Data-Over-Cable Service Interface Specifications
Business Services over DOCSIS

Layer 2 Virtual Private Networks

CM-SP-L2VPN-I01-060328

ISSUED

Notice

This DOCSIS® specification is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party. This document is furnished on an AS-IS basis and neither CableLabs, nor other participating entity, provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

Document Status Sheet

Document Control Number:	CM-SP-L2VPN-I01-060328			
Document Title:	Layer 2 Virtual Private Networks			
Revision History:	D01 - Released August 12, 2005 D02 - Released September 30, 2005 D03 – Released December 5, 2005 D04 – Released February 09, 2006 D05 – Released March 17, 2006 I01 – Released March 28, 2006			
Date:	March 28, 2006			
Status:	~~Work in Progress~~	~~Draft~~	Issued	~~Closed~~
Distribution Restrictions:	~~Focus Team Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	Public

Key to Document Status Codes:

Work in Progress An incomplete document, designed to guide discussion and generate feedback, that may include several alternative requirements for consideration.

Draft A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.

Issued A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.

Closed A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks:

Contents

Figures

Tables

This page intentionally left blank.

1 INTRODUCTION

This specification describes requirements on both CMTSs and CMs in order to implement a DOCSIS Layer-2 Virtual Private Network (DOCSIS L2VPN) feature.

The L2VPN feature allows cable operators to offer a Layer 2 Transparent LAN Service (TLS) to commercial enterprises, which is one of the principal goals of the CableLabs Business Services over DOCSIS (BSoD) initiative.

1.1 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

MUST This word means that the item is an absolute requirement of this specification.

MUST NOT This phrase means that the item is an absolute prohibition of this specification.

SHOULD This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

SHOULD NOT This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

Some normative statements require a CM or CMTS to silently ignore a condition which may be defined in future specifications. A requirement to silently ignore a condition means that the CM or CMTS:

- MAY increment a vendor-specific statistic;
- MUST NOT generate a log message; and
- MUST otherwise ignore the condition and continue operation as if the condition did not occur.

1.2 Conformance

A DOCSIS CMTS that claims to implement the DOCSIS L2VPN feature MUST implement the normative provisions of this document. A DOCSIS CM that claims conformance for DOCSIS L2VPN feature MUST implement the normative requirements of this document.

A CMTS or CM implementing this specification is said to be L2VPN compliant. For the remainder of this document, all references to a CMTS refer to an L2VPN compliant CMTS. A CM that has not implemented this specification is termed an L2VPN non-compliant CM.

An L2VPN-compliant CMTS MUST support an L2VPN non-compliant CM. This permits a cable operator to offer L2VPN subscriber service with currently deployed non-compliant CMs. Use of non-compliant CMs involves certain limitations that are detailed in Appendix IV. Using compliant CMs for L2VPN subscriber service avoids those limitations. The requirements for CMs to comply with this L2VPN specification are summarized in Section 7.

2 REFERENCES

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement normative references.

[IEEE 802.1Q] IEEE Std 802.1Q Virtual Bridged Local Area Networks, May 7, 2003.

[RFI 2.0] DOCSIS Radio Frequency Interface Specification, CM-SP-RFIv2.0-I10-051209, December 9, 2005, Cable Television Laboratories, Inc.

[BPI-PLUS] BPI+ Specification, CM-SP-BPI+-I12-050812, August 12, 2005, Cable Television Laboratories, Inc.

2.2 Informative References

[CH1.1] CableHome 1.1 Specification, CH-SP-CH1.1-I10-051214, December 14, 2005, Cable Television Laboratories, Inc.

[eDOCSIS] eDOCSIS Specification, CM-SP-eDOCSIS-I07-051209, December 9, 2005, Cable Television Laboratories, Inc.

[RFC 2547] E. Rosen Y. Rekhter BGP/MPLS VPNs, IETF RFC 2547, March 1999.

[RFC 2674] E. Bell et al Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions, IETF RFC 2674, August 1999.

[RFC 2685] B. Fox, B. Gleeson Virtual Private Network Identifier, IETF RFC 2685, Sept. 1999.

[RFC 3985] S. Bryant et al, Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture, IETF RFC 3985, March 2005.

[PKT-PROV] PacketCable Provisioning, PKT-SP-PROV-I11-050812, August 12, 2005, Cable Television Laboratories, Inc.

[ID-BRIDGE] V. Ngai, et al, Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions, Internet draft <draft-ietf-bridge-ext-v2-07.txt> (or later), 2005-8-22; available from www.ietf.org.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone 303-661-9100; Fax 303-661-9199; Internet: http://www.cablelabs.com /
- Internet Engineering Task Force (IETF); Internet: http://www.ietf.org
- IEEE Standard Specifications; Internet http://www.ieee.org

3 TERMS AND DEFINITIONS

This specification uses the following terms in addition to those defined in [RFI 2.0].

Bridged Network
A set of IEEE 802 LANs interconnected by IEEE 802.1D MAC bridges.

Compliant CM
A CM that implements this DOCSIS L2VPN specification.

DOCSIS L2PDU
A Packet PDU of a DOCSIS MAC Frame, i.e., the L2PDU following a MAC Header with FC_TYPE=00. This definition means that a MAC Management message with FC_TYPE=11 is *not* considered to be a DOCSIS L2PDU, even though the form of a MAC Management Message Header is the same form as an L2PDU.

DOCSIS MAC Frame
The unit of transmission on the DOCSIS cable RF interface, consisting of a MAC Header and a (possibly null) Data PDU. The FC_TYPE field of MAC Header identifies the Data PDU as either a Packet PDU (FC_TYPE=00), or a MAC-specific PDU (FC_TYPE=11).

Flooding
An operation of an L2 Bridge in which it replicates an L2PDU addressed to a group MAC or unlearned individual MAC address to all Bridge Ports other than the L2PDU's ingress port.

Group MAC (GMAC) Address
An IEEE 6-byte MAC address with the first transmitted bit (the group bit) set to 1, indicating that the address refers to a group of MAC hosts. In the canonical representation of MAC addresses used for Ethernet transmission, the Group bit is the least significant bit of the first byte. The all-1s broadcast MAC address is considered to be a GMAC address.

Individual MAC Address
An IEEE 6-byte MAC address with the first transmitted bit (the group bit) set to 0, indicating that the address refers to a single MAC host. For the Ethernet MAC addresses of DOCSIS, the group bit is the least significant bit of the first byte of the MAC address.

L2 Forwarder
A network element that forwards layer 2 packets from one L2 interface to another L2 interface. A Layer 2 Forwarder may operate in Point-to-Point or Multipoint forwarding mode, i.e., forwarding between only two interfaces without learning; or Multipoint, forwarding unicast-destined packets only to the interface from which a MAC address was learned.

L2 Interface
A physical interface port or virtual circuit on which an L2PDU is transmitted. Physical L2 interface ports include an Ethernet NSI at a CMTS or the CMCI port at a CM. Virtual circuit L2 Interfaces include a CMTS Network System Interface (NSI) PseudoWire (PW) and a CMTS single-CM BPI Security Association. An L2 Interface may or may not have an ifIndex assigned to it.

L2 Virtual Private Network (L2VPN)
A set of LANs and the L2 Forwarders between them that enable hosts attached to the LANs to communicate with Layer 2 Protocol Data Units (L2PDUs). A single L2VPN forwards L2PDUs based only on the Destination MAC (DMAC) address of the L2PDU, transparent to any IP or other Layer 3 address. A cable operator administrative domain supports multiple L2VPNs, one for each subscriber enterprise to which Transparent LAN Service is offered.

L2VPN Identifier
An octet string that uniquely identifies an L2VPN within a cable operator administrative domain, corresponding to a single subscriber enterprise.

L3 Forwarder
A network element that forwards a Layer 3 PDU from an ingress interface to one or more egress interfaces. Also called a Router.

L2 Protocol Data Unit (L2PDU)	A sequence of bytes consisting of a Destination MAC Address (DMAC), Source MAC Address (SMAC), (optional) Tag Header(s), EtherType/Length, L2 Payload, and CRC.
Learning	An operation of a layer 2 Bridge by which it associates the Source MAC (SMAC) address of an incoming L2PDU with the Bridge Port from which it arrived.
Multipoint L2 Forwarding	Operation of an L2 Forwarder among multiple L2 networks that forwards individual MAC destined packets only to the interface from which a source MAC address was learned and that floods group MAC destined packets to all interfaces.
Non-compliant CM	A CM that does not implement this DOCSIS L2VPN specification.
Point-to-Point L2 Forwarding	Operation of an L2 Forwarder between only two L2 networks with no source MAC address learning.
Security Association (SA)	An association between the CMTS and a set of CMs in a MAC Domain that enables encrypted communication between the CMTS and the CM set. A Single CM SA is one with a single CM, and enables a private point-to-point L2 Network connection between the CMTS and the CPE LAN of that CM. A Security Association Descriptor (SA-Descriptor) is a multiple-part message element defined in the DOCSIS Baseline Privacy specification [BPI-PLUS] that includes a Security Association ID (SAID).
Security Association ID (SAID)	A 14-bit identifier that appears in a BPI Extended Header (BPI-EH) of a DOCSIS PDU packet to identify the key used to encrypt the packet.
Tag Header	A 16-bit Tag Protocol ID (0x8100) followed by a 16-bit Tag Control field. The Tag Control field consists of a 3-bit User Priority field, a 1-bit Canonical Format Indicator, and a 12-bit VLAN ID [IEEE 802.1Q].
Transparent LAN Service (TLS)	A service offering of a cable operator that implements a private L2VPN among the CPE networks of the CMs of single subscriber enterprise.
Virtual LAN (VLAN)	A *subset* of the LANs of an IEEE 802.1 Bridged Network to which a VLAN Identifier (VLAN ID) is assigned. An L2VPN may consist of several VLANs, each with different VLAN IDs, and even of VLANs on different IEEE 802.1 Bridged Networks with the same VLAN ID.
Virtual LAN Identifier (VLAN ID)	An IEEE 802.1Q VLAN ID is a 12-bit number that identifies a VLAN within an IEEE 802.1 Bridged Network. An IEEE 802.1ah stacked VLAN ID consists of an outer Service 12-bit VLAN ID and an inner Customer 12-bit VLAN ID.
Provisioning L2VPN	An L2VPN for the pre-registration traffic of DHCP, TOD, and TFTP that provisions eCMs and eSAFE hosts. May be combined with a Management L2VPN.
Management L2VPN	An L2VPN for the post-registration SNMP traffic to eCM or eSAFE devices. May be combined with a Provisioning L2VPN.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

BPI	Baseline Privacy Interface
BSoD	Business Services over DOCSIS
CMIM	CM Interface Mask
CRC	Cyclic Redundancy Check
DIME	Downstream IP Multicast Encryption
DMAC	Destination MAC
DUT	Downstream Unencrypted Traffic
eCM	Embedded Cable modem [eDOCSIS]
eMTA	Embedded Media Transport Agent [PKT-PROV]
ePS	Embedded Portal Services [CH1.1]
eSAFE	Embedded Service/Application Functional Entity [eDOCSIS]
GMAC	Group MAC address
L2	Layer 2
L2VPN	Layer 2 Virtual Private Network
MAC	Media Access Control
SAID	Security Association Identifier
SID	(Upstream) Service Identifier
SMAC	Source MAC
TLS	Transparent LAN Service
TOD	Time of Day
VPN	Virtual Private Network

5 THEORY OF OPERATION (INFORMATIVE)

5.1 L2VPN Features

The ability to implement Layer 2 Virtual Private Networking to arbitrary sets of CMs enables a number of significant DOCSIS features:

- Transparent LAN Service
- Multiple ISP L2VPNs
- Management L2VPNs

5.1.1 Transparent LAN Service

Data networking between the multiple sites of commercial businesses represents a significant business opportunity for cable operators. Commercial data networks are usually implemented with private point-to-point data connections such as Frame Relay, ISDN, or ATM virtual circuits, often with equipment that provides transparent delivery of layer 2 Ethernet LAN packets. A service that interconnects subscriber enterprise LANs with Layer 2 forwarding is called Transparent LAN Service (TLS).

The DOCSIS RFI standard [RFI 2.0] was originally intended for residential subscriber connection to the public Internet. This specification standardizes, within DOCSIS, the control and data plane operation of CMTSs and CMs in order to offer Transparent LAN Service to commercial subscriber enterprises.

The term TLS refers to a particular service offering to commercial enterprise customers. The particular technology that provides this service is called a Layer 2 Virtual Private Network (L2VPN). A cable operator offers TLS by implementing one L2VPN for each commercial enterprise.

An example DOCSIS-based commercial TLS service is depicted in Figure 5–1:

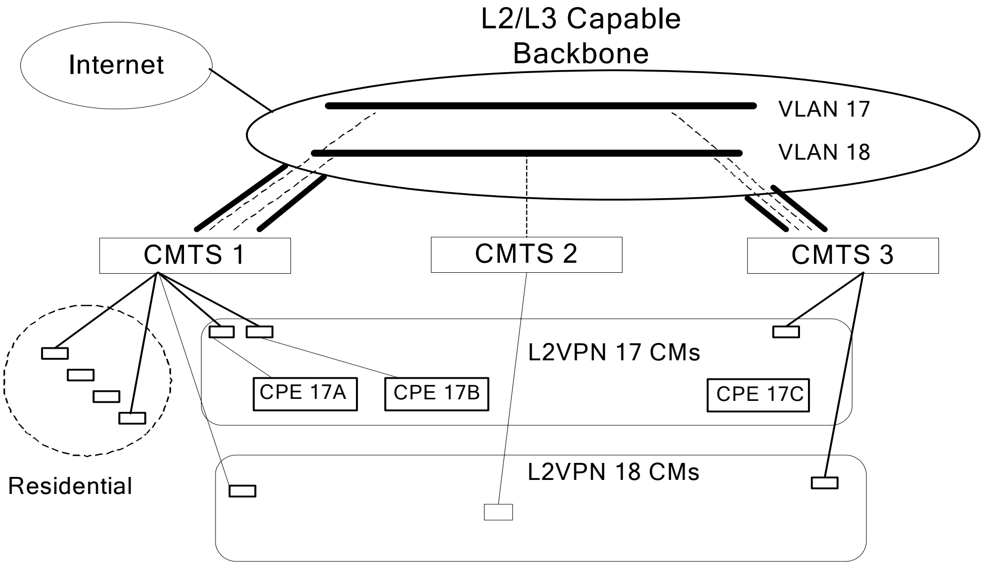

Figure 5–1 - Transparent LAN Service

Figure 5–1 depicts a Transparent LAN Service offered to two commercial enterprises; one denoted as L2VPN 17, and one as L2VPN 18. All of the CMTSs have the usual set of residential subscribers, which are depicted on CMTS 1 only. CMTS 1 provides L2VPN service to two CMs on L2VPN 17, and one on L2VPN 18. CMTS 2 provides L2VPN service to one L2VPN 18 CM. CMTS 3 provides service to one CM on L2VPN 17, and one on L2VPN 18.

The example shows that the cable operator's L2 backbone implements a single Virtual LAN (VLAN) for each customer. In this document, the term VLAN has a specific meaning as referring to the IEEE 802.1Q definition, as a subset of LANs, within a Bridged Network, to which is assigned a 12-bit VLAN ID. In this example, CMTS1 directly encapsulates upstream L2 packets from L2VPN 17 onto a IEEE 802.1Q tagged Ethernet packet with a VLAN ID tag 17, and forwards them onto a trunk Ethernet Network System Interface (NSI) port, to the cable operator's backbone.

In the example, CMTS 1 implements multipoint L2 Forwarding, so it is responsible for bridging packets between its two CMs attached to L2VPN 17. This includes learning the Source MAC (SMAC) addresses of CPE17A and CPE17B, and associating them with the CM, from which those CPE attach.

CMTS1 implements only a single attachment circuit to VLAN 17 on the backbone. When a downstream unicast packet from VLAN 17 arrives at CMTS1, it looks up the Destination MAC (DMAC) in its learning database and forwards the packet to the correct CM.

CMTS 3, however, may implement only point-to-point L2 forwarding, where it transparently forwards all individual and group MAC destined packets, in a point-to-point manner, between the CM attached to CPE 17C and IEEE 802.1Q VLAN ID 17 on its NSI Ethernet port, to the backbone.

In the backbone, a cable operator Layer 2 Bridge, connects the various Ethernet trunk interfaces from the CMTSs, and bridges together each VLAN. The TLS service offered by the operator to L2VPN17 provides for a transparent layer 2 bridged connection between CPEs 17A, 17B, and 17C. From the enterprise customer's point of view, such CPE are managed and operated as if they were on a customer-private Ethernet LAN. Usually, they will have an IP address on the same IP subnet owned by the enterprise. The enterprise usually assigns the IP address to each CPE, and typically has its own DHCP server to do so. Indeed, each enterprise can use the same overlapping private IP subnet space. Unlike Layer 3 VPN technologies, the cable operator does not need to co-ordinate IP address subnet assignment with the enterprise customers. From the operator's point of view, the enterprise LAN subscribers are completely isolated at layer 2 from all other residential subscribers, and from every other L2VPN.

An enterprise TLS may include not only the LANs attached to CMs, but also any other LANs bridged to the customer's VLAN in the IEEE 802.1Q-compliant Bridge in the cable operator's backbone.

5.1.2 Multiple ISP L2VPNs

The L2VPN feature permits a cable operator to support multiple Internet Service Providers (ISPs) by providing a separate L2VPN for each ISP. The cable operator provides all CM provisioning, and the CM configuration file determines a L2VPN for forwarding all CPE traffic. Each ISP is assigned a separate L2VPN. The ISP is responsible for providing the DHCP servers and IP addressing for all CPEs on the CMs attached to their L2VPN.

The advantage of L2VPNs for multiple ISP operation is that it completely separates the IP address space management and IP routing of the ISP, from that of the cable operator. In contrast, multiple ISP features, based on layer 3 VPNs, usually require co-ordination of IP address assignment and router security configuration between the MSO Provider Edge and ISP Customer Edge routers.

5.1.3 Management L2VPNs

The DOCSIS L2VPN feature allows a CMTS to implement an L2VPN solely for the provisioning and management of embedded Cable Modems (eCMs) and embedded Service/Application Functional Entities (eSAFEs) [eDOCSIS], such as an embedded Media Transport Agent (eMTA) [PKT-PROV], or embedded CableHome® Portal Services functionality (ePS) [CH1.1]. Implementing a separate L2VPN for provisioning and management of eCM and eSAFE traffic, isolates those devices from the Internet and from the subscriber, enhancing security.

Prior to registration, the CM transmits on a temporary SID, and all such traffic is considered to be forwarded by the Non-L2VPN Forwarder. A CMTS could be implemented to forward pre-registration traffic onto a single Provisioning L2VPN. The Provisioning VPN would be configured in a vendor-specific manner.

When a CM registers, it reads L2VPN Encodings from its configuration file that can configure its eCM and eSAFE devices to forward-on an L2VPN. This post-registration L2VPN is called a Management L2VPN, because post-registration traffic is primarily SNMP for managing the device.

5.1.4 Other L2VPN-enabled Features

Some features required by the specification are enhancements to overall DOCSIS operation otherwise unrelated to Layer 2 VPNs:

- Interface-based Classification
- DUT Filtering
- Enabling eSAFE DHCP Snooping Control

Interface-based classification allows packets to be classified according to the CM internal or external bridge port interface, and is described in Section 6.6.5. This feature may be used, for example, to classify packets to, or from the embedded MTA interface, without relying on the particular IP subnet of that interface.

Downstream Unencrypted Traffic (DUT) filtering is applicable to CMTS vendor-specific Layer 3 VPN operation to prevent the Group MAC traffic, that is broadcast to residential CMs, from leaking into the supposedly private CPE networks of Layer 3 VPN subscribers. DUT Filtering is described in Section 6.5.2.1.

DHCP Snooping Control is an explicit TLV that authorizes the CMTS to automatically learn the MAC address of embedded eSAFE hosts, such as eMTAs, by intruding on their DHCP traffic. This may be used in conjunction with CMTS vendor-specific features that forward DHCP or other packets from eSAFE hosts in a special manner. The Enable eSAFE DHCP Snooping Control feature is described in Section 6.6.4.1.

5.2 CMTS Layer 2 Forwarding Architecture

5.2.1 L2VPN and Non-L2VPN Forwarding

A CMTS is considered to have an entirely separate packet forwarder for L2VPN forwarding that differs from Non-L2VPN forwarder for residential traffic, as depicted in Figure 5–2 below:

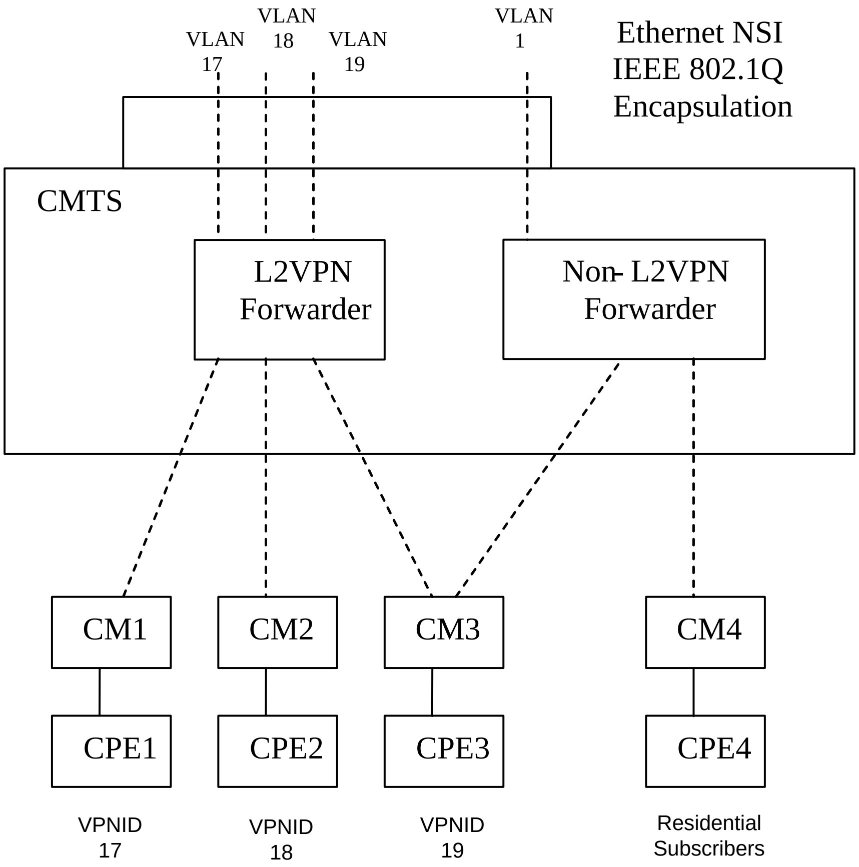

Figure 5–2 - CMTS L2VPN and Non-L2VPN Forwarding

To support L2VPN operation, a CMTS's Network System Interface (NSI) must be capable of distinguishing L2VPN from non-L2VPN downstream traffic, and determining the L2VPN of the downstream traffic. The encapsulation format of L2VPN traffic on a CMTS' NSI ports and the particular field values, within that encapsulation that distinguish a particular L2VPN, are called the NSI L2VPN Encapsulation information. In the example above, IEEE 802.1Q VLAN ID tags are used as the L2VPN Encapsulation format on an Ethernet NSI port.

In general, L2VPN and non-L2VPN traffic is mixed on the same NSI port. In the example above, the CMTS implements a non-L2VPN IP router interface on VLAN ID 1, which may even be the native VLAN, with an untagged encapsulation. Residential traffic, such as CPE4 connected to CM4, continues to be routed through the CMTS's IP routing forwarder onto the router's sub-interface on VLAN ID 1. The other CPE, however, are bridged at layer 2 from the Ethernet interface of the CM to a configured 802.1Q VLAN ID on the NSI port. In Figure 5–2 above, the CMTS implements a Point-to-Point forwarding model where it forwards CPE traffic from CM1 to 802.1Q VLAN ID 17, CPE traffic from CM2 to 802.1Q VLAN ID 18, and CPE traffic from one of the upstream service flows of CM3 to 802.1Q VLAN ID 19. The other upstream service flow of CM3 is forwarded to the non-L2VPN forwarder.

In the upstream direction, the CMTS distinguishes L2VPN from non-L2VPN traffic based on the Upstream Service Flow from which the traffic arrives, and the source MAC address of the traffic. Certain Upstream SFs are configured with Forwarding L2VPN Encodings that identify a particular L2VPN. The L2VPN encoding includes a CM Interface Mask (CMIM) that identifies which CM-side hosts forward upstream to the L2VPN. By default, only CPE hosts attached to the CMCI interface of a CM forward to an L2VPN; the CM and its internal eSAFE hosts do not forward to an L2VPN.

An SF configured to forward CPE traffic to an L2VPN is considered to be an attachment circuit in the context of IETF Virtual Private LAN Service (VPLS). A CMTS VPLS L2VPN Forwarder is responsible for forwarding packets between attachment circuits and pseudowires on NSI ports (e.g., MPLS or L2TPv3 tunnels).

5.2.2 Point-to-Point and Multipoint L2VPN Forwarding Modes

This specification uses the term layer 2 forwarding rather than bridging because commercial L2VPN service can be offered without necessarily implementing a learning MAC Layer Bridge on the CMTS as defined by IEEE 802.1Q. The CMTS MAY implement a Point-to-Point layer 2 forwarding mode that forwards packets between a single NSI port and a single CM (or SF). If the CMTS does implement a learning MAC layer bridge between NSI and RF interfaces, this specification terms it the Multipoint layer 2 forwarding mode.

