

SCTE • ISBE[®]

S T A N D A R D S

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 136-1 2019

**Layer 2 Virtual Private Networks for IP Cable Modem
Systems**

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called “documents”) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long-term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE•ISBE members.

SCTE•ISBE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE•ISBE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE•ISBE web site at <http://www.scte.org>.

All Rights Reserved
© Society of Cable Telecommunications Engineers, Inc. 2019
140 Philips Road
Exton, PA 19341

Note: DOCSIS® is a registered trademark of Cable Television Laboratories, Inc., and is used in this document with permission.

Contents

1	INTRODUCTION	7
1.1	Requirements	7
1.2	Conformance	7
1.3	Conventions	8
2	REFERENCES	9
2.1	Normative References	9
2.1.1	<i>SCTE References</i>	9
2.1.2	<i>Standards from Other Organizations</i>	9
2.1.3	<i>Published Materials</i>	10
2.2	Informative References	10
2.3	<i>SCTE References</i>	10
2.4	<i>Standards from Other Organizations</i>	10
2.1	Published Materials	11
3	TERMS AND DEFINITIONS	12
4	ABBREVIATIONS AND ACRONYMS.....	14
5	THEORY OF OPERATION (INFORMATIVE).....	19
5.1	L2VPN Features.....	19
5.1.1	<i>Transparent LAN Service</i>	19
5.1.2	<i>Multiple ISP L2VPNs</i>	21
5.1.3	<i>Management L2VPNs</i>	21
5.1.4	<i>Other L2VPN-enabled Features</i>	22
5.1.5	<i>High Availability</i>	22
5.2	CMTS Layer 2 Forwarding Architecture.....	23
5.2.1	<i>L2VPN and Non-L2VPN Forwarding</i>	23
5.2.2	<i>Point-to-Point and Multipoint L2VPN Forwarding Modes</i>	24
6	L2VPN OPERATION (NORMATIVE).....	27
6.1	CMTS Bridging Model Requirements.....	27
6.2	Configuring L2VPN Forwarding	27
6.2.1	<i>VPNID Subtype</i>	30
6.2.2	<i>Downstream Classifier L2VPN Encoding</i>	30
6.2.3	<i>L2VPN SA-Descriptor Subtype</i>	31
6.2.4	<i>Vendor-Specific L2VPN Encoding</i>	31
6.2.5	<i>Configuration Error Requirements</i>	32
6.2.6	<i>Network System Interface (NSI) Encapsulation</i>	32
6.2.7	<i>Virtual Private LAN Service (VPLS) and Virtual Private Wire Service</i>	34
6.3	CMTS Upstream L2VPN Forwarding.....	38
6.4	CMTS Downstream L2VPN Forwarding.....	39
6.4.1	<i>Multipoint Downstream Forwarding</i>	40
6.4.2	<i>DOCSIS 3.0 L2VPN Downstream Multicast Forwarding</i>	40
6.5	L2VPN Isolation and Privacy	41
6.5.1	<i>Protecting L2VPN Traffic</i>	41
6.5.2	<i>Preventing Leaking of non-L2VPN Traffic</i>	42
6.6	CM and eSAFE Exclusion.....	43
6.6.1	<i>CM and eSAFE Host Forwarding Model</i>	43
6.6.2	<i>Cable Modem MAC Bridge Interface Masks</i>	44
6.6.3	<i>Embedded Host Exclusion</i>	44
6.6.4	<i>CMTS embedded host MAC Address Learning</i>	45
6.6.5	<i>Interface-based Classification</i>	45
6.7	L2VPN Quality Of Service.....	46

6.7.1	DOCSIS QoS.....	46
6.7.2	Backbone Network QoS.....	46
6.8	Stacked 802.1Q Tags or Tag-in-Tag operation.....	48
6.9	Spanning Tree and Loop Detection.....	49
6.10	High Availability.....	49
6.10.1	802 Encapsulation - Active/Standby Layer 2 Trunk Ports.....	49
6.10.2	802 Encapsulation - Link Aggregation.....	49
6.10.3	MPLS Encapsulation High Availability.....	50
6.11	MPLS Encapsulation - PW Redundancy.....	50
7	CABLE MODEM REQUIREMENTS.....	51
8	SERVICE OPERATIONS, ADMINISTRATION, AND MAINTENANCE (OAM).....	53
8.1	Introduction.....	53
8.2	Service OAM Configuration.....	53
8.2.1	CM.....	54
8.2.2	CMTS.....	55
8.3	Fault Management.....	55
8.3.1	Continuity Check Messages (CCM).....	55
8.3.2	Loopback.....	57
8.3.3	Linktrace.....	58
8.4	Performance Management.....	59
8.4.1	Frame Delay.....	59
8.4.2	Synthetic Frame Loss.....	60
9	LAYER 2 CONTROL PROTOCOL HANDLING.....	62
ANNEX A	CMTS DOCS-L2VPN-MIB REQUIREMENTS (NORMATIVE).....	63
A.1	DOCS-L2VPN-MIB Conformance.....	63
A.2	DOCS-L2VPN-MIB Definitions.....	67
ANNEX B	PARAMETER ENCODINGS (NORMATIVE).....	89
B.1	Capabilities.....	89
B.1.1	L2VPN Capability.....	89
B.1.2	Embedded Service/Application Functional Entity (eSAFE) Host Capability.....	89
B.1.3	Downstream Unencrypted Traffic (DUT) Filtering.....	89
B.2	Downstream Unencrypted Traffic (DUT) Filtering Encoding.....	89
B.2.1	Downstream Unencrypted Traffic (DUT) Control.....	90
B.2.2	Downstream Unencrypted Traffic (DUT) CMIM.....	90
B.3	L2VPN Encoding.....	90
B.3.1	VPN Identifier.....	91
B.3.2	NSI Encapsulation Subtype.....	91
B.3.3	eSAFE DHCP Snooping.....	96
B.3.4	CM Interface Mask (CMIM) Subtype.....	96
B.3.5	Attachment Group ID.....	97
B.3.6	Source Attachment Individual ID.....	98
B.3.7	Target Attachment Individual ID.....	98
B.3.8	Upstream User Priority.....	98
B.3.9	Downstream User Priority Range.....	99
B.3.10	L2VPN SA-Descriptor Subtype.....	99
B.3.11	Vendor Specific L2VPN Subtype.....	99
B.3.12	Pseudowire ID (deprecated).....	99
B.3.13	Pseudowire Type.....	99
B.3.14	L2VPN Mode.....	100
B.3.15	Tag Protocol Identifier (TPID) Translation.....	100
B.3.16	L2CP Processing.....	102
B.3.17	DAC Disable/Enable Configuration.....	102

