(config-if)#`
		Enables PPPoE on the interface, allowing PPPoE sessions to be created through that interface. (The **pppoe enable** command is not available until you enable VPDN operations, using the **vpdn enable** command as shown in the procedure given in the Enabling VPDN Operations on the Cisco CMTS, on page 119.)
		
		Note Enabling PPPoE on a cable interface also automatically enables it on all subinterfaces.

	Command or Action	Purpose

Step 5	**hold-queue** *n* **in**
	
	Example:
	`Router(config-if)# hold-queue 1000 in`
	
	Example:
	`Router(config-if)#`
		(Optional) Specify the maximum number of data packets that can be stored in the input queue during PPPoE sessions. The valid range is 0 to 65535 packets, with a default of 75.
		
		Note To support a large number of simultaneous PPPoE sessions, set the input queue value to at least 1000 packets to avoid dropped packets.

Step 6	**hold-queue** *n* **out**
	
	Example:
	`Router(config-if)# hold-queue 1000 out`
	
	Example:
	`Router(config-if)#`
		(Optional) Specify the maximum number of data packets that can be stored in the output queue during PPPoE sessions. The valid range is 0 to 65535 packets, with a default of 40.
		
		Note To support a large number of simultaneous PPPoE sessions, set the output queue value to at least 1000 packets to avoid dropped packets.
		Note Repeat Step 3 through Step 6 for each cable interface that supports PPPoE sessions.

Step 7	**exit**
	
	Example:
	`Router(config-if)# exit`
	
	Example:
	`Router(config)#`
		Exits interface configuration mode.

Step 8	**exit**
	
	Example:
	`Router(config)# exit`
	
	Example:
	`Router#`
		Exits global configuration mode.

Configuring a Cisco Router as LNS

Use the following commands, starting in user EXEC mode, to enable and configure a Cisco router, such as the Cisco 6400, to act as the L2TP network server (LNS), so that it can terminate the L2TP tunnels initiated by the Cisco CMTS router when it is acting an L2TP access concentrator (LAC).

Note Before performing this procedure on the LNS router, you must also enable VPDN operations, using the procedure given in the Enabling VPDN Operations on the Cisco CMTS, on page 119. In addition, you must also create and configure a virtual-interface template, using the procedure given in the Configuring a Virtual Template on the Cisco CMTS, on page 121.

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	
	Example:
	`Router(config)#`
		Enters global configuration mode.

Step 3	**vpdn-group** *number*
	
	Example:
	`Router(config)# vpdn-group 1`
	
	Example:
	`Router(config-vpdn)#`
		Select the VPDN group number and enters VPDN-group configuration mode.

Step 4	**accept-dialin**
	
	Example:
	`Router(config-vpdn)# accept-dialin`
	
	Example:
	`Router(config-config-vpdn-acc-in)#`
		Configures the router to accept dial-in calls and enters VPDN accept dialin configuration mode.

Step 5	**protocol l2tp** **Example:** `Router(config-vpdn-acc-in)# protocol pppoe`	Configures the VPDN group for the L2TP protocol so that it can access the PPPoE server.

	Command or Action	Purpose
	Example: `Router(config-vpdn-acc-in)#`	

Step 6	**virtual-template** *number*
	Example:
	`Router(config-vpdn-acc-in)# virtual-template 1`
	Example:
	`Router(config-vpdn-acc-in)#`
		Specifies the number of the virtual-interface template to be used when configuring a PPPoE session.
		Note Specify the number of a virtual-interface template that has been created using the procedure given in the Configuring a Virtual Template on the Cisco CMTS, on page 121.

Step 7	**exit**
	Example:
	`Router(config-vpdn-acc-in)# exit`
	Example:
	`Router(config-vpdn)#`
		Exits VPDN accept dialin configuration mode.

Step 8	**terminate-from hostname** *hostname*
	Example:
	`Router(config-vpdn)# terminate-from hostname ciscocmts-router`
	Example:
	`Router(config-vpdn)#`
		Configures this group so that it terminates L2TP tunnels from the specified hostname. The *hostname* should be the host name for the Cisco CMTS that is configured for PPPoE termination.

Step 9	**no l2tp tunnel authentication**
	Example:
	`Router(config-vpdn)# no l2tp tunnel authentication`
	Example:
	`Router(config-vpdn)#`
		Disables authentication for the creation of the L2TP tunnel (but continues to authenticate individual user sessions).

Step 10	**exit** **Example:** `Router(config-vpdn)# exit`	Exits VPDN-group configuration mode.

	Command or Action	Purpose
	Example: `Router(config)#`	

Step 11	**virtual-template** *number* **pre-clone** *number*
	Example:
	`Router(config)# virtual-template 1 pre-clone 2000`
	Example:
	`Router(config)#`
		(Optional) Creates the specified number of virtual interfaces in advance, which can speed up the bring up of individual sessions and reduce the load on the router's processor when a large number of sessions come online at the same time.
		• *number* = Number of virtual interfaces to be created in advance. This value should match the total number of PPPoE sessions that the router is expected to support.
		Note Pre-cloning is not recommended when using virtual subinterfaces.

Step 12	**exit**
	Example:
	`Router(config)# exit`
	Example:
	`Router#`
		Exits global configuration mode.

Clearing PPPoE Sessions

To clear all PPPoE sessions for a particular MAC address, use the **clear cable host** command:

```
Router# clear cable host
 mac-address

Router#
```

The following example shows a PPPoE session for a particular host being cleared:

```
Router# show interface c3/0 modem 0

SID   Priv bits  Type      State       IP address      method    MAC address
1     00         modem     offline     3.18.1.5        dhcp      0030.80bc.2303
1     00         host      offline                     pppoe     0010.2937.b254
Router# clear cable host 0010.2937.b254

Router# show interface c3/0 modem 0

SID   Priv bits  Type      State       IP address      method    MAC address
1     00         modem     offline     3.18.1.5        dhcp      0030.80bc.2303
Router#
```

Enabling SNMP Traps for Active PPPoE Sessions

In Cisco IOS Release 12.2(8)BC1 and later releases, you can enable SNMP traps to inform you when the number of active PPPoE sessions exceeds a threshold value, using the following procedure.

Note Configure the threshold value using the **threshold-sessions** option for the **pppoe limit max-sessions** command when configuring the VPDN group for PPPoE sessions. For more information about PPPoE traps, see the CISCO-PPPOE-MIB.

Note To enable SNMP traps, you must also configure the router to support SNMP sessions and specify at least one SNMP manager to receive the SNMP traps.

DETAILED STEPS

	Command or Action	Purpose

Step 1	**enable**
	
	Example:
	`Router> enable`
	
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	`Router# configure terminal`
	
	Example:
	`Router(config)#`
		Enters global configuration mode.

Step 3	**snmp-server enable traps pppoe**
	
	Example:
	`Router(config)# snmp-server enable traps pppoe`
	
	Example:
	`Router(config)#`
		Enables SNMP traps to be sent whenever the number of active sessions exceeds a user-configurable threshold.

Step 4	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

	Command or Action	Purpose
	Example: `Router#`	

Monitoring the PPPoE Termination Feature

To display users who have registered with the Cisco CMTS using PPPoE, use the **show interface cable modem** command. For information on this command, see the *Cisco CMTS Cable Command Reference* here

To display the virtual-template interface number being used by a PPPoE client, use the **show vpdn session** command.

```
Router# show vpdn session

L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions
34854 14116 R7732-07-ISP1 est    135.1.1.1       1701  1
LocID RemID TunID Intf          Username               State  Last Chg Fastswitch
2     56    34854 Vi1           ppp1@isp1.com          est    00:02:11 enabled
%No active L2F tunnels
%No active PPTP tunnels
PPPoE Tunnel and Session Information Total tunnels 1 sessions 1
PPPoE Tunnel Information
Session count: 1
PPPoE Session Information
SID       RemMAC          LocMAC       Intf     VASt  OIntf         VLAN/
                                                                     VP/VC
1      0050.da80.c13e  0005.00e0.8c8b  Vi1      UP    Ca8/0/1
Router#
```

To display the current VPDN domains, use the **show vpdn domain** command:

```
Router# show vpdn domain
Tunnel          VPDN Group
------          ----------
domain:isp1.com 2 (L2TP)
Router#
```

Configuration Examples for PPPoE Termination

This section lists the following sample configurations for the PPPoE Termination feature:

PPPoE Termination on a Cisco CMTS without L2TP Tunneling

The following configuration configures the Cisco CMTS router to perform PPPoE termination. Traffic from the cable modem users is then sent out over the router's WAN interfaces as IP packets, allowing basic Internet access.

```
version 12.2
!
hostname ubr-pppoe
!
ip cef
no ip domain-lookup
ip domain-name client.com
vpdn enable
no vpdn logging
!
! VPDN group 1 configures the router to accept PPPoE connections and specifies the
! virtual template to be used to configure the virtual interfaces that are created
! for each PPPoE session.
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
  pppoe limit per-mac 100
!
! Increase size of small buffers to account for keepalive packets for PPPoE sessions
buffers small permanent 1024
buffers small max-free 1024
buffers small initial 1024
!
interface Ethernet1/0
 ip address 10.100.0.1 255.255.255.0
 ip route-cache flow
 half-duplex
!
! "pppoe enable" command must be configured on each cable interface that is to accept
! PPPoE sessions, but you do not need to configure this command on subinterfaces
interface Cable6/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 589250000
 no cable upstream 0 shutdown
 cable upstream 1 frequency 35008000
 cable upstream 1 power-level 0
 no cable upstream 1 shutdown
 no cable upstream 2 shutdown
 pppoe enable
!
interface Cable6/0.1
 ip address 10.1.1.1 255.255.255.0 secondary
 ip address 10.10.1.1 255.255.255.0
 cable helper-address 10.100.0.100
 no cable proxy-arp
 cable dhcp-giaddr policy
!
 interface Cable6/0.2
 ip address 10.1.2.1 255.255.255.0 secondary
 ip address 10.10.2.1 255.255.255.0
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
interface Cable6/0.3
 ip address 10.1.3.1 255.255.255.0
 cable source-verify
```

```
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
! Virtual Template 1 configures the virtual interfaces that will be used
! for PPPoE sessions
interface Virtual-Template1
 ip unnumbered Ethernet1/0
 ip mtu 1492
 ip pim sparse-mode
 peer default ip address pool default
 ppp authentication chap
 no logging event link-status
 no cdp enable
!
```

PPPoE Termination on a Cisco CMTS with L2TP Tunneling

The following configuration configures the Cisco CMTS router to perform PPPoE termination. Traffic received from the cable modem users is sent over the L2TP tunnel to the router that is acting as the L2TP Network Server (LNS).

```
version 12.2
!
hostname ubr-pppoe-l2tp
!
! User name/password sent to LNS to create the L2TP tunnel.
username cmts-user password 0 cmts-password
! User name/password used by LNS to authenticate tunnel creation
username lns-user password 0 lns-password
! User name/password for a PPPoE user - typically this information
! is configured on the RADIUS authentication servers.
username pppoe-user@client.com password 0 user-password
ip cef
no ip domain-lookup
ip domain-name client.com
vpdn enable
no vpdn logging
!
! VPDN group 1 configures the router to accept PPPoE connections and specifies the
! virtual template to be used to configure the virtual interfaces that are created
! for each PPPoE session.
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
  pppoe limit per-mac 100
!
! VPDN group 2 configures the group to be used for the L2TP tunnel to the
! LNS (at the IP address of 10.10.15.2) which will be used for PPPoE
! sessions from clients using the domain name as "client.com".
vpdn-group 2
 request-dialin
  protocol l2tp
  domain client.com
 initiate-to ip 10.10.15.2
local name ubr-pppoe-l2tp
 no l2tp tunnel authentication
!
! Increase size of small buffers to account for keepalive packets for PPPoE sessions
buffers small permanent 1024
buffers small max-free 1024
buffers small initial 1024
!
interface Ethernet1/0
 ip address 10.100.0.1 255.255.255.0
 ip route-cache flow
 half-duplex
```

```
!
! "pppoe enable" command must be configured on each cable interface that is to accept
! PPPoE sessions, but you do not need to configure this command on subinterfaces
interface Cable6/0
 no ip address
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 589250000
 no cable upstream 0 shutdown
 cable upstream 1 frequency 35008000
 cable upstream 1 power-level 0
 no cable upstream 1 shutdown
 no cable upstream 2 shutdown
 pppoe enable
!
interface Cable6/0.1
 ip address 10.1.1.1 255.255.255.0 secondary
 ip address 10.10.1.1 255.255.255.0
 cable helper-address 10.100.0.100
 no cable proxy-arp
 cable dhcp-giaddr policy
!
interface Cable6/0.2
 ip address 10.1.2.1 255.255.255.0 secondary
 ip address 10.10.2.1 255.255.255.0
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
interface Cable6/0.3
 ip address 10.1.3.1 255.255.255.0
 cable source-verify
 cable dhcp-giaddr policy
 cable helper-address 10.100.0.100
!
! Virtual Template 1 configures the virtual interfaces that will be used
! for PPPoE sessions
interface Virtual-Template1
 ip unnumbered Ethernet1/0
 ip mtu 1492
 ip pim sparse-mode
 peer default ip address pool default
 ppp authentication chap
 no logging event link-status
 no cdp enable
```

PPPoE Client Configuration on a Cisco Router

The following configuration configures a Cisco router that supports PPPoE to act as a PPPoE client. This router connects to the cable modem and performs the PPPoE authentication with the Cisco CMTS that is performing the PPPoE termination.