In Point-to-Point L2VPN Forwarding Mode, each attachment circuit has a different NSI Encapsulation value. For example, with IEEE 802.1Q encapsulation, each attachment circuit (i.e., CM or SF) is configured with a different 802.1Q VLAN ID. In Point-to-Point mode, the L2VPN forwarder simply forwards upstream and downstream data between one NSI port and one attachment circuit, without learning the MAC addresses of CPE packets. The logical VPNID to which a CM or SF attaches should be configured with the attachment circuit, but its value is otherwise ignored by the CMTS in Point-to-Point forwarding mode. An external L2VPN Bridge on the cable operator's backbone actually performs the layer 2 MAC address learning for each L2VPN, and bridges packets between the VLAN IDs or pseudo-wires of the packets within their NSI Encapsulation.

An example of Point-to-Point Forwarding Mode is depicted in Figure 5–3 below:

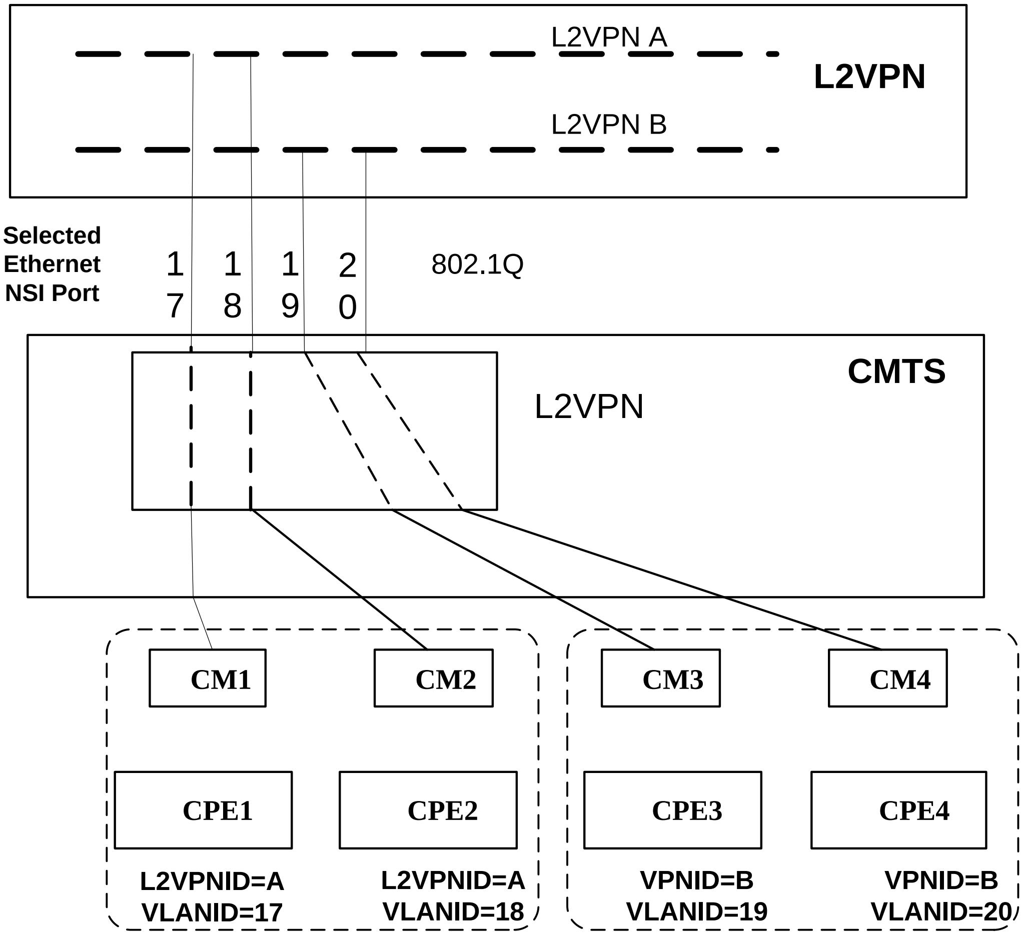

Figure 5–3 - Point-to-Point Forwarding Mode

Four CMs are configured for L2VPN operation. Each CM's L2VPN Encoding includes a logical VPNID A or B, along with a statically configured NSI Encapsulation subtype that configures the use of IEEE 802.1Q with a different VLAN ID for each CM (VLAN IDs 17 through 20). The CMTS's L2VPN Forwarder forwards traffic from the NSI port on those VLAN IDs in a point-to-point manner, to and from the configured CM. Although the L2VPN Forwarder in Point-to-Point mode does not use the VPNID configuration, it must still be configured in each forwarding L2VPN Encoding for at least information purposes. An L2VPN Bridge Layer 2 switch, external to the CMTS, is configured to treat the NSI encapsulations for VLAN ID 17 and 18 as separate logical bridge ports for L2VPN A, and to learn CPE MAC addresses on those bridge ports. Likewise, the external L2VPN Bridge is configured to consider the encapsulations with VLAN IDs 19 and 20, as separate bridge ports of the broadcast domain that is L2VPN B.

With IEEE 802.1Q NSI Encapsulation Point-to-Point Forwarding Mode, limits the number of L2VPN subscriber modems supported on a CMTS to 4093 CMs, due to the 12-bit limit of an IEEE 802.1Q VLAN ID.

Multipoint Forwarding mode means that the CMTS forwards downstream L2VPN packets to potentially multiple cable modems. The CMTS builds a layer 2 Forwarding Database (FDB) of the CPE MAC addresses it learns from the source MAC address of upstream packets. A Multipoint L2VPN Forwarder uses this FDB to select which CM to forward downstream L2VPN traffic. If the destination is a group MAC address, or is an unknown individual MAC address, a Multipoint L2VPN Forwarder floods the traffic to all attachment circuits and NSI ports other than the one from which the packet was received. A Multipoint L2VPN forwarder also directly forwards packets between attachment circuits (CMs or SFs), configured to the same logical L2VPN.

With Multipoint Forwarding, an NSI Encapsulation value is needed only for each logical L2VPN, not for each attachment circuit. This allows support of any number of *modems* for L2VPN service, because the 12-bit IEEE 802.1Q VLAN ID, used as an NSI Encapsulation value, will only limit the number of enterprise L2VPN *networks*.

An example of Multipoint Forwarding Mode is depicted in Figure 5–4 below.

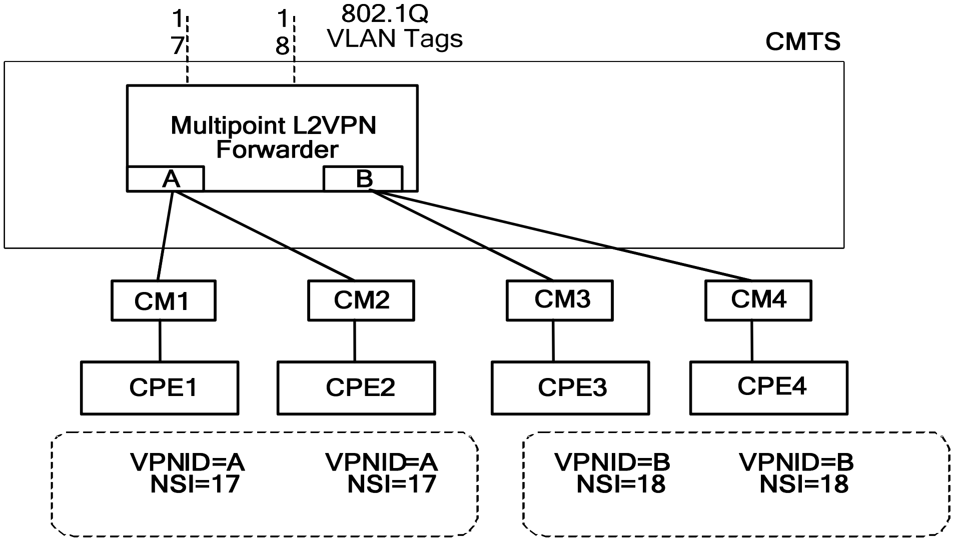

Figure 5–4 - Multipoint L2VPN Forwarding Mode Example

In this example, both CM1 and CM2 are configured for L2VPN forwarding to VPNID A, and configured to use an NSI Encapsulation of IEEE 802.1Q VLAN ID 17. The Multipoint L2VPN forwarder learns the MAC addresses of CPE1 and CPE2 in order to determine to which CM to forward downstream unicast traffic received from the network port on VLAN ID 17. Likewise CM3 and CM4 are configured with VPNID B and both are configured to use IEEE 802.1Q VLAN ID 18 as their NSI Encapsulation. The Multipoint L2VPN forwarder learns the MAC addresses of CPE3 and CPE4 on L2VPN B. The non-L2VPN forwarder is not shown in the Figure 5–4.

This specification permits qualification of CMTSs with either Point-to-Point or Multipoint forwarding modes. DOCSIS qualification testing shall use the forwarding mode indicated by the vendor's PICS submission for all L2VPNs. This specification is written assuming that a CMTS selects one mode or the other for all L2VPNs. There are no requirements, however, that prevent a vendor from implementing different forwarding modes for different sets of L2VPNs.

6 L2VPN OPERATION (NORMATIVE)

6.1 CMTS Bridging Model Requirements

The CMTS MUST transparently forward DOCSIS L2PDUs received from an Upstream Service Flow configured to receive packets for a particular L2VPN to NSI ports configured to encapsulate packets for that L2VPN. The CMTS MUST transparently forward packets received with an NSI encapsulation configured for a particular L2VPN to a downstream DOCSIS L2PDU encrypted in a SAID unique to that L2VPN and CM to which the packet is forwarded.

A CMTS SHOULD implement a VLAN-capable bridging function as specified by IEEE 802.1S. For purposes of 802.1S conformance, each bridge port implemented on an RF interface SHOULD be considered to be a fully-tagged 802.1Q interface for which the incoming VLAN ID is determined by the upstream SID, and the outgoing VLAN ID is tagged with a BPI SAID. A L2VPN compliant CMTS MUST NOT insert an 802.Q tag on downstream RF packets.

The CMTS MAY restrict configuration of an NSI Encapsulation service multiplexing value (e.g., IEEE 802.1Q VLAN ID) to a single SF. In this Point-to-Point forwarding mode, the CMTS MAY omit learning of CPE MAC addresses into a Forwarding Database. A Point-to-Point CMTS MUST support multiple per-SF L2VPN Encodings with the same NSI Encapsulation subtype as long as they are on the same CM.

If the CMTS permits more than one SF to be configured to bridge to the same NSI Encapsulation service multiplexing value, it is said to implement Multipoint forwarding mode. In Multipoint forwarding mode, the CMTS MUST associate learned CPE source MAC addresses with the particular CM from which they were learned.

A CMTS MUST support both L2VPN and non-L2VPN forwarding on the same RF MAC domain. A CMTS MUST transparently bridge CPE traffic from CMs configured with L2VPN Encodings according to this specification. A CMTS MUST forward with its normal, non-L2VPN packet forwarding algorithms CPE traffic from CMs with no L2VPN Encodings, except as specified in this specification.

A CMTS MUST support both L2VPN and non-L2VPN forwarding of upstream traffic from different service flows when only per-SF L2VPN Encodings are signaled.

6.2 Configuring L2VPN Forwarding

A set of one or more L2VPN Encoding configuration settings in a CM configuration file controls whether and how the CMTS performs L2VPN forwarding of upstream and downstream CPE packets.

The L2VPN Encoding parameter is encoded as a General Extension Information (GEI) parameter, meaning it is encoded as a subtype of the Vendor Specific Information type 43 parameter using, vendor ID 0xFFFFFF ([RFI 2.0] C.1.1.17.1). By encoding the L2VPN Encoding as a GEI parameter, it may be included in the configuration file of any DOCSIS CM, including DOCSIS 1.0 CMs.

The L2VPN Encoding parameter may appear in the following locations:

- At the top level of a CM configuration file, in which case it is called a per-CM L2VPN Encoding;
- As a subtype of a GEI nested in an Upstream Service Flow Encoding (type 24), in which case it is called a per-SF or Forwarding L2VPN Encoding;
- As a sub-type of a GEI nested in a Downstream Packet Classification Configuration Setting (type 23), in which case it is called a Downstream Classifier L2VPN Encoding;
- As a sub-type of a GEI nested in an Upstream Packet Classifier Configuration Setting (type 22), in which case it is called an Upstream Classifier L2VPN Encoding.

The L2VPN Encoding parameter itself is defined as a multi-part parameter with several nested subtype parameters. The following Table 6–1 lists each of the subtypes and describes in which location the subtype is defined, as required or optional for that location.

Table 6–1 - L2VPN Encoding Subtype Location Summary

Subtype Number	Subtype Parameter	Top Level (per-CM)	Upstream Service Flow	Downstream Classifier	Upstream Classifier
43.5.1	VPN Identifier	Required	Required	Required	
43.5.2	NSI Encapsulation	Optional(3)			
43.5.3	Enable eSAFE DHCP Snooping	Optional(1)			
43.5.4	CM Interface Mask	Optional		Optional(1)	Optional(1)
43.5.5	Attachment Group ID	Optional(3)			
43.5.6	Source Attachment Individual ID	Optional(3)			
43.5.7	Target Attachment Individual ID	Optional(3)			
43.5.8	Ingress User Priority		Optional		
43.5.9	User Priority Range			Optional	
43.5.10	L2VPN SA-Descriptor	Required(2)			
43.5.43	Vendor-Specific	Optional	Optional	Optional	Optional

Table Notes:

(1) The CMTS MUST accept a parameter identified as optional(1) in Table 6–1 in a non-forwarding L2VPN Encoding.

(2) The CMTS inserts the L2VPN SA-Descriptor Subtype in its first message to a CM in any MAC Management Message that includes a Forwarding L2VPN Encoding; the L2VPN SA-Descriptor Subtype is not configured in a CM configuration file.

(3) This is a Per L2VPN configuration on the NSI port that is defined in a per-CM L2VPN Encoding only for Point-to-Point forwarding mode.

If a subtype is not defined as Required or Optional in a location, the CMTS SHOULD silently ignore it when it appears in that location. If a subtype is not defined as Required or Optional in a location, the cable modem SHOULD silently ignore it when it appears in that location. A CMTS MUST silently ignore unrecognized subtypes in an L2VPN Encoding. A CM MUST silently ignore unrecognized subtypes in an L2VPN Encoding.

The top-level L2VPN Encoding controls the per-L2VPN CM and CMTS behavior specific to a particular L2VPN. The Upstream Service Flow L2VPN Encoding specifies which upstream service flow(s) will carry L2VPN traffic. Proper L2VPN operation requires at least one upstream service flow to be configured for L2VPN forwarding.

Because multiple upstream service flows can be configured to forward to the same L2VPN, all of the per-L2VPN parameters common to the L2VPN itself are encoded in the single top-level L2VPN encoding rather than requiring or permitting them to be duplicated in multiple upstream service flow encodings.

Upstream L2VPN forwarding is configured on a per-SF basis. The cable operator can configure at least one upstream service flow in a CM configuration file with an L2VPN Encoding that defines the VPN Identifier to which the CMTS forwards upstream traffic from that SF. The per-CM or top-level L2VPN encoding is required in a CM configuration file only for point-to-point forwarding mode, in order to define the NSI encapsulation format for that L2VPN so that the CMTS can determine to which CM to forward downstream L2VPN traffic. With Multipoint forwarding mode for an L2VPN, multiple CMs may forward to multiple NSI encapsulations, so any per-CM NSI encapsulation configuration is not defined.

The simplest CM configuration file for L2VPN operation contains:

- For Multipoint mode, a single per-SF L2VPN Encoding within the primary upstream SF definition; or
- For Point-to-Point mode, single per-SF L2VPN Encoding within the primary upstream SF definition and a single per-CM L2VPN Encoding with an NSI Encapsulation subtype for that L2VPN.

In a Registration Response message, the CMTS always includes a per-CM L2VPN encoding (adding a per-CM L2VPN encoding if necessary) that provides at least one L2VPN SA-Descriptor for encrypting and labeling downstream packets as L2VPN traffic for the CM. The CMTS MAY assign more than one SAID to the same L2VPN, in which case multiple L2VPN SA-Descriptor subtypes may appear in a top-level L2VPN Encoding.

Unless configured otherwise, the CMTS delivers downstream L2VPN traffic to a single cable modem on the CM’s primary downstream service flow. The operator can specify enhanced Quality of Service (QOS) for downstream L2VPN traffic with a separate downstream service flow for L2VPN forwarding in the CM’s configuration file. Downstream L2VPN traffic can be classified to that particular downstream service flow by defining a classifier that includes a Downstream Classifier L2VPN Encoding that references the service flow.

The CMTS MUST reject the registration of a CM with an invalid L2VPN Encoding. A valid CM configuration contains any number of per-SF L2VPN Encodings, Downstream Classifier L2VPN Encodings and Upstream Classifier L2VPN Encodings. The CMTS MUST accept a CM registration request that contains multiple per-SF L2VPN Encodings that forward to the same VPN ID.

A valid per-SF L2VPN Encoding appears as a subtype in the Upstream Service Flow Encoding (type 24) of a DOCSIS 1.1 CM configuration file, REG-REQ, DSA-REQ, or DSC-REQ message. The per-SF L2VPN Forwarding Encoding configures the CMTS to perform L2VPN bridge forwarding for all CPE packets received in the described service flow. A valid per-SF L2VPN Forwarding Encoding contains one L2VPN ID subtype. The CMTS includes a per-CM L2VPN encoding in its REG-RSP. After registration, a CM MAY include per-CM L2VPN encodings at the top level of Dynamic Service MAC Managements messages that otherwise add, change, or delete forwarding per-SF L2VPN encodings.

In order to configure particular CPE MAC addresses for L2VPN forwarding, the CM can be configured with Upstream Packet Classification Encodings that match the desired source CPE MAC address. The CM classifies the packet to an upstream service flow that is configured to forward to a particular L2VPN. The Upstream Packet Classification Encoding that references a forwarding Upstream SF L2VPN encoding does not contain a VPNID subtype itself.

The CMTS MUST consider an upstream service flow to be configured for per-SF L2VPN forwarding when a REG-REQ, DSA-REQ, or DSC-REQ contains exactly one valid per-SF L2VPN Forwarding Encoding within an Upstream Service Flow Encoding. A valid per-SF L2VPN Forwarding Encoding contains one VPNID subtype. The CMTS MUST reject a service flow transaction that contains more than one per-SF L2VPN Encoding.

The CMTS MUST accept a valid DSC-REQ with a valid per-SF L2VPN Encoding and change the upstream forwarding treatment of packets received from that SF accordingly. This includes, for example, adding, changing, or deleting any permitted subtype of a per-SF L2VPN encoding, including the VPN ID subtype.

The CMTS MUST remove per-SF L2VPN forwarding for an SF when the SF is deleted with a valid Dynamic Service Delete (DSD) transaction or a Dynamic Service Change (DSC) transaction completes that omits a previously signaled per-SF L2VPN Encoding.

The CMTS MUST support multiple per-SF L2VPN Encodings, each on a separate SF, with the same VPNID Subtype value.

A multipoint forwarding CMTS MAY accept the per-VPN subtypes defined only for point-to-point mode, but CMTS operation with different subtype values on different CMs is not defined.

6.2.1 VPNID Subtype

The VPNID Subtype is an opaque byte sequence that identifies a logical Layer 2 Virtual Private Network. All hosts attached to the same logical L2VPN communicate with each other as if they were attached to the same private LAN. An L2VPN is a network that forwards packets based only on layer 2 information such as the Ethernet MAC addresses and any VLAN ID tags encapsulating the packet. The term VLAN ID should be used only to describe the 12-bit VLAN ID field encoded in an IEEE 802.1Q tag, or IEEE 802.1ad tag pair of an L2VPN packet forwarded on an NSI port.

A cable operator is expected to configure a unique VPNID for each commercial enterprise to which it offers Transparent LAN service. The cable operator may choose any format desired for the VPNID, but it should be globally unique. One suggested approach is RFC 2685, which defines a mechanism for assigning 7-byte globally unique VPN Ids, based on combining a 3-byte Organization Unique ID for the organization assigning the ID (e.g., the cable operator itself), with a 4-byte VPN ID assigned by that organization. Another suggested approach is RFC 2547, which describes an 8-byte Route Distinguisher that may be used as a globally-unique VPNID.

The CMTS MUST ignore a per-SF L2VPN encoding that omits a VPNID subtype or that contains more than one VPNID subtype. The CMTS MUST support at least four (4) different values of VPNID per CM, signaled in four or more per-SF L2VPN Encodings.

In an IETF Virtual Private LAN Service (VPLS) application, the VPNID is intended to be the Attachment Group ID (AGI) signaled between the CMTS and other VPLS network elements.

6.2.2 Downstream Classifier L2VPN Encoding

A Downstream Classifier L2VPN Encoding is an L2VPN Encoding that appears in a Downstream Packet Classification Encoding [RFI 2.0] C.2.1.2. The presence of an L2VPN Encoding within a Downstream Packet Classification Encoding restricts the classifier to apply to only packets forwarded by the L2VPN Forwarder. Furthermore, only classifiers that contain an L2VPN Encoding apply to packets forwarded by the L2VPN Forwarder. In other words, downstream classifiers apply either to L2VPN or non-L2VPN traffic, but never both.

A Downstream Classifier L2VPN Encoding may contain zero or one VPN ID subtypes and/or zero or one User Priority Range subtypes. It may contain no subtypes at all (i.e., a zero-length 43.5 parameter), in which case the classifier applies to all L2VPN forwarded downstream packets to the CM, regardless of VPN ID or user priority.

The presence of a VPNID subtype within a Downstream Classifier L2VPN Encoding instructs the CMTS to apply the classifier to only downstream L2VPN-forwarded traffic on the indicated L2VPN. Because the L2VPN of L2VPN-forwarded traffic is always *implied* on the DOCSIS RF interface, and is not explicitly present in the packet contents, this is the only way to classify downstream L2VPN-forwarded traffic to a particular service flow based on the VPNID itself.

If the Downstream Classifier L2VPN Encoding contains a User Priority Range subtype, the classifier applies only to L2VPN packets forwarded downstream with an egress user priority within the indicated range (inclusive). This allows high priority L2VPN traffic to be classified to downstream service flows with enhanced QOS.

The egress user priority value matched by a User Priority Range subtype is the priority as logically transmitted by the L2VPN forwarder downstream onto the DOCSIS MAC Layer interface. This means that it is the value *after* any regeneration of the user priority value by the L2VPN forwarder. A CMTS vendor MAY implement vendor-specific mechanisms to determine and regenerate the user priority of downstream L2VPN forwarded packets.

A CMTS MUST reject the registration of a CM with a Downstream Packet Classifier Encoding that contains more than one L2VPN Encoding.

6.2.3 L2VPN SA-Descriptor Subtype

The L2VPN SA-Descriptor Subtype is a multiple-part encoding defined in the BPI+ Specification [BPI-PLUS] that provides:

- the Baseline Privacy (BPI) Security Association Identifier (SAID) that the CMTS uses to encrypt downstream L2VPN traffic for the L2VPN identified in the L2VPN Encoding;
- a Cryptographic Suite that identifies the encryption algorithm;
- and a Security Association Type (SA-Type).

A CMTS MUST encode the L2VPN SA-Descriptor as a Dynamic(2) SA-Type. A CM MUST ignore the SA-Type and consider it to be of type Dynamic(2).

Upstream L2VPN traffic is always encrypted in the Primary SAID of the CM that transmits the traffic upstream.

The L2VPN SA-Descriptor Subtype is not signaled in a CM configuration file. Instead, the CMTS adds one or more L2VPN SA-Descriptor Subtypes to top-level per-CM L2VPN Encodings of its REG-RSP to the CM, adding the per-CM L2VPN Encoding to the REG-RSP if necessary. After a CM completes BPI Authentication, it initiates a Traffic Encrypting Key (TEK) transaction with the CMTS for each L2VPN SA-Descriptor in a REG-RSP message.

The CMTS includes an L2VPN SAID in an L2VPN SA-Descriptor Subtype encoding at the top level of a CMTS-initiated DSA-REQ or DSC-REQ message that otherwise defines a L2VPN forwarding upstream SF. Likewise, the CMTS includes an L2VPN SA-Descriptor Subtype in a top-level L2VPN Encoding in its DSA-RSP or DSC-RSP responses to a CM-initiated dynamic service transaction, defining an L2VPN forwarding upstream service flow. A SAID signaled in an L2VPN SA-Descriptor Subtype Encoding is referred to as an L2VPN SAID. A SAID known to the CM only from messages other than an L2VPN SA-Descriptor Subtype is called a non-L2VPN SAID. Section 6.5 below describes how BPI encryption isolates L2VPN and non-L2VPN traffic on the RF network.

After the completion of any Dynamic Service MAC Management message transaction that introduces a new SAID to the CM, the CM initiates a TEK transaction with the CMTS to obtain the keying material for the new SAID.

In Point-to-Point L2VPN forwarding mode, the CMTS assigns an Individual L2VPN SAID to each CM. If the CM forwards more than one L2VPN, the CMTS assigns a different Individual L2VPN SAID for each L2VPN. In Multipoint L2VPN forwarding mode, the CMTS assigns a Group L2VPN SAID for all CMs forwarding the L2VPN to share.

6.2.4 Vendor-Specific L2VPN Encoding

The Vendor Specific L2VPN Encoding subtype is accepted in any L2VPN Encoding location, and provides information specific to the CMTS or CM vendor. For example, it may indicate to a CMTS vendor a particular NSI port sub-interface to which the L2VPN forwards the traffic in a point-to-point model. The Vendor Specific L2VPN Encoding may be binary or ASCII; its definition is left to the CMTS vendor.