B.3.18	<i>Pseudowire Class</i>	103
B.3.19	<i>Service Delimiter</i>	103
B.3.20	<i>Virtual Switch Instance Encoding</i>	104
B.3.21	<i>BGP Attribute sub TLV</i>	105
B.3.22	<i>VPN-SG Attribute sub TLV</i>	106
B.3.23	<i>Pseudowire Signaling</i>	106
B.3.24	<i>L2VPN SOAM Subtype</i>	107
B.3.25	<i>Network Timing Profile Reference</i>	110
B.3.26	<i>L2VPN DSID</i>	110
B.3.27	<i>L2VPN L2 Multipoint Forwarding Mode</i>	111
B.4	<i>Confirmation Codes</i>	111
B.5	<i>L2VPN Error Encoding</i>	111
B.5.1	<i>L2VPN Errored Parameter</i>	111
B.5.2	<i>L2VPN Error Code</i>	112
B.5.3	<i>L2VPN Error Message</i>	112
B.6	<i>CM Interface Mask Classification Criteria</i>	112
B.7	<i>L2VPN MAC Aging Encoding</i>	113
B.7.1	<i>L2VPN MAC Aging Mode</i>	113
APPENDIX I	EXAMPLE L2VPN ENCODINGS (INFORMATIVE)	115
I.1	<i>Point-to-Point Example</i>	115
I.2	<i>Multipoint Example</i>	118
I.3	<i>Upstream L2VPN Classifier Example</i>	121
APPENDIX II	IEEE 802.1Q ENCAPSULATION (INFORMATIVE)	123
APPENDIX III	EMBEDDED VLAN CM BRIDGING MODEL (INFORMATIVE)	124
III.1	<i>IEEE 802.1Q and Embedded VLAN Model</i>	125
III.2	<i>Embedded Bridge MAC Domain Service Primitives</i>	126
APPENDIX IV	L2VPN NON-COMPLIANT CM RESTRICTIONS (INFORMATIVE)	128
IV.1	<i>Leaking through non-compliant CMs</i>	128

Figures

Figure 5-1	- Transparent LAN Service	19
Figure 5-2	- TLS over a MPLS Network	21
Figure 5-3	- CMTS L2VPN and Non-L2VPN Forwarding	23
Figure 5-4	- Point-to-Point Forwarding Mode	25
Figure 5-5	- Multipoint L2VPN Forwarding Mode Example	26
Figure 6-1	- CM, eMTA, and CPE Forwarding	43
Figure 8-1	- Operator and EVC MEG Level	55
Figure 8-2	- CCM in the MSO Network	56
Figure 8-3	- Loopback in the MSO Network	57
Figure 8-4	- Linktrace functionality in the MSO Network	58
Figure 8-5	- Frame Delay functionality in the MSO Network	60
Figure 8-6	- Frame Loss Functionality in the MSO Network	61
Figure I-1	- Point-To-Point L2VPN Traffic Forwarding Example	115
Figure I-2	- Multipoint L2VPN Forwarding of Traffic Example	118
Figure II-1	- Ethernet 802.1Q Tags	123
Figure III-1	- L2VPN Embedded VLAN (eVLAN) Model	124

Tables

Table 6–1 - L2VPN Encoding Subtype Location Summary	28
Table 6–2 - Cable Modem MAC Bridge Interfaces.....	44
Table 6–3 - eSAFE DHCP Snooping Substrings	45
Table 8–1 - High Level Operations and References	53
Table 8–2 - Service OAM Terminology.....	54
Table 8–3 - Flags Format in CCM PDU.....	56
Table 9–1 - L2CP Frames and Actions.....	62
Table I–1 - Point-to-Point CM1 L2VPN Encoding.....	116
Table I–2 - Point-to-Point CM2 L2VPN Encoding.....	116
Table I–3 - Point-to-Point CM3 L2VPN Encoding.....	117
Table I–4 - Multipoint CM1 L2VPN Encoding.....	119
Table I–5 - Multipoint CM2 L2VPN Encoding.....	119
Table I–6 - Multipoint CM3 L2VPN Encoding.....	120
Table I–7 - Multipoint CM4 L2VPN Encoding.....	120
Table I–8 - Upstream L2VPN Classifier Encoding.....	121
Table IV–1 - Non-L2VPN leaking through Non-compliant CMs configured for L2VPN.....	128

1 INTRODUCTION

This standard 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 Business Services over DOCSIS (BSoD) initiative.