Note This configuration is for the Cisco 1600 router and needs to be adjusted to fit the interfaces that might be present on other types of routers.

```
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 request-dialin
 protocol pppoe
!
!
```

```
interface Ethernet0
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
!
interface Dialer1
 mtu 1492
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ppp chap hostname joeuser@client.com
 ppp chap password 7 12139CA0C041104
!
ip nat inside source list 1 interface Dialer1 overload
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 1 permit any
```

PPPoE Configuration for the L2TP Network Server

The following sample configuration shows a Cisco router being configured to act as the L2TP Network Server (LNS). This router terminates the L2TP tunnel from the Cisco CMTS and forwards the traffic from the PPPoE sessions to the corporate network.

```
!
hostname lns-router
!
! User name/password for the LNS itself
username lns-user password 0 lns-password
! User name/password for the Cisco CMTS
username cmts-user password 0 cmts-password
! Username and password for the PPPoE client - typically this information is
! configured on the RADIUS authentication servers
username pppoe-user@client.com password 0 user-password
!
ip subnet-zero
ip cef
ip domain-name client.com
!
vpdn enable
no vpdn logging
!
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname ubr-pppoe-l2tp
 no l2tp tunnel authentication
!
! Allows the LNS to preconfigure virtual templates
! for the PPPoE sessions, allowing the sessions to come up faster
virtual-template 1 pre-clone 2000
!
interface loopback 0
ip address 9.10.7.1 255.255.255.0
!
!
interface Virtual-Template1
 ip unnumbered loopback 0
 ip mroute-cache
 ip mtu 1492
 peer default ip address pool pool-1 pool-2
!
ip local pool pool-1 9.10.7.3 9.10.7.254
ip local pool pool-2 9.10.8.1 9.10.8.254
```

Additional References

For additional information related to configuring PPPoE Termination on the Cisco CMTS, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring PPP over Ethernet	Configuring Broadband Access: PPP and Routed Bridge Encapsulation, Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2, at the following URL: http://www.cisco.com/c/en/us/td/docs/ios/12_2/wan/configuration/guide/fwan_c/wcfppp.html
Enabling SNMP Traps for PPPoE Active Sessions	*PPPoE Session-Count MIB* , at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftpscmib.htm
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference Guide,* at the following URL: http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-software-releases-12-2-mainline/products-installation-and-configuration-guides-list.html

Standards

Standards[6]	Title
SP-RFIv1.1-I08-020301	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablemodem.com)

6 Not all supported standards are listed.

MIBs

MIBs[7]	MIBs Link
CISCO-PPPOE-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

7 Not all supported MIBs are listed.

RFCs

RFCs[8]	Title
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2866	RADIUS Accounting

8 Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PPPoE Termination

Feature History	
Release	Modification

Feature History	
Release 12.1(5)T	This feature was introduced for the Cisco uBR7200 series routers. **Note** The Cisco IOS Release 12.1T and 12.2T trains are no longer supported for the Cisco uBR7200 series routers.
Release 12.2(4)BC1a	This feature was supported on the 12.2BC train for the Cisco uBR7100 series and Cisco uBR7246VXR routers.
Release 12.2(8)BC1	Support was added for SNMP support with the CISCO-PPPOE-MIB.
Release 12.2(8)BC2	Support was added for bundled cable interfaces.
Supported Platforms	
Cisco uBR7100 series, Cisco uBR7246VXR router	

Note The PPPoE Termination feature is not supported on the Cisco uBR10012 universal broadband router in any Cisco IOS software release. The PPPoE Termination is also not supported on any Cisco CMTS router when running Cisco IOS Release 12.1 EC. Effective with Cisco IOS Release 12.2(33)SCD, the PPPoE Termination feature is not supported on the Cisco uBR7200 router.

CHAPTER 8

Service Flow Mapping to MPLS-VPN on the Cisco CMTS

First Published: February 14, 2008Last Updated: July 11, 2012

This document describes the Service Flow Mapping to MPLS-VPN feature, which enhances the existing multiprotocol label switching (MPLS) VPNs support to provide more flexible managed access for multiple ISP support over a hybrid fiber-coaxial (HFC) cable network.

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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

Contents

Prerequisites for Mapping Service Flows to MPLS-VPN

- To support static service-flow to MPLS-VPN functionality, the Cisco uBR7200 series routers must be running Cisco IOS Release 12.2(11)BC2 or later releases and the Cisco uBR10000 series routers must be running Cisco IOS Release 12.3(13)BC or later releases.
- To support dynamic service-flow to MPLS-VPN functionality, the Cisco CMTS routers must be running Cisco IOS Release 12.3(13)BC or later releases.
- All Cisco CMTSes must be configured for the proper virtual routing and forwarding (VRF) interfaces, as specified by the documentation in the Additional References, on page 166.
- To support static service-flow to MPLS VPN mapping, the DOCSIS configuration file editor must support the inclusion of Vendor-specific Options (TLV subtype 43) in the Upstream Service Flow Encodings parameter set (TLV type 24). The new option to be added is called the VPN Route Distinguisher (RD) parameter (TLV subtype 4) and must be preceded by the Cisco Vendor ID (00000C).

For example, using the Cisco DOCSIS Configurator tool, you would specify the following fields in the ASCII configuration file:

```
24 (Upstream Service Flow Block)
  S43 (Vendor Specific Options)
   T08 (Vendor ID) = 00 00 0c
   T04 (VPN Route Distinguisher) = xx xx xx xx xx xx xx xx
```

where the VPN RD contains eight hexadecimal bytes. The first two hexadecimal bytes specify the format of the remaining six bytes:

-
  - If bytes 1 and 2 are 00 00, bytes 3 and 4 specify the 16-bit autonomous system (AS) number, and bytes 5 to 8 specify a unique 32-bit identifier.
  - If bytes 1 and 2 are 00 01, bytes 3 to 6 specify the 32-bit IP address, and bytes 7 and 8 specify a unique 16-bit identifier.

Configure the VPN RD parameter to the same *route-distinguisher* ID that you have specified on the Cisco CMTS using the **rd** command in VRF configuration submode.

- To support DOCSIS configuration file-based dynamic service-flow to MPLS VPN mapping, the DOCSIS configuration file editor must support the inclusion of the Cisco Vendor-specific Dynamic Flow VPN RD parameter (TLV subtype 13).

For example, using the Cisco DOCSIS Configurator tool, you would specify the following fields in the ASCII configuration file:

```
43 (Vendor Specific Info)
    S8 (Vendor ID)  = 0-0-c
    S13 (Dynamic Flow VPN RD)  = xx xx xx xx xx xx xx xx
```

where the eight-byte VPN RD uses the same format as specified above.

The table shows the Cisco CMTS hardware compatibility prerequisites for this feature.

Note The hardware components introduced in a given Cisco IOS Release will be supported in all subsequent releases unless otherwise specified.

Table 14: Service Flow Mapping to MPLS-VPN Hardware Compatibility Matrix

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • PRE2 **Cisco IOS Release 12.2(33)SCB and later** • PRE4 **Cisco IOS Release 12.2(33)SCH and later** • PRE5	**Cisco IOS Release 12.2(33)SCB and later** • Cisco uBR10-MC5X20U/H **Cisco IOS Release 12.2(33)SCC and later** • Cisco UBR-MC20X20V **Cisco IOS Release 12.2(33)SCE and later** • Cisco uBR-MC3GX60V [9]
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V [10]
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCA and later** • NPE-G1 **Cisco IOS Release 12.2(33)SCB and later** • NPE-G2	**Cisco IOS Release 12.2(33)SCA and later** • Cisco uBR-E-28U • Cisco uBR-E-16U • Cisco uBR-MC28U/X **Cisco IOS Release 12.2(33)SCD and later** • Cisco uBR-MC88V

9 The Cisco uBR-3GX60V cable interface line card is not compatible with PRE2.
10 The Cisco uBR-MC88V cable interface line card is compatible only with NPE-G2.

Note The combination of a PRE4 and Cisco Half-Height Gigabit Ethernet (HHGE) is not supported in the same chassis.

Restrictions for Mapping Service Flows to MPLS-VPN

- Cable modems using this feature should use a unique DOCSIS configuration file that creates an upstream packet classifier and service flow corresponding to each customer premises equipment (CPE) or media terminal adapter (MTA) device that needs to have its traffic routed to a different MPLS VPN than to the one the cable modem natively belongs.
- The DOCSIS configuration file for a cable modem must be updated whenever a CPE device that needs to use a different MPLS VPN than the cable modem's native MPLS VPN is added or removed, or whenever the MAC address for a CPE device changes. The cable modem must also be reset to execute the changes in the DOCSIS configuration file.
- By default, dynamically generated upstream service flows use the MPLS VPN with which a cable modem is natively associated. In order to specify a different MPLS VPN for use by dynamically generated upstream service flows, it is necessary to do one of the following:
  - Specify an RD in the Cisco Vendor-specific Info Subtype Option 13 within the cable modem's DOCSIS configuration file.
  - Use the global or cable interface command **cable dynamic-flow vrf** to specify an MPLS VPN name.

Information About Mapping Service Flows to MPLS-VPN

The Service Flow Mapping to MPLS-VPN feature provides the following benefits to cable service providers and their partners and customers:

- Allows the service provider to maintain full control over the cable modems and other devices that are directly connected to the cable plant.
- Provides a highly flexible, scalable, and easy to manage system.
- Supports overlapping IP address ranges.
- Provides secure support for multiple intranets and extranets.
- Supports multiple IP Quality of Service (QoS) classes.
- Enables the Cisco CMTS router to support the mapping of dynamic service flows to an MPLS VPN by using the **cable dynamic-flow vrf** command, or the Dynamic Flow VPN RD parameter (Cisco Vendor-specific Info Subtype 13) in a DOCSIS configuration file.

The Cisco CMTS routers provide managed access by means of MPLS VPNs configured over cable subinterfaces, with each subinterface configured for a specific ISP and each cable modem associating itself and all connected CPE to a specific subinterface. This use of MPLS VPNs gives service providers a manageable way to offer users access to multiple ISPs over the same physical HFC cable network.

This system works very well when all CPE devices behind a cable modem are using the same ISP. However, users are increasingly requesting more complex networks that would allow multiple CPE devices to access different ISPs through the same cable modem. For example, different users in one household might want to use different PCs to access different ISPs. Another increasingly common situation is that one user requires a secure VPN connection for telecommuting through one ISP, while other users in the household use other computers to access the public Internet through a separate ISP.

As another example, a service provider offering a PacketCable voice-over-IP (VoIP) service may wish to allow one ISP to manage and operate the voice component of the cable network, and another to manage and operate the data component.

The Service Flow Mapping to MPLS-VPN feature solves this problem by using DOCSIS 1.1 upstream packet classifiers and service flow IDs (SFIDs) to map individual CPE devices to separate MPLS-VPN interfaces. The SFID to MPLS-VPN mapping occurs as follows:

1. The service provider creates for each cable modem a DOCSIS configuration file that contains the following information:
   - Secondary upstream service flows that specify QoS profiles for CPE devices that must be associated with a particular MPLS VPN where that MPLS VPN is different from the cable modem's native MPLS VPN assignment.
   - For each upstream service flow, a Vendor-specific QoS Parameter (TLV type 43, subtype 04) that identifies the MPLS VPN RD for packets using this particular service flow.
   - Upstream packet classifiers that correspond to the secondary upstream service flows, so that the cable modem may direct packets from the CPE in question to the correct service flows. To accomplish this, each classifier must contain the MAC address of CPE that are to be associated with the service flow and consequently with the MPLS VPN. This would typically be accomplished by making use of the Source MAC Address parameter (TLV type 10, subtype 2).