A CMTS implementation MAY permit a Vendor Specific L2VPN Encoding to *replace* an otherwise required VPNID or NSI Encapsulation subtype, but vendor-specific L2VPN Encodings MUST NOT be required by a CMTS for L2VPN certification testing.

6.2.5 Configuration Error Requirements

A Multipoint forwarding CMTS MUST reject—with a reject-multipoint-NSI confirmation code—a registration or dynamic service transaction that attempts to configure multiple upstream forwarding L2VPN Encodings to the same L2VPN ID but with different values of the NSI Encapsulation, AGI, TAII, or SAII subtypes.

A Point-to-Point forwarding CMTS MUST reject—with a reject-VLAN-ID-in-use confirmation code—a registration or service flow transaction with an L2VPN NSI Encapsulation subtype that requires forwarding on the L2VPN Selected Port with a VLAN ID already assigned for non-L2VPN purposes. A Point-to-Point forwarding CMTS MUST reject an attempt to configure an L2VPN Selected Port with a VLAN ID already assigned by an L2VPN NSI Encapsulation Subtype encoding.

A Point-to-Point forwarding CMTS MUST reject—with a reject-multipoint-L2VPN confirmation code—a registration or service flow transaction that attempts to configure more than one cable attachment circuit (i.e., CM) with the same L2VPN NSI Encapsulation service multiplexing value.

6.2.6 Network System Interface (NSI) Encapsulation

Modern LAN switches and routers implement a rich set of layer 2 bridging features, and wide-area L2VPN operation over MPLS and IP tunneled backbone networks is an active area of product innovation and standardization efforts. This specification does *not* fully specify the layer 2 forwarding of Ethernet packets between CMTSs. It does attempt to specify the configuration of L2VPN forwarding within a single CMTS, and in particular between an RF Interface attachment circuit of a CM and an NSI interface. CMTS vendors are encouraged to support existing and future layer 2 backbone bridging protocols and features when forwarding layer 2 traffic, to and from a DOCSIS RFI MAC interface.

6.2.6.1 NSI Encapsulation Subtype

Although this specification primarily specifies L2VPN operation on the DOCSIS RF interface, it also specifies a limited degree of operation on an NSI interface for the following reasons:

- To standardize the L2VPN configuration for certification testing; and
- To standardize among CMTS vendors a useful subset of L2VPN capabilities.

This specification defines an NSI Encapsulation Subtype of an L2VPN Encoding B.3.2 to optionally describe how an L2VPN's packets are encapsulated on a single selected NSI port. The CMTS vendor implementation may permit this Selected NSI Port to change in the event of port failure or other events. A CMTS vendor MAY use the NSI Encapsulation subtype for additional scenarios, and MAY use vendor specific subtypes of the NSI Encapsulation to support vendor-specific mapping of attachment circuits to backbone pseudo-wires or internal virtual switch instances.

This specification requires CMTSs to implement only a single L2VPN NSI Encapsulation format: IEEE 802.1Q tagging, with a statically configured 12-bit VLAN ID value as the Service Multiplexing value. If the CMTS implements other L2VPN encapsulation formats on an NSI port, it should use the NSI Encapsulation Subtype encoding if the particular format code is defined for the subtype.

When an NSI Encapsulation VLAN ID is statically configured, it is expected to apply to only the Selected Ethernet port. The selection of a particular NSI interface for forwarding a particular L2VPN, or attachment circuit, is vendor-specific. The Vendor-Specific L2VPN Subtype may be used for this purpose.

A point-to-point forwarding CMTS MUST reject a CM registration or service flow transaction with an L2VPN Encoding that omits the NSI Encapsulation subtype or a vendor-specific subtype that identifies the NSI service multiplexing value. A multipoint forwarding CMTS does not require an NSI Encapsulation subtype in an L2VPN Encoding, but MUST accept and implement the subtype if it is specified. A CMTS in either forwarding mode MUST reject a CM registration or service flow transaction with an L2VPN Encoding that contains an NSI Encapsulation subtype for a VPNID that differs from the NSI Encapsulation subtype for that VPNID within any other accepted L2VPN Encoding.

Within the IEEE 802.1Q NSI Encapsulation, VLAN ID values 0, 1, and 4095 are not permitted as a configured VLAN ID. VLAN ID 0 is reserved for priority-only tags in IEEE 802.1Q. VLAN ID 1 is reserved as the default port-based VLAN ID in IEEE 802.1Q. Allowing subscriber L2VPNs to configure onto VLAN ID 1, risks inadvertent layer 2 forwarding of out-of-band management traffic on that subscriber L2VPN. VLAN ID 4095 (all '1's) is reserved by the IEEE.

It is a matter of vendor specific implementation as to whether the CMTS accepts non-L2VPN traffic on an NSI port with a priority-only IEEE 802.1Q tag (i.e., with VLAN ID 0).

6.2.6.2 IEEE 802.1ad L2VPN Forwarding

The IEEE 802.1ad standard describes a dual tagging approach for L2VPN forwarding in a backbone. A packet has an outer 12-bit VLAN ID tag and an inner 12-bit VLAN ID tag. The NSI Encapsulation Subtype allows the pair of 12-bit VLAN ID tags to be configured for each CM or SF performing L2VPN forwarding. The configuration of the dual tags depends on the L2VPN Forwarding Mode of the CMTS and the IEEE 802.1ad networking elements in the backbone.

6.2.6.2.1 Point-to-Point CMTS Forwarding with Point-to-Point 802.1ad Forwarding

In this scenario, the IEEE 802.1ad networking elements in the backbone simply forward point-to-point without learning MAC addresses. The outer 802.1ad tag identifies a destination network element that performs the L2VPN Bridging functions of MAC address learning on a bridge port and forwarding/flooding among those bridge ports. The inner 802.1ad tag identifies a particular bridge port on that external L2VPN Bridge element.

The CMTS is not otherwise configured with the IP address or identity of the destination node in this case. It is configured with only the two VLAN ID tags to use for NSI port encapsulation.

When dual-tagged 802.1ad frames are forwarded in the backbone network, the intermediate nodes only use the outer VLAN ID tag to make forwarding decisions. For example, 802.1ad supports provision of forwarding frames based on the outer tag value without a MAC address lookup.

The L2VPN Bridge addressed by the outer VLAN ID tag is separately configured as to which logical customer L2VPN each inner-tag bridge port is connected.

6.2.6.2.2 Point-to-Point CMTS Forwarding with L2VPN Bridging Network Element

IEEE 802.1ad can be leveraged to construct a backbone networking element to perform the L2VPN switching function of MAC layer learning and forwarding/flooding between attachment circuits belonging to the same L2VPN.

In this scenario, the inner VLAN ID tag represents the logical L2VPN, and the outer VLAN ID tag represents an individual attachment circuit to that logical L2VPN. The IEEE 802.1ad L2VPN switch considers the outer VLAN ID tag to represent a separate virtual trunk interface, while the inner tag represents a logical switch. The 802.1ad L2VPN switch builds an L2 Forwarding Database based on the MAC addresses it learns from each virtual trunk interface, and forwards/floods packets among those virtual trunk interfaces. In this manner, it provides L2VPN switch forwarding between all attachment circuits of an L2VPN. Using this technique, over 4000 L2VPN service instances can be supported between one CMTS and the IEEE 802.1ad L2VPN Switch, and each of these can have over 4000 cable modems/service flow associations at the CMTS.

6.2.7 Virtual Private LAN Service (VPLS) and Virtual Private Wire Service

6.2.7.1 MPLS and L2TPv3 NSI Encapsulation

The MPLS and L2TPv3 NSI Encapsulation subtype formats are intended to support the interoperation of DOCSIS L2VPN Forwarding with forthcoming Virtual Private Wire Service (VPWS) and Virtual Private LAN Service (VPLS) standards from the IETF. The IETF model is based on attachment circuits to L2VPN Forwarder entities. Each CM with at least one upstream forwarding SF for an L2VPN corresponds to an attachment circuit to the L2VPN. Because the DOCSIS L2VPN feature permits multiple service flows for the same L2VPN, and does not associate particular downstream service flows to upstream service flows, a cable attachment circuit to an L2VPN is considered to be the CM, not an individual service flow on the CM.

Layer 2 packets are intended to be forwarded on pseudo-wires across an NSI port, with a pseudo-wire being an MPLS path or an L2TPv3 tunnel session. A particular pseudo-wire is identified at ingress to an endpoint with a stack of one or more MPLS labels or an L2TPv3 session ID. The IETF L2VPN protocols plan to support the dynamic selection of these tunnel encapsulation values by negotiating the creation of pseudo-wires between endpoints that implement the same logical L2VPN. This is the primary reason for a globally unique VPNID Subtype to be configured for each per-SF L2VPN Forwarding Encoding. For endpoints implementing compatible dynamic tunnel creation protocols, only the VPNID and NSI Encapsulation Protocol fields need to be configured for a DOCSIS CM or SF.

In cases where pseudo-wire encapsulation values (i.e., MPLS label or L2TPv3 session ID values) cannot be dynamically negotiated, they may be configured with L2VPN Vendor Specific Subtype parameters or other vendor-specific CMTS configuration.

6.2.7.2 VPLS/VPWS Configuration

The control plane signaling for VPLS uses three configurable fields for identifying L2VPNs and attachment circuits:

- Attachment Group ID
- Source Attachment Individual ID (SAII); and
- Target Attachment Individual ID (TAII)

In order to standardize the DOCSIS configuration of these fields in a CM configuration file, this specification defines a subtype of an L2VPN encoding for each field.

The Attachment Group ID (AGI) subtype of an L2VPN Encoding is currently defined only in a per-SF Forwarding L2VPN Encodings. It provides the value for the AGI field when setting up an NSI backbone MPLS or L2TPv3 pseudowire for a cable attachment circuit. It is applicable only for Point-to-Point forwarding between the attachment circuit and the pseudowire. See [RFC 3985] for a description of the architecture of Pseudo Wire Emulation.

The Source Attachment Individual ID (SAII) subtype is defined only in a per-SF Forwarding L2VPN Encoding. It indicates the value dynamically signaled by the L2VPN Forwarder as the SAII field when advertising an NSI Encapsulation service multiplexing value such as an MPLS label or L2TPv3 session identifier. This field is used only for IETF L2VPN applications such as Virtual Private LAN Service (VPLS) or Virtual Private Wire Service (VPWS) when the CMTS operates in Point-to-Point forwarding mode between NSI pseudowires and CM/SF attachment circuits. The configured SAII is intended to match the Target Attachment Individual ID (TAII) of an incoming dynamic pseudowire establishment request.

The Target Attachment Individual ID (TAII) subtype is defined only in a per-SF forwarding L2VPN Encoding. It provides the value dynamically signaled by the L2VPN Forwarder as the TAII field when initiating the establishment of a IETF L2VPN pseudowire on an NSI interface. This field is used only for IETF L2VPN applications such as VPLS or VPWS when the CMTS is initiating a pseudowire to a remote network element that is implementing Point-to-Point forwarding. The TAII is intended to match the SAII of one of the attachment circuits of the remote network element.

A CMTS SHOULD use any configured Attachment Group ID (AGI) Subtype, Source Attachment Individual ID (SAII) Subtype or Target Attachment Individual ID (TAII) Subtypes configured in a forwarding L2VPN Encoding for the values of the corresponding fields with IETF-specified protocols that attempt to establish an NSI pseudowire switched to an attachment circuit.

6.3 CMTS Upstream L2VPN Forwarding

The CMTS MUST NOT interpret an 802.1Q tag already appearing in an upstream packet as providing either the priority or L2VPN identifier for L2VPN forwarding bridging. This includes a priority-only tag. The CMTS MUST transparently forward any subscriber-provided 802.1Q tag. If the subscriber-tagged packet is forwarded on an 802.1Q NSI Ethernet port, the CMTS MUST prepend an outer 802.1Q tag before the inner subscriber-provided tag.

The CMTS MUST be able to send and receive for L2VPN forwarding on all interfaces a 1522 byte packet that includes one stacked subscriber tag, plus any service-delimiting L2VPN information on the interface. For example, on an Ethernet NSI interface accepting 802.1Q tags for L2VPN NSI Encapsulation, the CMTS accepts and forwards a 1526 byte Ethernet packet. Such a packet is forwarded to the downstream RF MAC domain as a 1522 byte packet consisting of a nominal maximum length 1518 Ethernet packet with one four-byte subscriber non-service delimiting tag.

The CMTS MUST NOT count learned L2VPN CPE MAC addresses learned from upstream packets towards any enforced docsSubMgtCpeControlMaxCPEIp setting for the CM [RFI 2.0] C.1.1.18.1. This setting applies only to learned subscriber IP addresses that are forwarded in a non-L2VPN manner. Multipoint mode CMTSs have a separate requirement to limit the number of source MAC addresses learned on each L2VPN.

The CMTS MUST NOT apply subscriber management filtering [RFI 2.0] C.1.1.18 to upstream L2VPN forwarded packets.

The CMTS MUST NOT perform the TOS Overwrite function [RFI 2.0] C.2.2.6.10 for upstream L2VPN-forwarded packets.

An L2VPN forwarder maintains an out-of-band 3-bit user priority associated with each forwarded packet. The CMTS MUST use the 3-bit user priority field of IEEE 802.1Q tags as its user priority when accepting L2VPN forwarded packets with an IEEE 802.1Q NSI Encapsulation. The CMTS MUST use this user priority when classifying downstream packets. The CMTS MUST encode the egress value of user priority as specified for the NSI Encapsulation format (e.g., in the user-priority bits of an IEEE 802.1Q tag). The CMTS SHOULD provide mapping of egress user priority to NSI port transmission traffic class as specified by IEEE 802.1S. The number of NSI port transmission traffic classes is vendor-specific. 1109a If an upstream service flow L2VPN Encoding omits the IEEE 802.1 User Priority subtype, the CMTS MUST by default forward such packets to an NSI port with IEEE 802.1Q NSI Encapsulation with a user priority of zero. The CMTS MAY forward with non-zero default user priority values with vendor-specific configuration.

The CMTS MUST support both L2VPN and non-L2VPN forwarding of upstream traffic from a Forwarding L2VPN service flow based on checking the source MAC address against a CM Interface Mask configured for the SF. The CMTS MUST direct packets from the source MAC addresses indicated with a '1' in the CM Interface Mask to the L2VPN forwarder. The CMTS MUST NOT direct to the L2VPN Forwarder packets from the eCM and at least one other eSAFE source MAC address, even when received on an L2VPN forwarding upstream service flow, when the interfaces corresponding to those source MAC addresses are indicated with a '0' in the CM Interface Mask.

A CMTS MAY recognize when the CM Interface Masks in the set of Upstream Packet Classifier L2VPN Encodings of a compliant CM permit it to avoid checking upstream source MAC addresses and instead forward upstream packets to the L2VPN or non-L2VPN forwarder solely on the basis of the upstream service flow.

The CMTS MUST recognize a CM Interface Mask criterion in a Downstream Packet Classifier L2VPN Encoding regardless of whether the Encoding classifies L2VPN or non-L2VPN traffic. The CMTS MUST classify the destination MAC address of a downstream packet as one of three classes: 1) A CM MAC address; 2) a CPE MAC address; or 3) an eSAFE MAC address of a particular eSAFE host type. The CMTS MUST consider the criterion to be matched when the destination MAC address of the downstream layer 2 packet is a CM MAC address or eSAFE MAC address that corresponds to a host type with a '1' in the CM Interface Mask. The CMTS MUST consider the criterion to be matched when the destination MAC address is a CPE MAC address and the CM Interface Mask has *any* CPE host type bit set, i.e., any of bits 1 or 5-15 set. The CMTS MUST consider the criterion to be unmatched when the destination MAC address is a CM or eSAFE MAC address and the single CM Interface mask bit corresponding to that host type has a '0' bit. The CMTS MUST consider the criterion to be unmatched when the destination MAC address is a CPE MAC address and the CM Interface Mask has a zero bit in all CPE host type positions, i.e., has a zero bit in positions 1 and 5-15.

The CMTS MUST reject any attempt (i.e., registration or DSx transaction) to configure multiple Upstream Classifier L2VPN Encodings that classifies to the same upstream Service Flow but with a different VPNID Subtypes. The CMTS uses the upstream SF to determine a single VPNID for L2VPN forwarding.

6.4 CMTS Downstream L2VPN Forwarding

The CMTS MUST reject any REG-REQ with an L2VPN Encoding if BPI is not also enabled in the REG-REQ. The CMTS MUST reject any DSA-REQ or DSC-REQ with an L2VPN Encoding if BPI is not also enabled for the CM.

The CMTS MUST NOT apply subscriber management filters ([RFI 2.0] section C.1.1.18) to downstream L2VPN forwarded traffic.

The CMTS MUST accept a single Downstream Classifier L2VPN Encoding in a Downstream Packet Classification Encoding of a REG-REQ, DSA-REQ, or DSC-REQ message. A CMTS MUST apply classifier rules that contain an L2VPN Encoding only to packets forwarded by the L2VPN Forwarder. Furthermore, only classifiers containing an L2VPN Encoding may be applied against downstream L2VPN forwarded traffic.

- The CMTS MUST reject the registration of cable modems with invalid Downstream Packet Classification Encodings.
- A valid Downstream Classification L2VPN Encoding contains zero or one VPNID subtypes, zero or one User Priority Range subtypes, and any number of Vendor Specific L2VPN Parameter subtypes. The CMTS MUST silently ignore all invalid L2VPN Encoding subtypes.
- The CMTS MUST accept as valid and silently ignore any unrecognized L2VPN Encoding subtypes.
- The CMTS MUST accept multiple Downstream Classification Configuration Settings with a Downstream Classifier L2VPN Encoding that classify different L2VPN VPN IDs to the same referenced service flow.
- The CMTS MUST support the same Classifier criteria options for Downstream Classifier L2VPN Encodings as it does for non-L2VPN Downstream Classifier L2VPN Encodings.
- The CMTS MUST interpret a Downstream Packet Classifier Encoding containing no other criteria than a Classifier L2VPN encoding as matching *all* packets forwarded downstream on the L2VPN identified by the VPNID of the Classifier L2VPN Encoding, and classify all such packets to the referenced service flow.
- The CMTS MAY accept multiple Downstream Classifier L2VPN Encodings with the same VPNID classifying packets to different service flows. Operation is undefined when more than one Downstream Classifier matches a particular downstream packet.
- The CMTS MUST reject a service flow transaction request containing an invalid Downstream Classifier L2VPN Encoding.
- If the L2VPN Encoding contains a User Priority Range subtype, the CMTS MUST match the classifier only to L2VPN forwarded packets with an egress user priority within the indicated range. Otherwise, the classifier applies to all egress user priorities.

With the acceptance of a valid Downstream Classifier L2VPN Encoding, the L2VPN forwarder of the CMTS MUST forward on the referenced service flow of the classifier all single-CM downstream traffic destined for CPE attached to that CM. For Point-to-Point mode, this means all downstream traffic on the L2VPN; for Multipoint mode this means unicast traffic destined to CPE MAC addresses learned from upstream traffic from the CM. If downstream L2VPN forwarded traffic is not classified to a particular downstream service flow, the CMTS MUST forward single-CM traffic on the CM's primary downstream service flow.

The CMTS MUST classify layer 2 packets as they appear on the RFI interface, that is, NOT including any service-delimiting 802.1Q tag that appeared on the CMTS NSI port. This means that the 802.1Q Packet

Classification Encodings [RFI 2.0] C.2.1.7 apply only to the subscriber-private or inner 802.1Q tag, and not the VLAN ID of the L2VPN-forwarded packet.

A CMTS MUST NOT apply Subscriber Management filters [RFI 2.0] C.1.1.18 to downstream L2VPN traffic.

A CMTS MUST forward downstream L2VPN-forwarded packets for different L2VPNs on different downstream service flows. This provides isolation of QOS for L2VPN service.

Unless explicitly configured to combine the forwarding data base of different L2VPNs, the CMTS L2VPN Forwarder MUST maintain upstream and downstream separation of L2 forwarded traffic between attachment circuits configured with different VPNIDs. The number of CMs or SFs supported for L2VPN Forwarding is CMTS vendor-specific. The number of unique VPNIDs supported by a CMTS is vendor-specific.

6.4.1 Multipoint Downstream Forwarding

The CMTS MUST reject (with a reject-permanent confirmation code) a registration or service flow transaction that would require defining L2VPN SAIDs exceeding the CM's Downstream SAID capability ([RFI 2.0] C.1.3.1.7).

A Multipoint forwarding mode CMTS MUST learn the source MAC addresses of upstream CPE traffic and associate them with a particular CM on that L2VPN.

A Multipoint forwarding CMTS MUST limit the number of MAC addresses permitted to be learned on any single L2VPN to a configurable value that applies to all L2VPNs. The CMTS SHOULD permit configuration of the maximum number of MAC addresses per L2VPN on a per-L2VPN basis.

A Multipoint forwarding CMTS MUST forward downstream packets encrypted on different L2VPN SAIDs on different service flows.

6.5 L2VPN Isolation and Privacy

A key goal of this specification is to *isolate* traffic between L2VPN and non-L2VPN subscribers, as well as between different L2VPN subscribers. Non-L2VPN (i.e., residential) subscribers should not be able to see traffic forwarded to L2VPN subscribers, and L2VPN subscribers, moreover, should not see traffic intended for non-L2VPN residential subscribers.

6.5.1 Protecting L2VPN Traffic

This specification uses BPI encryption to isolate L2VPN from non-L2VPN traffic in the downstream. This requires a cable operator to configure CMs providing L2VPN service to enable Baseline Privacy Interface (BPI) operation. The cable operator is expected to configure all CMs, with and without L2VPN forwarding, to enable BPI, so that all such CMs can receive encrypted IP multicast traffic.

The CMTS MUST reject an attempt (i.e., a registration or DSx transaction) to configure a forwarding L2VPN Encoding if the CM is not also configured to support BPI operation.

A CMTS MUST assign at least one L2VPN SAID for downstream forwarding to each separate L2VPN forwarded by the CMTS on a downstream channel. A single L2VPN SAID assigned for all CMs on the same L2VPN is called a Group L2VPN SAID. The CMTS MAY assign L2VPN SAID values to be different for the same L2VPN on different downstream channels. A CMTS MAY assign multiple L2VPN SAIDs to the same L2VPN on the same downstream channel, e.g., to assign an Individual L2VPN SAID to each CM in Point-to-Point forwarding mode. The CMTS MUST assign a Group or Individual L2VPN SAID that differs from any other Primary SAID assigned on that channel. A CMTS MAY assign multiple SAIDs to the same L2VPN on the same CM.

A CMTS MUST add to the forwarding L2VPN Encoding of its REG-RSP and Dynamic Service messages to an L2VPN-compliant CM one or more L2VPN SA-Descriptor Subtypes for its assigned L2VPN SAID(s) for downstream forwarding to that L2VPN on the CM's downstream channel. The CMTS MUST encode separate top-level L2VPN encodings for each separate L2VPN ID.A CMTS MAY add L2VPN SA-Descriptor Subtypes in messages to non-compliant CMs, but they will be ignored by the CM. The CMTS MUST describe the L2VPN SAIDs with an SA-Type of Dynamic in an L2VPN SA-Descriptor Encoding.

A CMTS does NOT include SA Descriptors for all L2VPN SAIDs it assigned for a registering modem in its initial BPI Authorization Reply to the CM after registration.

A CMTS MUST encrypt all downstream L2VPN forwarded traffic in an L2VPN SAID assigned to the L2VPN.

The CMTS MUST NOT forward downstream L2VPN traffic to a CM until that CM has completed BPI Authorization and TEK negotiation for the L2VPN SAID in which the traffic is to be encrypted.

A Point-to-Point forwarding CMTS SHOULD assign the same Group L2VPN SAID to different CMs on the same MAC domain attaching to the same L2VPN Identifier, but MAY choose to assign an Individual L2VPN SAID unique for the CM.

A Multipoint forwarding CMTS MUST assign at least one broadcast L2VPN SAID to all CMs on the same MAC Domain attaching to the same L2VPN Identifier. The Multipoint forwarding CMTS MUST forward downstream broadcast packets of the L2VPN encrypted on such a broadcast L2VPN SAID.

A CMTS MAY support vendor-specific configuration to dynamically start or discontinue L2VPN forwarding through a registered CM. A CMTS that discontinues L2VPN forwarding through a CM MUST dynamically delete all upstream service flows forwarding to that L2VPN, and MUST signal a top-level L2VPN encoding to the CM that omits all SA-Descriptors for that L2VPN. This signals the CM to discontinue downstream decryption for the L2VPN SAIDs associated with the L2VPN.

6.5.2 Preventing Leaking of non-L2VPN Traffic

One issue with L2VPN operation is downstream non-L2VPN layer 2 traffic to a Group MAC (GMAC) address, i.e., a layer 2 broadcast or multicast. Downstream non-L2VPN broadcast traffic includes CMTS-originated ARPs to non-L2VPN CPEs and CMTS router advertisements for RIP or OSPF. By default, *all* cable modems—L2VPN and non-L2VPN—will forward to their CPE interface downstream broadcast traffic that is *not* encrypted. Furthermore, unencrypted non-L2VPN GMAC traffic sent to the same multicast Ethernet Destination Address used by a private L2VPN would also be forwarded by an L2VPN CM to its CPE interface. Without special attention, downstream non-L2VPN GMAC traffic will leak onto the L2VPN subscriber's supposedly private CPE network.