In order to speed time to market, [L2VPN-DG] offers guidelines to CMTS manufacturers as to how to phase the implementation of requirements defined in this standard. Phase designations are only applicable to CMTS products. Cable modems are expected to support all required L2VPN features in Phase 1.

The present document corresponds to and is the technical equivalent of the CableLabs CM-SP-L2VPN-I15-150528 [L2VPN-IP].

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 standard.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this standard.
"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 standards. 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 standard 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 standard 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 standard are summarized in Section 7.

1.3 Conventions

In this standard, the following convention applies any time a bit field is displayed in a figure or a table. The bit field should be interpreted by reading the figure or a table from left to right, then from top to bottom, with the MSB being the first bit read and the LSB being the last bit read.

2 REFERENCES

2.1 Normative References

The following documents contain provisions, which, through reference in this text, constitute provisions of this document. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision; and while parties to any agreement based on this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1.1 SCTE References

[MULPIv3.0]	ANSI/SCTE 135-2 2019, DOCSIS 3.0 Part 2: MAC and Upper Layer Protocols
[MULPIv3.1]	ANSI/SCTE 220-2 2016, DOCSIS 3.1 Part 2: MAC and Upper Layer Protocols Interface
[OSSIV3.0]	ANSI/SCTE 135-4 2019, DOCSIS 3.0 Part 4: Operations Support Systems Interface
[RFI 2.0]	ANSI/SCTE 79-1 2016, DOCSIS 2.0 Part 1: DOCSIS Radio Frequency Interface
[BPI+]	ANSI/SCTE 23-2 2017, DOCSIS 1.1 Part 2: Baseline Privacy Plus Interface

2.1.2 Standards from Other Organizations

[802.1AX]	IEEE 802.1AX, IEEE Standard for Local and metropolitan area networks--Link Aggregation, 2008.
[802.1D]	IEEE 802.1D, IEEE Standard for Local and metropolitan area networks - Media Access Control (MAC) Bridges, June 2004.
[802.1Q]	IEEE Std 802.1Q, IEEE Standard for Local and metropolitan area networks - Media Access Control (MAC) Bridges and Virtual Local Area Networks, August 2011.
[DOCSIS MAC]	Refers to [MULPIv3.1], [MULPIv3.0] and [RFI 2.0].
[ID LDPv6]	IETF Internet draft, Updates to LDP for IPv6, draft-ietf-mpls-ldp-ipv6-17, February 2015, <u>http://tools.ietf.org/html/draft-ietf-mpls-ldp-ipv6-17</u> .
[MEF 30.1]	MEF Technical Specification 30.1: Service OAM Fault Management Implementation Agreement: Phase 2, April 2013.
[MEF 31]	MEF Technical Specification 31: Service OAM Fault Management Definition of Managed Objects, January 2011.
[MEF 35]	MEF Technical Specification 35: Service OAM Performance Monitoring Implementation Agreement, April 2012.
[MEF 36]	MEF Technical Specification 36: Service OAM SNMP MIB for Performance Monitoring, January 2012.
[PWYPES]	MPLS Pseudowire Types Registry, March 30, 2010, Internet Assigned Numbers Authority.
[RFC 2544]	IETF RFC 2544, Benchmarking Methodology for Network Interconnect Devices, March 1999.
[RFC 2918]	IETF RFC 2918, Route Refresh Capability for BGP-4, September 2000.
[RFC 3031]	IETF RFC3031, Multiprotocol Label Switching Architecture, January 2001.
[RFC 3032]	IETF RFC 3032, MPLS Label Stack Encoding, January 2001.
[RFC 3931]	IETF RFC 3931, Layer Two Tunneling Protocol - Version 3 (L2TPv3), March 2005.
[RFC 4385]	IETF RFC 4385, Pseudowire Emulation Edge-to-Edge (PWE3). Control Word for Use over an MPLS PSN, February 2006.

- [RFC 4447] IETF RFC 4447, Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP), April 2006.
- [RFC 4448] IETF RFC 4448, Encapsulation Methods for Transport of Ethernet over MPLS Networks, April 2006.
- [RFC 4667] IETF RFC 4667, Layer 2 Virtual Private Network (L2VPN) Extensions for Layer 2 Tunneling Protocol (L2TP), September 2006.
- [RFC 4761] IETF RFC 4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling, January 2007.
- [RFC 4762] IETF RFC 4762, Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling, January 2007.
- [RFC 4893] IETF RFC 4893, BGP Support for Four-octet AS Number Space, May 2007.
- [RFC 5036] IETF RFC 5036, LDP Specification, October 2007.
- [RFC 5286] IETF RFC 5286, Basic Specification for IP Fast Reroute: Loop-Free Alternates, September 2008.
- [RFC 5925] IETF RFC 5925, The TCP Authentication Option, June 2010.
- [RFC 6074] IETF RFC 6074, Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs), January 2011.
- [RFC 6624] IETF RFC 6624, Layer 2 Virtual Private Networks Using BGP for Auto-Discovery and Signaling, May 2012.
- [Y.1564] ITU-T Recommendation Y.1564 (03/11), Ethernet service activation test methodology.
- [Y.1731] ITU-T Recommendation Y.1731 (11/13), OAM functions and mechanisms for Ethernet based networks.