Note The DOCSIS configuration file also must create a primary downstream (DS) and a primary upstream (US) service flow and packet classifier, as well as other required parameters, but these are not used for the SFID to MPLS-VPN mapping.

2. The cable modem downloads the DOCSIS configuration file during its registration process and configures itself for the proper service flows and packet classifiers.
3. The cable modem then comes online, at which point it begins receiving packets from its CPE devices. The cable modem uses the packet's source MAC address to match the packet to the proper packet classifier, which then identifies the correct SFID to use. The cable modem then transmits the packet to the Cisco CMTS using this upstream SFID.
4. The Cisco CMTS examines the packet to determine its SFID, and then uses the Vendor-specific QoS Parameter associated with that service flow to route the packet to the appropriate MPLS-VPN interface.
5. When a dynamic upstream service flow is generated, as in the case with a PacketCable VoIP phone call, the Cisco CMTS determines the MPLS VPN to associate the new upstream service flow by one of several methods in the following order of precedence:
   a. If the cable modem's DOCSIS configuration file contains the Dynamic Flow VPN RD parameter (Cisco Vendor-specific Info Subtype 13), then the dynamic service flow's VPN is set to the one using the RD as specified in the parameter.
   b. If the cable interface on which the modem is online has had the **cable dynamic-flow vrf** command applied, then the dynamic service flow's VPN is set to the MPLS VPN specified by that command.

c If the global **cable dynamic-flow vrf** command is applied, then the dynamic service flow's VPN is set to the MPLS VPN specified by this command.

d Finally, the dynamic service flow's VPN is set to the VPN to which the cable modem is associated.

If the DOCSIS configuration file for the cable modem does not contain an MPLS-VPN route, the packets from that cable modem are routed according to the routing tables on the Cisco CMTS.

MPLS QoS via TLV for non-L2VPN Service Flow

The MPLS QoS via TLV for non-L2VPN Service Flow feature is a QoS enhancement based on MPLS Traffic Class (TC) bits for MPLS L3VPN. This feature is introduced in Cisco IOS Release 12.2(33)SCG to mark TC bits for MPLS L3VPN imposition packets and classify DS packets based on TC bits of MPLS disposition packets, using vendor-specific TLVs.

The MPLS TC bits were previously known as MPLS EXP bits. RFC 5462 has renamed the MPLS EXP field to MPLS TC field.

VoIP SFID Mapping

The introduction of WB MTAs and the resequencing delays with the DS bonded traffic are pushing voice traffic towards non-bonded channels.

Starting with Cisco IOS Release 12.2(33)SCB, as the WB MTA uses the cable interface line card (CLC) DS interface as the primary interface, it can also protect voice traffic from edge quadrature amplitude modulation (e-QAM) and shared port adapter (SPA) failures. It also helps in leveraging the CLC redundancy feature to protect voice calls.

The VoIP Service Flow ID (SFID) Mapping feature leverages Data-over-Cable Service Interface Specifications (DOCSIS) 3.0 Service Flow (SF) Attribute-based assignment, which allows forwarding to Bonding groups or to single channel on a per-SF basis.

The CPE constructs DSX (Dynamic-service DOCSIS mac-management) messages that does not conform to DOCSIS 3.0 specifications and does not includes the SF Attribute parameters. However, the Cisco CMTS should control these factors and whenever voice calls are initiated; the Cisco CMTS must add SF Attributes, configured by the user, to the DSX messages.

Prerequisites for VOIP SFID Mapping

- DOCSIS 3.0-compatible voice CPE and DOCSIS 3.0-compatible PacketCable specifications.
- The Required Attribute Mask and Forbidden Attribute Mask should be configured globally.
- Mask values above zero must be inserted to all dynamic voice DS requests from WB CMs.
- The SF assignment must follow the mask values inserted in DSX message to determine forwarding.
- The Type-Length-Values (TLVs) inserted at the Required Attribute Mask and Forbidden Attribute Mask should not be sent back. They are not supported while sending Dynamic Service Response (DSx-RSP) through embedded media terminal adapter (eMTA) and could lead to cable modem (CM) error.

Restrictions for VOIP SFID Mapping

- The VoIP SFID Mapping feature is supported only on the Cisco uBR10012 Universal Broadband Router.
- DS SF Attribute TLVs inserted by the Cisco CMTS are skipped from TLV encoding.

How to Configure the Service Flow Mapping to MPLS-VPN feature

The following section provides information on how to configure the Service Flow Mapping to MPLS-VPN feature. Each task in the list is identified as either required or optional.

Note This section describes only the configuration tasks needed to enable the Service Flow Mapping to MPLS-VPN feature. It does not describe the basic MPLS-VPN configuration tasks. For information on configuring MPLS-VPN routes, see the documentation listed in the Additional References, on page 166.

Creating a DOCSIS Configuration File

The Cisco CMTS automatically maps service flows to MPLS-VPN interfaces when an upstream service flow includes the VPN RD parameter as a vendor-specific TLV. The VPN RD parameter points to the *route-distinguisher* ID that has been specified using the **rd** command in VRF configuration submode.

You must create a corresponding upstream packet classifier that identifies the source MAC address that will use this SFID-to-MPLS VPN mapping. To create a DOCSIS configuration file that contains both of these parameters, use the following procedure.

Note This procedure uses the Cisco DOCSIS Configurator tool to create the DOCSIS configuration file. However, you can use any tool that creates DOCSIS-compatible configuration files.

Note For information about the **rd** command, see the command reference.

Step 1 Obtain the MAC addresses for the CPE devices that must be associated with a different MPLS VPN than the cable modem's native MPLS VPN association.

Step 2 Create an upstream packet classifier for each CPE device, specifying the service flow reference of the appropriate upstream service flow and the source MAC address of the CPE, along with the other appropriate parameters. For example, the following configuration for classifier 14 specifies that the service flow with service flow reference 7 should be used for the MAC address at 00 00 0C A1 B2 C3:

Example:

```
22 (Upstream Packet Classification Encoding Block)
```

```
   S01 (Classifier Reference)           = 14
   S03 (Service Flow Reference)         = 7
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 00 0C A1 B2 C3
```

Step 3 Create a matching upstream service flow for this CPE device. This service flow must include all necessary parameters, as well as a vendor-specific VPN RD parameter (TLV subtype 4) that identifies the route-distinguisher ID for the VRF route that has been created for this user.
The route-distinguisher ID consists of two integers that can be in the following two forms:

- Type 0—Contains a 16-bit autonomous system (AS) number and a unique 32-bit identifier.
- Type 1—Contains a 32-bit IP address and a unique 16-bit identifier.

Configure the VPN RD parameter to the same *route-distinguisher* ID that you have specified on the Cisco CMTS using the **rd** command in VRF configuration submode. For example, if you configured a type 0 route using the following CLI commands:

Example:

```
ip vrf isp1
 rd 64000:1
```

Configure the matching upstream service flow with the following parameters:

Example:

```
24 (Upstream Service Flow Encodings)
   S43 (Vendor Specific Options) = 8.3.0.0.12.4.8.0.0.250.0.0.0.0.1
```

The Vendor-specific Options field translates into two TLVs. The first TLV is of type 8 (Vendor ID), length 3, and value of 00.00.0C hexadecimal to identify Cisco Systems. The second TLV is of type 4 (VPN RD), length 8, and value of 00.00.FA.0.0.0.0.1 (hexadecimal).

Tip If you are using the graphical interface in the Cisco DOCSIS Configurator tool to create the DOCSIS configuration file, enter the entire dotted decimal string into the “Vendor Specific QoS” field in the Upstream and Downstream Service Flow screens. Using the above example, you would enter “8.3.0.0.12.4.8.0.0.0.250.0.0.0.1” into this field.

Similarly, if you configured a type 1 route using the following CLI commands:

Example:

```
ip vrf isp2
 rd 10.10.10.15:1
```

Configure the matching upstream service flow with the following parameters:

Example:

```
24 (Upstream Service Flow Encodings)
   S43 (Vendor Specific Options) = 8.3.0.0.12.4.8.0.1.10.10.10.15.0.1
```

Similarly, the Vendor-specific Options field translates into two TLVs. The first TLV is of type 8 (Vendor ID), length 3, and value of 00.00.0C hexadecimal to identify Cisco Systems. The second TLV is of type 4 (VPN RD), length 8, and value of 00.01.0A.0A.0A.0F.00.01 (hexadecimal).

Step 4 Repeat this procedure for each upstream packet classifier and service flow that is to be mapped to an MPLS-VPN interface.

Mapping Dynamic Service Flows

If the MPLS VPN to which dynamic service flows are mapped must be set on a per-cable-modem basis, rather than on a per-cable-interface or per-Cisco-CMTS basis, then the Dynamic Flow VPN RD parameter (Cisco Vendor-specific Info Subtype 13) must be added to the DOCSIS configuration. The Dynamic Flow VPN RD parameter is used to specify the route-distinguisher ID for the VRF route that has been created for use by dynamic service flows.

Note In general, the MPLS VPN to which dynamic service flows must be mapped should be the same MPLS VPN as specified for static service-flow to MPLS VPN mapping.

Step 1 Refer to Step 3 of Creating a DOCSIS Configuration File, on page 151.

Step 2 Configure the VPN RD parameter to the same route-distinguisher ID that you have specified on the Cisco CMTS by means of the **rd** command in VRF configuration submode. For example, if you configured a type 0 route by means of the following CLI commands:

Example:
```
ip vrf isp1
rd 64000:1
```

Configure the matching Dynamic Flow VPN RD parameter as follows:

Example:
```
43 (Vendor Specific Info)
    S8 (Vendor ID)  = 0-0-c
    S13 (Dynamic Flow VPN RD)  = 0-0-fa-0-0-0-0-1
```

The Vendor-specific Options field translates into two TLVs:

- The first TLV is of type 8 (Vendor ID), length 3, and value of 00.00.0C (hexadecimal), to identify Cisco Systems.
- The second TLV is of type 4 (VPN RD), length 8, and value of 00.00.FA.0.0.0.0.1 (hexadecimal).

Similarly, if you configured a type 1 route by means of the following CLI commands:

Example:
```
ip vrf isp2
rd 10.10.10.15:1
```

Configure the matching upstream service flow with the following parameters:

Example:

```
43 (Vendor Specific Info)
    S8 (Vendor ID)  = 0-0-c
    S13 (Dynamic Flow VPN RD)  = 0-1-a-a-a-f-0-1
```

Similarly, the Vendor-specific Options field translates into two TLVs:

- The first TLV is of type 8 (Vendor ID), length 3, and value of 00.00.0C (hexadecimal) to identify Cisco Systems.
- The second TLV is of type 4 (VPN RD), length 8, and value of 00.01.0A.0A.0A.0F.00.01 (hexadecimal).

The per-cable-modem Dynamic Flow VPN RD parameter takes precedence over any per-cable-interface or per-Cisco-CMTS dynamic service flow to MPLS VPN configuration.

Step 3 If the MPLS VPN to which dynamic service flows are mapped must be set on a per-cable-interface basis, as opposed to per cable modem or per-Cisco-CMTS, then use the following the cable interface configuration command:

Example:

```
Router# interface cable
 x/y/zRouter(config-if)# cable dynamic-flow vrf
 vrf-name
```

For example, if you configured the following VRF for use with dynamically generated service flows:

Example:

```
ip vrf isp1
 rd 64000:1
```

Then you could use the following per-cable-interface command to ensure that dynamic service flows are mapped:

Example:

```
Router# interface cable
 x/y/zRouter(config-if)# cable dynamic-flow vrf
 isp1
```

The per-cable-interface dynamic service flow to MPLS VPN configuration takes precedence over the global per-Cisco-CMTS dynamic service flow to MPLS VPN configuration, but not over the per-cable-modem Dynamic Flow VPN RD parameter.