This specification addresses the non-L2VPN GMAC leakage problem with the following mechanisms:

- Downstream Unencrypted Traffic (DUT) Filtering;
- Downstream IP Multicast Encryption (DIME)

6.5.2.1 Downstream Unencrypted Traffic (DUT) Filtering

A cable operator can prevent the leaking of clear-text, non-L2VPN traffic, through L2VPN-compliant CMs by enabling the Downstream Unencrypted Traffic (DUT) Filtering Encoding. When DUT Filtering is enabled, a DUT CM Interface Mask (DUT CMIM) is defined to limit the forwarding of downstream unencrypted traffic to only the interfaces with a '1' bit for that interface in the CMIM. The DUT CMIM by default contains '1' bits only for the internal eCM and eSAFE host interfaces, requiring the CM to prevent forwarding of such traffic to the CMCI interface(s) on the CM. DUT filtering alone prevents non-L2VPN GMAC leaking onto an L2VPN subscriber's CPE network.

6.5.2.2 Downstream IP Multicast Encryption (DIME)

CMs by default must enable GMAC promiscuous forwarding for L2VPN operation, and in most DOCSIS 2.0 and earlier CMs, this causes all unencrypted GMAC traffic to be delivered to CM software. Although the DUT Filtering of the CM's software indeed prevents this traffic from leaking onto the CPE interface, if it is significant, it may affect the forwarding performance of the desired L2VPN traffic through the CM. It is desirable to allow the L2VPN CMs to use their hardware-based SAID filters to drop high-volume non-L2VPN GMAC traffic.

In most CMTS deployments, it is expected that IP multicast session traffic will be the most significant source of high-volume downstream GMAC traffic. It is desirable to encrypt this traffic in a SAID that is unknown by the L2VPN CMs, so that their hardware will filter the packets before delivering it to L2VPN software.

A CMTS MUST implement a configurable option to enable or disable Downstream IP Multicast Encryption (DIME). With DIME enabled, the CMTS MUST encrypt all non-L2VPN downstream IP Multicast traffic that is either statically joined with the BPI+ MIB or dynamically joined with upstream SA-MAP requests from a CM. DIME does not require the CMTS to encrypt non-L2VPN downstream *unjoined* IP multicasts, (e.g., RIPv2 or OSPF multicasts).

By encrypting joined non-L2VPN IP multicast traffic in a non-L2VPN SAID, the potentially high volume downstream non-L2VPN multicast traffic is required to be filtered by DOCSIS 2.0 CMs implementing this specification.

Since the non-L2VPN GMAC traffic is encrypted in a SAID unknown to the L2VPN CM, the CM filters the downstream traffic and prevents it from leaking onto the private CPE network.

6.5.2.3 Mixing L2VPN and non-L2VPN forwarding on the same CM

The L2VPN feature supports mixing of L2VPN and non-L2VPN forwarding for different CPE hosts connected to the same CM. In this case, the L2VPN and non-L2VPN traffic are of course not isolated on the CMCI network(s) of the CM, both in the upstream and in the downstream direction. To support mixed L2VPN and non-L2VPN, the cable operator can configure Upstream L2VPN Classifiers L2VPN Encodings in the CM with a rule that identifies the particular type of traffic to be forwarded on the L2VPN, (e.g., traffic with the source MAC address of a particular CPE).

This specification does not require the CM to restrict the forwarding between L2VPN and non-L2VPN CPE hosts when they are connected on different CMCI ports of a CM. The embedded VLAN (eVLAN) model of CM forwarding, if implemented on the CM, can provide this isolation (Appendix III).

DUT filtering should not be enabled when mixing L2VPN and non-L2VPN CPE hosts on the same CM, because it is necessary for the non-L2VPN CPEs to still receive downstream ARPs and DHCP broadcasts. With DUT Filtering disabled, however, all downstream non-encrypted GMAC traffic will pass to the mixed CPE network. To prevent this, Downstream IP Multicast Encryption (DIME) can be enabled to prevent the forwarding of unjoined multicast traffic to the mixed-mode CPE LAN.

6.6 CM and eSAFE Exclusion

This specification uses the term included to mean traffic forwarded through the L2VPN forwarder, and excluded to mean all other non-L2VPN traffic.

Subscriber Transparent LAN Service requires that all CPE traffic be included in L2VPN forwarding while traffic from embedded CMs and any other embedded hosts co-located with the CM be excluded from L2VPN forwarding.

The L2VPN feature can be configured, however, so that eCM and eSAFE traffic can be forwarded on separate L2VPNs if desired.

6.6.1 CM and eSAFE Host Forwarding Model

Figure 6–1 depicts the overall CMTS and CM L2VPN forwarding model for CMs and eSAFE Hosts.

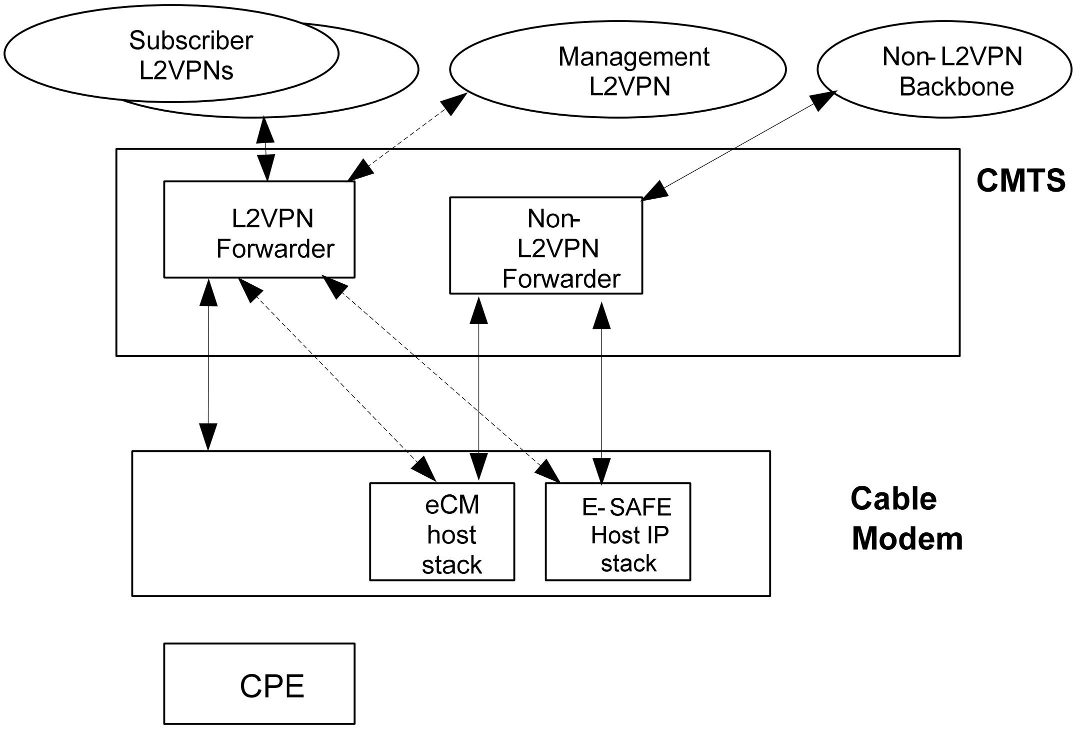

Figure 6–1 - CM, eMTA, and CPE Forwarding

For TLS service, traffic to and from the eCM's and eSAFE's host IP stack is excluded from L2VPN forwarding, and is forwarded with the CMTS's normal non-L2VPN forwarder, as depicted with a solid line in Figure 6–1.

With the Management L2VPN feature, the eCM's post-registration traffic is classified to an L2VPN Forwarding service flow and included for L2VPN forwarding (dotted line). Any pre-registration eCM traffic cannot use the L2VPN feature because encryption in an L2VPN SAID is not possible prior to registration.

The management traffic to and from an eSAFE host can use the same Management L2VPN as the eCM, or its own separate Management L2VPN, as desired.

6.6.2 Cable Modem MAC Bridge Interface Masks

In accordance with the MAC bridging model described in [eDOCSIS], a CM implementing this specification is considered to implement a set of MAC Bridge Interfaces, as summarized below.

Table 6–2 - Cable Modem MAC Bridge Interfaces

ifIndex	Description
(0)	(eCM: self Host interface)
1	Primary CPE Interface, also ePS: CableHome embedded Portal Services
2	RF Interface
16	eMTA: PacketCable embedded Media Transport Agent host interface
17	eSTB-IP: OpenCable embedded Set Top Box IP Host interface
18	eSTB-DSG: OpenCable embedded Set Top Box DOCSIS Set-top Gateway interface

This specification introduces the convention that ifIndex 0 is considered by convention to apply to the internal host interface to the CM's management IP stack, or its self interface.

L2VPN layer 2 forwarding in a CM is considered to occur only on an explicit list of the above MAC Bridge interfaces. For example, Transparent LAN Service involves bridging only from the RF MAC Interface (ifIndex 2) to the Primary CPE Interface (ifIndex 1). TLS is not permitted to access the eCM's self interface or any other eSAFE host interface.

For each L2VPN that is forwarded within a CM, a CM Interface Mask (CMIM) parameter is configured with the set of MAC Bridge interfaces that are permitted to forward packets to and from that L2VPN. Each MAC Bridge interface is assigned a bit position in the CMIM mask corresponding to its ifIndex value. The eCM's host interface is assigned CMIM bit position 0.

The CMIM parameter for an L2VPN is encoded in the same per-SF L2VPN encoding that defines the L2VPN VPNID. If the CMIM subtype is omitted from a forwarding L2VPN encoding, its default value is the one appropriate for TLS service, (i.e., with only the RF Interface (ifIndex 2) and Primary CPE Interface (ifIndex 1) bits set). The CMIM parameter is encoded in the same manner as the Basic Encoding Rules of an SNMP BITS object type. In a CMIM Subtype TLV, the bit mask is encoded as a variable length octet string where bit position 0 is the most significant bit of the first octet; position 1 is the next most-significant bit; position 7 is the least significant bit of the first octet. Bit position 8 is the most significant bit of the second octet. As an example, the default CMIM value, with bit positions 1 and 2 set, can be encoded as a single octet with the value 0x60.

6.6.3 Embedded Host Exclusion

When a CMIM mask has a value of zero in a MAC bridge interface position, all traffic from that interface is configured to be excluded from L2VPN forwarding. In particular, the eCM self host interface (CMIM interface bit position 0) is excluded from Transparent LAN Service L2VPNs. When the eCM self host interface is excluded from a CMIM subtype for an L2VPN forwarding upstream SF, the CMTS MUST exclude from upstream L2VPN forwarding all traffic that contains a source MAC that matches the CM host's MAC address.

Because non-compliant CMs are unable to classify L2VPN from non-L2VPN upstream traffic, a CMTS MUST support both L2VPN and non-L2VPN forwarding of upstream traffic from a Forwarding L2VPN service flow of a non-compliant CM based on checking the source MAC address against a CM Interface Mask configured for the SF. The CMTS MUST direct packets from included host types to the L2VPN forwarder. The CMTS MUST NOT deliver traffic from excluded host types to the L2VPN Forwarder.

A CMTS MUST support exclusion of the CM MAC address and at least one other eSAFE MAC address on all L2VPN forwarding service flows from both non-compliant CMs and compliant CMs. Non-compliant CMs may have at most, one eSAFE MAC address checked in this manner. This specification does not support L2VPN forwarding from a non-compliant CM with more than one eSAFE host. This specification supports L2VPN forwarding from compliant CMs with more than one eSAFE host only by configuring Upstream Packet Classification encodings that explicitly classify the non-L2VPN forwarding eSAFE traffic to non-L2VPN forwarding upstream service flows.

6.6.4 CMTS embedded host MAC Address Learning

A CMTS MUST learn the MAC address of an embedded CM from the Source MAC address of the CM's initial ranging request message and include it in the docsDevCmCmtsStatusTable.

The CMTS uses two techniques to learn the MAC address of eSAFE hosts:

- For L2VPN-compliant CMs, the CMTS MUST learn the eSAFE MAC addresses from the eSAFE Host Capability encodings section A.3.2 when the CM registers;
- For non-L2VPN-compliant CMs, the CMTS MUST snoop upstream DHCP packets to determine the eSAFE MAC addresses.

6.6.4.1 Enable eSAFE DHCP Snooping Subtype

The CMTS MUST enable DHCP snooping to determine eSAFE MAC addresses from a non-compliant CM when an Enable eSAFE DHCP Snooping subtype is present in any per-SF L2VPN Encoding A.5.3. The value of the encoding is a bit mask that enables particular eSAFE hosts to be snooped. The CMTS MUST NOT enable DHCP snooping when the Enable eSAFE DHCP Snooping subtype is absent from all per-SF L2VPN encodings or does not have a '1' bit for the particular eSAFE host type when it is present. This is to prevent spoofing of eSAFE by unauthorized non-embedded CPEs.

When eSAFE DHCP snooping is enabled, the CMTS MUST support detection of the eSAFE host type of a MAC address, from the initial substring of option 60 of the broadcast DHCP DISCOVER packet, from the eSAFE host that is relayed by the CMTS, when option 60 is present. When eSAFE DHCP snooping is enabled, the CMTS MUST support detection of the eSAFE host type of a MAC address from option 43, subtype 2 of a DHCP DISCOVER packet from the eSAFE host that is relayed by the CMTS, when option 43, subtype 2 is present. The following Table 6–3 provides the values of these DHCP options for each currently defined eSAFE host type:

Table 6–3 - eSAFE DHCP Snooping Substrings

ESAFE Host Type	DHCP Option 60 substring	DHCP Option 43, sub-option 2 substring
Embedded Media Transport Agent [PKT-PROV]	pktc	EMTA
Embedded Portal Services [CH1.1]	CableHome	EPS

The CMTS MUST learn the eSAFE's MAC address from the client hardware identifier field of the snooped DHCP-DISCOVER packet.

Once the CMTS learns the MAC addresses of eSAFE hosts, the CMTS thereafter excludes from L2VPN forwarding, all upstream traffic from that DOCSIS host MAC address.

6.6.5 Interface-based Classification

The RF MAC Domain implements the DOCSIS Upstream Packet Classifiers that classify an L2PDU bridged to the MAC Domain interface into an upstream Service Flow.

In an Upstream Packet Classification encoding, the CMIM subtype represents a rule that matches the ingress bridge port of the L2PDU. This allows classifiers to classify CPE, eCM, and eSAFE traffic generically, by host type, instead of requiring static classifiers to be based on the actual MAC or assigned IP address of the host.

The Host Classification capability is most useful when implementing Management L2VPNs for isolating CM and eSAFE management traffic from payload traffic on a layer 2 backbone. It allows the CM's classifiers to classify upstream eCM and/or eSAFE traffic to a separate L2VPN forwarding upstream service flow for the Management L2VPN.

6.7 L2VPN Quality Of Service

6.7.1 Service Flow Separation

An important aspect of the L2VPN service offering by an operator is isolation not only of traffic forwarding, but also of Quality of Service. It should not be possible for one L2VPN traffic flow (or even a non-L2VPN traffic flow) with excessive traffic to significantly affect the QOS received by any other L2VPN's flows. Accordingly, this specification requires that the downstream traffic for each L2VPN be isolated from each other and from non-L2VPN traffic by placing the traffic in a separate Service Flow (SF). In the case of Point-to-Point mode forwarding, this happens automatically because each CM already has a primary downstream service flow. In the case of Multipoint mode forwarding, this specification requires each L2VPN to have a separate service flow for its downstream flooded group MAC and unknown individual MAC destined traffic.

6.7.2 IEEE 802.1 User Priority

The IEEE 802.1 layer 2 bridging model uses the concept of a user priority with 8 possible values to indicate the QOS to be provided when forwarding an L2PDU [IEEE 802.1Q]. This field is used to provide differentiated QOS to different traffic flows *within the same* L2VPN.

When an L2PDU is forwarded with an IEEE 802.1 Tag on a trunk Ethernet NSI interface, the user priority of the packet is encoded in the upper 3 bits of an 802.1Q Tag Control value. Appendix II provides details of the IEEE 802.1Q encapsulation.

A CMTS MUST accept the priority bits of a service-delimiting 802.1Q tag on NSI port input as the L2VPN ingress user priority attribute of the packet. The CMTS MUST maintain the user priority of the packet within the L2VPN forwarder (possibly regenerating it via vendor-specific configuration), and use the egress value of user priority for matching against the User Priority Range subtype of Downstream Classifier L2VPN Encodings.

In the upstream direction, this specification requires the user priority of upstream L2VPN traffic to be explicitly configured as the Ingress User Priority subtype of a forwarding L2VPN Encoding It requires the L2VPN forwarder to maintain that user priority (possibly regenerated) when encoding the IEEE 802.1Q tag for egress out of an NSI port. If the Ingress User Priority subtype is omitted, the CMTS assumes the ingress user priority is zero. By requiring the user priority to be explicitly configured in the Forwarding L2VPN encoding, this prevents CPE from submitting L2VPN packets with arbitrary user priority onto the cable operator's L2VPN backbone.

6.7.3 Downstream User Priority Range Classification

This specification defines a User Priority Range subtype of an L2VPN Encoding that appears as a new rule matching criterion in a downstream Service Flow Packet Classifier encoding. The User Priority Range subtype is described in B.3.9. When a User Priority Range subtype is present in a Downstream Service Flow Packet Classifier Encoding, the CMTS MUST match the classifier only to L2VPN forwarded packets with a user priority within the indicated range.

6.7.4 Upstream Ingress User Priority

This specification calls for the CMTS to associate a configured user priority for an upstream L2VPN forwarding service flow based on a configured Ingress User Priority subtype of the per-SF L2VPN Encoding that defined the SF. The Ingress User Priority subtype is described in section B.3.8.

A CMTS MAY implement vendor-specific configuration to select the ingress user priority of upstream L2VPN packets. The particular bridging model implemented by the CMTS (e.g., IEEE 802.1S or IEEE 802.1ad) MAY provide for the regeneration of an upstream ingress user priority to a different internal user priority for the packet in the CMTS.

The CMTS MUST NOT use any priority only tag applied by CPE to determine the ingress user priority of an upstream packet. If necessary, the CM can be configured to classify the upstream priority-only CPE-tagged packet to a service flow that is configured with an explicit Ingress User Priority subtype. If the CMTS implements an IEEE 802.1ad bridge forwarder, the CMTS MAY map the inner customer user priority tag to the outer service user priority tag.

Note that the user priority parameter of an L2VPN packet defines only the priority of the packet's forwarding across the bridges of the L2 backbone; it does not affect the forwarding of the packet upstream or downstream on the DOCSIS RF interface. Only the QOS Parameter Set of the service flow to which the packet is classified defines the priority for forwarding the packet on a DOCSIS RF interface.

6.7.5 Layer 2 Backbone Network QOS

On the bridged network of the L2 Backbone, the bridging priority of an L2VPN packet may be indicated in a variety of ways:

- In the user priority bits of an outer IEEE 802.1 tag;

- In the EXP experimental bits of an MPLS pseudowire label;
- In the DSCP bits of an L2TPv3 pseudowire encapsulation.

The CMTS MUST transmit an L2VPN upstream packet on an NSI port with the egress user priority encoded as appropriate for its NSI encapsulation. The mapping of egress user priority to MPLS EXP bits or DSCP values is beyond the scope of this specification.

For IETF pseudowire NSI encapsulation of L2VPN traffic, the determination of downstream ingress user priority and the encoding of upstream egress user priority based on MPLS EXP bits or L2TPv3 DSCP values is beyond the scope of this specification.

6.8 Stacked 802.1Q Tags or Tag-in-Tag operation

The selection of the particular L2VPN for upstream bridged traffic is always indicated by the VPNID subtype of the L2VPN Encoding. This specification does not address the interpretation of 802.1Q tags applied by CPE and received by the Ethernet port of a CM for forwarding upstream. Such tags are considered non-service delimiting, and are always ignored for purposes of L2VPN selection by the DOCSIS CMTS. These non-service delimiting tags are forwarded as part of the CPE payload. DOCSIS CMTSs and CMs conforming to this specification support forwarding of maximum length Ethernet packets with a single subscriber non-service delimiting 802.1Q tag. This means that a CM supporting this specification is able to forward 1522 byte packets between its RF and CPE interfaces and a CMTS is able to forward 1526 byte packets on its 802.1Q tagging Ethernet NSI port.

When a packet with an inner CPE-supplied non-service delimiting tag is forwarded onto an NSI port that is also using IEEE 802.1Q Encapsulation, the CMTS adds an outer service-delimiting tag with the configured NSI Encapsulation VLAN ID. This is called stacked or tag-in-tag 802.1Q tagging. The IEEE 802.1P/Q Packet Classification Encoding criteria in section [RFI 2.0] C.2.1.7 apply to only the non-service delimiting CPE-supplied 802.1Q tag as the packet appears on the RF interface, not the outer service-delimiting tag value as the packet appears on an NSI port. For example, the CM may classify upstream CPE packets to a particular service flow, based on the priority bits of the CPE-applied tag.

In order to prevent CPE abuse of backbone L2 user priorities, the CMTS MUST NOT interpret a priority-only tag applied by the CPE as defining the upstream ingress user priority of an L2VPN packet. The user priority of an upstream packet is defined only by the configured IEEE 802.1 User Priority subtype of the per-SF Forwarding L2VPN Encoding that applies to the packet. A CPE-applied priority-only tag is treated as a non-service delimiting tag and is stacked as an inner tag when forwarded by the CMTS. If a CPE-applied priority-tag is desired to select the upstream ingress user priority, the CM should be configured to classify the packet to a service flow with an explicit Ingress User Priority subtype. This allows the cable operator to control the priority of L2 forwarded packets on the backbone.

In the downstream direction, the IEEE 802.1P/Q Packet Classification Encoding criteria of [RFI 2.0] C.2.1.7, apply only to any inner, non-service delimiting tag in the packet as it appears on the RF interface. Note that CMTSs are not required to implement these layer 2 criteria in the downstream direction. What is usually desired, however, is to classify downstream traffic according to the priority or VLAN ID of the outer, service delimiting tag as the packet appeared *on the NSI interface*. This specification defines Downstream Classifier L2VPN Encodings to permit classification based on the packet's VPNID and user priority as signaled in its NSI encapsulation.

6.9 Spanning Tree and Loop Detection

[RFI 2.0] describes the DOCSIS Spanning Tree Protocol (DSTP). Unfortunately, few, if any, CMs implement DSTP, so this protocol cannot be relied upon to avoid L2VPN bridging loops. An operator is expected to configure subscriber L2VPN networks in a loop-free manner, or to rely upon subscriber equipment itself implementing the IEEE Spanning Tree Protocol to break any bridging loop on a subscribers L2VPN. This section describes CMTS requirements to prevent L2VPN denial of service when a subscriber accidentally or intentionally configures a bridging loop.

The CMTS MUST transparently forward the IEEE Spanning Tree Protocol (STP) on the subscriber's layer 2 VPN.

A CMTS MAY implement the DOCSIS Spanning Tree protocol and transmit DSTP BPDUs on all NSI and RF interfaces configured for L2VPN operation. The CMTS MUST transmit DOCSIS Spanning Tree Protocol packets as untagged on an IEEE 802.1Q NSI interface and encrypted in a SAID provided to the L2VPN CMs on a CMTS MAC domain RF interface. A CMTS MAY implement a DOCSIS Spanning Tree (DST) SAID specifically for DST forwarding to the CPE ports of all L2VPN CMs.

A CMTS MUST prevent a bridging loop for one L2VPN from denying all forwarding or flooding of traffic on any other non-looped L2VPN. A CMTS MAY require configuration of both downstream and upstream service flow maximum forwarding rates to meet this requirement, as long as such limits are no less than 10% of link capacity.

7 CABLE MODEM REQUIREMENTS

A CM MUST accept one or more L2VPN SA-Descriptor Subtypes added by a CMTS to any forwarding L2VPN Encoding in a REG-RSP or DSx-RSP message to the CM. The CM associates the SAIDs of the SA-Descriptors in the L2VPN Encoding with the single L2VPN identified in the L2VPN Encoding. The CM MUST be capable of associating any number of its available SAIDs to an L2VPN. The CM MUST be capable of associating more than one SAID to a single L2VPN A CM receiving an L2VPN Encoding with an L2VPN SA-Descriptor Subtype for a SAID not previously established on that CM MUST initiate a BPKM TEK transaction to establish the new L2VPN SAID [BPI-PLUS]. A CM receiving an L2VPN SA-Descriptor Subtype in a REG-RSP MUST wait for BPI Authorization to complete before initiating the BPKM TEK. The CM determines that a downstream packet is to be forwarded on an L2VPN when the packet is encrypted with an L2VPN SAID. A CM MUST replace the set of L2VPN SAIDs of an L2VPN when receiving a top-level L2VPN Encoding in a MAC Management message that identifies that L2VPN. The CM MUST discontinue downstream decryption of an L2VPN SAID when it receives in a dynamic service flow message a top-level L2VPN Encoding for an L2VPN ID that omits the SA-Descriptor subtype with that SAID.

A CM MUST promiscuously forward all downstream group MAC (GMAC) destined traffic that is encrypted in an L2VPN SAID signaled to the CM, regardless of the GMAC destination of the packet.

The CM MUST NOT apply the multicast filtering or forwarding rules of [RFI 2.0] section 5.3.1.3.1 to downstream GMAC traffic encrypted in an L2VPN SAID. A CM MUST continue to implement downstream DOCSIS 2.0 group MAC forwarding rules for all unencrypted packets and packets encrypted in a non-L2VPN SAID.

A CM MUST NOT implement the IGMP Multicast Forwarding rules of [RFI 2.0] section 5.3.1.3.1 for any upstream packets (e.g., IGMP Membership Reports) classified to a forwarding L2VPN service flow. The CM MUST continue to implement DOCSIS IGMP Multicast Forwarding rules for upstream IGMP Membership Reports not classified to a forwarding L2VPN service flow.