2.1.3 Published Materials

- No normative references are applicable.

2.2 Informative References

The following documents might provide valuable information to the reader but are not required when complying with this document.

2.3 SCTE References

- [eDOCSIS] ANSI/SCTE 107 2017, Embedded Cable Modem Devices
- [eRouter] ANSI/SCTE 140 2013, Cable Modem IPv4 and IPv6 eRouter Specification
- [PKT-PROV] ANSI/SCTE 24-5 2016, IPCablecom Part 5: Media Terminal Adapter (MTA) Device Provisioning Requirements for the Delivery of Real-Time Services over Cable Television Using Cable Modems

2.4 Standards from Other Organizations

- [DPoE ARCHv1.0] DPoE-SP-ARCHv1.0-I03-140807, August 7, 2014, DOCSIS Provisioning of EPON, DPoE Architecture Specification, Cable Television Laboratories, Inc.
- [DPoE DEMARCV1.0] DPoE-SP-DEMARCV1.0- I04-140807, August 7, 2014, DOCSIS Provisioning of EPON, DPoE Demarcation Device Specification, Cable Television Laboratories, Inc.

[DPoE IPNEv1.0]	DPoE-SP-IPNEv1.0-I08-140807, August 7, 2014, DOCSIS Provisioning of EPON, IP Network Element Requirements, Cable Television Laboratories, Inc.
[DPoE MEFv2.0]	DPoE-SP-MEFv2.0-I03-140807, August 7, 2014, DOCSIS Provisioning of EPON, Metro Ethernet Forum Specification, Cable Television Laboratories, Inc.
[DPoE MULPIv1.0]	DPoE-SP-MULPIv1.0-I10-150319, March 19, 2015, DOCSIS Provisioning of EPON, DPoE MAC and Upper Layer Protocols Requirements, Cable Television Laboratories, Inc.
[L2VPN-DG]	L2VPN Development Guidelines Technical Report, CM-TR-L2VPN-DG-V02-121206, December 6, 2012, Cable Television Laboratories, Inc.
[MEF 6.1.1]	MEF 6.1.1, Layer 2 Control Protocol Handling Amendment to MEF 6.1, January 2012.
[RFC 2685]	IETF RFC 2685, Virtual Private Network Identifier, September 1999.
[RFC 3107]	IETF RFC 3107, Carrying Label Information in BGP-4, May 2001.
[RFC 3209]	IETF RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels, December 2001.
[RFC 3270]	IETF RFC 3270, Multi-Protocol Label Switching (MPLS) Support of Differentiated Services, May 2002.
[RFC 3985]	IETF RFC 3985, Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture, March 2005.
[RFC 4363]	IETF RFC 4363, Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions, January 2006.
[RFC 4364]	IETF RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs), February 2006.
[RFC 4664]	IETF RFC 4664, Framework for Layer 2 Virtual Private Networks (L2VPNs), September 2006.
[L2VPN-IP]	Data-Over-Cable Service Interface Specifications, Business Services over DOCSIS®, Layer 2 Virtual Private Networks for IP Cable Modem Systems, CM-SP-L2VPN-I15-150528, May 28, 2015, Cable Television Laboratories, Inc.

2.1 Published Materials

- No informative references are applicable.

3 TERMS AND DEFINITIONS

This standard 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 standard.
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 <i>not</i> 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).
Downstream Service Identifier (DSID)	A 20-bit value in a DOCSIS extended header that identifies a stream of packets distributed to the same cable modem or group of cable modems. The DSID value is unique within a MAC Domain. For sequenced packets, the DSID identifies the resequencing context for downstream packet bonding in the CM.
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 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.
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.
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.
Management L2VPN	An L2VPN for the post-registration SNMP traffic to eCM or eSAFE devices. May be combined with a Provisioning L2VPN.
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 standard.
Point-to-Point L2 Forwarding	Operation of an L2 Forwarder between only two L2 networks with no source MAC address learning.
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.
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 standard [BPI+] 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 [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 <i>subset</i> 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 802.1Q (formerly known as 802.1ah) stacked VLAN ID consists of an outer Service 12-bit VLAN ID and an inner Customer 12-bit VLAN ID.
Resequencing Downstream Service Identifier	A downstream service identifier for which the CMTS signals packet resequencing attributes.

4 ABBREVIATIONS AND ACRONYMS

This standard uses the following abbreviations:

AC	Attachment Circuit
AGI	Attachment Group Identifier
AS	Autonomous System
ASN	Autonomous System Numbers
ASCII	American Standard Code for Information Interchange
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BEB	Backbone Edge Bridge
BGP	Border Gateway Protocol
BPI	Baseline Privacy Interface
BPKM	Baseline Privacy key Management
BSoD	Business Services over DOCSIS
CCM	Continuity Check Message
CE-ID	Customer Edge Identifier
CFI	Canonical Format Indicator
CM	Cable Modem
CMCI	Cable Modem to Customer Premises Equipment Interface
CMIM	CM Interface Mask
CMTS	Cable Modem Termination System
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check
DA	Destination Address
DAC	DEMARC Automatic Configuration
DEI	Drop Eligibility Indicator
DEMARC	DPoE Demarcation Device
DHCP	Dynamic Host Configuration Protocol
DIME	Downstream IP Multicast Encryption
DMAC	Destination MAC
DMM	Delay Measurement Message
DMR	Delay Measurement Reply
DOCSIS	Data-Over-Cable Service Interface Specifications
DPoE	DOCSIS Provisioning of EPON
DS	Downstream
DSCP	Differentiated Services Code Point
DSG	DOCSIS Set-top Gateway