Step 4 If the MPLS VPN to which dynamic service flows are mapped must be set on a per-Cisco-CMTS basis, as opposed to per cable modem or per cable interface, then use the global configuration command:

Example:

```
Router# cable dynamic-flow vrf
 vrf-name
```

For example, if you configured the following VRF for use with dynamically generated service flows:

Example:

```
ip vrf isp2
 rd 10.10.10.15:1
```

Then you could use the following per-cable-interface command to ensure that dynamic service flows are mapped:

Example:

```
Router# interface cable
 x/y/zRouter(config-if)# cable dynamic-flow vrf
 isp2
```

Configuring MPLS QoS via TLV for non-L2VPN Service Flow

Note This feature is configured using a cable modem configuration file and is dependent on the general configuration of the L3VPN.

This section describes how to configure traffic class bits for MPLS imposition and disposition packets and on how to use vendor-specific TLVs with AToM L2VPN and MPLS L3VPN.

Restrictions for Configuring MPLS QoS via TLV

- This feature supports only PRE4. It will not support PRE2.
- This feature supports only IPv4. It will not support IPv6.
- This feature supports only Cisco uBR10012 routers. The Cisco uBR7200 series routers is not supported.
- This feature does not support SNMP.
- This feature does not support dynamic service flows.
- Only up to four VPNs and eight upstream service flows per CM can be configured.
- For a VPN, only a maximum of eight DS classifiers (using TC bits in the range from 0 to 7) can be configured.
- If TC bits downstream classifiers are configured for a VPN, then the downstream MPLS packets belonging to the VPN are processed only on TC bits classification. It will not process general IP header field classification.

Traffic Class for MPLS Imposition Packets

The table lists the vendor-specific TLV to be included in the cable modem configuration file to configure TC bits for MPLS imposition packets. The MPLS-TC-SET TLV is defined in the upstream and is associated with the VPN RD in upstream service flow encoding.

Table 15: TLV to Configure TC Bits for MPLS Imposition Packets

TLV Name	SubType	Length	Value
MPLS-TC-SET TLV	43.5.43.34	1	Imposition MPLS-TC-SET bits

Traffic Classification for MPLS Disposition Packets

The table lists the vendor-specific TLV to be included in the cable modem configuration file to classify DS packets based on TC bits of MPLS disposition packets.

The MPLS-TC-RANGE TLV is defined only under DS classifier encodings. It supports multi-downstream flow in a CM belonging to the same MPLS L3VPN, associated with the VPN RD in downstream classifier encoding.

Table 16: TLV to Classify TC Bits for MPLS Disposition Packets

TLV Name	SubType	Length	Value
MPLS-TC-RANGE	43.5.43.35	2	MPLS-TC-low and MPLS-TC-high

Using Vendor-Specific TLVs with AToM L2VPN and MPLS L3VPN

If both AToM L2VPN (L2 MPLS) and MPLS L3VPN (L3 MPLS) are using the same set of TLVs (MPLS-TC-SET and MPLS-TC-RANGE), then you should differentiate them. Configure the TLVs for upstream service flow encoding and downstream classifier encodings as indicated below:

Upstream Service Flow Encoding

- For L2VPN, configure MPLS-TC-SET (43.5.43.34) and L2VPN ID (43.5.1).
- For MPLS L3VPN, configure MPLS-TC-SET (43.5.43.34) and VPN RD (43.5.1).

Note Do not configure the TLVs for L2VPN and MPLS L3VPN at the same time for upstream service flow encodings, as it will result in a TLV error.

Downstream Classifier Encoding

- L2VPN—Configure MPLS-TC-RANGE (43.5.43.35) and L2VPN ID (43.5.1).
- MPLS L3VPN—Configure MPLS-TC-RANGE (43.5.43.35) and VPN RD (43.5.1).

Monitoring and Maintaining Examples for Service Flow Mapping to MPLS-VPN Feature

This section provides examples of the commands that show the configuration and current status of the cable modems (CMs) that are using the Service Flow Mapping to MPLS-VPN feature. These examples display a number of CMs that are online, and the last CM (with the primary service identifier [SID] of 6) has three CPE devices connected to separate ISPs.

Displaying CMs and CPE devices

To display the number of CMs that are currently registered and online, use the **show cable modem** command:

```
Router# show cable modem

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (db)   Offset  CPE Enb
0030.8047.b41f 5.108.1.21      C3/0/U2   online(pt)  1    0.75   2821    0   Y
0007.0e03.1349 5.109.1.9       C3/0/U0   online      2   *0.00   2816    0   N
0007.0e03.12bd 5.108.1.18      C3/0/U0   online(pt)  3    -0.25  2812    0   Y
0030.80bc.22d5 5.108.1.20      C3/0/U0   online(pt)  4    0.25   2819    0   Y
0007.0e03.1331 5.111.1.6       C3/0/U0   online      5    -0.25  2816    0   N
00a0.73b0.4cc1 5.110.1.6       C3/0/U0   online(pt)  6    -0.25  2990    3   Y
```

To display the CPE devices that are associated with each CM, use the **show interface cable modem** command:

```
Router# show interface cable 3/0 modem 0

SID   Priv bits  Type      State     IP address      method    MAC address
1     11         modem     up        5.108.1.21      dhcp      0030.8047.b41f
2     00         modem     up        5.109.1.9       dhcp      0007.0e03.1349
3     11         modem     up        5.108.1.18      dhcp      0007.0e03.12bd
4     11         modem     up        5.108.1.20      dhcp      0030.80bc.22d5
5     00         modem     up        5.111.1.6       dhcp      0007.0e03.1331
6     11         modem     up        5.110.1.6       dhcp      00a0.73b0.4cc1
6     11         host      unknown   131.1.2.30      dhcp      0002.e323.ac08
6     11         host      unknown   129.1.2.18      dhcp      0050.046b.8b97
6     11         host      unknown   130.1.2.24      dhcp      0050.da80.c13e
```

To display the MPLS VPN RD to be used by dynamic service flows from a cable modem using the Dynamic Flow VPN RD parameter (Cisco Vendor-specific Info Subtype 13), use the **show cable modem verbose** command:

```
Router# show cable modem 0007.0e02.afa5 verbose
MAC Address                         : 00a0.73b0.4cc1
IP Address                          : 5.110.1.6
Prim Sid                            : 6
Interface                           : C3/0/U0
sysDescr                            :
Upstream Power                      : 0.00 dBmV (SNR = 33.83 dB)
Downstream Power                    : 0.00 dBmV (SNR = ----- dB)
Timing Offset                       : 2290
Initial Timing Offset               : 2290
Received Power                      :  0.00 dBmV
```

```
MAC Version                          : DOC1.1
QoS Provisioned Mode                 : DOC1.1
Enable DOCSIS2.0 Mode                : Y
Phy Operating Mode                   : tdma
Capabilities                         : {Frag=Y, Concat=Y, PHS=Y, Priv=BPI+}
Sid/Said Limit                       : {Max US Sids=4, Max DS Saids=0}
Optional Filtering Support           : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support           : {Taps/Symbol= 1, Num of Taps= 8}
Number of CPE IPs                    : 0(Max CPE IPs = 16)
CFG Max-CPE                          : 5
Flaps                                : 0()
Errors                               : 0 CRCs, 0 HCSes
Stn Mtn Failures                     : 0 aborts, 0 exhausted
Total US Flows                       : 1(1 active)
Total DS Flows                       : 1(1 active)
Total US Data                        : 1606 packets, 129106 bytes
Total US Throughput                  : 43 bits/sec, 0 packets/sec
Total DS Data                        : 28 packets, 1792 bytes
Total DS Throughput                  : 0 bits/sec, 0 packets/sec
Active Classifiers                   : 0 (Max = NO LIMIT)
DSA/DSX messages                     : permit all
Dynamic Secret                       : 4E7AD0AEA48F94DE0EB773494B57EA74
Dynamic flows mapped to VPN RD       : 64000:1

! The dynamic mapping is listed above.
Total Time Online                    : 1d3h
```

Displaying SID and MPLS Mappings

To display the mapping of currently used SIDs to SFIDs and their current state, use the **show interface cable sid verbose** command:

```
Router# show interface cable 3/0 sid verbose

Sid  Prim  MAC Address    IP Address      Type Age      Admin   Sched  Sfid
                                                         State   Type
1          0030.8047.b41f 5.108.1.21      stat 3h43m    enable  RSVD   3
2          0007.0e03.1349 5.109.1.9       stat 3h43m    enable  RSVD   5
3          0007.0e03.12bd 5.108.1.18      stat 3h43m    enable  BE     7
4          0030.80bc.22d5 5.108.1.20      stat 3h43m    enable  BE     9
5          0007.0e03.1331 5.111.1.6       stat 3h42m    enable  BE     11
6          00a0.73b0.4cc1 5.110.1.6       stat 08:19    enable  BE     13
7    6     00a0.73b0.4cc1 5.110.1.6       stat 08:19    enable  BE     15
8    6     00a0.73b0.4cc1 5.110.1.6       stat 08:19    enable  BE     16
9    6     00a0.73b0.4cc1 5.110.1.6       stat 08:19    enable  BE     17
10   6     00a0.73b0.4cc1 5.110.1.6       dyn  02:35    enable  UGS    18
```

To display the mappings between SFIDs and the MPLS VPN subinterface, use the **show interface cable sid association** command:

```
Router# show interface cable 3/0 sid association

Sid  Prim Online     IP Address      MAC Address    Interface     VRF Name
1         online(pt) 5.108.1.21      0030.8047.b41f Bu1.101       isp1
2         online     5.109.1.9       0007.0e03.1349 Bu1.102       isp2
3         online(pt) 5.108.1.18      0007.0e03.12bd Bu1.101       isp1
4         online(pt) 5.108.1.20      0030.80bc.22d5 Bu1.102       isp1
5         online     5.111.1.6       0007.0e03.1331 Bu1.102       isp2
6         online(pt) 5.110.1.6       00a0.73b0.4cc1 Bu1.103       isp3
7    6                                             Bu1.101       isp1
8    6                                             Bu1.102       isp2
9    6                                             Bu1.103       isp3
10   6                                             Bu1.102       isp2
```

Displaying Service Flow Configurations

To display the basic mapping of service flows and packet classifiers, use the **show interface cable service-flow** command. To display complete service flow configuration information, add the **verbose** keyword.

The following examples display the service flow information for the CM that is using the primary SID of 6 and the SFID of 13:

```
Router# show interface cable 3/0 service-flow 13

Sfid  Sid   Mac Address     QoS Param Index   Type    Dir    Curr   Active
                            Prov  Adm  Act                   State  Time
13    6     00a0.73b0.4cc1   7     7    7     prim    US     act    12:59


Router# show interface cable 3/0 13 verbose

Sfid                                     : 13
Mac Address                              : 00a0.73b0.4cc1
Type                                     : Primary
Direction                                : Upstream
Current State                            : Active
Current QoS Indexes [Prov, Adm, Act]     : [7, 7, 7]
Active Time                              : 13:02
Sid                                      : 6
Traffic Priority                         : 0
Maximum Sustained rate                   : 0 bits/sec
Maximum Burst                            : 3044 bytes
Minimum Reserved Rate                    : 0 bits/sec
Admitted QoS Timeout                     : 200 seconds
Active QoS Timeout                       : 0 seconds
Packets                                  : 13
Bytes                                    : 1833
Rate Limit Delayed Grants                : 8
Rate Limit Dropped Grants                : 0
Current Throughput                       : 0 bits/sec, 0 packets/sec
Classifiers: NONE
```

The following examples display the service flow information for the first CPE device that is using the CM, which is using the primary SID of 6. This CPE device is using a secondary SID of 7 and the SFID of 15, and is using the VRF configuration named **isp1**.

```
Router# show interface cable 3/0 15

Sfid  Sid   Mac Address     QoS Param Index   Type    Dir    Curr   Active
                            Prov  Adm  Act                   State  Time
15    7     00a0.73b0.4cc1   8     8    8     sec(S)  US     act    13:33


Router# show interface cable 3/0 15 verbose

Sfid                                     : 15
Mac Address                              : 00a0.73b0.4cc1
Type                                     : Secondary(Static)
Direction                                : Upstream
Current State                            : Active
Current QoS Indexes [Prov, Adm, Act]     : [8, 8, 8]
Active Time                              : 13:36
Sid                                      : 7
Traffic Priority                         : 0
Maximum Sustained rate                   : 1000000 bits/sec
Maximum Burst                            : 65224 bytes
Minimum Reserved Rate                    : 0 bits/sec
Admitted QoS Timeout                     : 0 seconds
Active QoS Timeout                       : 0 seconds
Packets                                  : 56
```

```
Bytes                                   : 8608
Rate Limit Delayed Grants               : 0
Rate Limit Dropped Grants               : 0
Current Throughput                      : 0 bits/sec, 0 packets/sec
Classifiers:
Classifier Id                           : 1
Service Flow Id                         : 15
CM Mac Address                          : 00a0.73b0.4cc1
Direction                               : upstream
Activation State                        : active
Classifier Matching Priority            : 0
PHSI                                    : 0
Number of matches                       : -
Ethernet/LLC Classifier Parameters      :
Source MAC                              : 0000.0CA1.B2C3
```