A compliant CM MUST restrict bridge forwarding of downstream packets encrypted in an L2VPN SAID to only the bridge interfaces indicated with a '1' bit in the CM Interface Mask (CMIM) configured for that L2VPN. For example, the CM does not deliver downstream L2VPN traffic to the eCM or any eSAFE internal host if the CMIM omits that host interface (i.e., contains a '0' bit for that interface), even if the packet is addressed to the individual destination MAC address for the host. Likewise, the CM does not deliver L2VPN-labelled group MAC (GMAC) destined traffic to internal hosts when that L2VPN's CMIM omits the internal host interface.

A CM MUST support a classification rule criterion signaled with a CM Interface Mask (CMIM) in an L2VPN Encoding of an Upstream Classifier Packet Encoding, whether or not that Encoding classifies to a Forwarding L2VPN service flow. The CM MUST consider the criterion to be matched when the source MAC address of an upstream packet is for a host type with a '1' bit in the CM Interface Mask. The CM MUST consider the criterion to be unmatched and forward or drop a packet accordingly, when the source MAC address is for a host type with a '0' bit in the CM Interface Mask.

A CM MUST support the Downstream Unencrypted Traffic (DUT) Filtering feature as described in B.2, and advertise this in a DUT Filtering Capability Encoding B.1.3. When DUT Filtering is enabled, a CM MUST restrict bridge forwarding of downstream unencrypted traffic to only the interfaces indicated in the DUT CM Interface Mask (DUT CMIM) implied or configured by the DUT Filtering Encoding.

Because CMIM bit position 1 (corresponding to CM bridge ifIndex 1) represents the *set* of *all* CPE interfaces in L2VPN Forwarding, DUT Filtering, and Upstream Classifier Encodings, a compliant CM that implements more than one CPE interface MAY assign a CMIM bit position in the range of 5..15 to represent its single primary CPE interface. This is so that CMIM values (and other DOCSIS interface-specific filters) can represent the primary CPE interface by itself, independent of the set of all other CPE interfaces. The CM MUST continue to report only ifIndex 1 as its primary CPE interface.

A CM MUST forward upstream and downstream packets as large as 1522 bytes, which provides for a single subscriber 802.1Q tag on a maximum length Ethernet packet.

A CM MUST advertise the L2VPN Capability subtype of the Modem Capabilities Encoding A.3.1 of its Registration Request.

A CM with embedded eSAFE hosts MUST advertise them to the CMTS in a Registration Request message with an eSAFE Host Capability Encoding A.3.2 for each eSAFE host.

A CM MUST silently ignore an L2VPN Encoding in any TLV context not mentioned in this specification. A CM MUST silently ignore any unrecognized L2VPN Encoding subtype and process all recognized L2VPN Encodings normally.

Annex A CMTS DOCS-L2VPN-MIB Requirements (Normative)

A CMTS MUST implement the DOCS-L2VPN-MIB. A CM does not implement DOCS-L2VPN-MIB.

A.1 DOCS-L2VPN-MIB Conformance

Legend:

M	Mandatory
NA	Not Applicable
RO	Read-Only
RC	Read-Create

DOCS-L2VPN-MIB				
DocsL2vpnIdToIndexTable (Point-to-Point and Multipoint)				
Object	CM	Access	CMTS	Access
docsL2vpnIdToIndexIdx	NA	NA	M	RO
docsL2vpnIndexToIdTable (Point-to Point and Multipoint)				
Object	CM	Access	CMTS	Access
DocsL2vpnIndexToIdId	NA	NA	M	RO
docsL2vpnCmTable				
docsL2vpnCmCompliantCapability	NA	NA	M	RO
docsL2vpnCmDutFilteringCapability	NA	NA	M	RO
docsL2vpnCmDutCMIM	NA	NA	M	RO
docsL2vpnCmDhcpSnooping	NA	NA	M	RO
docsL2vpnVpnCmTable				
Object	CM	Access	CMTS	Access

docsL2vpnVpnCmDhcpSnooping	NA	NA	M	RO
docsL2vpnVpnCmCMIM	NA	NA	M	RO
docsL2vpnVpnCmVendorSpecific	NA	NA	M	RO
docsL2vpnVpnCmStatsTable (Point-to-Point and Multipoint)				
Object	CM	Access	CMTS	Access
docsL2vpnVpnCmStatsUpstreamPkts	NA	NA	M	RO
docsL2vpnVpnCmStatsUpstreamDiscards	NA	NA	M	RO
docsL2vpnVpnCmStatsDownstreamPkts	NA	NA	M	RO
docsL2vpnVpnCmStatsDownstreamDiscards	NA	NA	M	RO
docsL2vpnPortStatusTable (Point-to-Point and Multipoint)				
Object	CM	Access	CMTS	Access
docsL2vpnPortStatusSAID	NA	NA	M	RO
docsL2vpnSfStatusTable (Point-to-Point and Multipoint)				
Object	CM	Access	CMTS	Access
docsL2vpnSfStatusL2vpnId	NA	NA	M	RO
docsL2vpnSfStatusIngressUserPriority	NA	NA	M	RO
docsL2vpnSfStatusVendorSpecific	NA	NA	M	RO
docsL2vpnPktClassTable (Point-to-Point and Multipoint)				

Object	CM	Access	CMTS	Access
docsL2vpnPktClassL2vpnId	NA	NA	M	RO
docsL2vpnPktClassUserPriRangeLow	NA	NA	M	RO
docsL2vpnPktClassUserPriRangeHigh	NA	NA	M	RO
docsL2vpnPktClassCmim	NA	NA	M	RO
docsL2vpnPktClassVendorSpecific	NA	NA	M	RO
docsL2vpnCmNsiTable (Point-to-Point Only)				
Object	CM	Access	CMTS	Access
docsL2vpnCmNsiEncapSubtype	NA	NA	M	RO
docsL2vpnCmNsiEncapValue,	NA	NA	M	RO
docsL2vpnCmNsiAGI,	NA	NA	M	RO
docsL2vpnCmNsiSAII	NA	NA	M	RO
docsL2vpnCmVpnCpeTable (Multipoint Only)				
Object	CM	Access	CMTS	Access
docsL2vpnCmVpnCpeMacAddress	NA	NA	M	RO
docsL2vpnVpnCmCpeTable (Multipoint only)				
Objects	CM	Access	CMTS	Access
docsL2vpnVpnCmCpeMacAddress	NA	NA	M	RO
docsL2vpnDot1qTpFdbExtTable (Multipoint only)				
Objects	CM	Access	CMTS	Access

docsL2vpnDot1qTpFdbExtTransmitPkts	NA	NA	M	RO
docsL2vpnDot1qTpFdbExtReceivePkts	NA	NA	M	RO
docsL2vpnDot1qTpGroupExtTable (Multipoint only)				
Objects	CM	Access	CMTS	Access
docsL2vpnDot1qTpGroupExtTransmitPkts	NA	NA	M	RO
docsL2vpnDot1qTpGroupExtReceivePkts	NA	NA	M	RO

A.2 DOCS-L2VPN-MIB Definitions

```
DOCS-L2VPN-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Unsigned32,
    Integer32,
    Counter32                FROM SNMPv2-SMI

    TEXTUAL-CONVENTION,
    TruthValue,
    MacAddress               FROM SNMPv2-TC

    MODULE-COMPLIANCE,
    OBJECT-GROUP             FROM SNMPv2-CONF

    ifIndex                  FROM IF-MIB

    dot1dBasePort            FROM BRIDGE-MIB

    dot1qFdbId,
    dot1qTpFdbAddress,
    dot1qVlanIndex,
    dot1qTpGroupAddress      FROM Q-BRIDGE-MIB

    docsIfCmtsCmStatusIndex FROM DOCS-IF-MIB

    docsQosServiceFlowId,
    docsQosPktClassId        FROM DOCS-QOS-MIB

    clabProjDocsis           FROM CLAB-DEF-MIB;

docsL2vpnMIB MODULE-IDENTITY
    LAST-UPDATED  "200603280000Z"  -- March 28, 2006
    ORGANIZATION  "CableLabs"
    CONTACT-INFO
        "Postal: Cable Television Laboratories, Inc.
        858 Coal Creek Circle
        Louisville, Colorado 80027-9750
        U.S.A.
        Phone:  +1 303-661-9100
        Fax:   +1 303-661-9199
        E-mail: mibs@cablelabs.com"
    DESCRIPTION
        "This is the management MIB for devices complying to the
        DOCSIS L2VPN Feature."
    REVISION "200603280000Z"
    DESCRIPTION
        "Initial version."
    ::= { clabProjDocsis 8 }

--------------------------------------------------------------
--
-- Textual Conventions
--
DocsL2vpnIdentifier ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "255a"
    STATUS      current
    DESCRIPTION
            "An externally administered octet string identifying an
            L2VPN. An implementation MUST support a length of at least
            16 octets. The octet string is used as an index. As such,
            the CMTS enforces that objects of type DocsL2vpnIdentifier
            are unique per CMTS. An MSO is encouraged to define
            DocsL2vpnIdentifier values as globally unique."
    SYNTAX      OCTET STRING (SIZE(1..16))

DocsL2vpnIndex ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "An integer value locally generated by the agent for each
            known DocsL2vpnIdentifier administrative identifier. It is
            intended to be used as a short index for tables in this MIB
            module in lieu of an object of the type
            DocsL2vpnIdentifier."
    SYNTAX      Unsigned32 (0..4294967295)

DocsNsiEncapSubtype ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "An enumerated integer that defines the default
            encapsulation on NSI ports of an L2VPN-forwarded packet.
            A CMTS implementation MUST support ieee802.1q(2).
            A CMTS MAY omit support for all NSI  encapsulations
            other than ieee802.1q(2)."
    SYNTAX      INTEGER {
        other(1),
        ieee8021q(2),
        ieee8021ad(3),
        mpls(4),
        l2tpv3(5)
    }

DocsNsiEncapValue ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "The encapsulation value for L2VPN forwarded packets on NSI
            ports. The value of an object of this type depends on the
            value of an associated object of type DocsEncapSubtype:

            other(1): vendor specific,
            ieee8021q(2): 802.1Q tag with VLAN ID in lower 12 bits,
            ieee8021ad(3): pair of 16-bit values with service provider
            in lower 12 bits of the first 16-bit value and customer
            VLAN ID in the lower 12 bits of the second 16-bit value,
            mpls(4): must be zero length string,
            l2tpv3(5): must be zero length string."

    SYNTAX      OCTET STRING

-- Cable Modem Interface List

DocsL2vpnIfList ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "A object of this type indicates a set of CM
            MAC bridge interfaces, encoded as a BITS syntax with a ?1?
            Bit for each interface included in the set.

            Bit position eCM(0) represents a conceptual interface to
            the internal 'self' host MAC of the eCM itself. All other
            bit positions K correspond to CM MAC bridge port interface
            index with ifIndex value K.

            A BITS object is encoded as an OCTET STRING, which may have
            length zero. Bit position 0 is encoded in the most
            significant bit of the first octet, proceeding to
            bit position 7 in the least significant bit. Bit position 8
            is encoded in the most significant bit of the second octet,
            and so on.

            In a CM, ifIndex value 1 corresponds to the primary CPE
            interface. In CableHome devices, this interface is assigned
            to the embedded Portal Services (ePS) host interface, which
            provides a portal to the primary physical CPE interface.
            In many contexts of a DocsL2VpnIfList, a '1' in bit
            position 1 corresponds to 'any' or 'all' CPE interfaces
            when the CM contains more than one CPE interface.

            ifIndex value 2 corresponds to the docsCableMacLayer
            RF MAC interface.

            ifIndex values 3 and 4 correspond to the
            docsCableDownstream and docsCableUpstream interfaces,
            respectively, which are not separate MAC bridge port
            interfaces. Bit positions 3 and 4 are unused in this type;
            they must be saved and reported as configured, but
            otherwise ignored.

            ifIndex values 5 through 15 are reserved for individual
            CPE interfaces for devices that implement more than one
            CPE interface. In such devices, DocsL2vpnIfList bit
            position 1 corresponds to the set of all CPE interfaces.
            A CM with more than one CPE interface MAY assign a
            DocsL2vpnIfList bit position within the range of 5..15 to
            refer to the single primary CPE interface.

            ifIndex value 16 is assigned to any embedded Multimedia
            Terminal Adapter (eMTA) as defined by PacketCable.

            ifIndex value 17 is assigned to the IP management host
            interface of an embedded Set Top Box (eSTB). ifIndex value
            18 is reserved for the DOCSIS Set-top Gateway (DSG) traffic
            delivered to an eSTB.
            ifIndex values 19 through 31 are
            reserved for future defined embedded Service Application."
    SYNTAX      BITS {
        eCm(0),
        cmci(1),
        docsCableMacLayer(2),
        docsCableDownstream(3),
        docsCableUpstream(4),
        -- 5..15 reserved for other CPE interfaces
        eMta(16),
        eStbIp(17),
        eStbDsg(18)
        -- 19..31 reserved for other eSAFE interfaces
    }

---------------------------------------------------------------

-- Placeholder for notifications
--
docsL2vpnMIBNotifications OBJECT IDENTIFIER ::= { docsL2vpnMIB 0 }

--  None defined

--
-- L2VPN MIB Objects
--

docsL2vpnMIBObjects OBJECT IDENTIFIER ::= { docsL2vpnMIB 1 }

----------------------------------------------------------------------
--
-- Point-to-Point and Point-to-Multipoint
--
-- The following objects are required for both
-- Point-to-Point and Point-to-Multipoint operation.
--

----------------------------------------------------------------
--
-- L2VPN Identifier to L2VPN Index mapping table
--
docsL2vpnIdToIndexTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnIdToIndexEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Table indexed by the octet string DocsL2vpnIdentifier that
            provides the local agent's internally assigned docsL2vpnIdx
            value for that DocsL2vpnIdentifier value. The mapping of
            DocsL2vpnIdentifier to docsL2vpnIdx is 1-1. The agent
            must instantiate a row in both docsL2vpnIndexToIdTable and
            docsL2vpnIdToIndexTable for each known L2VPN Identifier."
    ::= { docsL2vpnMIBObjects 1 }

docsL2vpnIdToIndexEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnIdToIndexEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Maps a DocsL2vpnIdentifier octet string into the local
            agent's locally assigned docsL2vpnIdx value."
    INDEX { docsL2vpnId }
    ::= { docsL2vpnIdToIndexTable 1 }
```

```
DocsL2vpnIdToIndexEntry ::= SEQUENCE
    {
        docsL2vpnId            DocsL2vpnIdentifier,
        docsL2vpnIdToIndexIdx  DocsL2vpnIndex
    }

docsL2vpnId OBJECT-TYPE
    SYNTAX      DocsL2vpnIdentifier
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An externally configured octet string that identifies an
            L2VPN."
    ::= { docsL2vpnIdToIndexEntry 1 }

docsL2vpnIdToIndexIdx OBJECT-TYPE
    SYNTAX      DocsL2vpnIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "An internally assigned index value for a known L2VPN."
    ::= { docsL2vpnIdToIndexEntry 2 }

----------------------------------------------------------------
--
-- L2VPN Index to L2VPN Identifier mapping tables
--
docsL2vpnIndexToIdTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnIndexToIdEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Table indexed by agent's local docsL2vpnIdx that provides
            the global L2VPN Identifier. The mapping of docsL2vpnIdx to
            DocsL2vpnIdentifier is 1-1. The agent must instantiate a
            row in both docsL2vpnIndexToIdTable and
            docsL2vpnIdToIndexTable for each known L2VPN."
    ::= { docsL2vpnMIBObjects 2 }

docsL2vpnIndexToIdEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnIndexToIdEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Provides the L2VPN Identifier for each locally-assigned
            L2vpn Index."
    INDEX { docsL2vpnIdx }
    ::= { docsL2vpnIndexToIdTable 1 }

DocsL2vpnIndexToIdEntry ::= SEQUENCE
    {
        docsL2vpnIdx              DocsL2vpnIndex,
        docsL2vpnIndexToIdId      DocsL2vpnIdentifier
    }

docsL2vpnIdx OBJECT-TYPE
    SYNTAX      DocsL2vpnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An internally assigned index value for a known L2VPN."
    ::= { docsL2vpnIndexToIdEntry 1 }
```

```
docsL2vpnIndexToIdId OBJECT-TYPE
    SYNTAX      DocsL2vpnIdentifier
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "An administered octet string that externally identifies an
            L2VPN."
    ::= { docsL2vpnIndexToIdEntry 2 }

----------------------------------------------------------------------
--
-- L2VPN CM Table
--  Point-to-Point and Multipoint mode
--
docsL2vpnCmTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnCmEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table describes L2VPN per-CM information that
            is in common with all L2VPNs for the CM, regardless
            of forwarding mode."
    ::= { docsL2vpnMIBObjects 3 }

docsL2vpnCmEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnCmEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry is indexed by Cable Modem Index that
            describes L2VPN information for a single CM that is in
            common with all L2VPNs implemented by the CM,
            regardless of the L2VPN forwarding mode.

            An entry in this table is created for every CM that
            registers with a forwarding L2VPN encoding."
    INDEX { docsIfCmtsCmStatusIndex }
    ::= { docsL2vpnCmTable 1 }

DocsL2vpnCmEntry ::= SEQUENCE {
        docsL2vpnCmCompliantCapability      TruthValue,
        docsL2vpnCmDutFilteringCapability   TruthValue,
        docsL2vpnCmDutCMIM                  DocsL2vpnIfList,
        docsL2vpnCmDhcpSnooping             DocsL2vpnIfList
    }

docsL2vpnCmCompliantCapability OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object reports whether an L2VPN forwarding CM is
            compliant with the DOCSIS L2VPN specification, as reported
            in the L2VPN Capability encoding in the CM's registration
            request message.

            If the capability encoding was omitted, this object must
            report the value false(2)."
    ::= { docsL2vpnCmEntry 1 }

docsL2vpnCmDutFilteringCapability OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object reports whether an L2VPN forwarding CM is
            capable of Downstream Unencrypted Traffic (DUT) Filtering,
            as reported in the CM's registration request message.

            If the capability encoding was omitted, this object must
            report the value false(2)."
    ::= { docsL2vpnCmEntry 2 }

docsL2vpnCmDutCMIM OBJECT-TYPE
    SYNTAX      DocsL2vpnIfList
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object reports the value configured in a per-CM
            L2VPN Encoding for Downstream Unencrypted Traffic (DUT)
            Cable Modem Interface Mask (CMIM).

            The DUT CMIM is a bit string with a '1' for each bit
            position K for an internal or external CM interface with
            ifIndex K to which the CM permits DUT to be forwarded. A CM
            capable of DUT filtering MUST discard DUT to interfaces
            with a '0' in the DUT CMIM.

            If a CM's top-level registration request L2VPN Encoding
            contained no DUT CMIM subtype, this object is reported
            with its default value of a '1' in bit position 0
            (corresponding to the eCM's own 'self' host) and a '1' in
            each bit position K for which an eSAFE interface exists at
            ifIndex K. In other words, the default DUT CMIM includes
            the eCM and all eSAFE interfaces.

            This value is reported independently of whether the CM is
            actually capable of performing DUT filtering."
    ::= { docsL2vpnCmEntry 3 }

docsL2vpnCmDhcpSnooping OBJECT-TYPE
    SYNTAX      DocsL2vpnIfList
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object reports the value of the Enable DHCP Snooping
            subtype of a top-level L2VPN Encoding.

            It has the syntax of a CM Interface List bitmask and
            represents a set of CM MAC bridge interfaces
            corresponding to eSAFE hosts for which the CMTS is enabled
            to snoop DHCP traffic in order to learn the eSAFE host MAC
            address on that interface.

            Only bits corresponding to eSAFE host MAC addresses may be
            validly set in this object, including cpe(1) for ePS
            and the eSAFE interfaces in bits positions 16 through 31."
    ::= { docsL2vpnCmEntry 4 }

---------------------------------------------------------------------
--
-- L2VPN/CM Table
--  Point-to-Point and Multipoint mode
--
```

```
docsL2vpnVpnCmTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnVpnCmEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table describes the operation of L2VPN forwarding
            on each CM."
    ::= { docsL2vpnMIBObjects 4 }

docsL2vpnVpnCmEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnVpnCmEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry is indexed by VPN ID and Cable Modem Index that
            describes the operation of L2VPN forwarding for a single
            L2VPN on a single CM."
    INDEX { docsL2vpnIdx, docsIfCmtsCmStatusIndex }
    ::= { docsL2vpnVpnCmTable 1 }

DocsL2vpnVpnCmEntry ::= SEQUENCE {
        docsL2vpnVpnCmCMIM                DocsL2vpnIfList,
        docsL2vpnVpnCmIndividualSAId      Integer32,
        docsL2vpnVpnCmVendorSpecific      OCTET STRING
    }

docsL2vpnVpnCmCMIM OBJECT-TYPE
    SYNTAX      DocsL2vpnIfList
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A Cable Modem Interface Mask represents a set of
            MAC bridge interfaces within the CM. This object
            represents the CMIM within a forwarding per-SF L2VPN
            encoding, which specifies a set of CM MAC bridge
            interfaces to which L2VPN forwarding is restricted.

            If the CMIM Subtype is omitted from a forwarding
            per-SF encoding, its default value includes only
            cpePrimary(1) and cableMac(2), which can be encoded
            with a single octet with the value 0x60."
    ::= { docsL2vpnVpnCmEntry 1 }

docsL2vpnVpnCmIndividualSAId OBJECT-TYPE
    SYNTAX      Integer32 (0..16383)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The BPI+ Security Association ID in which traffic intended
            for point-to-point forwarding through an individual CM is
            forwarded.

            If the CMTS does not allocate an individual SAID for
            multipoint forwarding (as is recommended),it MUST
            report this object as zero."
    ::= { docsL2vpnVpnCmEntry 2 }

docsL2vpnVpnCmVendorSpecific OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object encodes the concatenation of all Vendor
```

```
                Specific Subtype encodings that appeared in any
                registration per-CM L2VPN Encoding associated with this
                entry."
    ::= { docsL2vpnVpnCmEntry 3 }

---------------------------------------------------------------------
--
-- L2VPN/CM Statistics Table
--  Point-to-Point and Multipoint mode
--
docsL2vpnVpnCmStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnVpnCmStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains statistics for forwarding of
            packets to and from a CM on each VPN."
    ::= { docsL2vpnMIBObjects 5 }

docsL2vpnVpnCmStatsEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnVpnCmStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry is indexed by VPN ID and Cable Modem Index."
    INDEX { docsL2vpnIdx, docsIfCmtsCmStatusIndex }
    ::= { docsL2vpnVpnCmStatsTable 1 }

DocsL2vpnVpnCmStatsEntry ::= SEQUENCE {
        docsL2vpnVpnCmStatsUpstreamPkts       Counter32,
        docsL2vpnVpnCmStatsUpstreamBytes      Counter32,
        docsL2vpnVpnCmStatsUpstreamDiscards   Counter32,
        docsL2vpnVpnCmStatsDownstreamPkts     Counter32,
        docsL2vpnVpnCmStatsDownstreamBytes    Counter32,
        docsL2vpnVpnCmStatsDownstreamDiscards Counter32
    }

docsL2vpnVpnCmStatsUpstreamPkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of L2vpn-forwarded packets received
            from this instance's Cable Modem on
            this instance's L2VPN."
    ::= { docsL2vpnVpnCmStatsEntry 1 }

docsL2vpnVpnCmStatsUpstreamBytes OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of L2vpn-forwarded bytes received
            from this instance's Cable Modem on
            this instance's L2VPN."
    ::= { docsL2vpnVpnCmStatsEntry 2 }

docsL2vpnVpnCmStatsUpstreamDiscards OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of L2-forwarded packets
            discarded from this instance's
            Cable Modem on this instance's VPN."
    ::= { docsL2vpnVpnCmStatsEntry 3 }

docsL2vpnVpnCmStatsDownstreamPkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of L2-forwarded packets
            transmitted to this instance's
            Cable Modem on this instance's VPN."
    ::= { docsL2vpnVpnCmStatsEntry 4 }

docsL2vpnVpnCmStatsDownstreamBytes OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of L2-forwarded bytes
            transmitted to this instance's
            Cable Modem on this instance's VPN."
    ::= { docsL2vpnVpnCmStatsEntry 5 }

docsL2vpnVpnCmStatsDownstreamDiscards OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of L2-forwarded packets that were discarded
            before they could be transmitted to this instance's
            Cable Modem on this instance's VPN."
    ::= { docsL2vpnVpnCmStatsEntry 6 }

----------------------------------------------------------------------
--
-- VPN Port Status Table
--  (Point-to-Point and Multipoint mode)
--
docsL2vpnPortStatusTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnPortStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table displays summary information for the
            run-time state of each VPN that is currently operating
            on each bridge port."
    ::= { docsL2vpnMIBObjects 6 }

docsL2vpnPortStatusEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnPortStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Information specific to the operation of L2VPN forwarding
            on a particular CMTS 'bridge port'. A CMTS 'bridge port'
            may be defined by the CMTS vendor, but is advantageously a
            single DOCSIS MAC Domain."
    INDEX { dot1dBasePort, docsL2vpnIdx }
    ::= { docsL2vpnPortStatusTable 1 }

DocsL2vpnPortStatusEntry ::= SEQUENCE {
        docsL2vpnPortStatusGroupSAId   Integer32
    }

docsL2vpnPortStatusGroupSAId OBJECT-TYPE
    SYNTAX      Integer32 (0..16383)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Group SAID associated with this VPN on a
            particular CMTS MAC domain. This SAID is used to encrypt
            all downstream flooded bridge traffic sent to CMs on
            this VPN and CMTS MAC domain bridge port.

            A value of '0' means there is no associated Group SAID for
            this VPN and bridge port, e.g., if the L2VPN uses
            point-to-point individual SAIDs only for forwarding.

            A bridge port that is not a CMTS MAC
            domain will report a value of '0'."
    ::= { docsL2vpnPortStatusEntry 1 }

----------------------------------------------------------------------
--
-- L2VPN Service Flow Status Table
--  (Point-to-Point and Multipoint mode)
--
-- This table has a row for each upstream SF with a per-SF L2VPN
-- Encoding.
--

docsL2vpnSfStatusTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnSfStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
           "This table displays SF-specific L2VPN forwarding status
           for each upstream service flow configured with a per-SF
            L2VPN Encoding.

            Objects which were signaled in a per-SF L2VPN Encoding but
            apply for the entire CM are shown in the
            docsL2vpnVpnCmTable."
    ::= { docsL2vpnMIBObjects 7 }

docsL2vpnSfStatusEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnSfStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "SF-specific L2VPN forwarding status information for each
            upstream service flow configured with a per-SF L2VPN
            Encoding. The ifIndex is of type docsCableMacLayer(127)."
    INDEX { ifIndex, docsQosServiceFlowId }
    ::= { docsL2vpnSfStatusTable 1 }

DocsL2vpnSfStatusEntry ::= SEQUENCE {
        docsL2vpnSfStatusL2vpnId              OCTET STRING,
        docsL2vpnSfStatusIngressUserPriority  Unsigned32,
        docsL2vpnSfStatusVendorSpecific       OCTET STRING
    }

docsL2vpnSfStatusL2vpnId OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object represents the value of the L2VPN Identifier
            subtype of a per-SF L2VPN Encoding."
    ::= { docsL2vpnSfStatusEntry 1 }

docsL2vpnSfStatusIngressUserPriority OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object provides the configured Ingress User Priority
            subtype of a per-SF L2VPN Encoding for this CM. If the
            subtype was omitted, this object's value is zero."
    ::= { docsL2vpnSfStatusEntry 2 }

docsL2vpnSfStatusVendorSpecific OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object provides the set of configured Vendor Specific
            subtypes within a per-SF L2VPN Encoding for a CM. If no
            Vendor Specific subtype was specified, this object is a
            zero length octet string. If one or more Vendor Specific
            subtype parameters was specified, this object represents
            the concatenation of all such subtypes."
    ::= { docsL2vpnSfStatusEntry 3 }

---------------------------------------------------------------------
--
-- L2VPN Classifier Table
--  (Point-to-Point and Multipoint mode)
--

docsL2vpnPktClassTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnPktClassEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table 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."
    ::= { docsL2vpnMIBObjects 8 }

docsL2vpnPktClassEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnPktClassEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry in this table extends a single row
            of docsQosPktClassTable for a rule that applies only to
            downstream L2VPN forwarded packets.
            The index ifIndex is an ifType of docsCableMaclayer(127)."
    INDEX {
        ifIndex,
        docsQosServiceFlowId,
        docsQosPktClassId
    }
    ::= { docsL2vpnPktClassTable 1 }

DocsL2vpnPktClassEntry ::= SEQUENCE {
        docsL2vpnPktClassL2vpnId           DocsL2vpnIdentifier,
        docsL2vpnPktClassUserPriRangeLow   Unsigned32,
        docsL2vpnPktClassUserPriRangeHigh  Unsigned32,
        docsL2vpnPktClassCMIM              DocsL2vpnIfList,
        docsL2vpnPktClassVendorSpecific    OCTET STRING
    }

docsL2vpnPktClassL2vpnId OBJECT-TYPE
    SYNTAX      DocsL2vpnIdentifier
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The locally assigned L2VPN index corresponding to the VPN
            Identifier subtype of a Downstream Classifier L2VPN
            Encoding."
    ::= { docsL2vpnPktClassEntry 1 }

docsL2vpnPktClassUserPriRangeLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The lower priority of the user Priority Range subtype
            of a Downstream Classifier L2VPN Encoding. If the subtype
            was omitted, this object has value 0."
    ::= { docsL2vpnPktClassEntry 2 }

docsL2vpnPktClassUserPriRangeHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The higher priority of the user Priority Range subtype
            of a Downstream Classifier L2VPN Encoding. If the subtype
            was omitted, this object has value 7."
    ::= { docsL2vpnPktClassEntry 3 }

docsL2vpnPktClassCMIM OBJECT-TYPE
    SYNTAX      DocsL2vpnIfList
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Cable Modem Interface Mask (CMIM) signaled in a
            Packet Classifier Encoding.  In a Downstream Packet
            Classifier Encoding, a specified CMIM value restricts the
            classifier to match packets with a Destination MAC address
            corresponding to the interfaces indicated in the CMIM mask.
            The eCM self and any eSAFE interface bits correspond to
            the individual eCM and eSAFE host MAC addresses.

            In an Upstream Packet Classifier encoding, a specified CMIM
            value restricts the classifier to match packets with an
            ingress bridge port interface matching the bits in the
            CMIM value.

            If the CMIM subtype was omitted, this object should be
            reported as a zero length octet string."
    ::= { docsL2vpnPktClassEntry 4 }

docsL2vpnPktClassVendorSpecific OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object provides the set of configured
            Vendor Specific subtypes within a Packet Classifier
            Encoding for a CM. If no Vendor Specific subtype was
            specified, this object is a zero length octet string.
            If one or more Vendor Specific subtype parameters was
            specified, this object represents the concatenation of all
            such subtypes."
    ::= { docsL2vpnPktClassEntry 5 }

----------------------------------------------------------------------
--
-- L2VPN CM NSI Table
--  Point-to-Point Only
--
docsL2vpnCmNsiTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnCmNsiEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table describes the NSI configuration for a single
            CM when operating in point-to-point forwarding mode for an
            L2VPN."
    ::= { docsL2vpnMIBObjects 9 }

docsL2vpnCmNsiEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnCmNsiEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry indexed by VPN ID and Cable Modem Index that
            describes the point-to-point forwarding between a single
            NSI encapsulation and a single CM. This table is
            implemented only for a CM forwarding an L2VPN on a
            point-to-point basis. It is associated with a single
            per-CM L2VPN encoding."
    INDEX { docsL2vpnIdx, docsIfCmtsCmStatusIndex }
    ::= { docsL2vpnCmNsiTable 1 }

DocsL2vpnCmNsiEntry ::= SEQUENCE {
        docsL2vpnCmNsiEncapSubtype        DocsNsiEncapSubtype,
        docsL2vpnCmNsiEncapValue          DocsNsiEncapValue,
        docsL2vpnCmNsiAGI                 OCTET STRING,
        docsL2vpnCmNsiSAII                OCTET STRING,
        docsL2vpnCmNsiTAII                OCTET STRING
    }

docsL2vpnCmNsiEncapSubtype OBJECT-TYPE
    SYNTAX      DocsNsiEncapSubtype
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The General Encapsulation Information (GEI) subtype of the
            Network System Interface (NSI) encapsulation configured
            for the CM."
    ::= { docsL2vpnCmNsiEntry 1 }

docsL2vpnCmNsiEncapValue OBJECT-TYPE
    SYNTAX      DocsNsiEncapValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The encapsulation value for L2VPN forwarded packets on NSI
            ports."
    ::= { docsL2vpnCmNsiEntry 2 }

docsL2vpnCmNsiAGI OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object is the configuration of any Attachment Group
            Identifier subtype in the per-SF L2VPN Encoding
            represented by this row. If the subtype was omitted, this
            object's value is a zero length string."
   ::= { docsL2vpnCmNsiEntry 3 }

docsL2vpnCmNsiSAII OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object is the configuration of any Source
            Attachment Individual ID subtype in the L2VPN Encoding
            represented by this row. If the subtype was omitted, this
            object's value is a zero length string."
    ::= { docsL2vpnCmNsiEntry 4 }

docsL2vpnCmNsiTAII OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object is the configuration of any Target
            Attachment Individual ID subtype in the L2VPN Encoding
            represented by this row. If the subtype was omitted, this
            object's value is a zero length string."
    ::= { docsL2vpnCmNsiEntry 5 }

----------------------------------------------------------------------
--
-- Point-to-Multipoint Only
--
-- The following objects are required for Point-to-Multipoint
-- operation only.
--
----------------------------------------------------------------------
--
-- Cable Modem/Vpn/CPE Table
--  (Point-to-Multipoint only)
--

docsL2vpnCmVpnCpeTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnCmVpnCpeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table is a list of CPEs, indexed by the VPNs on a
            Cable Modem."
    ::= { docsL2vpnMIBObjects 10 }

docsL2vpnCmVpnCpeEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnCmVpnCpeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
```

```
            "This table is a list of CPEs, indexed by the VPNs on a
            Cable Modem."
    INDEX { docsIfCmtsCmStatusIndex,
        docsL2vpnIdx,
        docsL2vpnCmVpnCpeMacAddress }
    ::= { docsL2vpnCmVpnCpeTable 1 }

DocsL2vpnCmVpnCpeEntry ::= SEQUENCE {
        docsL2vpnCmVpnCpeMacAddress   MacAddress
    }

docsL2vpnCmVpnCpeMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Customer Premise Equipment (CPE) Mac Address
            that is attached to this instances Cable Modem
            and bridging on this instance's VPN Id."
    ::= { docsL2vpnCmVpnCpeEntry 1 }

--------------------------------------------------------------------
--
-- VPN/Cable Modem/CPE Table
--  (Point-to-Multipoint only)
--
docsL2vpnVpnCmCpeTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnVpnCmCpeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains a list of bridging CPEs, indexed by
            L2VPN Index and the corresponding CMs on that VPN."
    ::= { docsL2vpnMIBObjects 11 }

docsL2vpnVpnCmCpeEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnVpnCmCpeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains a list of bridging CPEs, indexed by
            VPN and the corresponding CMs on that VPN."
    INDEX  { docsL2vpnIdx,
        docsIfCmtsCmStatusIndex,
        docsL2vpnVpnCmCpeMacAddress }
    ::= { docsL2vpnVpnCmCpeTable 1 }

DocsL2vpnVpnCmCpeEntry ::= SEQUENCE {
        docsL2vpnVpnCmCpeMacAddress   MacAddress
    }

docsL2vpnVpnCmCpeMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Customer Premise Equipment (CPE) Mac Address
            that is attached to this instances Cable Modem
            and bridging on this instance's L2vpn Index."
    ::= { docsL2vpnVpnCmCpeEntry 1 }

--------------------------------------------------------------------
--
```

```
-- dot1qTpFdbTable Extension
--  (Point-to-Multipoint only)
--
docsL2vpnDot1qTpFdbExtTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnDot1qTpFdbExtEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains packet counters for
            Unicast MAC Addresses within a VPN."
    ::= { docsL2vpnMIBObjects 12 }

docsL2vpnDot1qTpFdbExtEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnDot1qTpFdbExtEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table extends the dot1qTpFdbTable only for RF network
            bridge port entries.  It is implemented by an agent only
            if the agent implements dot1qTpFdbTable for RF network
            bridge ports."
    INDEX { dot1qFdbId, dot1qTpFdbAddress }
    ::= { docsL2vpnDot1qTpFdbExtTable 1 }

DocsL2vpnDot1qTpFdbExtEntry ::= SEQUENCE {
        docsL2vpnDot1qTpFdbExtTransmitPkts    Counter32,
        docsL2vpnDot1qTpFdbExtReceivePkts     Counter32
    }

docsL2vpnDot1qTpFdbExtTransmitPkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of packets where the Destination
            MAC Address matched this instance
            dot1qTpFdbAddress and packet was bridged on
            a VPN, where the VPN ID matched this
            instance's dot1qFdbId."
    ::= { docsL2vpnDot1qTpFdbExtEntry 1 }

docsL2vpnDot1qTpFdbExtReceivePkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of packets where the Source MAC
            Address matched this instance dot1qTpFdbAddress
            and the packet was bridged on a VPN,
            where the docsL2vpnIdx matched this instance's
            dot1qFdbId."
    ::= { docsL2vpnDot1qTpFdbExtEntry 2 }

--------------------------------------------------------------------
--
-- dot1qTpGroupTable Extension
--  (Point-to-multipoint only)
--
docsL2vpnDot1qTpGroupExtTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnDot1qTpGroupExtEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
```

```
            "This table contains packet counters for
            Multicast MAC Addresses within a VPN."
    ::= { docsL2vpnMIBObjects 13 }

docsL2vpnDot1qTpGroupExtEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnDot1qTpGroupExtEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table extends the dot1qTpGroupTable only for RF
            Network bridge port entries.  It is implemented by an agent
            Only if the agent implements dot1qTpGroupTable for RF
            network bridge ports."
    INDEX { dot1qVlanIndex, dot1qTpGroupAddress }
    ::= { docsL2vpnDot1qTpGroupExtTable 1 }

DocsL2vpnDot1qTpGroupExtEntry ::= SEQUENCE {
        docsL2vpnDot1qTpGroupExtTransmitPkts    Counter32,
        docsL2vpnDot1qTpGroupExtReceivePkts     Counter32
    }

docsL2vpnDot1qTpGroupExtTransmitPkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of packets where the Destination
            MAC Address matched this instance
            dot1qTpGroupAddress and packet was bridged on
            a VPN, where the docsL2vpnIdx matched this
            instance's dot1qVlanIndex."
    ::= { docsL2vpnDot1qTpGroupExtEntry 1 }

docsL2vpnDot1qTpGroupExtReceivePkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of packets where the Source MAC
            Address matched this instance dot1qTpGroupAddress
            and the packet was bridged on a VPN,
            where the docsL2vpnIdx matched this instance's
            dot1qVlanIndex."
    ::= { docsL2vpnDot1qTpGroupExtEntry 2 }

----------------------------------------------------------------------

--
-- Conformance definitions
--
docsL2vpnConformance  OBJECT IDENTIFIER ::= { docsL2vpnMIB 2 }
docsL2vpnCompliances  OBJECT IDENTIFIER ::= { docsL2vpnConformance 1 }
docsL2vpnGroups       OBJECT IDENTIFIER ::= { docsL2vpnConformance 2 }

docsL2vpnCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for the Cable Modem Termination
            Systems that implement the DOCSIS L2VPN Feature."

    MODULE    -- docsL2vpn
      -- conditionally mandatory groups
    GROUP docsL2vpnBaseGroup
    DESCRIPTION
            "Mandatory in all CMTSs."

    GROUP docsL2vpnPointToPointGroup
    DESCRIPTION
            "Mandatory in all CMTSs that implement point-to-point L2VPN
            forwarding."

    GROUP docsL2vpnMultipointGroup
    DESCRIPTION
            "Mandatory in all CMTSs that implement Multipoint
            L2VPN Forwarding Mode for any L2VPN."

    ::= { docsL2vpnCompliances 1 }

docsL2vpnBaseGroup OBJECT-GROUP
    OBJECTS {
        docsL2vpnIdToIndexIdx,
        docsL2vpnIndexToIdId,

        docsL2vpnCmCompliantCapability,
        docsL2vpnCmDutFilteringCapability,
        docsL2vpnCmDutCMIM,
        docsL2vpnCmDhcpSnooping,

        docsL2vpnVpnCmCMIM,
        docsL2vpnVpnCmVendorSpecific,
        docsL2vpnVpnCmIndividualSAId,

        docsL2vpnVpnCmStatsUpstreamPkts,
        docsL2vpnVpnCmStatsUpstreamBytes,
        docsL2vpnVpnCmStatsUpstreamDiscards,
        docsL2vpnVpnCmStatsDownstreamPkts,
        docsL2vpnVpnCmStatsDownstreamBytes,
        docsL2vpnVpnCmStatsDownstreamDiscards,

        docsL2vpnPortStatusGroupSAId,

        docsL2vpnSfStatusL2vpnId,
        docsL2vpnSfStatusIngressUserPriority,
        docsL2vpnSfStatusVendorSpecific,

        docsL2vpnPktClassL2vpnId,
        docsL2vpnPktClassUserPriRangeLow,
        docsL2vpnPktClassUserPriRangeHigh,
        docsL2vpnPktClassCMIM,
        docsL2vpnPktClassVendorSpecific
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects in common for both
            Point-to-Point and Multipoint L2VPN forwarding
            Modes."
    ::= { docsL2vpnGroups 1 }

docsL2vpnPointToPointGroup OBJECT-GROUP
    OBJECTS {
        docsL2vpnCmNsiEncapSubtype,
        docsL2vpnCmNsiEncapValue,
        docsL2vpnCmNsiAGI,
        docsL2vpnCmNsiSAII,
        docsL2vpnCmNsiTAII
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects in common for only the
            Point-to-Point forwarding mode."
    ::= { docsL2vpnGroups 2 }

docsL2vpnMultipointGroup OBJECT-GROUP
    OBJECTS {
        docsL2vpnCmVpnCpeMacAddress,

        docsL2vpnVpnCmCpeMacAddress,

        docsL2vpnDot1qTpFdbExtTransmitPkts,
        docsL2vpnDot1qTpFdbExtReceivePkts,

        docsL2vpnDot1qTpGroupExtTransmitPkts,
        docsL2vpnDot1qTpGroupExtReceivePkts
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects required only for Multipoint
            forwarding mode."
    ::= { docsL2vpnGroups 3 }
END
```