DSID	Downstream Service Identifier
DSx	Dynamic Service addition, change or deletion
DUT	Downstream Unencrypted Traffic
eCM	Embedded Cable modem [eDOCSIS]
eMTA	Embedded Multimedia Terminal Adapter [PKT-PROV]
EPON	Ethernet Passive Optical Network
eRouter	Embedded DOCSIS Router
eSAFE	Embedded Service/Application Functional Entity [eDOCSIS]
eSTB	Embedded Set-top Box
ETH-RDI	Ethernet Remote Defect Indication
EXP	Experimental bits
FD	Frame Delay
FDB	Forwarding Database
FEC	Forwarding Equivalence Class
FLM	Frame Loss Measurement
IANA	Internet Assigned Numbered Authority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization of the International Telecommunication Union
GMAC	Group Media Access Control
L2	Layer 2
L2CP	Layer 2 Control Protocol
L2PDU	Layer 2 Protocol Data Unit
L2TP	Layer 2 Tunneling Protocol
L2VPN	Layer 2 Virtual Private Network
LAN	Local Area Network
LBM	Loopback Message
LBR	Loopback Reply
LDP	Labeled Distribution Protocol
LLC	Logical Link Control
LSB	Least Significant Bit
LSP	Label Switched Paths

LTM	Linktrace Message
LTR	Linktrace Reply
M	Mandatory
MA	Maintenance Association[802.1Q]
MAC	Media Access Control
MAID	Maintenance Association Identifier [802.1Q]
MD	Maintenance Domain [802.1Q]
MEG	Maintenance Entity Group
MEP	Maintenance association End Point [IEEE 802.1Q]
MEPID	Maintenance Entity Group End Point Identifier
MIB	Management Information Base
MIC	Message Integrity Check
MIP	Maintenance domain Intermediate Point [802.1Q]
MP-BGP	MultiProtocol BGP
MPLS	Multiprotocol Label Switching
MSB	Most Significant Bit
MSO	Multiple Systems Operator
MTA	Multimedia Terminal Adapter
MTU	Maximum Transmission Unit
MULPI	MAC and Upper Layer Protocols Interface
NA	Not Applicable
NLRI	Network Layer Reachability Information
NSI	Network System Interface
OAM	Operations, Administration, and Maintenance
OSPF	Open Shortest Path First
OSSI	Operations System Support Interface
P2P	Point to Point
PB	Provider Backbone
PBB	Provider Backbone Bridging
PCP	Priority Code Point
PDU	Protocol Data Unit
PE	Provider Edge
PICS	Protocol Implementation Conformance Statement
PSN	Packet Switched Network
PW	Pseudowire
PWid	Pseudowire identifier
QoS	Quality of Service
RC	Read-Create

RD	Route Distinguisher
RF	Radio Frequency
RIP	Routing Information Protocol
RO	Read-Only
RSP	Response
RSVP-TE	Resource Reservation Protocol-Traffic Engineering
RT	Route Target
SA	Source Address
SA-MAP	Security Address Mapping
SAID	Security Association Identifier
SAII	Source Attachment Individual Identifier
SF	Service Flow
SID	(Upstream) Service Identifier
SG	Serving Group
SLA	Service Level Agreements
SLM	Synthetic Loss Message
SLR	Synthetic Loss Reply
SMAC	Source MAC
SNMP	Simple Network Management Protocol
SOAM	Service Operations, Administration, and Maintenance
TAII	Target Attachment Individual Identifier
TCI	Tag Control Information
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transparent LAN Service
TLV	Type/Length/Value
TOD	Time of Day
TOS	Type of Service
TPID	Tag Protocol Identifier
UCA	User Customer Address
UDC	Upstream Drop Classifier
UNI	User Network Interface
VE	VPLS Edge
VE-ID	VPLS Edge Identifier
VID	VLAN Identifier
VPLS	Virtual Private LAN Services
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service

VSI Virtual Switch Instance

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 [DOCSIS MAC] was originally intended for residential subscriber connection to the public Internet. This standard 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.