The following example displays the service flow information for the second CPE device that is using the CM, which is using the primary SID of 6. This CPE device is using a secondary SID of 8 and the SFID of 16, and is using the VRF configuration named **isp2**.

```
Router# show interface cable 3/0 service-flow 16

Sfid  Sid   Mac Address     QoS Param Index   Type    Dir    Curr   Active
                            Prov  Adm  Act                   State  Time
16    8     00a0.73b0.4cc1   8     8    8     sec(S)  US     act    14:04


Router# show interface cable 3/0 service-flow 16 verbose

Sfid                                    : 16
Mac Address                             : 00a0.73b0.4cc1
Type                                    : Secondary(Static)
Direction                               : Upstream
Current State                           : Active
Current QoS Indexes [Prov, Adm, Act]    : [8, 8, 8]
Active Time                             : 14:08
Sid                                     : 8
Traffic Priority                        : 0
Maximum Sustained rate                  : 1000000 bits/sec
Maximum Burst                           : 65224 bytes
Minimum Reserved Rate                   : 0 bits/sec
Admitted QoS Timeout                    : 0 seconds
Active QoS Timeout                      : 0 seconds
Packets                                 : 155
Bytes                                   : 20418
Rate Limit Delayed Grants               : 0
Rate Limit Dropped Grants               : 0
Current Throughput                      : 0 bits/sec, 0 packets/sec
Classifiers:
Classifier Id                           : 2
Service Flow Id                         : 16
CM Mac Address                          : 00a0.73b0.4cc1
Direction                               : upstream
Activation State                        : active
Classifier Matching Priority            : 0
PHSI                                    : 0
Number of matches                       : -
Ethernet/LLC Classifier Parameters      :
Source MAC                              : 0000.0CA1.B2D4
```

The following example displays the service flow information for the third CPE device that is using the CM, which is using the primary SID of 6. This CPE device is using a secondary SID of 9 and the SFID of 17, and is using the VRF configuration named **isp3**.

```
Router# show interface cable 3/0 service-flow 17

Sfid  Sid   Mac Address     QoS Param Index   Type    Dir    Curr   Active
                            Prov  Adm  Act                   State  Time
```

```
17    9     00a0.73b0.4cc1   8     8    8     sec(S)  US     act    14:33

Router# show interface cable 3/0 service-flow 17 verbose

Sfid                                    : 17
Mac Address                             : 00a0.73b0.4cc1
Type                                    : Secondary(Static)
Direction                               : Upstream
Current State                           : Active
Current QoS Indexes [Prov, Adm, Act]    : [8, 8, 8]
Active Time                             : 14:36
Sid                                     : 9
Traffic Priority                        : 0
Maximum Sustained rate                  : 1000000 bits/sec
Maximum Burst                           : 65224 bytes
Minimum Reserved Rate                   : 0 bits/sec
Admitted QoS Timeout                    : 0 seconds
Active QoS Timeout                      : 0 seconds
Packets                                 : 141
Bytes                                   : 16152
Rate Limit Delayed Grants               : 0
Rate Limit Dropped Grants               : 0
Current Throughput                      : 33 bits/sec, 0 packets/sec
Classifiers:
Classifier Id                           : 3
Service Flow Id                         : 17
CM Mac Address                          : 00a0.73b0.4cc1
Direction                               : upstream
Activation State                        : active
Classifier Matching Priority            : 0
PHSI                                    : 0
Number of matches                       : -
Ethernet/LLC Classifier Parameters      :
Source MAC                              : 0000.0CA1.B2E5
```

The following example displays the service flow information for a dynamically generated PacketCable service flow on the modem with a primary SID of 6. The dynamic service flow is using a secondary SID of 10 and an SFID of 18, and is using the VRF configuration named isp2.

```
Router# show interface cable 3/0 service-flow 18 verbose
Sfid                                    : 18
Mac Address                             : 00a0.73b0.4cc1
Type                                    : Secondary(Dynamic)
Direction                               : Upstream
Current State                           : Active
Current QoS Indexes [Prov, Adm, Act]    : [0, 5, 5]
Active Time                             : 02:59
Sid                                     : 10
Admitted QoS Timeout                    : 200 seconds
Active QoS Timeout                      : 0 seconds
Packets                                 : 8967
Bytes                                   : 2080344
Rate Limit Delayed Grants               : 0
Rate Limit Dropped Grants               : 0
Current Throughput                      : 92399 bits/sec, 49 packets/sec
Classifiers:
Classifier Id                           : 1
Service Flow Id                         : 18
CM Mac Address                          : 00a0.73b0.4cc1
Direction                               : upstream
Activation State                        : active
Classifier Matching Priority            : 64
PHSI                                    : 0
Number of matches                       : -
IP Classification Parameters            :
IP Source Address                       : 4.22.96.99
Source IP Address Mask                  : 255.255.255.255
Destination IP Address                  : 4.18.39.12
Destination IP Address Mask             : 255.255.255.255
```

```
IP Protocol Type                        : 17
Source Port Low                         : 16622
Source Port High                        : 16622
Destination Port Low                    : 17640
Destination Port High                   : 17640
```

Configuration Examples

This section provides the following configuration examples:

Example: DOCSIS Configuration File

The following example shows a cable modem being configured to support three MPLS VPN routes. This includes three upstream packet classifiers and three upstream service-flow parameter sets. It also shows the configuration required to have dynamic service flows associated with a particular MPLS VPN:

```
CM-CONFIG
=========
03 (Net Access Control)         = 1
18 (Maximum Number of CPE)      = 100
28 (Max Number of Classifiers)  = 4
29 (Privacy Enable)             = 1
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 10
   S03 (Service Flow Reference)         = 3
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 00 0C A1 B2 C3
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 12
   S03 (Service Flow Reference)         = 5
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 00 0C A1 B2 D4
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 14
   S03 (Service Flow Reference)         = 7
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 00 0C A1 B2 E5
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 1
   S06 (QoS Parameter Set Type)         = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 2
   S06 (QoS Parameter Set Type)         = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 3
   S06 (QoS Parameter Set Type)         = 7
   S08 (Max Sustained Traffic Rate)     = 1000000
   S09 (Maximum Traffic Burst)          = 65224
   S12 (Timeout Active QoS Parms)       = 0
   S13 (Timeout Admitted QoS Parms)     = 0
   S15 (Service Flow Sched Type)        = 2
   S43 (Vendor Specific Options) = 8.3.0.0.12.4.8.0.0.250.0.0.0.0.1
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 5
   S06 (QoS Parameter Set Type)         = 7
   S08 (Max Sustained Traffic Rate)     = 1000000
   S09 (Maximum Traffic Burst)          = 65224
   S12 (Timeout Active QoS Parms)       = 0
   S13 (Timeout Admitted QoS Parms)     = 0
   S15 (Service Flow Sched Type)        = 2
   S43 (Vendor Specific Options) = 8.3.0.0.12.4.8.0.0.246.24.0.0.0.1
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 7
   S06 (QoS Parameter Set Type)         = 7
```

```
   S08 (Max Sustained Traffic Rate)     = 1000000
   S09 (Maximum Traffic Burst)          = 65224
   S12 (Timeout Active QoS Parms)       = 0
   S13 (Timeout Admitted QoS Parms)     = 0
   S15 (Service Flow Sched Type)        = 2
   S43 (Vendor Specific Options) = 8.3.0.0.12.4.8.0.0.253.232.0.0.0.1
43 (Vendor Specific Info)
    S8 (Vendor ID)  = 0-0-c
    S13 (Dynamic Flow VPN RD)  = 0-0-fa-0-0-0-0-1
#<EOF>
```

Example: MPLS VPN Interface Configuration

The following example shows the corresponding VRF configurations with the three VRF route-designators that match the MPLS-VPN configuration that is used on the cable modem:

```
ip vrf MGMT
 rd 1:1
 route-target export 62000:1
 route-target import 62000:1
 route-target import 63000:1
 route-target import 64000:1
 route-target import 65000:1
!
ip vrf isp1
 rd 64000:1
 route-target export 64000:1
 route-target import 64000:1
 route-target import 62000:1
!
ip vrf isp2
 rd 63000:1
 route-target export 63000:1
 route-target import 63000:1
 route-target import 62000:1
!
ip vrf isp3
 rd 65000:1
 route-target export 65000:1
 route-target import 65000:1
 route-target import 62000:1
!
interface Bundle1
 no ip address
 hold-queue 1024 in
!
interface Bundle1.100
 ip vrf forwarding MGMT
 ip address 10.22.32.1 255.255.255.0
 cable dhcp-giaddr policy
 cable helper-address 4.104.0.66
!
interface Bundle1.101
 ip vrf forwarding isp1
 ip address 10.22.64.1 255.255.224.0
 ip address 4.22.64.1 255.255.224.0 secondary
 cable dhcp-giaddr policy
 cable helper-address 4.104.0.66
!
interface Bundle1.102
 ip vrf forwarding isp2
 ip address 10.22.96.1 255.255.224.0
 ip address 4.22.96.1 255.255.224.0 secondary
 cable dhcp-giaddr policy
 cable helper-address 4.104.0.66
!
interface Bundle1.103
 ip vrf forwarding isp3
```

```
 ip address 10.22.128.1 255.255.224.0
 ip address 4.22.128.1 255.255.224.0 secondary
 cable dhcp-giaddr policy
 cable helper-address 4.104.0.66
!
```

Example: Upstream Service Flow Marking TLV

The following example shows a sample CM configuration TLV for the provisioning of TC bits for MPLS imposition packets:

```
24 (Upstream Service Flow Encoding)
   S01 (Service Flow Reference)         = 2
   S06 (QoS Parameter Set Type)         = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = 00 00 0c
       T004 (VPN Route Distinguisher) = xx xx xx xx xx xx xx xx
            S005 (Vendor specific L2VPN TLV)
            S043 (Cisco Vendor Specific)
       T034 (MPLS-TC-SET) = 04 # MPLSTC-SET = 4
```

Example: Downstream Packet Classification TLV

The following example shows a sample CM configuration TLV for classifying downstream packets based on TC bits of MPLS disposition packets:

```
23 (Downstream Packet Classification Encoding)
   S01 (Classifier Reference)           = 13
   S03 (Service Flow Reference)         = 13
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = 00 00 0c
       S004 (VPN Route Distinguisher) = xx xx xx xx xx xx xx xx
       S005 (Vendor specific L2VPN TLV)
           S043 (Cisco Vendor Specific)
           S035 (MPLS-TC-RANGE)   = 04  05      # MPLSTC-EGRESS_RANGE= 4 – 5
```

Example: MPLS QoS Configuration File

The following example shows a cable modem being configured to mark TC bits for MPLS L3VPN imposition packets and classify downstream packets based on TC bits of MPLS L3VPN disposition packets, using vendor-specific TLVs:

```
CM-CONFIG
=========
03 (Net Access Control)                     = 1
18 (Maximum Number of CPE)       = 16
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 2
   S03 (Service Flow Reference)        = 2
   S05 (Rule Priority)                             = 2
   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)             = 40 80 ff
22 (Upstream Packet Classification Encoding Block)
```

```
   S01 (Classifier Reference)              = 4
   S03 (Service Flow Reference)        = 4
   S05 (Rule Priority)                             = 4
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = a0 e0 ff
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 12
   S03 (Service Flow Reference)        = 12
   S05 (Rule Priority)                             = 2
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 01 01
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 13
   S03 (Service Flow Reference)        = 13
   S05 (Rule Priority)                             = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 02 02
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 14
   S03 (Service Flow Reference)        = 14
   S05 (Rule Priority)                             = 4
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 03 03
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)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 08 08 03 00 00 0c 22 01 04
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 3
   S06 (QoS Parameter Set Type)     = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 08 08 03 00 00 0c 22 01 05
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 4
   S06 (QoS Parameter Set Type)     = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 08 08 03 00 00 0c 22 01 06
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 11
   S06 (QoS Parameter Set Type)     = 7
   S07 (Traffic Priority)                        = 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
25 (Downstream Service Flow Encodings)
```

```
   S01 (Service Flow Reference)        = 15
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 16
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 17
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 18
   S06 (QoS Parameter Set Type)     = 7
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 19
   S03 (Service Flow Reference)        = 19
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)            = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 00 00
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 15
   S03 (Service Flow Reference)        = 15
   S05 (Rule Priority)                            = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)            = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 04 04
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 16
   S03 (Service Flow Reference)        = 16
   S05 (Rule Priority)                            = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)            = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 05 05
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 17
   S03 (Service Flow Reference)        = 17
   S05 (Rule Priority)                            = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)            = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 06 06
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 18
   S03 (Service Flow Reference)        = 18
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)            = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 07 07
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 19
   S06 (QoS Parameter Set Type)     = 7
#<EOF>
```

Additional References

The following sections provide references related to the Cisco CMTS routers.