Annex B Parameter Encodings (Normative)

B.1 Capabilities

B.1.1 L2VPN Capability

This capability indicates whether the CM is compliant with the Layer 2 Virtual Private Network requirements for a CM that are specified in Section 7. L2VPN operation may still be performed with CMs that do not implement these requirements, but with possible limitations.

Type	Length	Value
5.17	1	0 CM not compliant with DOCSIS L2VPN Section 7 (default) 1 CM compliant with DOCSIS L2VPN Section 7

B.1.2 Embedded Service/Application Functional Entity (eSAFE) Host Capability

This capability encoding informs the CMTS of the type and MAC address of an eSAFE host embedded with the CM. This is necessary for the CMTS to guarantee proper IPv4 and (future) IPv6 forwarding of upstream traffic from the eSAFE host. A separate eSAFE Host Capability encoding is required for each separate eSAFE host embedded with the CM.

Type	Length	Value
5.18	7	eSAFE ifIndex (1 byte), eSAFE MAC address (6 bytes) eSAFE ifIndex: 1 ePS 15 eMTA 17 eSTB-IP 18 eSTB-DSG

B.1.3 Downstream Unencrypted Traffic (DUT) Filtering

This capability indicates whether the CM supports the DUT Filtering feature as described in section 6.5.2.1.

Type	Length	Value
5.19	1	0 DUT Filtering not supported (default) 1 DUT Filtering supported

B.2 Downstream Unencrypted Traffic (DUT) Filtering Encoding

The DUT Filtering parameter is intended for CMs implementing layer 2 or layer 3 Virtual Private Networks. In such networks, downstream traffic intended for the private network is always encrypted with BPI. Because the RF downstream is broadcast to all CMs, however, unencrypted group MAC traffic intended for *other* CMs will leak onto the VPN CM's CMCI ports unless filtered in the VPN CM. This parameter allows VPN CMs to filter all downstream unencrypted traffic, to both individual and group MAC destinations.

GEI-Encapsulated DUT Filtering Encoding:

Type	Length	Value
45	1..N	Byte 1 (DUT Control) Bit 0 = 0: Disable DUT Filtering (default) Bit 0 = 1: Enable DUT Filtering. Bits 1..7: Reserved. Bytes 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.

If the DUT Filtering Encoding is omitted, or the DUT filtering Encoding Control byte value is zero, then the CM bridges downstream unencrypted traffic, received from its RF interface (ifIndex 2) according to relevant DOCSIS specifications, namely forwarding unicast MAC traffic to the internal (eCM/eSAFE) or external (CPE) bridge port from which a source MAC was learned or configured and forwarding IGMP-learned or configured group MAC (GMAC) traffic to all other internal and external bridge ports.

If the DUT Filtering Encoding is present and the Enable DUT Filtering bit is set, the CM MUST restrict forwarding of downstream unencrypted traffic (for both individual and group MAC destinations) to only the set of interfaces indicated in a DUT CM Interface Mask (DUT CMIM) configured or implied by the encoding. An explicit DUT CMIM follows the DUT Control byte, and has the format as defined in B.3.4. Note that CMIM bit positions, as a BITS string, are numbered from left (most significant) to right (least significant), in the sequence of octets that represent the BITS string.

If no bytes follow the DUT Control Byte (i.e., the DUT Filtering Encoding has a length of only 1 byte), the implied DUT CMIM includes the eCM (CMIM bit position 0) and all implemented eSAFE interfaces on the CM (CMIM bit positions 16 and higher), but excludes all CPE interfaces. This implied DUT CMIM permits a cable operator to configure a DUT Filtering Encoding that is generic for all CM device types offering Transparent LAN Service.

B.3 L2VPN Encoding

The L2VPN Encoding parameter is a multi-part encoding that configures how the CMTS performs Layer 2 Virtual Private Network bridging for CPE packets. L2VPN operation is specified in Section 6.

An L2VPN Encoding is termed a per-SF L2VPN Encoding when it appears as a subtype of the Upstream Service Flow Encoding (type 24). The encoding is a Downstream Classifier L2VPN Encoding when it appears in a Downstream Packet Classification Configuration Setting (type 23). It is termed an Upstream Classifier L2VPN encoding when it appears in an Upstream Packet Classification Configuration Setting (type 22).

A Forwarding L2VPN Encoding is one that contains an L2VPN VPNID subtype that configures forwarding of packets on a particular L2VPN.

The L2VPN Encoding is encoded as General Extension Information (GEI) ([RFI 2.0] C.1.1.17.1) as a Vendor Specific encoding with vendor ID 0xFFFFFF. GEI subtype 5 is assigned for L2VPN Encodings.

GEI-Encapsulated L2VPN Encoding:

Type	Length	Value
43.5	n	L2VPN subtype/length/value tuples

The L2VPN Encoding itself contains one or more L2VPN subtype encodings.

B.3.1 VPN Identifier

The VPN Identifier (VPNID) subtype encoding is an opaque octet string identifier that associates an attachment circuit (i.e., a CM or one SF of a CM) or a Downstream Classifier to a particular layer 2 virtual private network. VPN ID values are advantageously configured as printable ASCII strings. VPNID values are unique within a single CMTS. VPNID values are advantageously configured as unique across *all* CMTSs within the administrative domain of the cable operator operating the CMTS. VPNID values can be configured to be *globally* unique in order to facilitate inter-domain L2VPN forwarding.

For scaleability, a cable operator can configure VPNID strings to algorithmically map to globally-unique binary octet strings. Examples of globally-unique binary octet strings for VPNs include the 7-byte VPN ID format described in [RFC 2685] and the 8-byte Route Distinguisher described in [RFC 2547]. A single VPNID subtype is present in valid Forwarding L2VPN Encodings.

In general, multiple attachment circuits (i.e., CM/SFs) can connect to the same L2VPN, and so would be configured with the same VPNID subtype value. If the CMTS performs only point-to-point L2VPN forwarding for the indicated L2VPN to an NSI port, it enforces that the L2VPN Encoding also contains an NSI Encapsulation Subtype.

A CMTS performing Multipoint L2VPN Forwarding MUST perform transparent learning layer 2 forwarding between 802.1Q bridge ports, cable modems, and service flows configured with the same VPNID.

In per-SF L2VPN Encodings, the VPNID identifies the L2VPN on which upstream traffic is to be forwarded. In Downstream Classifier L2VPN Encodings within a Downstream Packet Classification Setting, the VPNID configures the classifier to apply to only L2VPN-forwarded downstream traffic on the L2VPN identified by the VPNID.

A CMTS SHOULD use the value of the VPNID with any signaling protocols that dynamically determine Service Multiplexing field values on L2VPN packets encapsulated on an NSI port. The VPNID is intended to be (or map to) the attachment group identifier (AGI) for IETF L2VPN working group signaling protocols.

The CMTS MUST support configuration of VPNID values of at least 16 octets, and no more than 255 octets. The number of unique VPNID values supported by the CMTS is vendor-specific.

Sub-Type	Length	Value
43.5.1	1..N	An opaque octet string that identifies a Layer 2 Virtual Private Network. N is vendor specific, but must be within the range 16..255.

B.3.2 NSI Encapsulation Subtype

At a minimum, this subtype is required only to specify how the CMTS encapsulates Point-to-Point L2VPN-forwarded packets on a single Selected Ethernet NSI port, primarily for L2VPN feature certification testing. It is intended, however, to also standardize cable operator configuration of IETF Pseudo Wire Emulation [RFC 3985] of each cable attachment circuit (CM or SF) across the NSI backbone.

In Selected Ethernet mode, the CMTS is configured to forward all L2VPN traffic through a single Ethernet NSI port at any given time. When a Selected Ethernet Port is identified, the CMTS MUST accept the IEEE 802.1Q NSI Encapsulation Format Code in Forwarding L2VPN Encodings and MAY accept the other codes.

Although the NSI Encapsulation Subtype is intended primarily for Point-to-Point forwarding modes, the CMTS MAY accept it in Multipoint mode (including in the Selected Ethernet mode). In this case, the CMTS MUST enforce that L2VPN Encodings with the same VPN Identifier subtype that include an NSI Encapsulation Subtype MUST all have the same NSI Encapsulation Subtype encoding value.

The value of the NSI Encapsulation Subtype is a single Format Code-Length-Value tuple that identifies an NSI Encapsulation Format Code and possibly, an NSI Encapsulation Service Multiplexing value.

Sub-Type	Length	Value
43.5.2	n	A single NSI encapsulation format code/length/value tuple

If the NSI Encapsulation Subtype or an L2VPN Vendor Specific Subtype does not statically configure a Service Multiplexing value, the CMTS MUST dynamically select and learn the Service Multiplexing value for a forwarding L2VPN Encoding from the CMTS's L2VPN peers across the NSI interface. Dynamically learned Service Multiplexing values may be different on different NSI ports.