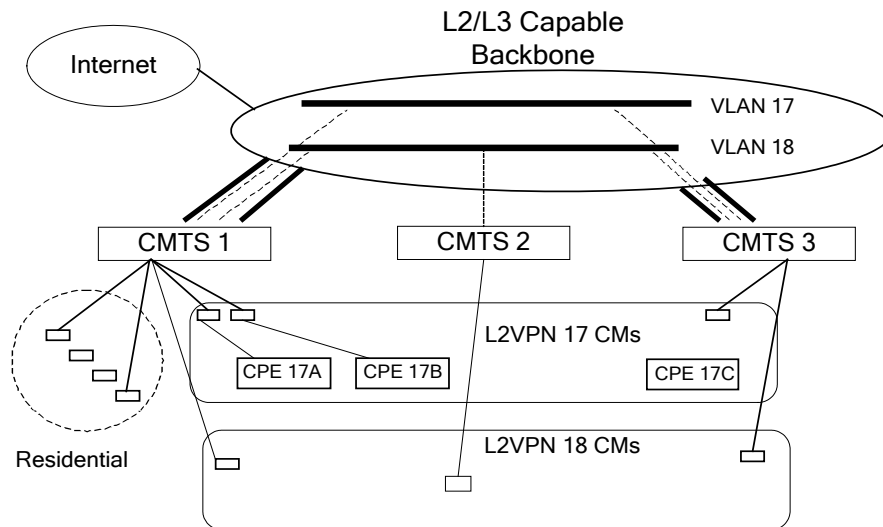


Figure 5–1 - Transparent LAN Service

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 [802.1Q] definition, as a

subset of LANs, within a Bridged Network, to which is assigned a 12-bit VLAN ID. In this example, CMTS 1 directly encapsulates upstream L2 packets from L2VPN 17 onto an 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. Bridging requires the CMTS to learn the Source MAC (SMAC) addresses of CPE17A and CPE17B, and associate them with the CM to which each CPE device is attached.

CMTS 1 implements only a single attachment circuit to VLAN 17 on the backbone. When a downstream unicast packet from VLAN 17 arrives at CMTS 1, 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.

As shown in Figure 5–2, cable operators can offer both port-based Ethernet Private Line (EPL) and VLAN-based Ethernet Virtual Private Line (EVPL) service over an MPLS network. In such a network, the CMTS can serve as a Provider Edge (PE) router and map DOCSIS service flows into MPLS pseudowires.

In the example below, a cable operator provides EPL service to a single commercial enterprise denoted as L2VPN 17. Both 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 19. CMTS 2 provides L2VPN service to one L2VPN 19 CM.

The example shows that the cable operator's MPLS backbone implements a single pseudowire for each customer. In this example, CMTS 1 directly encapsulates upstream L2 packets from L2VPN 19 into an IETF [RFC 4448] Ethernet over MPLS pseudowire and forwards them to the cable operator's backbone via a Network System Interface (NSI) port.

In the example, CMTSs 1 and 2 implement point-to-point L2 Forwarding. Each CMTS implements only a single attachment circuit to the IP/MPLS pseudowire on the backbone. When a downstream unicast packet from VLAN 19 arrives at CMTS 1, it looks up the pseudowire mapping in its database and transparently forwards all individual and group MAC destined packets, in a point-to-point manner, to the correct CM.

In the backbone, cable operator core IP/MPLS routers forward pseudowire traffic between the two MPLS PE CMTSs. The TLS service offered by the operator to L2VPN 19 provides for a transparent layer 2 bridged connection between CPEs 19A and 19B. From the enterprise customer's point of view, such CPE are managed and operated as if they were on a customer-private Ethernet LAN. As with the example in Figure 5–1, 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.

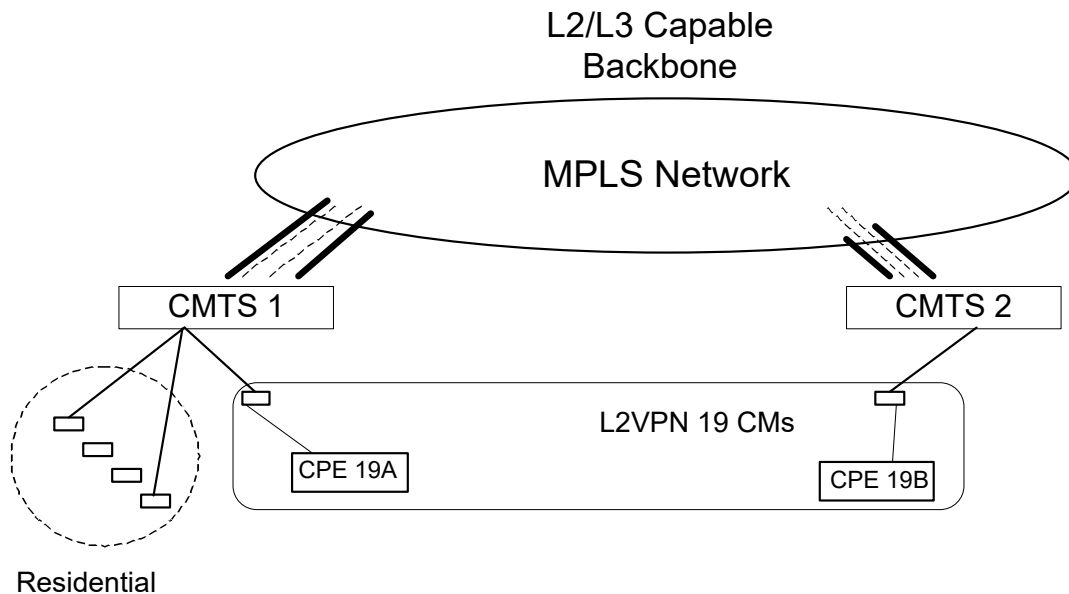


Figure 5-2 - TLS over a MPLS Network

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 Multimedia Terminal Adapter (eMTA) [PKT-PROV], or eRouter [eRouter]. 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 standard 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.

5.1.5 High Availability

This document uses the term "Layer 2 trunk port" to describe an NSI port configured to forward L2VPN packets encapsulated with a layer 2 tag as specified by IEEE 802, e.g., IEEE 802.1Q.

