



L2VPN Support over Cable

First Published: February 14, 2008, Cisco IOS Release 12.2(33)SCA

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 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) interface.
- Downstream traffic is forwarded on a per-CM basis and upstream traffic is forwarded on a per-SF basis. For L2VPN Support over Cable, upstream traffic for the same L2VPN can use multiple upstream service flows and downstream traffic can use different downstream service flows.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for L2VPN Support over Cable”](#) section on page 753.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

Contents

- [Prerequisites for L2VPN Support over Cable, page 742](#)
- [Restrictions for L2VPN Support over Cable, page 742](#)
- [Information About L2VPN Support over Cable, page 743](#)
- [How to Configure L2VPN Support over Cable, page 747](#)
- [Configuration Examples for L2VPN over Cable, page 750](#)
- [Additional References, page 751](#)
- [Feature Information for L2VPN Support over Cable, page 753](#)

Prerequisites for L2VPN Support over Cable

- You have the following hardware running Cisco IOS Release 12.2(33)SCA or later:
 - Cisco uBR10012 (with PRE-2) or
 - Cisco uBR7246VXR (with NPE-G1 or NPE-G2)
- You are using crypto-supported images. Refer to the [Cross-Platform 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+.

Restrictions for L2VPN Support over Cable

L2VPN Support over Cable has the following general restrictions:

- DOCSIS 1.0 CMs are not supported. For other specific CM requirements, refer to the “Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks” specification that can be found using the [“Additional References” section on page 751](#).
- Load balancing, Dynamic Channel Change (DCC), and DSx are not supported for CMs that are enabled for L2VPN support.
- DSx (Dynamic Service Add [DSA], Dynamic Service Change [DSC], and Dynamic Service Delete [DSD]) is not supported. Therefore, L2VPN TLVs are also not supported in DSx TLVs.
- Multipoint L2VPN is not supported, and any SNMP MIBs for multipoint L2VPN are not supported.
- eSAFE DHCP snooping is not supported (L2VPN subtype 43.5.3)
- A maximum of 1024 L2VPNs are supported on a single cable line card.
- A maximum of 8 upstream SFs per L2VPN are supported.
- A maximum of 8 downstream classifiers per L2VPN are supported.
- eSAFE exclusion is supported for only one eSAFE host. If the REG-REQ for a compliant CM specifies multiple eSAFE hosts, then eMTA (ifIndex 16) will be selected as the eSAFE host to be excluded by the Cisco CMTS router. If eMTA is not included as part of the capability of the CM, then the first eSAFE host in the capability is selected for exclusion.
- The maximum length of the Cable Modem Interface Mask (CMIM) is 4 bytes.

- The following areas of the Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks specification are not supported:
 - 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.
 - Acceptance of multiple Downstream Classifier L2VPN Encoding with the same VPN ID to classify packets to different service flows is not supported.
 - Assignment of multiple SAIDs to the same L2VPN on the same CM is not supported. The primary SAID is used for encrypting all downstream traffic.
 - Assignment of the same group-level L2VPN SAID to different CMs on the same MAC domain attaching to the same L2VPN identifier is not supported.
 - Implementation of the DOCSIS Spanning Tree Protocol (DSTP) and transmission of DSTP BPDUs on all NSI and RF interfaces configured for L2VPN operation is not supported.
 - Implementation of a DSTP SAID specifically for DSTP forwarding to the 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 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 4 VPN IDs per CM.
- Supports multiple upstream service flows (SFs) per CM, with one or more SFs belonging to the same VPN ID.
- Supports a single Ethernet Network System Interface (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 L2VN 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 Cable Modem Interface Mask (CMIM) and 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.