NSI Encapsulation Format Code	Length	Service Multiplexing Value
43.5.2.1	0	Other: The L2VPN NSI Encapsulation format is other than those specified below. In this case, L2VPN Vendor Specific Subtype Encodings (GEI Subtype 5.43) MUST provide the NSI Encapsulation Format and any desired static Service Multiplexing values.
43.5.2.2	2	IEEE 802.1Q. Value is the 16-bit IEEE 802.1Q tag (most significant byte first) that contains, in its least significant 12 bits, a VLAN ID used to recognize packets for the L2VPN on the Selected Ethernet NSI port. The most significant 4 bits of the 16-bit tag value are reserved. The CMTS SHOULD ignore the most significant 4 bits of the 16-bit NSI Encapsulation IEEE 802.1Q tag value. The maximum number of unique VLAN ID values accepted by a CMTS is vendor specific. A CMTS MUST accept the full 12-bit range of VLAN ID values for the unique values it does accept.
43.5.2.3	4	IEEE 802.1ad. Value is a pair of 16-bit values (most significant byte first), with the first 16-bit field containing a Service Provider VLAN ID in the least significant 12 bits, and the second 16-bit field containing the Customer VLAN ID in the least significant 12 bits. The most significant 4 bits of each 16-bit value are reserved. The maximum number of Service Provider and Customer VLAN ID values the CMTS accepts is vendor specific, but the CMTS MUST accept the full 12-bit range of VLAN ID values.
43.5.2.4	5 or 17	MPLS Peer. Value is a one-byte InetAddressTypeCode (ipv4(1) or ipv6(2)) followed by an IPv4 or IPv6 InetAddress. The attachment circuit's L2VPN traffic is intended to forward over an MPLS label switched path to the peer. The CMTS SHOULD dynamically select and learn the label stack for incoming and outgoing label stacks, respectively. The CMTS MAY use Vendor Specific L2VPN Subtypes to statically configure the ingress and egress label stacks. The CMTS MAY limit statically configured MPLS label values to a vendor-specific range.
43.5.2.5	5 or 17	L2TPv3 Peer. Value is a one-byte InetAddressTypeCode (ipv4(1) or ipv6(2)) followed by an IPv4 or IPv6 InetAddress. The attachment circuit's L2VPN traffic is intended to forward within an L2TPv3 tunnel to the addressed peer. The CMTS SHOULD dynamically select and learn the local and remote session IDs for each tunnel. The CMTS MAY use Vendor Specific L2VPN Subtypes to statically configure session IDs, L2TPv3 peer network addresses, and other information as required by the vendor. The CMTS MAY limit statically configured session ID or other Service Multiplexing values to a vendor-specific range.

B.3.3 eSAFE DHCP Snooping

This parameter is defined only in a per-SF forwarding L2VPN encoding. The parameter is a bit mask with bit positions defined for each potential eSAFE host type. A '1' in the eSAFE host type's bit position enables the CMTS to automatically detect the MAC address of that eSAFE host by snooping DHCP traffic forwarded between the CM and a DHCP server. The bit positions in the eSAFE DHCP Snooping parameter match those of the CM Interface Mask (CMIM) for the interface associated with the eSAFE host type.

SubType	Length	Value
43.5.3	1..N	Bit mask of eSAFE hosts enabled for DHCP Snooping Bit 1 (0x40 00 00): CableHome Embedded Portal Services (ePS) Bit 16 (0x00 00 80) PacketCable-EMTA Bit 17 (0x00 00 40) eSTB-IP Bit 18 (0x00 00 20) eSTB-DSG Bits 19..31 (0x00 00 1F FF) Other eSAFE interfaces

B.3.4 CM Interface Mask (CMIM) Subtype

This parameter is a bit mask that describes a set of eCM interface indexes [eDOCSIS]. In a Forwarding L2VPN Encoding, the CM Interface Mask Subtype describes the set of bridge port interfaces on which the CM forwards packets of the L2VPN.

Each bit of CMIM corresponds to a logical bridge port interface of a MAC layer 2 bridge implemented in the eCM of a cable modem. The parameter is encoded as the octet string of the Basic Encoding Rules encoding of an SNMP BITS bit string. Bit position K in the BITS encoding corresponds to eDOCSIS MAC bridge interface K. By convention, bit position 0 corresponds to the eCM's self host interface. The eCM self MAC address is signaled as if it were on a bridge port interface ifIndex of zero (0), even though no such interface actually exists.

SubType	Length	Value
43.5.4	N	SNMP BITS -encoded bit map with bit position K representing eCM logical interface index value K. Bit position 0 represents the eCM self host itself. Bit position 0 is the most significant bit of the first octet. Refer to [eDOCSIS] for latest logical interface index assignments. Bit 0 (0x80): eCM self host interface Bit 1 (0x40): primary CPE Interface (also ePS) Bit 2 (0x20) RF interface Bits 3,4 reserved Bits 5..15 (0x07 FF) Other CPE Interfaces Bits 16-31, embedded logical interfaces. Currently defined interfaces include: Bit 16 (0x00 00 80) PacketCable-EMTA Bit 17 (0x00 00 40) eSTB-IP Bit 18 (0x00 00 20) eSTB-DSG Bits 19..31 (0x00 00 1F FF) Other eSAFE interfaces

If the CM Interface Mask subtype is not present in a Forwarding L2VPN Encoding, its default value is for the Primary CPE Interface (index 1) and the cable RF interface (index 2) only, i.e., CMIM value 0x60. A CM MUST silently ignore CMIM bit positions for unimplemented interfaces. A CMTS MAY signal that a CMIM value represents all possible CPE interfaces with the CMIM value for positions 1 and 5-15, i.e., the CMIM value 0x47 FF.

B.3.5 Attachment Group ID

If present, the CMTS SHOULD use this subtype value as the Attachment Group ID (AGI) signaling element, associated with a VPN Identifier, when dynamically establishing an NSI pseudowire for Point-to-Point forwarding of the attachment circuit. It is applicable only in conjunction with MPLS or L2TPv3 NSI Encapsulation and Point-to-Point forwarding between the attachment circuit and the pseudowire.

SubType	Length	Value
43.5.5	0..16	Opaque byte string that identifies the CM or SF as an attachment circuit for IETF Layer 2 VPN signaling protocols.

B.3.6 Source Attachment Individual ID

If present, the CMTS SHOULD use this subtype value as the source attachment individual identifier (SAII) signaling element associated with the local pseudowire attachment when establishing an NSI backbone pseudowire for the cable attachment circuit. It is applicable only in conjunction with an MPLS or L2TPv3 NSI Encapsulation subtype and Point-to-Point forwarding between the cable attachment circuit and the pseudowire.

SubType	Length	Value
43.5.6	0..16	Opaque byte string signaled as SAII circuit for IETF Layer 2 VPN signaling protocols.

B.3.7 Target Attachment Individual ID

If present, the CMTS SHOULD use this subtype value as the target attachment individual identifier (TAII) signaling element associated with the remote pseudowire attachment when establishing an NSI PseudoWire for the attachment circuit. It is applicable only in conjunction with an MPLS or L2TPv3 NSI Encapsulation subtype and Point-to-Point forwarding between the cable attachment circuit and the pseudowire.

SubType	Length	Value
43.5.7	0..16	Opaque byte string that identifies the CM or SF as an attachment circuit for IETF Layer 2 VPN signaling protocols.

B.3.8 Ingress User Priority

IEEE 802.1 bridging protocols require the detection or generation, optional regeneration, and signaling of a user priority attribute of all bridged packets. The Ingress User Priority subtype is used to configure the incoming IEEE 802.1 user priority of upstream L2VPN packets. It is defined in only upstream per-SF Forwarding L2VPN Encodings.

Unless the L2VPN forwarder is otherwise configured, CMTS MUST transmit the ingress priority signaled with this subtype as the user priority bits of an IEEE 802.1Q tag when it forwards the packet to an NSI port with IEEE 802.1Q encapsulation. If this subtype is omitted in a Forwarding L2VPN Encoding, the CMTS considers the incoming user priority to be zero (0). This subtype appears no more than once in a valid Forwarding L2VPN Encoding.

SubType	Length	Value
43.5.8	1	Ingress IEEE 802.1 user priority value in the range 0..7 encoded in the least significant three bits. Higher values indicate higher priority.

B.3.9 User Priority Range

In a Downstream Packet Classification Encoding, the presence of an L2VPN Encoding with this subtype restricts the classifier to only packets forwarded downstream with the indicated range of user priority values (inclusive). The classified user priority is as transmitted on the DOCSIS MAC layer interface, and so is considered to be *after* any ingress default user priority selection or user priority regeneration performed by the L2VPN Forwarder. This subtype may appear only in a Downstream Classifier L2VPN Encoding, and at most, once in single L2VPN Encoding. If this subtype is omitted, the classifier applies to all egress user priority values.

SubType	Length	Value
43.5.9	2	Pri-low, pri-high. 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.

B.3.10 L2VPN SA-Descriptor Subtype

The CMTS adds this subtype in downstream Registration Response and Dynamic Service messages that contain forwarding L2VPN Encodings to inform an L2VPN-compliant CM of the SAID value(s) under which the CMTS will encrypt the downstream traffic forwarded to that L2VPN through the CM. A valid L2VPN Encoding may have multiple L2VPN SA-Descriptor Subtypes.

SubType	Length	Value
43.5.10	N	SA-Descriptor encoding as specified in [BPI-PLUS] that provides the SAID value under which the CMTS encrypts downstream traffic forwarded an L2VPN. The SA-Type of the SA-Descriptor must be Dynamic.

B.3.11 Vendor Specific L2VPN Subtype

This subtype is interpreted by the CMTS in a vendor-specific fashion. An example usage is to configure the NSI sub-interface or virtual circuit to which upstream packets from the CM or SF are bridged in a Point-to-Point mode. The vendor-specific subtype contents can be binary or ASCII encoded data.

GEI Type	Length	Value
43.5.43	N	08, 3, vendor ID, following by vendor-specific type/length/value tuples.

B.4 Confirmation Codes

This section defines new confirmation codes for L2VPN operation. It extends the list of confirmation codes in section C.4 of [RFI 2.0].

Additional Confirmation Codes defined for the DOCSIS L2VPN feature include:

- reject-VLAN-ID-in-use(26): indicates that an IEEE802.1q or IEEE802.1ad VLAN-ID requested for the NSI encapsulation of L2VPN traffic is already assigned for use by non-L2VPN traffic. See Section 6.2.5.
- reject-multipoint-L2VPN(27): indicates that Multipoint L2VPN forwarding mode is not supported and a CM is attempting to configure more than one L2VPN attachment circuit to the same L2VPN. See Section 6.2.5.
- reject-multipoint-NSI(28): indicates that a multipoint forwarding L2VPN contained multiple L2VPN encodings with different NSI encapsulation values.

B.5 L2VPN Error Encoding

This encoding provides additional information from the CM when it rejects an L2VPN Encoding signaled by the CMTS. The CM MUST include an L2VPN Error Encoding in its MAC management response when it rejects an L2VPN Encoding in a REG-RSP, DSA-REQ, DSA-RSP, DSC-REQ or DSC-RSP.

GEI Type	Length	Value
43.5.254	N	L2VPN Error Encoding, consisting of exactly one L2VPN Errored Parameter encoding, exactly one L2VPN Error Code encoding, and zero or one L2VPN Error Message encoding.

B.5.1 L2VPN Errored Parameter

This parameter provides a sequence of Type and Subtypes that identify the location and subtype of the L2VPN Encoding that is rejected. A valid L2VPN Error Encoding contains exactly one L2VPN Errored Parameter type string.

GEI Type	Length	Value
43.5.254.1	N	Sequence of Type and Subtypes

The type/subtype sequence starts at the top level of TLV encodings of the MAC Management Message that included the L2VPN Encoding. This sequence depends on the location of the L2VPN encoding, as described in section 6.2. In particular:

- An L2VPN Error Parameter string for a top-level L2VPN Encoding starts with two bytes for the GEI Type code for the L2VPN Encoding, or (43.5);
- An L2VPN Error Parameter string for an Upstream Service Flow Encoding starts with the type code for that encoding (24) followed by the L2VPN Encoding GEI Type, or (24.43.5);
- An L2VPN Error Parameter string for a Downstream Packet Classification Configuration Setting starts with the type for that encoding (23) followed by the L2VPN Encoding GEI Type, or (23.43.5);
- An L2VPN Error Parameter string for an Upstream Packet Classification Configuration Setting starts with the type for that encoding (22) followed by the L2VPN Encoding GEI Type, or (22.43.5).

If the entire L2VPN Encoding is rejected, the CM MAY include in the L2VPN Error Parameter type string only the two or three bytes that identify the location of a full L2VPN Encoding. If the reason for rejection is due to a particular subtype of the L2VPN Encoding, the CM SHOULD include additional bytes in the L2VPN Error Parameter type string to identify the particular subtype of the L2VPN Encoding that it rejected. One reason for rejecting an entire L2VPN encoding is that the maximum number of L2VPNs supported by the CM has been exceeded. One reason for rejecting a particular subtype, e.g., the L2VPN SA-Descriptor Subtype Encoding, it that the number of SAIDs supported by the CM has been exceeded.

B.5.2 L2VPN Error Code

This parameter provides a confirmation code as defined from section C.4 of [RFI 2.0] to identify a reason why an L2VPN Encoding or subtype was rejected. A valid L2VPN Error Encoding contains exactly one L2VPN Confirmation code

GEI Type	Length	Value
43.5.254.2	1	Confirmation Code

B.5.3 L2VPN Error Message

This parameter, if present, provides a message for display on the CMTS console log for the reason for the rejection. A CM SHOULD include this parameter in an L2VPN Error Encoding. A valid L2VPN Error Encoding contains zero or one L2VPN Error Message subtypes.

GEI Type	Length	Value
43.5.254.3	N	Zero-terminated string of ASCII characters.

B.6 CM Interface Mask Classification Criteria

This specification defines a generic mechanism for classifying upstream and downstream traffic based on the ingress or intended egress logical interface ports on the CM.

In an Upstream Packet Classifier Encoding (type 22), the CM Interface Mask Subtype defines a rule criteria for matching the ingress interface of an L2PDU.

In a Downstream Packet Classifier Encoding (type 23), the CM Interface Mask Subtype defines a rule criteria for matching a unicast downstream destination MAC address. In either case, the CMIM Subtype encoding within a Packet Classifier Encoding applies to both L2VPN and non-L2VPN traffic.

Each bit of CMIM corresponds to a logical bridge port interface of a MAC layer 2 bridge implemented in the eCM of a cable modem. The parameter is encoded as the octet string of the Basic Encoding Rules encoding of an SNMP BITS bit string. Bit position K in the BITS encoding corresponds to eDOCSIS MAC bridge interface K. By convention, bit position 0 corresponds to the eCM's self host interface (i.e., the CM’s IP stack) The eCM self MAC address is signaled as if it were on a bridge port interface ifIndex of zero (0), even though no such interface actually exists.

SubType	Length	Value
[22/23].13	N	SNMP BITS -encoded bit map with bit position K representing eCM logical interface index value K. Bit position 0 represents the eCM self host itself. Bit position 0 is the most significant bit of the first octet. The Embedded DOCSIS specification [eDOCSIS] defines the interface index assignments. For information purposes, current assignments include: Bit 0 (0x80): eCM self host interface Bit 1 (0x40): primary CPE Interface (also ePS) Bit 2 (0x20) RF interface Bits 3,4 reserved Bits 5..15 (0x07 FF) Other CPE Interfaces Bits 16-31, Logical CPE Interfaces for eSAFE hosts. Current assignments include: Bit 16 (0x00 00 80) PacketCable-EMTA Bit 17 (0x00 00 40) eSTB-IP Bit 18 (0x00 00 20) eSTB-DSG Bits 19..31 (0x00 00 1F FF) Other eSAFE interfaces

In an Upstream Classifier Encoding, a CM MUST silently ignore bit positions for unimplemented interfaces. For example, an upstream CMIM classifier criteria intended to match only external CPE interfaces of a CM has a CMIM mask value setting bits 1 and 5-15, i.e., an encoding of 0x47 FF.

In a Downstream Classifier Encoding, that includes a CMIM criteria, the CMTS checks the destination MAC address to determine whether it is the CM’s self host MAC address or a recognized eSAFE host MAC address. Any other unicast MAC address is considered to be a CPE MAC address. The CMTS does not know on what particular CPE interface the CM has learned a CPE MAC address. The CMTS considers only bit 1 of the CMIM to match a CPE MAC address in a Downstream Packet Classifier Encoding. The maximum number of eSAFE destination MAC addresses recognized by a CMTS is vendor specific.

Appendix I Example L2VPN Encodings (informative)

The L2VPN Encoding is always encapsulated using a General Extension Information (GEI) encoding, which uses the type code 43 with the reserved Vendor ID of 0xFFFFFF.

I.1 Point-to-Point Example

This section describes L2VPN Encodings for three CMs performing point-to-point L2VPN forwarding of all traffic on their default upstream service flow. Two of the CMs are externally bridged to the same enterprise (L2VPN ID 0234560001); one of the CMs is bridged to a separate enterprise (L2VPN ID 0234560002). The example is depicted below:

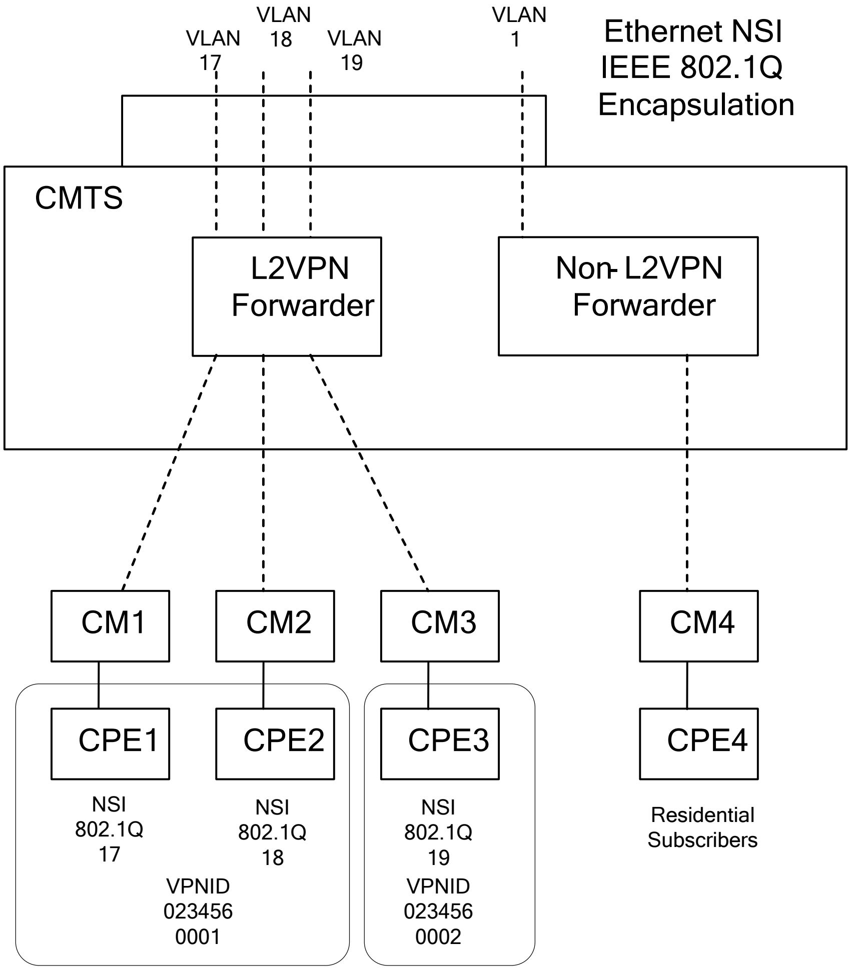

Figure I–1 - Point-To-Point L2VPN Traffic Forwarding Example

Table I–1 - Point-to-Point CM1 L2VPN Encoding

Point-to-Point CM1 Configuration File				
43				Per-CM L2VPN Encoding
20				Overall length
	08 03 FFFFFF			Vendor ID : 0xFFFFFF for GEI
	05			GEI 43.5 for L2VPN Encoding
	13			Length of GEI.5 Subtype
		01 05 x0234560001		VPNID Subtype
		02		NSI Encapsulation Subtype
		04		Length of GEI.5.2 Subtype
			02	IEEE 802.1Q Format Subtype
			02	Length of GEI.5.2.2 Subtype
			0x0011	VLAN ID 17
24				Upstream Service Flow Encoding
19				Length
	6			QOS Param Set Type Subtype
	1			
		0x07		
	43			Vendor-Specific Subtype:
	14			Overall length
		08 03 FFFFFF		Vendor ID for GEI
		05		GEI 43.5 for L2VPN Encoding
		7		Length of GEI.5 Subtype
			01 05 x0234560001	VPNID Subtype
45				DUT Filtering:
01				Overall Length
	01			DUT Filtering enabled

Table I–2 - Point-to-Point CM2 L2VPN Encoding

Point-to-Point CM2 Configuration File				
43				Per-CM L2VPN Encoding
20				Overall length
	08 03 FFFFFF			Vendor ID : 0xFFFFFF for GEI
	05			GEI 43.5 for L2VPN Encoding
	13			Length of GEI.5 Subtype
		01 05 x0234560001		VPNID Subtype
		02		NSI Encapsulation Subtype
		04		Length of GEI.5.2 Subtype
			02	IEEE 802.1Q Format Subtype
			02	Length of GEI.5.2.2 Subtype
			0x0012	VLAN ID 18
24				Upstream Service Flow Encoding
19				Length
	6			QOS Param Set Type Subtype
	1			
		0x07		
	43			Vendor-Specific Subtype:
	14			Overall length
		08 03 FFFFFF		Vendor ID for GEI
		05		GEI 43.5 for L2VPN Encoding
		7		Length of GEI.5 Subtype
			01 05 x0234560001	VPNID Subtype
45				DUT Filtering:
01				Overall Length
	01			DUT Filtering enabled

CPE2 is externally bridged to the same L2VPN as CPE1 (VPNID x0234560001), but all L2VPN forwarding for CPE2 occurs on the NSI IEE 802.lQ VLAN ID 18.

Table I–3 - Point-to-Point CM3 L2VPN Encoding

Point-to-Point CM3 Configuration File				
43				Per-CM L2VPN Encoding
20				Overall length
	08 03 FFFFFF			Vendor ID : 0xFFFFFF for GEI
	05			GEI 43.5 for L2VPN Encoding
	13			Length of GEI.5 Subtype
		01 05 x0234560002		VPNID Subtype
		02		NSI Encapsulation Subtype
		04		Length of GEI.5.2 Subtype
			02	IEEE 802.1Q Format Subtype
			02	Length of GEI.5.2.2 Subtype
			0x0013	VLAN ID 19
24				Upstream Service Flow Encoding
19				Length
	6			QOS Param Set Type Subtype
	1			
		0x07		
	43			Vendor-Specific Subtype:
	14			Overall length
		08 03 FFFFFF		Vendor ID for GEI
		05		GEI 43.5 for L2VPN Encoding
		7		Length of GEI.5 Subtype
			01 05 x0234560002	VPNID Subtype
45				DUT Filtering:
01				Overall Length
	01			DUT Filtering enabled

I.2 Multipoint Example

This section provides an example of L2VPN encodings for Multipoint forwarding, as depicted below. For Multipoint forwarding, the NSI encapsulation for an L2VPN may be configured in either of two ways:

- As CMTS vendor specific configuration; or
- In the CM configuration file of one or more of the CMs in the L2VPN.

In the example below, the NSI encapsulation for each L2VPN appears in the CM configuration file for all CMs.

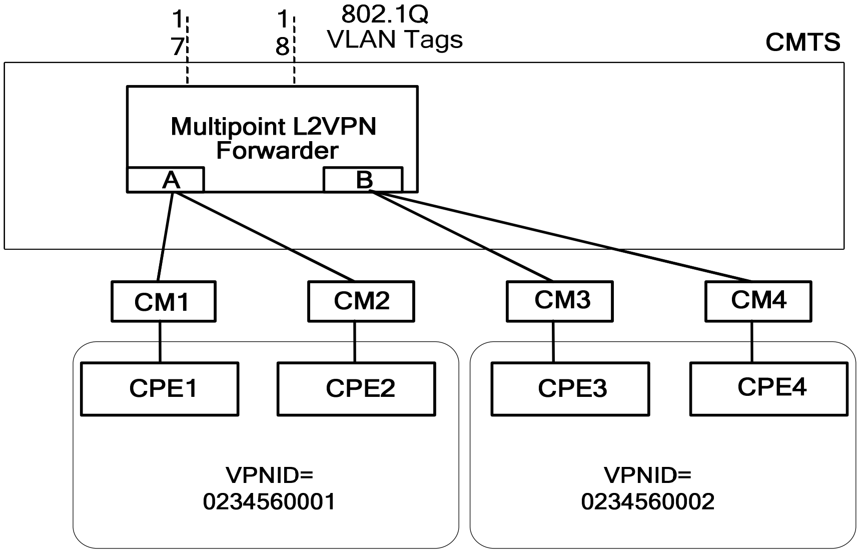

Figure I–2 - Multipoint L2VPN Forwarding of Traffic Example

Table I–4 - Multipoint CM1 L2VPN Encoding

Multipoint CM1 Config File				
43				Per-CM L2VPN Encoding
20				Overall length
	08 03 FFFFFF			Vendor ID : 0xFFFFFF for GEI
	05			GEI 43.5 for L2VPN Encoding
	13			Length of GEI.5 Subtype
		01 05 x0234560001		VPNID Subtype
		02		NSI Encapsulation Subtype
		04		Length of GEI.5.2 Subtype
			02	IEEE 802.1Q Format Subtype
			02	Length of GEI.5.2.2 Subtype
			0x0011	VLAN ID 17
24				Upstream Service Flow Encoding
19				Length
	6			QOS Param Set Type Subtype
	1			
		0x07		
	43			Vendor-Specific Subtype:
	14			Overall length
		08 03 FFFFFF		Vendor ID for GEI
		05		GEI 43.5 for L2VPN Encoding
		7		Length of GEI.5 Subtype
			01 05 x0234560001	VPNID Subtype
45				DUT Filtering:
01				Overall Length
	01			DUT Filtering enabled

Table I–5 - Multipoint CM2 L2VPN Encoding

Multipoint CM2 Config File				
43				Per-CM L2VPN Encoding
20				Overall length
	08 03 FFFFFF			Vendor ID : 0xFFFFFF for GEI
	05			GEI 43.5 for L2VPN Encoding
	13			Length of GEI.5 Subtype
		01 05 x0234560001		VPNID Subtype
		02		NSI Encapsulation Subtype
		04		Length of GEI.5.2 Subtype
			02	IEEE 802.1Q Format Subtype
			02	Length of GEI.5.2.2 Subtype
			0x0011	VLAN ID 17
24				Upstream Service Flow Encoding
19				Length
	6			QOS Param Set Type Subtype
	1			
		0x07		
	43			Vendor-Specific Subtype:
	14			Overall length
		08 03 FFFFFF		Vendor ID for GEI
		05		GEI 43.5 for L2VPN Encoding
		7		Length of GEI.5 Subtype
			01 05 x0234560001	VPNID Subtype
45				DUT Filtering:
01				Overall Length
	01			DUT Filtering enabled

Note: The L2VPN Encodings for Multipoint CM2 are exactly the same as for CM1.