This standard defines requirements for the CMTS to maintain L2VPN forwarding in the event of any single NSI port failure. One technique is to support forwarding of all L2VPN traffic using a layer 2 IEEE 802 Ethernet encapsulation (e.g., 802.1Q) through a single "layer 2 trunk port" at a time, and support configuration of multiple possible trunk ports, only one of which is "active". Another technique is to implement L2VPN forwarding across a set of NSI ports using [802.1AX] Link Aggregation.

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 5–3.

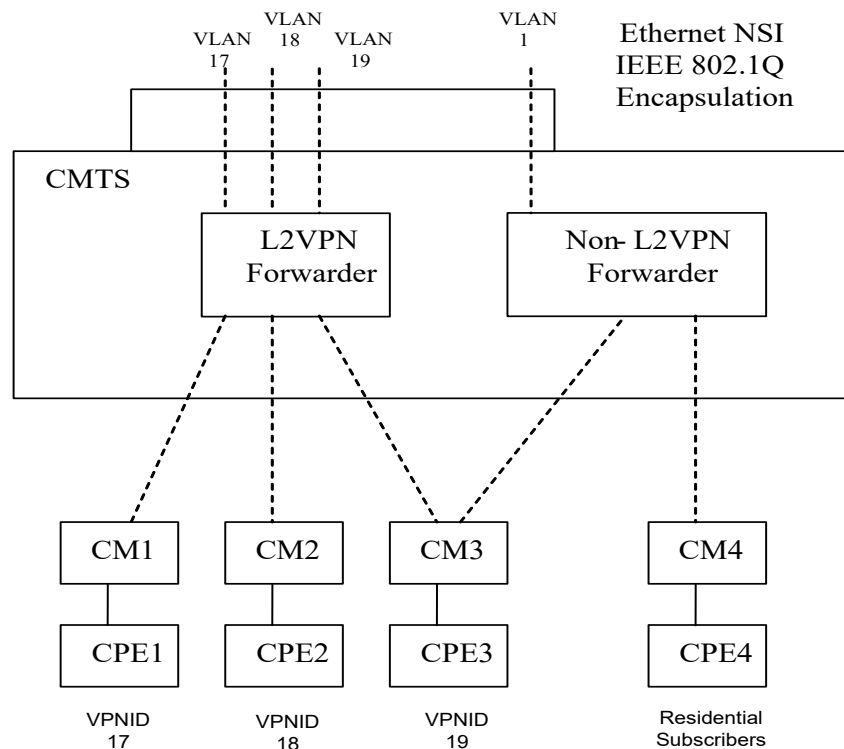


Figure 5–3 - CMTS L2VPN and Non-L2VPN Forwarding

To support L2VPN operation, a CMTS's Network System Interface (NSI) has to 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 5–3 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 standard 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 [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 standard 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. Similarly, using point-to-point Ethernet over MPLS [RFC 4385] [RFC 4448] encapsulation, each attachment circuit is configured with a different pseudowire identifier. 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 5–4.

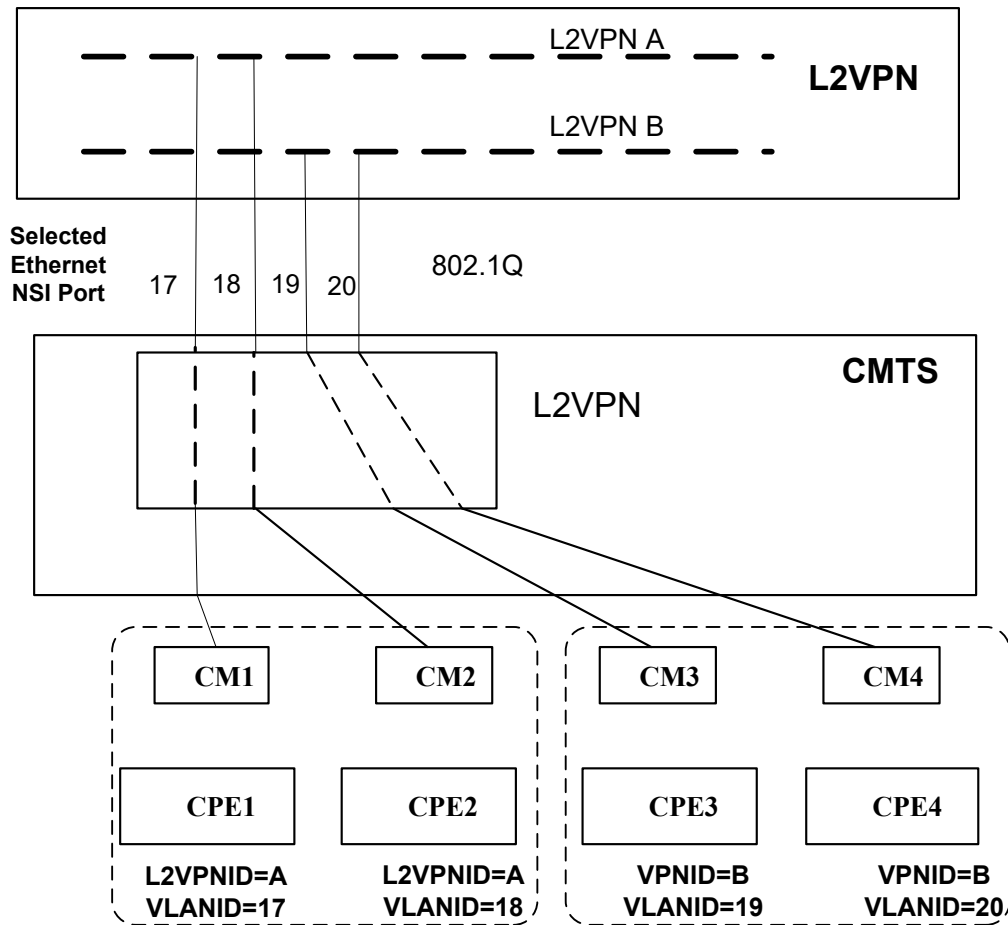


Figure 5–4 - Point-to-Point Forwarding Mode

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 [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 still has to 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, the number of L2VPN subscriber modems supported on a CMTS is limited 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 5–5.