Related Documents

Related Topic	Document Title
Cisco CMTS command reference	*Cisco IOS CMTS Cable Command Reference Guide,* at the following URL: http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
Cisco IOS Release 12.2	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URLs: http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-software-releases-12-2-mainline/products-installation-and-configuration-guides-list.html http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-software-releases-12-2-mainline/products-command-reference-list.html
Configuring cable features	*Cisco IOS CMTS Cable Software Configuration Guide* , *Release 12.2SC* , at the following URL: http://www.cisco.com/web/techdoc/cable/Config/Sw_conf.html
Installing and configuring Cisco uBR7200 Series Universal Broadband Routers	Cisco uBR7200 Universal Broadband Routers, at the following URL: http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr7200/installation/guide/ub72khig.html
Installing and configuring the Cisco uBR10012 Router	Cisco uBR10012 Universal Broadband Router, at the following URL: http://www.cisco.com/c/en/us/td/docs/cable/cmts/ubr10012/quick/start/10kqsg_2.html
Service provider solution	Cisco Cable-Ready High Speed Data (HSD) Managed Access Solution for Service Providers, at the following URL: http://www.cisco.com/c/en/us/solutions/service-provider/cable-high-speed-data-hsd-solutions/index.html
MPLS VPN	Cisco uBR7200 Series MPLS VPN Cable Enhancements, which is at the following URL: http://www.cisco.com/c/en/us/td/docs/ios/cable/configuration/guide/12_2sc/Cisco_CMTS_Layer2_VPN/u72_mpls_vpn_cbl.html

Standards

Standard	Title
DOCSIS	Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification (SP-RFIv1.1-I08-020301)

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
RFC 1163	A Border Gateway Protocol
RFC 1164	Application of the Border Gateway Protocol in the Internet
RFC 2233	DOCSIS OSSI Objects Support
RFC 2283	Multiprotocol Extensions for BGP-4
RFC 2547	BGP/MPLS VPNs
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB
RFC 5462	Multiprotocol Label Switching (MPLS) Label Stack Entry: “EXP” Field Renamed to “Traffic Class” Field

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 Service Flow Mapping to MPLS-VPN on the Cisco CMTS Routers

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below 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.

Table 17: Feature Information for Service Flow Mapping to MPLS-VPN on the Cisco CMTS Routers

Feature Name	Releases	Feature Information
Service Flow Mapping to MPLS-VPN on the Cisco CMTS Routers	12.2(11)BC2	This feature was supported on the Cisco uBR7100 series and Cisco uBR7200 series universal broadband routers.
Mapping Dynamic Service Flows	12.3(13)BC	Support was added for mapping dynamic service flows on the Cisco uBR7200 series and the Cisco uBR10000 series.
VoIP SFID Mapping	12.2(33)SCB	Support was added for the VoIP SFID Mapping feature.

Feature Name	Releases	Feature Information
MPLS QoS via TLV for non-L2VPN SF	12.2(33)SCG	This feature allows to mark TC bits for MPLS L3VPN imposition packets and classify downstream packets based on TC bits of MPLS disposition packets, using vendor-specific TLVs. The following sections provide information about this feature:

CHAPTER 9

Transparent LAN Service over Cable

First Published: February 14, 2008

This document describes the Transparent LAN Service over Cable feature, which enhances existing Wide Area Network (WAN) support to provide more flexible Managed Access for multiple Internet service provider (ISP) support over a hybrid fiber-coaxial (HFC) cable network. This feature allows service providers to create a Layer 2 tunnel by mapping an upstream service identifier (SID) to an IEEE 802.1Q Virtual Local Area Network (VLAN).

Note Cisco IOS Release 12.2(33)SCA integrates support for this feature on the Cisco CMTS routers. This feature is also supported in Cisco IOS Release 12.3BC, and this document contains information that references many legacy documents related to Cisco IOS 12.3BC. In general, any references to Cisco IOS Release 12.3BC also apply to Cisco IOS Release 12.2SC.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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

Contents

• Feature Information for Transparent LAN Service over Cable, page 181

Prerequisites for Transparent LAN Service over Cable

The Transparent LAN Service over Cable feature has the following prerequisites:

- You must know the hardware (MAC) addresses of the cable modems that are to be mapped to IEEE 802.1Q VLANs.
- You must create a bridge group for each separate customer on the Layer 2 bridge aggregator, so that traffic from all of the Customer Premises Equipment (CPE) devices for the customer is grouped together into the same ATM or 802.1Q tunnel.

Restrictions for Transparent LAN Service over Cable

- Configuring ATM L2VPN or 802.1q for a particular cable modem removes any previous cable modem configuration on the Cisco uBR7246VXR router. For example, if TLS with 802.1q is configured on the router for a particular cable modem, and then you configure ATM L2VPN for the same cable modem, the Cisco uBR7246VXR router supports the latter and removes the former with no additional warning or system messages.
- We strongly recommend that TLS over Cable only be used when Baseline Privacy Interface (BPI) is enabled in the environment. If BPI is not enabled when using the TLS feature, traffic can flow between multiple virtual private networks (VPNs), and become vulnerable to denial-of-service attacks or snooping. We also recommend that remote networks be isolated with a gateway or firewall router when BPI is not enabled.

Commencing in Cisco IOS release 12.3(13a)BC, and later releases, when the TLS feature is used with Layer 2 VPNs, the participating cable modems *must* have the Baseline Privacy Interface security feature (BPI) enabled. Otherwise, the Cisco CMTS drops such Layer 2 traffic in the upstream or downstream.

- Packets are mapped to their Layer 2 tunnel only on the basis of Layer 2 information (the cable modem's MAC address and primary SID). Layer 3 services, such as access lists, IP address source-verify, and IP QoS, are not supported as packets are sent through the tunnel.
- All traffic from a cable modem is mapped to the same Layer 2 tunnel. It is not possible to differentiate traffic from different customer premises equipment (CPE) devices behind the cable modem.
- CPE learning is not available when using the Transparent LAN Service over Cable feature. When a cable modem is mapped to a Layer 2 tunnel, the **show interface cable modem** command shows that the IP addresses for its CPE devices are "unavailable."
- DOCSIS QoS is supported across the Layer 2 tunnel only on the primary SID. Traffic using secondary services uses the same Layer 2 tunnel as the primary SID.
- The Spanning Tree Protocol (STP) cannot be used with devices (cable modems, their CPE devices, and the endpoint CPE devices) that are using this feature. In particular, Spanning Tree Protocol cannot be used between the VLAN bridge aggregator and the endpoint customer devices.
- The following restrictions apply to Layer 2 tunnels over an ATM interface:

- The virtual connections (VC) on the ATM interface must be configured to use ATM Adaptation Layer 5 (AAL5) IEEE 802.1a Subnetwork Access Point (SNAP) encapsulation. On Cisco routers, this means that each PVC endpoint must be configured for the proper encapsulation using the **encapsulation aal5snap** command.

- The following restrictions apply to Layer 2 tunnels over an Ethernet IEEE 802.1Q VLAN interface:
  - IEEE 802.1Q tunnels are supported only on Ethernet, Fast Ethernet, Gigabit Ethernet and 10 Gigabit Ethernet interfaces.
  - The Cisco CMTS router supports a maximum of 4095 VLAN IDs, but the switches acting as the bridge aggregator might support a lower number of VLAN IDs. If this is the case, the Cisco CMTS should be configured only for the maximum number of VLANs that are supported by the bridge aggregator switches.

Information About Transparent LAN Service over Cable

This section contains the following:

Feature Overview

The Transparent LAN Service over Cable feature enables service providers to provide Layer 2 tunnels for traffic to and from cable modems. This allows customers to create their own virtual local area network (VLAN) using any number of cable modems in multiple sites.

On the Cisco CMTS, you map each cable modem (on the basis of its MAC address) to the appropriate VLAN. The CMTS then creates an internal database of this one-to-one mapping of cable modems to VLANs, and uses it to encapsulate packets for the appropriate VLAN.

The CMTS encapsulates the CPE traffic from mapped cable modems using the following method:

- IEEE 802.1Q Mapping—The cable modem's MAC address is mapped to an IEEE 802.1Q VLAN on a specific Ethernet interface, so that all traffic from the cable modem is tagged with the specified VLAN ID.

Traffic to and from this group of cable modems is bridged into a single logical network (the VLAN) by the bridge aggregator, creating a secure Virtual Private Network (VPN) for that particular group of cable modems. Traffic in one VLAN cannot be sent into another VLAN, unless specifically done so by an external router.

The switch acting as the Layer 2 Bridge Aggregator uses the VLAN tagging to forward the traffic to the appropriate destination. This frees up service providers from needing to know the addressing, routing, and topological details of the customer's network.

Transparent LAN Service and Layer 2 Virtual Private Networks

In addition, service providers can provide a Layer 2 VPN with only minimal configuration changes on the provider's routers. The service subscriber does not need to make any changes to their private network or cable modems, nor does the service provider have to provide any special DOCSIS configuration files to enable this feature.

Cisco IOS Release 12.3(13a)BC introduces the following changes or requirements for the TLS feature with Layer 2 VPNs:

- When the TLS feature is used with Layer 2 VPNs, the participating cable modems must have the Baseline Privacy Interface security feature (BPI) enabled. Otherwise, the Cisco CMTS drops such Layer 2 traffic in the upstream or downstream.
- Information about Customer Premises Equipment (CPE) does not display in the output of the **show cable modem** command.

IEEE 802.1Q Mapping

This section describes the mapping of cable modems to an IEEE 802.1Q VLAN, as it is available in the Transparent LAN Service over Cable feature:

Overview

The Transparent LAN Service over Cable feature enables service providers to provide Layer 2 tunnels over an Ethernet network, using IEEE 802.1Q standard tags. This allows customers to create their own virtual network using any number of cable modems in different sites.

On the Cisco CMTS, you map each cable modem (on the basis of its MAC address) to the appropriate VLAN. The CMTS then creates an internal database of this one-to-one mapping of cable modems to VLANs, and uses it to encapsulate packets for the appropriate VLAN.

The CMTS encapsulates the CPE traffic from mapped cable modems using VLAN tags, as defined in IEEE 802.1Q-1993, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks . The switch acting as the Layer 2 Bridge Aggregator uses the VLAN tagging to forward the packets to the appropriate destination.

Traffic to and from this group of cable modems is bridged into a single logical network by the bridge aggregator, creating a secure Virtual Private Network (VPN) for that particular group of cable modems. Traffic in one VLAN cannot be sent into another VLAN, unless specifically done so by an external router.

Details of IEEE 802.1Q Mapping

To implement the Transparent LAN Service over Cable feature using IEEE 802.1Q VLANs, a service provider must perform the following configuration steps:

1. Identify the cable modems and their MAC addresses that should be mapped to the IEEE 802.1Q VLANs.
2. Create the required VLANs on the router that is acting as the bridge aggregator.
3. Enable Layer 2 mapping on the Cisco CMTS, and then map each cable modem on that Cisco CMTS to the appropriate VLAN.

After the Transparent LAN Service over Cable feature has been enabled and configured to use IEEE 802.1Q mappings, the Cisco CMTS immediately begins mapping traffic between the associated cable modems and VLANs. For efficient mapping, the Cisco CMTS maintains an internal database that links each cable modem's primary service flow ID (SFID) and service ID (SID) to the appropriate VLAN and Ethernet interface. This ensures that all service flows from the cable modem are routed properly.