Table I–6 - Multipoint CM3 L2VPN Encoding

Multipoint CM3 Config File				
43				Per-CM L2VPN Encoding
20				Overall length
	08 03 FFFFFF			Vendor ID : 0xFFFFFF for GEI
	05			GEI 43.5 for L2VPN Encoding
	13			Length of GEI.5 Subtype
		01 05 x0234560002		VPNID Subtype
		02		NSI Encapsulation Subtype
		04		Length of GEI.5.2 Subtype
			02	IEEE 802.1Q Format Subtype
			02	Length of GEI.5.2.2 Subtype
			0x0012	VLAN ID 18
24				Upstream Service Flow Encoding
19				Length
	6			QOS Param Set Type Subtype
	1			
		0x07		
	43			Vendor-Specific Subtype:
	14			Overall length
		08 03 FFFFFF		Vendor ID for GEI
		05		GEI 43.5 for L2VPN Encoding
		7		Length of GEI.5 Subtype
			01 05 x0234560002	VPNID Subtype
45				DUT Filtering:
01				Overall Length
	01			DUT Filtering enabled

Table I–7 - Multipoint CM4 L2VPN Encoding

Multipoint CM4 Config File				
43				Per-CM L2VPN Encoding
20				Overall length
	08 03 FFFFFF			Vendor ID : 0xFFFFFF for GEI
	05			GEI 43.5 for L2VPN Encoding
	13			Length of GEI.5 Subtype
		01 05 x0234560002		VPNID Subtype
		02		NSI Encapsulation Subtype
		04		Length of GEI.5.2 Subtype
			02	IEEE 802.1Q Format Subtype
			02	Length of GEI.5.2.2 Subtype
			0x0012	VLAN ID 18
24				Upstream Service Flow Encoding
19				Length
	6			QOS Param Set Type Subtype
	1			
		0x07		
	43			Vendor-Specific Subtype:
	14			Overall length
		08 03 FFFFFF		Vendor ID for GEI
		05		GEI 43.5 for L2VPN Encoding
		7		Length of GEI.5 Subtype
			01 05 x0234560002	VPNID Subtype
45				DUT Filtering:
01				Overall Length
	01			DUT Filtering enabled

Note: The L2VPN Encoding for Multipoint CM4 is the same as for CM3.

I.3 Upstream L2VPN Classifier Example

This example shows classifying upstream traffic from a specific CPE1 onto an upstream L2VPN service flow, where all other CPEs attached to the CM forward to the non-L2VPN forwarder, as depicted below.

Table I–8 - Upstream L2VPN Classifier Encoding

Upstream L2VPN Classifier Cable Modem Config File				
43				Per-CM L2VPN Encoding
20				Overall length
	08 03 FFFFFF			Vendor ID : 0xFFFFFF for GEI
	05			GEI 43.5 for L2VPN Encoding
	13			Length of GEI.5 Subtype
		01 05 x0234560003		VPNID Subtype
		02		NSI Encapsulation Subtype
		04		Length of GEI.5.2 Subtype
			02	IEEE 802.1Q Format Subtype
			02	Length of GEI.5.2.2 Subtype
			0x0019	VLAN ID 25
24				Default Upstream Service Flow Encoding
07				Length
	01 02 0001			Service Flow Reference 0001
	06 01 07			QOS Param Set Type Subtype
24				L2VPN Upstream Service Flow Encoding
19				Length
	06 01 07			QOS Param Set Type Subtype
	43			Vendor-Specific Subtype:
	14			Overall length
		08 03 FFFFFF		Vendor ID for GEI
		05		GEI 43.5 for L2VPN Encoding
		7		Length of GEI.5 Subtype
			01 05 x0234560003	VPNID Subtype
22				Upstream Classifier Encoding
14				Length
	03 02 0001			Service Flow Reference to 0001
	10			Ethernet/LLC Packet Classification
	8			
		02		Source MAC Address
		6		Length
			x0001020000AA	MAC Address of CPE1

45				DUT Filtering:
01				Overall Length
	01			DUT Filtering enabled

Appendix II IEEE 802.1Q Encapsulation (informative)

This appendix provides background information on the format of IEEE 802.1Q tags on Ethernet side NSI interfaces. This is the standard mechanism for indicating the VLAN of a bridged packet on an Ethernet interface. A CMTS compliant with this specification is required to support recognition of IEEE 802.lQ encapsulation on an Ethernet interface when configured to do so.

Because the CMTS interprets the VLAN ID of the outermost 802.1Q tag of a packet coming into an NSI, the tag is called a service-delimiting tag.

The L2VPN Forwarder *strips* the service-delimiting IEEE 802.1Q tag from an Ethernet packet when forwarding it downstream, and *inserts* the service-delimiting IEEE 802.1Q tag when forwarding packets upstream. The particular VLAN to which an L2VPN packet belongs is explicitly indicated on an 802.1Q-encapsulated Ethernet interface, and is always implied when forwarded on the DOCSIS RF MAC interface.

This stripping and inserting of IEEE 802.1Q tags is depicted below:

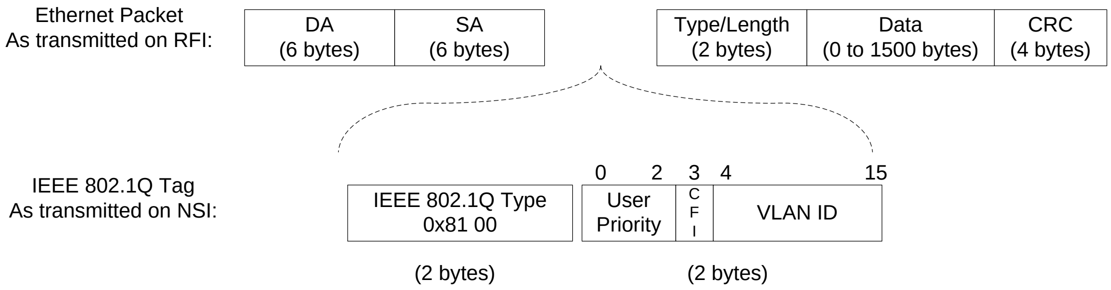

Figure II–1 - Ethernet 802.1Q Tags

An Ethernet packet is tagged with an IEEE 802.1Q tag by inserting four bytes between its original Source Address (SA) and original Length/Type field. The two-byte Ethernet Type code 0x8100 indicates that a 16-bit IEEE 802.1Q Tag follows. The tag value consists of a 3 bit user priority field in the most significant 3 bits, a Canonical Format Indicator (CFI) bit, and a 12-bit VLAN ID in the least significant bits. Operation of the CFI bit is defined by the IEEE, and is zero for Ethernet MAC addresses. All multi-byte fields are transmitted most significant byte first.

The User Priority field indicates a traffic forwarding priority in the range 0..7, with higher values indicating higher priority.

This specification permits, but does not require, the CMTS to use NSI port encapsulations other than IEEE 802.1Q to signal the L2VPN or attachment circuit for an L2VPN-forwarded packet. The particular NSI encapsulation used for L2VPN forwarding is intended to be configured in the NSI Encapsulation Subtype of an L2VPN Encoding.

Appendix III Embedded VLAN CM Bridging Model (informative)

This appendix proposes an Embedded VLAN model for CM internal packet bridge forwarding for consideration by the DOCSIS community. It is not currently a requirement for L2VPN certification on a CM.

The L2VPN specification uses the concept of a CM Interface Mask (CMIM) to define the set of internal and external bridge interfaces to which the CM may bridge downstream traffic. The CMIM, for example, defines the broadcast domain of both individual and group MAC-addressed downstream traffic. A broadcast domain is one interpretation of a virtual LAN, so in effect, the CMIM is defining an internal VLAN of the internal and external ports to which DUT and L2VPN traffic are forwarded.

The Embedded VLAN model expands the MAC Bridge of the eDOCSIS model to become a VLAN-capable MAC bridge with separate embedded VLAN (eVLAN) MAC forwarding domains. By using the concept of an eVLAN, the CM is able to isolate the eCM and eSAFE hosts from the MAC broadcast domains of customer private L2VPNs.

The following Figure III–1 depicts the Embedded VLAN Model for L2VPN-compliant CMs.

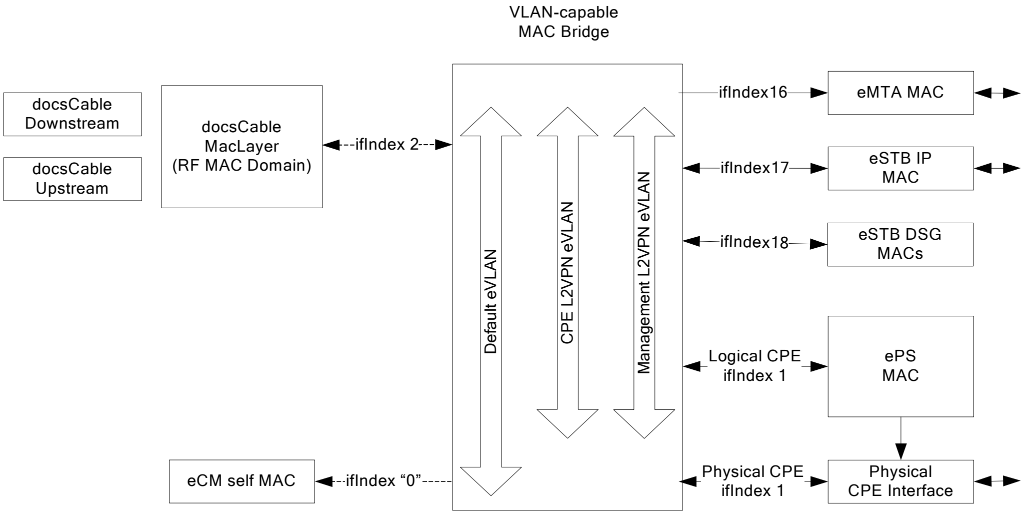

Figure III–1 - L2VPN Embedded VLAN (eVLAN) Model

The MAC Bridge of an embedded CM is considered to have a bridge port interface to the RF MAC Domain interface as ifIndex 2, and a Primary CPE bridge port interface at ifIndex 1. DOCSIS defines the operation of CPE forwarding by a residential CM as a layer-2 MAC bridging function between the RF interface and the CPE interface. In eDOCSIS, the eCM's own MAC address (its self MAC) is considered internal to the MAC bridge, and reachable by all bridge port interfaces.

The eDOCSIS specification defines an embedded Service/Application Functional Entity (eSAFE) as an entity co-located with an embedded Cable Modem (eCM) that contains its own MAC and IP address [eDOCSIS]. Currently defined eSAFEs include:

- PacketCable Embedded MTA (eMTA) host
- CableHome embedded Portal Services (ePS) host
- ESTB Embedded Set Top Box

Each of these eSAFE devices is considered to have a separate Logical CPE Interface to the MAC bridge, and is assigned a separate Interface Index (ifIndex) for management and control purposes. In the eDOCSIS architecture, the eCM's MAC Bridge is assumed to implement a single forwarding database, associating MAC addresses to each Logical CPE interface, and forwarding Layer 2 Protocol Data Units (L2PDUs) between all ports of the MAC bridge, according to the Destination MAC (DMAC) address of the L2PDU. The RF Interface, CPE interface(s), eCM MAC, and all eSAFE MACs are considered to be in the same layer 2 MAC broadcast domain, (i.e., on a single LAN).

The L2VPN specification will expand this architecture by introducing the concept of embedded VLANs (eVLANs) within the eCM's MAC bridge, where eVLANs have different sets of logical CPE ports. In order to control access to the eCM's self MAC address, (e.g., to isolate it from customer L2VPN access), the eCM MAC is considered to reside on a self-bridge port interface.

The L2VPN architecture introduces the concept of a Cable Modem Interface Mask (CMIM), with a bit position for each logical bridge port in the eCM's eVLAN-capable MAC Bridge. Each eVLAN in the MAC Bridge contains a CMIM value that represents which logical bridge ports belong to the eVLAN. The CMIM is represented as an SNMP BITS object encoding, where bit position K corresponds to bridge port interface ifIndex K. In a CMIM mask, the logical Self bridge port is assigned bit position 0 (i.e., as if it had ifIndex value 0). No ifStack entry is created for the Self bridge interface, because zero is an invalid value for an ifIndex value.

In the eCM's MAC Bridge, all non-L2VPN forwarding is considered to be bridged on a Default eVLAN that has a CMIM, with all interface bits set to 1. This corresponds to the normal, single-LAN MAC bridge forwarding defined before this L2VPN specification.

Separate eVLANs, however, may be defined with *subsets* of the eCM bridge port interfaces for independent layer 2 forwarding. In particular, customer Transparent LAN Service (TLS) is implemented by defining an eVLAN for the subscriber's L2VPN that contains only the RF Interface and the CPE Interface; a customer's TLS L2VPN is not permitted to access the eCM or any eSAFE hosts.

The eVLAN model allows a cable operator to implement Management L2VPNs for the eCM and eSAFE traffic, by defining an L2VPN with a CMIM that bridges only the RF interface, and the eCM self and/or eSAFE logical bridge interfaces.

III.1 IEEE802.1Q and Embedded VLAN Model

The operation and management of a MAC layer bridge with multiple VLANs is standardized with the [IEEE 802.1Q] specification. IEEE 802.1Q was first standardized in 1998 and has a standards-track MIB [RFC 2674]. The CMIM of an L2VPN can be considered to define the dot1qVlanCurrentEgressPorts bit mask of RFC 2674. If the eVLAN concept is adopted as the DOCSIS CM layer 2 forwarding model, RFC 2674 already defines a rich set of objects for reporting and controlling CM layer 2 operation.

The IEEE 802.1Q specification was significantly upgraded in 2003 by including many interim IEEE 802.1 extensions (including IEEE 802.1p). At the time of this specification, the MIB for the expanded IEEE 802.1Q-2003 is still in IETF draft form [ID-BRIDGE].

Adopting the eVLAN forwarding model allows future DOCSIS specifications to clearly separate RF interface operation from the layer 2 filtering, forwarding, and replication to the various internal and external physical interfaces on CM-based DOCSIS devices.

[IEEE 802.1Q] is extremely general purpose and sophisticated, and as a result, is also extremely complex. The specification is 327 pages long, and its draft MIB is 106 pages. Implementing even the minimum functions specified for compliance to the IEEE 802.1Q specification, or the minimum required objects for [RFC 2547], is far more functionality and control than appropriate for the embedded MAC bridge of an L2VPN-compliant CM.

And yet, the extensive capabilities and MIBs developed by the IEEE for multiple-VLAN bridging can and should serve as a model for the future enhancement of CM layer 2 forwarding specifications. The eVLAN concept has the power to represent all of the current eDOCSIS forwarding models and can cleanly represent the L2 forwarding models for future DOCSIS specifications for IPv6 forwarding and IP multicast enhancements. IEEE802.1Q-20003, for example, defines standard management objects for performing IP protocol based VLAN classification and even individual source MAC based VLAN classification.

This specification therefore uses IEEE 802.1Q and RFC2674 as informational-only conceptual guidelines for the required functionality of an L2VPN-compliant CM (and CMTS, for that matter). Future versions of this (and other) specifications may add additional layer 2 forwarding functions, and IEEE 802.1Q and the IETF [ID-BRIDGE] should serve as a guide for defining those functions.

As an example, the current L2VPN specification deals only with untagged packets on the eCM's logical bridge port interfaces. On the RF interface, the particular L2VPN (or as IEEE 802.1Q terms it, the particular VLAN) for an L2PDU is always *implied* at the CMTS or CM ingress MAC Domain by the upstream service flow or downstream SAID. Future versions of this specification may introduce the concept of IEEE 802.1Q service delimiting tags on the RF Interface and/or on the CPE interface of the eCM MAC Bridge. In this case, the future specification should use concepts and MIB objects as already standardized by the industry with IEEE 802.1Q and the IETF.

III.2 Embedded Bridge MAC Domain Service Primitives

Because of the Service Flow capabilities of a DOCSIS RF MAC Domain, an eCM's MAC Bridge is defined to provide the following conceptual service to the RF MAC Domain:

- Downstream (RF MAC Domain to Bridge):
  M_UNITDATA.request (
      L2PDU,
      eVLAN,
      user_priority)
- Upstream (Bridge to RF MAC Domain):
  M_UNITDATA.indication (
      L2PDU,
      eVLAN,
      user_priority,
      ingress_port)

Where:

- L2PDU is an (untagged) Ethernet PDU with DMAC, SMAC, EtherType, and 0 to 1500 bytes of L2 payload.
- eVLAN is a local identifier for a particular eVLAN;
- user_priority is an 8-valued priority for layer 2 forwarding of the L2PDU, as defined by [IEEE 802.1Q].
- ingress_port is the bridge's logical ifIndex value from which the L2PDU was received.

Downstream eCM bridge packet forwarding proceeds as follows:

1. The CM's MAC Domain (CM-MD) subcomponent receives a DOCSIS PDU from its docsCableDownstream interface that contains a non-MAC management L2PDU. The DOCSIS PDU may contain a BPI Extended Header or a Downstream Service Extended Header.
2. If the packet was encrypted with an L2VPN SAID, the CM-MD sets the requested bridge eVLAN to the one it created for the L2VPN; otherwise, the CM-MD sets the requested eVLAN to the Default eVLAN;
3. If the packet included a Downstream Service ID (DSID) that identifies the downstream service flow, the CM-MD sets the requested user_priority to the Traffic Priority parameter of the DS SF; otherwise, the CM-MD sets the requested user_priority to zero (0).

4. The CM-MD requests the MAC Bridge to forward the L2PDU on the requested eVLAN with the requested user_priority.
5. The MAC Bridge forwards the packet to an egress logical bridge port, according to the permitted egress ports as indicated in the CMIM for the eVLAN. It may flood the packet to multiple bridge ports.
6. If the MAC Bridge forwards the L2PDU to a physical CPE physical interface bridge port, it implements at least two IEEE 802.1Q Traffic Classes in order to provide QOS prioritized forwarding of layer 2 packets. CMs may implement from two to eight (8) traffic classes.
7. If the MAC Bridge forwards the L2PDU to the internal CableHome Portal Services (ePS) with a user_priority derived from a DS service flow Traffic Priority, the ePS uses this value as its Traffic Importance Number of the packet. This avoids an ePS re-classification of the packet with its cabhQos2PolicyTable MIB.

Upstream eCM bridge packet forwarding proceeds as follows:

1. The CPE physical interface receives an L2PDU. The CPE physical interface requests the eCM MAC Bridge to forward the packet with user_priority 0 and the Default eVLAN.
2. Alternatively, an internal eSAFE device may request the MAC bridge to forward an L2PDU with an explicit user_priority and eVLAN value.
3. The MAC bridge indicates an L2PDU to be transmitted to the CM MAC Domain (CM-MD) subcomponent with an indicated eVLAN, ingress interface, and user_priority.
4. The CM-MD uses the eVLAN to select a set of Upstream Packet Classifiers; the default eVLAN will select the non-L2VPN classifiers, while any other eVLAN will select the L2VPN Upstream Packet Classifiers only for the corresponding L2VPN.
5. The CM-MD uses the indicated ingress port to match classifier rules with a CMIM criterion, and uses the indicated user_priority to match classifier rules with a User Priority Range criterion. These criteria apply to both L2VPN and non-L2VPN forwarding.
6. The CM-MD classifies the L2PDU to an upstream service flow and forwards the packet to the docsCableUpstream interface.

At this time, the L2VPN specification requires such packets to be considered to have a received user_priority of zero (0). Future versions of this specification may implement various [IEEE 802.1Q] mechanisms for explicitly signaling (with priority-only tags), implicitly configuring (with default ingress user_priority), and regenerating the ingress user-priority.

Rather than modeling an ePS as directly outputting to the physical CPE port, the model should be modified to have the ePS transmit to a separate CableHome CPE eVLAN that includes only the ePS and physical CPE bridge ports. The Traffic Importance Number determined by the ePS becomes the user_priority of the ePS's request to transmit on the CableHome CPE eVLAN. This model makes it clear how CableHome (and any other future Layer 3 CPE forwarder) can share the physical CPE port with other forwarders to the physical CPE port in the eCM, while still maintaining QOS prioritization.

Appendix IV L2VPN Non-compliant CM Restrictions (informative)

The L2VPN service is primarily implemented at the CMTS. An operator can deploy L2VPN service using a compliant CMTS and non-compliant CMs. The restrictions when using non-compliant CMs are:

- L2VPN subscribers with non-compliant DOCSIS 1.1 and later CMs may not observe transparent forwarding of IP multicasts. This is especially troublesome when OSPF and RIPv2 advertisements are not forwarded to subscriber premise routers. Non-compliant DOCSIS 1.1 and 2.0 CMs still enforce IP Multicast forwarding rules, and so will block downstream forwarding of unjoined IP multicast groups. However, DOCSIS 2.0 CMs that implement the Static Multicast MAC parameter may be programmed to forward the desired multicast traffic. Non-compliant DOCSIS 1.0 CMs will not drop this multicast traffic. Some CM vendors also offer proprietary configurations to promiscuously forward all downstream IP multicasts.
- Unencrypted non-L2VPN layer 2 non-unicasts will leak onto L2VPN CPE networks. See section IV.1 for a further description of this issue.
- Non-compliant CMs may not forward maximum-sized packets with a subscriber tag; i.e., of length 1522 bytes. Stacked or Tag-in-tag operation may not be possible with such CMs.
- Non-compliant CMs cannot exclude downstream L2VPN traffic from reaching the IP stacks of the embedded CMs and embedded eSAFE hosts of the L2VPN's CMs.

Note: *upstream* traffic from the eCMs and (usually) eSAFE hosts is blocked, preventing bi-directional unauthorized access.

- Non-compliant CMs cannot join L2VPNs dynamically, i.e., via dynamic service flow messages initiated by the CMTS after registration. Non-compliant CMs must be statically configured to join all required L2VPNs based on the L2VPN Encodings configured in their CM configuration file or on the CMTS.

IV.1 Leaking through non-compliant CMs

This specification does not specify any mechanism to prevent the leakage of non-L2VPN unencrypted traffic through *non-compliant* CMs configured for L2VPN forwarding. Table IV–1 summarizes the conditions under which downstream non-L2VPN non-unicasts can leak into a subscriber's CPE network, when a non-compliant CM is configured for L2VPN forwarding.

Table IV–1 - Non-L2VPN leaking through Non-compliant CMs configured for L2VPN

Downstream Traffic Type	DIME	
	Enabled	Disabled
Arp/DHCP Broadcasts (unencrypted)	Leaks	Leaks
Unjoined IP Multicasts, e.g., RIPv2, OSPF. (unencrypted)	DOCSIS 1.0 CM: Leaks DOCSIS 1.1 CM: Blocked	DOCSIS 1.0 CM: Leaks DOCSIS 1.1 CM: Blocked
Joined IP Multicast (encrypted when DIME enabled)	Blocked	DOCSIS 1.0 CM: Leaks DOCSIS 1.1 CM: Blocked
DSG (unencrypted always)	DOCSIS 1.0 CM: Leaks DOCSIS 1.1 CM: Blocked	DOCSIS 1.0 CM: Leaks DOCSIS 1.1 CM: Blocked

Note: Leaking of the unencrypted non-L2VPN broadcast traffic (ARPs and DHCP) onto an L2VPN subscriber's network is usually not a major issue for the subscriber, because such traffic is relatively low. The high-volume joined IP multicast traffic is blocked even through non-compliant CMs when it is encrypted. Even the unencrypted multicast leaking through non-compliant DOCSIS 1.0 CMs can be avoided with appropriate IP filters in the DOCSIS 1.0 CM's configuration file.

Appendix V Acknowledgements (Informative)

Michael Patrick, Motorola
Harsh Parandekar, Cisco
Erich Arnold, Arris
Shengyou Zeng, Cisco
Stuart Hoggan, CableLabs
Kevin Luehrs, CableLabs