L2VPN Support over Cable

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) Cable Labs specification.

The L2VPN Support over Cable feature supports the following:

• The feature uses 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 L2VPNSupport 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, on page 1
Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 2
Prerequisites for L2VPN Support over Cable, on page 3
Restrictions for L2VPN Support over Cable, on page 3
Information About L2VPN Support over Cable, on page 4
Voice-Call Support on L2VPN CM, on page 8
How to Configure L2VPN Support over Cable, on page 8
Configuration Examples for L2VPN over Cable, on page 13
Additional References, on page 15
Feature Information for L2VPN Support over Cable, on page 16

Finding Feature Information

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.
Use Cisco Feature Navigator to find information about the platform support and Cisco software image support. To access Cisco Feature Navigator, go to the link [http://tools.cisco.com/ITDIT/CFN/](http://tools.cisco.com/ITDIT/CFN/). You do not require a cisco.com login account.

**Hardware Compatibility Matrix for the Cisco cBR Series Routers**

**Note**

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

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

<table>
<thead>
<tr>
<th>Cisco CMTS Platform</th>
<th>Processor Engine</th>
<th>Interface Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco cBR-8 Converged Broadband Router</td>
<td><strong>Cisco IOS-XE Release 3.15.0S and Later Releases</strong></td>
<td><strong>Cisco IOS-XE Release 3.15.0S and Later Releases</strong></td>
</tr>
<tr>
<td></td>
<td>Cisco cBR-8 Supervisor:</td>
<td>Cisco cBR-8 CCAP Line Cards:</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-CCAP-SUP-160G</td>
<td>• PID—CBR-LC-8D30-16U30</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-CCAP-SUP-60G</td>
<td>• PID—CBR-LC-8D31-16U30</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-SUP-8X10G-PIC</td>
<td>• PID—CBR-RF-PIC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PID—CBR-RF-PROT-PIC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco cBR-8 Downstream PHY Modules:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PID—CBR-D30-DS-MOD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PID—CBR-D31-DS-MOD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco cBR-8 Upstream PHY Modules:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PID—CBR-D30-US-MOD</td>
</tr>
</tbody>
</table>

1 Effective with Cisco IOS-XE Release 3.17.0S, CBR-CCAP-SUP-60G supports 8 cable line cards. The total traffic rate is limited to 60 Gbps. The total number of downstream service flows is limited to 72268, and downstream unicast low-latency flow does not count against the limits.
Table 2: Hardware Compatibility Matrix for the Cisco cBR Series Routers

<table>
<thead>
<tr>
<th>Cisco CMTS Platform</th>
<th>Processor Engine</th>
<th>Interface Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco cBR-8 Converged Broadband Router</td>
<td>Cisco IOS-XE Release 16.5.1 and Later Releases</td>
<td>Cisco IOS-XE Release 16.5.1 and Later Releases</td>
</tr>
<tr>
<td></td>
<td>Cisco cBR-8 Supervisor:</td>
<td>Cisco cBR-8 CCAP Line Cards:</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-SUP-250G</td>
<td>• PID—CBR-LC-8D30-16U30</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-CCAP-SUP-160G</td>
<td>• PID—CBR-LC-8D31-16U30</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-CCAP-SUP-60G</td>
<td>• PID—CBR-RF-PIC</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-SUP-8X10G-PIC</td>
<td>• PID—CBR-RF-PROT-PIC</td>
</tr>
</tbody>
</table>

Cisco cBR-8 Downstream PHY Modules:
• PID—CBR-D30-DS-MOD
• PID—CBR-D31-DS-MOD

Cisco cBR-8 Upstream PHY Modules:
• PID—CBR-D30-US-MOD
• PID—CBR-D31-US-MOD

Prerequisites for L2VPN Support over Cable

- You should use crypto-supported images.
- Cable modems must be configured to support BPI+.

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. 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 classify 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.
  • dot1q L2VPN is not supported over a port-channel with load-balancing vlan configured.

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 SUP 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.
• Supports 2000 bytes layer 2 MTU.

Point-to-Point L2VPN Forwarding Mode

The Cisco CMTS routers supports 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.

The image below 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.

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**

Cisco 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.

## Voice-Call Support on L2VPN CM

Voice calls are supported on L2VPN CMs. 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 cBR Series Converged Broadband Router—GigabitEthernet and TenGigabitEthernet

---

**Note**

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> cable l2-vpn-service xconnect nsi dot1q interface ethernet-intf[backup-interface ethernet-intf]</td>
<td>Configures WAN interface for DOT1Q L2VPN. (Optional) Backup-interface - If backup-interface is configured it means that BSoD VLAN redundancy feature is enabled.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# cable l2-vpn-service xconnect nsi dot1q interface Te4/1/0 backup-interface Te4/1/4</td>
<td></td>
</tr>
</tbody>
</table>

### 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 CM configuration file, see the [L2VPN Encodings in the CM Configuration File](#), on page 6.

### Manual Switchover Command Line Interface

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:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> cable l2-vpn dot1q-nsi-redundancy force-switchover from active-nsi-interface</td>
<td>Switches the active uplink port from the current active port to the specified port.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# cable l2-vpn dot1q-nsi-redundancy force-switchover from Te4/0/1</td>
<td></td>
</tr>
</tbody>
</table>
To display the dot1q L2VPN uplink redundancy information, use the `show cable l2-vpn dot1q-nsi-redundancy` as shown in the following 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

**Verifying L2VPN Support over Cable**

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

**Procedure**

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

**Example:**

```
Router# show cable l2-vpn xconnect 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 or customer, use the `show cable l2-vpn xconnect dot1q-vc-map customer` form of the command as shown in the following example:

**Example:**

```
Router# show cable l2-vpn xconnect dot1q-vc-map customer 0234560001
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 3**
To display information for a particular L2VPN ID on a specific cable modem, use the `show cable l2-vpn xconnect 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 xconnect dot1q-vc-map vpn 0014.f8c1.fd66
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 xconnect 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 xconnect 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 Support over Cable

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.

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.

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.

```
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 32 30 02 07 04 05 01 0a 4c 02 01 2b 06 26 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
24 (Upstream Service Flow Encodings)
  S01 (Service Flow Reference) = 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.

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.
### Additional References

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

#### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-SP-BPI+-I12-050812</td>
<td>Baseline Privacy Plus Interface Specification</td>
</tr>
<tr>
<td>CM-SP-L2VPN-I03-061222</td>
<td>Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks</td>
</tr>
</tbody>
</table>
Feature Information for L2VPN Support over Cable

Use Cisco Feature Navigator to find information about the 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 the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2VPN support over cable</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Router.</td>
</tr>
</tbody>
</table>