Point-to-Point L2VPN Forwarding Mode

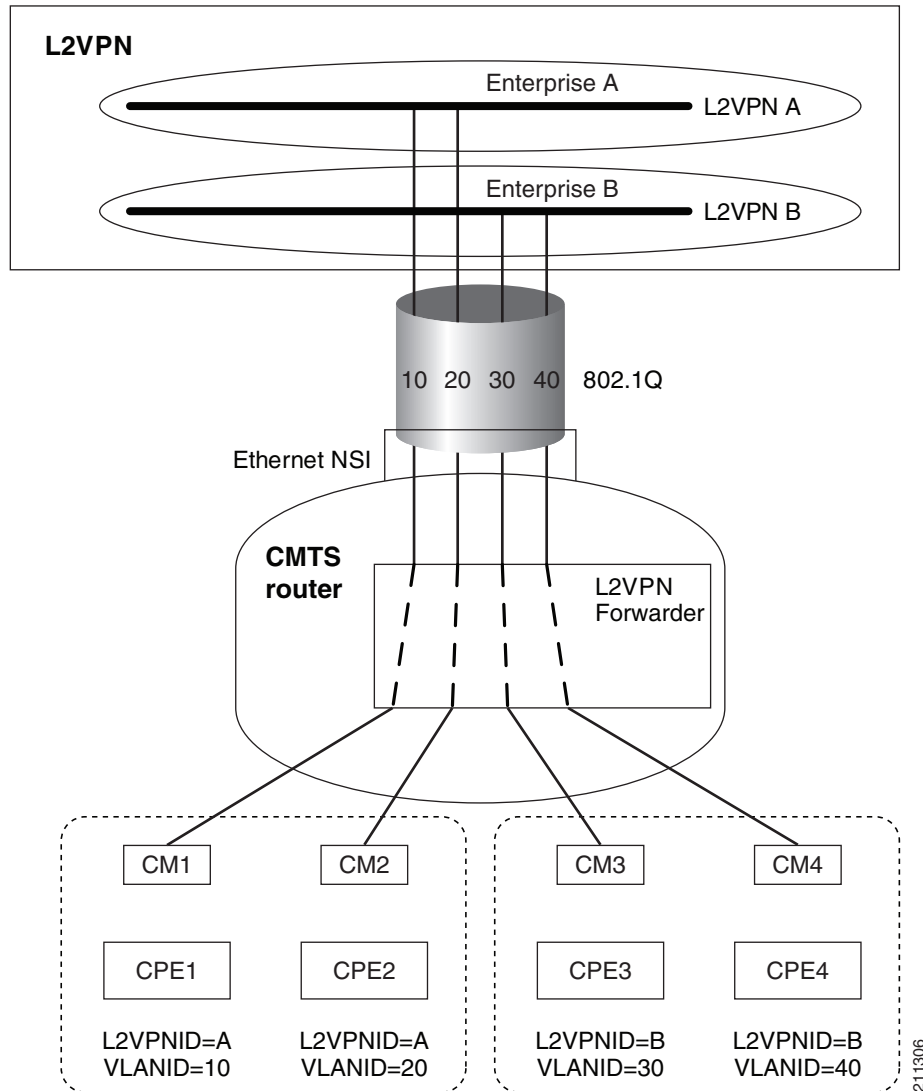
The Cisco CMTS routers in Cisco IOS Release 12.2(33)SCA support the point-to-point L2VPN forwarding mode described in the BSOD specification. Each attachment circuit (either SF or CM) on the Cisco CMTS router has a NSI encapsulation value, and is configured with an IEEE 802.1q VLAN ID.

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 Layer 2 L2VPN bridge on the cable operator's backbone network performs the MAC-address learning to bridge packets between VLAN IDs.

[Figure 1](#) shows an example of a point-to-point L2VPN network using IEEE 802.1q NSI encapsulation. In this example, 4 CMs are associated with 4 different VLAN IDs: 10, 20, 30, and 40. The CM's L2VPN Encoding 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 VLAN's 10 and 20 from CM1 and CM2 can be sent to Enterprise A's network, and traffic for VLAN's 30 and 40 from CM3 and CM4 can be sent to Enterprise B's network.

Figure 1 Point-to-Point L2VPN Network Diagram



L2VPN Encodings in the CM Configuration File

The cable modem (CM) configuration file contains a set of L2VPN encodings which control how the CMTS processes L2VPN forwarding of upstream and downstream CPE packets. 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 0xFFFFF.

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.

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, refer to the “Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks” specification that can be found using the [“Standards” section on page 751](#).

For information about how to use the configuration file generator on the Cisco CMTS, refer to the “DOCSIS Internal Configuration File Generator for the Cisco CMTS” document that can be found using the [“Related Documents” section on page 751](#).