When the Cisco CMTS receives a packet on an upstream, it looks up its SID to see if it is mapped to a VLAN. If so, and if the packet's source MAC address is not the cable modem's MAC address, the Cisco CMTS inserts

the appropriate IEEE 802.1Q VLAN tag into the packet's header and forwards the packet to the appropriate Ethernet interface. If the packet is not being mapped, or if the packet originated from the cable modem, the Cisco CMTS routes the packet using the normal Layer 3 processes.

When the Cisco CMTS receives a packet from a WAN interface that is encapsulated with an IEEE 802.1Q VLAN tag, it looks up the packet's SID to see if it belongs to a cable modem being mapped. If so, the Cisco CMTS strips off the VLAN tag, adds the proper DOCSIS header, and transmits the packet on the appropriate downstream interface. If the packet is not being mapped, the Cisco CMTS continues with the normal Layer 3 processing.

Benefits

The Transparent LAN Service over Cable feature provides the following benefits to cable service providers and their partners and customers:

- Provides Layer 2 level mapping, which is transparent to Layer 3 protocols and services. This means that service providers do not need to know the details of their customers' network topologies, routing protocols, or IP addressing.
- Allows service providers to maximize the use of their existing ATM or Ethernet WAN networks. Multiple customers can be combined on the same outgoing interface, while still ensuring that each customer's network is kept private while it is transmitted over the tunnel.
- Provides a highly flexible and scalable solution for multiple customers. The service provider needs to create only one bridge group for each VPN, and then only one VLAN mapping for each cable modem should participate in that VPN tunnel.
- Customers retain full control over their private networks, while service providers retain full control over cable modems and the rest of the cable and ATM networks. Only the CPE traffic from the cable modems is mapped into the ATM tunnel, while traffic originating at the cable modem continues to be processed as normal by the service provider's network.
- Allows service providers to mix tunneled and non-tunneled cable modems on the same DOCSIS cable network.
- Allows customers to create a single, secure virtual network with Ethernet Layer 2 connectivity for multiple sites.
- Allows multiple tunnels from different customers and endpoints to be aggregated into a single bridge, so as to maximize the use of bandwidth and other network resources.
- Supports the tunneling of multiple Layer 3, non-IP protocols, and not just IP Layer 3 services, as is the case with Layer 3 solutions, such as Multiprotocol Label Switching (MPLS) VPNs.
- All DOCSIS services, including BPI+ encryption and authentication, continue to be supported for all cable modems.

How to Configure the Transparent LAN Service over Cable

This section contains the following:

Configuring IEEE 802.1Q VLAN Mapping

This section describes how to enable Layer 2 mapping on the Cisco CMTS, and then to map particular cable modems to an IEEE 802.1Q VLAN.

Enabling and Configuring Layer 2 Tunneling for IEEE 802.1Q Mapping

This section describes how to enable Layer 2 mapping on the Cisco CMTS, and then to map particular cable modems to IEEE 802.1Q VLANs on an Ethernet, Fast Ethernet, or Gigabit Ethernet interface.

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	**cable l2-vpn-service dot1q** or**cable l2-vpn-service xconnect nsi dot1q**
	
	Example:
	`Router(config)# cable l2-vpn-service dot1q`
	`or`
	
	Example:
	`Router(config)# cable l2-vpn-service xconnect nsi dot1q`
		Note Use cable l2-vpn-service xconnect nsi dot1q command at this step, for Cisco IOS Release 12.2(33)SCC and later. Use cable l2-vpn-service dot1q command, for Cisco IOS Releases 12.2(33)SCA and 12.2(33)SCB.
		Enables Layer 2 tunneling for IEEE 802.1Q VLAN mapping.
		Note It is not required to configure VLAN trunking on the Cisco CMTS. Though VLAN trunking is supported, be aware of additional impact of VLAN trunking on the Cisco CMTS.

Step 4	**cable dot1q-vc-map** *mac-address ethernet-interface vlan-id* [*cust-name*] **Example:** `Router(config)# cable dot1q-vc-map 0000.0C04.0506 FastEthernet0/0 10`	Maps the specified MAC address of a cable modem to the indicated VLAN and Ethernet, Fast Ethernet, or Gigabit Ethernet interface. **Note** Repeat this command for each cable modem that is to be mapped to an IEEE 802.1Q VLAN.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Creating the IEEE 802.1Q VLAN Bridge Group

This section describes the minimum configuration needed to configure a Cisco router, which is acting as an IEEE 802.1Q VLAN bridge aggregator, so that it can terminate the VLANs being used with the Transparent LAN Service over Cable feature.

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` **Example:**	Enters global configuration mode.

Step 3	**interface** [**Ethernet** | **FastEthernet** | **GigabitEthernet** | **TenGigabitEthernet**] *x/0*
	
	Example:
	`Router(config)# interface fastethernet 1/0`
	
	Example:
	`Router(config-if)#`
		Enters interface configuration mode for the Ethernet interface that is in slot *x* .

Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.10.10.85 255.255.255.0`	Configures the interface with the specified IP address and subnet mask.

Step 5	**interface** [**Ethernet** | **FastEthernet** | **GigabitEthernet** | **TenGigabitEthernet**] *x/0.y*
	
	Example:
	`Router(config)# interface fastethernet 1/0.10`
	
	Example:
	`Router(config-if)#`
		Creates a subinterface on the Ethernet interface that is in slot *x* . The valid range for *y* is 1 to 4294967293, with no default.
		
		Note Note 1: To simplify network management, set the subinterface number to the same value as the VLAN ID that will use this subinterface (which in this case is 10). The valid range for the subinterface number is 1 to 4095. Note 2: The steps to create a subinterface is not essential for dot1q tagging of frames but it is recommended.

Step 6	**bridge group** *number*	Configures this subinterface to belong to the specified bridge group.

	Command or Action	Purpose
	Example: `Router(config-if)# bridge group 20`	The valid range for number is 1 to 255, with no default. **Note** Repeat steps Step 5 through Step 7 for each subinterface to be created and bridged.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Transparent LAN Service over Cable

This section lists sample configurations for the Transparent LAN Service over Cable feature on a CMTS router and on a Cisco router acting as an ATM bridge aggregator:

Example: Configuring IEEE 802.1Q VLAN Mapping

The following partial configuration for a Cisco uBR7246VXR router shows a typical configuration that shows a number of cable modems being mapped to two different IEEE 802.1Q VLANs.

```
cable l2-vpn-service dot1q
! Customer 1
cable dot1q-vc-map 000C.0e03.69f9 GigabitEthernet 1/0 10 Customer1
cable dot1q-vc-map 0010.7bea.9c95 GigabitEthernet 1/0 11 Customer1
cable dot1q-vc-map 0010.7bed.81c2 GigabitEthernet 1/0 12 Customer1
cable dot1q-vc-map 0010.7bed.9b1a GigabitEthernet 1/0 13 Customer1
! Customer 2
cable dot1q-vc-map 0002.fdfa.137d GigabitEthernet 1/0 20 Customer2
cable dot1q-vc-map 0006.28f9.9d19 GigabitEthernet 1/0 21 Customer2
cable dot1q-vc-map 000C.7b6b.58c1 GigabitEthernet 1/0 22 Customer2
cable dot1q-vc-map 000C.7bed.9dbb GigabitEthernet 1/0 23 Customer2
cable dot1q-vc-map 000C.7b43.aa7f GigabitEthernet 1/0 24 Customer2
cable dot1q-vc-map 0050.7302.3d83 GigabitEthernet 1/0 25 Customer2
...
```

Example: Configuring IEEE 802.1Q Bridge Aggregator

The following example shows a router being used as a bridge aggregator to transmit VLANs across the same Fast Ethernet interface, using IEEE 802.1Q tagging.

```
!
interface GigabitEthernet0/1
 ip address 10.10.10.31 255.255.255.0
 duplex full
 speed auto
!
interface GigabitEthernet0/1.10
 description Customer1-site10
 encapsulation dot1Q 10
 bridge-group 200
```

```
interface GigabitEthernet0/1.11
 description Customer1-site11
 encapsulation dot1Q 11
 bridge-group 200
interface GigabitEthernet0/1.12
 description Customer1-site12
 encapsulation dot1Q 12
 bridge-group 200
interface GigabitEthernet0/1.13
 description Customer1-site13
 encapsulation dot1Q 13
 bridge-group 200
!-----------------------------------
interface GigabitEthernet0/1.20
 description Customer2-site20
 encapsulation dot1Q 20
 bridge-group 201
interface GigabitEthernet0/1.21
 description Customer2-site21
 encapsulation dot1Q 21
 bridge-group 201
interface GigabitEthernet0/1.22
 description Customer2-site22
 encapsulation dot1Q 22
 bridge-group 201
interface GigabitEthernet0/1.23
 description Customer2-site23
 encapsulation dot1Q 23
 bridge-group 201
interface GigabitEthernet0/1.24
 description Customer2-site24
 encapsulation dot1Q 24
 bridge-group 201
interface GigabitEthernet0/1.25
 description Customer2-site25
 encapsulation dot1Q 25
 bridge-group 201
!
bridge 200 protocol ieee
bridge 201 protocol ieee
...
```

Additional References

Related Documents

Related Topic	Document Title
ATM Interface Configuration	Configuring ATM in the *Cisco IOS Wide-Area Networking Configuration Guide,* Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/wan/configuration/guide/fwan_c.html
ATM Interface Configuration	Configuring ATM in the *Cisco IOS Wide-Area Networking Configuration Guide,* Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/wan/configuration/guide/fwan_c.html

Related Topic	Document Title
ATM Interface Command Reference	ATM Commands in the *Cisco IOS Wide-Area NetworkingCommand Reference,* Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/wan/command/reference/fwan_r.html
Virtual LAN Configuration	Virtual LANS in the *Cisco IOS Switching Services Configuration Guide* , Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/fswtch_c.html
Virtual LAN Command Reference	*Cisco IOS Switching Services Command Reference* , Release 12.2, at the following URL: http://www.cisco.com/en/US/docs/ios/12_2/switch/command/reference/fswtch_r.html
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html

Standards

Standards	Title
SP-RFIv1.1-I08-020301	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification
IEEE 802.1Q, 1998 Edition	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks

RFCs

RFCs[11]	Title
RFC 1163	A Border Gateway Protocol
RFC 1164	Application of the Border Gateway Protocol in the Internet
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5)

RFCs[11]	Title
RFC 2233	DOCSIS OSSI Objects Support
RFC 2283	Multiprotocol Extensions for BGP-4
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

11 Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Transparent LAN Service over Cable

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below 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.

Table 18: Feature Information for Transparent LAN Service over Cable

Feature Name	Releases	Feature Information
Transparent LAN Service over Cable	Release 12.2(11)BC3	This feature was introduced for Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers to support Layer 2 encapsulation over ATM networks. The following sections provide information about this feature: The following commands were introduced or modified: • **cable dot1q-vc-map** • **cable l2-vpn-service atm-vc** • **cable l2-vpn-service dot1q** • **cable vc-map** • **debug cable l2-vpn** • **show cable l2-vpn vc-map**
IEEE 802.1Q Virtual Local Area Network	Release 12.2(15)BC2	Support was added for IEEE 802.1Q Virtual Local Area Network (VLAN) tagging on the Cisco uBR7246VXR universal broadband router. Support was also added for identifying mappings with a customer name. The following commands were introduced or modified: • **show cable l2-vpn dot1q-vc-map**
Transparent LAN Services	Release 12.3(9a)BC	Support was added for Transparent LAN Services (TLS) for the following Cisco CMTS platforms: • IEEE 802.1Q on the Cisco uBR10012 router with Cisco uBR10012 PRE2 performance routing engine modules • ATM on the Cisco uBR7246VXR router

CHAPTER 10

VRF Steering for Cisco CMTS Routers

First Published: June 20, 2011

The virtual routing and forwarding (VRF) steering feature allows provisioning of data traffic from cable modems to be contained to a specified VRF instance. This enables all traffic from and to a particular set of cable modems to be constrained to a VRF instance.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 at the end of this document.

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

Contents

Prerequisites for VRF Steering

The table shows the hardware compatibility prerequisites for this feature.

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

Table 19: Cable Hardware Compatibility Matrix for VRF Steering

Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	**Cisco IOS Release 12.2(33)SCF and later releases** • PRE2 • PRE4 **Cisco IOS Release 12.2(33)SCH and later releases** • PRE5	Cisco IOS Release 12.2(33)SCF and later releases • Cisco uBR10-MC5X20H • Cisco UBR-MC20X20V • Cisco uBR-MC3GX60V[12]
Cisco uBR7246VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCF and later releases** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCF and later releases** • Cisco uBR-MC28U/X • Cisco uBR-MC88V
Cisco uBR7225VXR Universal Broadband Router	**Cisco IOS Release 12.2(33)SCF and later releases** • NPE-G1 • NPE-G2	**Cisco IOS Release 12.2(33)SCF and later releases** • Cisco uBR-MC28U/X • Cisco uBR-MC88V

12 The Cisco uBR-MC3GX60V line card is not compatible with PRE2.

Restrictions for VRF Steering

- Customer premise equipment (CPE) cannot specify a VRF instance unlike the cable modem.
- Only a single instance of the cable vrf-steering cable-modem command is supported.
- Only IPv4 is supported.

Information About VRF Steering

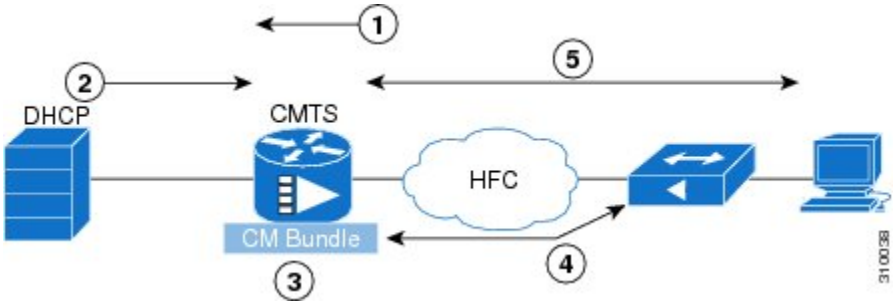
The VRF steering feature is developed to address the need for accommodating more IPv4 addresses when customers run out of IPv4 addresses for their CPE. This solution helps customers expand their existing IP address space until they move to the IPv6 address mode.

The availability of new IPv4 addresses is quickly coming to an end. In order to continue provisioning new subscribers, operators must switch to IPv6. This feature is designed to give the operators additional time to switch to IPv6 by expanding the use of non-traditional IPv4 addresses within their network. This feature allows the operator to create a private VRF for cable modems that are not routable outside of the operator network and choose any address since the CM addresses will not be routed externally. The CPE devices will continue to be provisioned with globally routable addresses, allowing them to peruse the internet.

VRF Steering Process

The figure and the following sequence of events describe the VRF steering process.

Figure 5: VRF Steering Process



1. The master bundle interface has at least 2 sub-bundles configured. The CPE is routed using the global sub-bundle interface. The CM is routed using the private VRF sub-bundle interface.
2. CM address negotiation happens using helper-address of the private VRF sub-bundle interface.
3. CPE address negotiation happens using helper-address of the global sub-bundle interface.
4. The Cisco CMTS steers all cable modem data traffic into the VRF. CM traffic that is punted to the route processor (RP) is forwarded only on the CM VRF.
5. At this point the CPE is able to get an IP address using the global Dynamic Host Configuration Protocol (DHCP) server. Since the CPE traffic is not classified, it uses the global routing table and is routable.

How to Configure VRF Steering

Configuring the VRF Steering

This section describes how to configure a VRF instance on the Cisco CMTS router.

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	**ip vrf vrf-name**
	
	Example:
	`Router(config)# ip vrf CM-VRF`
	
	Example:
	`rd 100:100`
	
	Example:
	`route-target export 100:100`
	
	Example:
	`route-target import 100:100`
		Defines a VRF instance and enters the interface configuration mode.
		• vrf-name—Name assigned to a VRF.

Step 4	**ip access-list extended** access-list-name
	
	Example:
	`Router(config)# ip access-list extended vrfcpe`
	
	Example:
	`permit ip 111.1.0.0 0.0.255.255 any`
	
	Example:
	`permit ip 112.1.0.0 0.0.255.255 any`
	
	Example:
	`permit ip 101.1.0.0 0.0.255.255 any`
		Specifies an extended IP access list to enable filtering for packets with IP helper-address destinations.
		• access-list-name—Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.

	Command or Action	Purpose

Step 5	**route-map** map-tag **permit** sequence-number
	
	Example:
	`Router(config)# route-map cpe permit 10`
	
	Example:
	`Router(config)#route-map cpe permit 10`
	
	Example:
	`Router(config-route-map)# match ip address vrfcpe`
	
	Example:
	`Router(config-route-map)# set global`
		Defines the conditions for redistributing routes from one routing protocol into another routing protocol, or to enable policy routing. The route map needs to reference the ACL.
		• map-tag—A meaningful name for the route map.
		• sequence-number—Number that indicates the position a new route map will have in the list of route maps already configured with the same name.

Step 6	**interface bundle** *n* **Example:** `Router(config-if)# interface Bundle1`	Adds the selected interface to the virtual bundle. If this is the first interface on which the virtual bundle is configured, this command enables the bundle on the specified interface. • *n*—Interface bundle number. You can configure as many as 40 virtual interface bundles on the Cisco CMTS. The numeric identifiers may range from 1 to 255.
Step 7	**cable vrf-steering cable-modem** *vrf-name* **Example:** `Router(config-if)# cable vrf-steering cable-modem CM-VRF`	Steers or directs cable modems to the specified VRF in the cable interface configuration mode. • *vrf-name*—The VPN Routing/ Forwarding instance name.
Step 8	interface bundle n.1 **Example:** `Router(config-if)# interface Bundle1.1`	Adds the selected interface to the virtual bundle. If this is the first interface on which the virtual bundle is configured, this command enables the bundle on the specified interface. • *n.1*—Interface sub-bundle number. You can configure as many as 40 virtual interface bundles on the Cisco CMTS. Numeric identifiers may range from 1 to 255.
Step 9	**ip address ip-address mask secondary** **Example:** `Router(config-subif)# ip address 112.1.1.1 255.255.0.0 secondary`	Sets a secondary IP address for an interface. **Note** Create a primary interface address before setting a secondary IP address. If the secondary address is used for a VRF table configuration with the vrf keyword, the vrf keyword must be specified also.

	Command or Action	Purpose
Step 10	**cable dhcp-giaddr policy** **Example:** `Router(config-subif)# cable dhcp-giaddr policy`	(Optional) Selects the control policy, so that the primary address is used for cable modems and the secondary addresses are used for hosts and other CPE devices.
Step 11	cable helper-address *IP-address* **Example:** `Router(config-subif)# cable helper-address 72.10.10.2`	Specifies a destination IP address for User Datagram Protocol (UDP) broadcast DHCP packets in cable subinterface configuration mode. • IP-address—The IP address of a DHCP server to which UDP broadcast packets will be sent.
Step 12	**exit** **Example:** `Router(config-subif)# exit`	Exits the subinterface configuration mode.
Step 13	interface bundle n.2 **Example:** `Router(config-if)# interface Bundle1.2`	Adds the selected interface to the virtual sub-bundle. If this is the first interface on which the virtual bundle is configured, this command enables the bundle on the specified interface. • *n.2*—Interface sub-bundle number. You can configure as many as 40 virtual interface bundles on the Cisco CMTS. Numeric identifiers may range from 1 to 255.
Step 14	ip vrf forwarding vrf-name **Example:** `Router(config-subif)# ip vrf forwarding CM-VRF`	Associates a VRF instance with an interface or subinterface. • vrf-name—Name assigned to a VRF.
Step 15	**ip address ip-address mask** **Example:** `Router(config-subif)# ip address 192.0.2.1 255.255.255.0`	Sets a primary or secondary IP address for the specified interface. • *mask*—Mask for the associated IP subnet address.
Step 16	**ip policy route-map** *map-tag* **Example:** `Router(config-subif)# ip policy route-map cpe`	Identifies a route map to use for policy routing on an interface. • *map-tag*—Name of the route map to use for policy routing. The name must match a map-tag value specified by a route-map command.
Step 17	**cable helper-address** IP-address **Example:** `Router(config-subif)# cable helper-address 192.0.2.200`	Specifies a destination IP address for User Datagram Protocol (UDP) broadcast Dynamic Host Configuration Protocol (DHCP) packets in cable subinterface configuration mode. • IP-address—The IP address of a DHCP server to which UDP broadcast packets will be sent.

	Command or Action	Purpose
Step 18	**cable source-route** **Example:** `Router(config-subif)# cable source-route`	Configures the VRF source route in the cable modem's sub- bundle interface configuration mode. **Note** This command is applicable to Cisco uBR10012 routers only.
Step 19	**exit** **Example:** `Router(config-subif)# exit`	Exits the subinterface configuration mode.

Troubleshooting Tips

Run the debug cable bundle vrf-steering command to display the interfaces selected during the configuration.

Configuration Examples for VRF Steering

This section provides the following configuration examples:

Example: VRF Steering for CMTS Routers

The following example shows how to configure VRF steering on CMTS routers:

```
Router> enable configure terminal
ip vrf CM-VRF
rd 100:100
route-target export 100:100
route-target import 100:100
! These commands apply to all the devices attached on this cable bundle.
!
interface Bundle1
 no ip address
 no cable arp filter request-send
 no cable arp filter reply-accept
 cable vrf-steering cable-modem CM-VRF
end
!Subinterface for CPEs.
!
interface Bundle1.1
 ip address 112.1.1.1 255.255.0.0 secondary
 ip address 111.1.1.1 255.255.0.0 secondary
 ip address 101.1.1.1 255.255.0.0
 cable dhcp-giaddr policy
 cable helper-address 72.10.10.2
! Subinterface for CMs. These CMs go into CM-VRF
!
interface Bundle1.2
 ip vrf forwarding CM-VRF
 ip address 72.10.10.1 255.255.0.0
 ip policy route-map cpe
 cable helper-address 72.10.10.2
 cable source-route
```

```
end
! Create ACL for CPE
!
ip access-list extended vrfcpe
 permit ip 111.1.0.0 0.0.255.255 any
 permit ip 112.1.0.0 0.0.255.255 any
 permit ip 101.1.0.0 0.0.255.255 any
!
! Create route-map for CPE
!
route-map cpe permit 10
 match ip address vrfcpe
 set global
end.
```

Verifying VRF Steering

To verify or view which VRF contains a specific cable modem in the ARP cache table, use the show ip arp vrf command in privileged EXEC mode.

The following is sample output from the show ip arp vrf command:

```
Router # show ip arp vrf
CM-VRF
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  203.0.113.1                0   0018.742c.6e00  ARPA   FastEthernet0/0/0
Internet  203.0.113.2                -   0014.f1e4.fb58  ARPA   FastEthernet0/0/0
Internet  198.51.100.1               -   0014.f1e4.fc31  ARPA   Bundle1.2
Internet  198.51.100.2               0   001e.6bfb.34e8  ARPA   Bundle1.2
Internet  198.51.100.3               0   0007.0e07.9f1f  ARPA   Bundle1.2
Internet  198.51.100.5               0   0025.2eaf.6bea  ARPA   Bundle1.2
Internet  198.51.100.6               0   001a.c3ff.d1a4  ARPA   Bundle1.2
Internet  198.51.100.7               0   001e.6bfb.1c7e  ARPA   Bundle1.2
```

Additional References

The following sections provide references related to the VRF Steering feature.

Related Documents

Related Topic	Document Title
Cisco uBR10012 Universal Broadband Router Documentation	*IPv6 on Cable* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ cmts_ipv6.html *Virtual Interface Bundling for the Cisco CMTS* http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ cmts_cbl_if_bundlg.html *Cisco uBR10012 Universal Broadband Router Hardware Installation Guide* http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/ installation/guide/hig.html *Cisco uBR10012 Universal Broadband Router Software Configuration Guide* http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/ configuration/guide/scg.html Cisco uBR10012 Universal Broadband Router Release Notes http://www.cisco.com/en/US/products/hw/cable/ps2209/ prod_release_notes_list.html
CMTS Command Reference	*Cisco IOS CMTS Cable Command Reference* http://www.cisco.com/en/US/docs/ios/cable/command/reference/ cbl_book.html

Standards

Standard	Title
None	

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFC	Title
None	

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 VRF Steering

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Note The below 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.

Table 20: Feature Information for VRF Steering

Feature Name	Releases	Feature Information
VRF Steering	12.2(33)SCF	The VRF steering feature allows provisioning of data traffic from cable modems to be contained to a specified VRF instance. In Cisco IOS Release 12.2(33)SCF, this feature was introduced on the Cisco CMTS routers. The following commands were introduced or modified: • cable source-route • cable vrf-steering cable-modem • **ip vrf** • **show ip arp vrf**