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 [“MIBs” section on page 752](#).

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 1](#) lists the tables in the DOCSIS-L2VPN-MIB supported by the Cisco CMTS routers. For more information, refer to the MIB documentation.

Table 1 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.
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 docsQosPktClassTable.
docsL2vpnCmNsiTable	Describes the NSI configuration for a single CM when operating in point-to-point forwarding mode for an L2VPN.

How to Configure L2VPN Support over Cable

This section contains the following procedures:

- [Configuring the Ethernet Network System Interface, page 747](#) (required)
- [Preparing the DOCSIS Configuration File for L2VPN Support, page 748](#) (required)
- [Verifying L2VPN Support over Cable, page 749](#) (required)

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 configure the NSI using a command on the Cisco CMTS router. It is not configurable through the CM configuration file.

Prerequisites

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

- Cisco uBR100012 Universal Broadband Router—Gigabit Ethernet.
- Cisco uBR7246VXR Universal Broadband Router—Fast Ethernet or Gigabit Ethernet

Restrictions

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable l2-vpn-service default-nsi *type number***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cable l2-vpn-service default-nsi <i>type number</i> Example: cable l2-vpn-service default-nsi GigabitEthernet4/0/0	Configures an Ethernet Network System Interface for Layer 2 VPN support over cable.

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”](#) section on page 745.

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. **show cable l2-vpn dot1q-vc-map**
2. **show cable l2-vpn dot1q-vc-map vpn vpnid**
3. **show cable l2-vpn dot1q-vc-map mac-address vpn vpnid**
4. **show cable l2-vpn dot1q-vc-map mac-address vpn vpnid verbose**
5. **show cable l2-vpn dot1q-vc-map mac-address verbose**

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:

```
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:

```
Router# show cable l2 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 dot1q-vc-map vpn** form of the command along with specification of the cable modem MAC address, as shown in the following 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 dot1q-vc-map vpn verbose** form of the command along with specification of the cable modem MAC address, as shown in the following 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 dot1q-vc-map verbose** form of the command along with specification of the cable modem MAC address, as shown in the following 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
```

Configuration Examples for L2VPN over Cable

Specifying the Ethernet NSI Interface: Example

You can specify the Ethernet Network System Interface (NSI) within the cable modem (CM) configuration file, or using the **cable l2-vpn-service default-nsi** global configuration command as shown in the following example:

```
cable l2-vpn-service default-nsi GigabitEthernet4/0/0
```

Additional References

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

Related Documents

Related Topic	Document Title
Cable modem configuration file creation	“DOCSIS Internal Configuration File Generator for the Cisco CMTS” http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_dsis_cfg_gen_ps2209_TSD_Products_Configuration_Guide_Chapter.html
SNMP configuration information	<i>Cisco IOS Configuration Fundamentals Configuration Guide, Part 3: Cisco IOS System Management</i> , “Configuring SNMP Support” section http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html
SNMP command information	<i>Cisco IOS Network Management Command Reference, Release 12.2SB</i> http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html

Standards

Standard	Title
CM-SP-BPI+-I12-050812	<i>Baseline Privacy Plus Interface Specification</i> http://www.cablemodem.com/downloads/specs/CM-SP-BPI+_I12-050812.pdf
CM-SP-L2VPN-I03-061222	<i>Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks</i> http://www.cablemodem.com/downloads/specs/CM-SP-L2VPN-I03-061222.pdf
CM-SP-RFIv2.0-I11-060602	<i>Radio Frequency Interface Specification</i> http://www.cablemodem.com/downloads/specs/CM-SP-RFI2.0-I11-060602.pdf
IEEE 802.1ad	<i>IEEE 802.1ad-2005 IEEE Standards for Local and metropolitan area networks—Virtual Bridged Local Area Networks</i> http://www.ieee.org
IEEE 802.1q	<i>IEEE Std 802.1Q Virtual Bridged Local Area Networks</i> 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://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/cisco/web/support/index.html

Feature Information for L2VPN Support over Cable

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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



Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release. Unless noted otherwise, subsequent releases of that Cisco IOS software release also support that feature.

Table 2 Feature Information for Multicast VPN and DOCSIS 3.0 Multicast QoS Support

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CDDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0910R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.