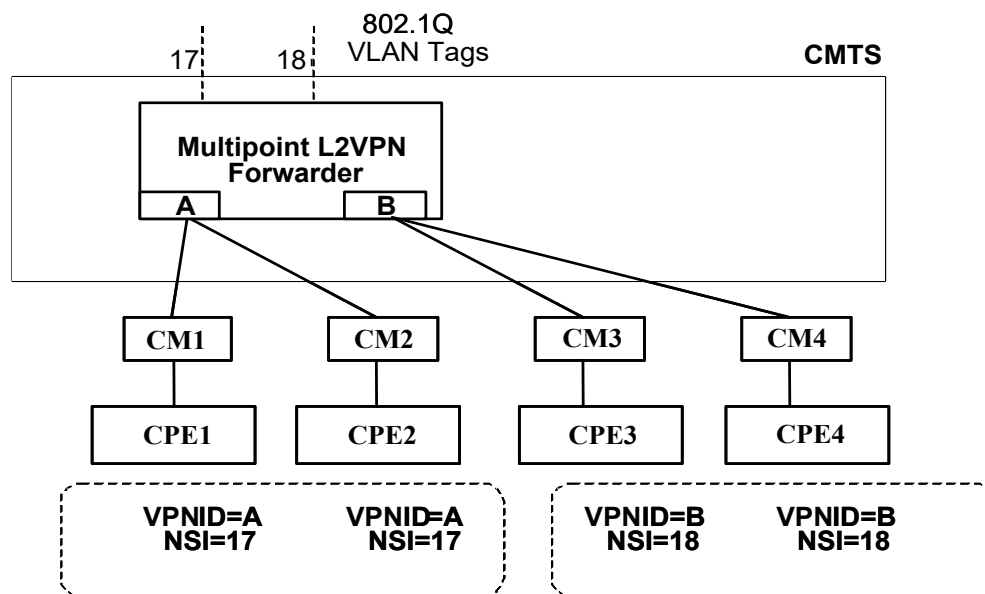


Figure 5–5 - Multipoint L2VPN Forwarding Mode Example

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 5–5.

This standard permits qualification of CMTSs with either Point-to-Point or Multipoint forwarding modes. DOCSIS qualification testing uses the forwarding mode indicated by the vendor's PICS submission for all L2VPNs. This standard 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 [802.1Q]. For purposes of [eRouter] 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. SFs carrying L2VPN traffic could be carried over bonded channels if the CMTS and CM support Channel Bonding as defined in [MULPIv3.0]. Consequently, the use of resequencing DSIDs is not precluded by this standard.

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 standard. 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 standard.

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. This traffic could arrive on a single channel or on a bonded channel group, provided that Channel Bonding is supported by both the CM and CMTS.

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 0xFFFFFFFF ([DOCSIS MAC]). 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	Upstream User Priority		Optional		
43.5.9	Downstream User Priority Range			Optional	
43.5.10	L2VPN SA-Descriptor	Required(2)			
43.5.11	deprecated				
43.5.12	deprecated				
43.5.13	L2VPN Mode (4)				
43.5.14	TPID Translation (4)				
43.5.15	L2CP Processing (4)				
43.5.16	Demarc Autoconfiguration (4)				
43.5.17	deprecated (4)				
43.5.18	Pseudowire Class (4)				
43.5.19	Service Delimiter (4)				
43.5.20	Virtual Switch Instance (4)	Optional			
43.5.21	BGP Attribute	Optional	Optional	Optional	
43.5.22	L2VPN Serving Group (4)				
43.5.23	Pseudowire Signaling	Optional			
43.5.24	Service OAM	Optional			
43.5.25	Network Timing Profile Reference (4)				
43.5.26	L2VPN DSID (5)	Optional			
43.5.27	L2VPN L2 Multipoint Forwarding Mode	Optional			
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.
- (4) This TLV is specific to DOCSIS Provisioning of EPON (DPoE) Systems.
- (5) This TLV is specific to DOCSIS 3.0 and later L2VPN systems

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. In point-to-point forwarding mode, a CMTS MUST support one per-CM L2VPN Encoding with an NSI Encapsulation subtype and at least one Upstream Service Flow L2VPN Encoding per CM. 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, REG-REQ-MP, 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 or REG-RSP-MP. 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, REG-REQ-MP, 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 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 4364], 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.

6.2.1.1 BGP VPNID Subtype

The BGP VPNID Subtype is a 4-byte integer value that also identifies a logical Layer 2 Virtual Private Network. BGP VPNID Subtype is required only if BGP auto-discovery and LDP signaling [RFC 6074] is to be used by CMTS for L2VPN dynamic discovery.

A cable operator is expected to configure a unique BGP VPNID for each commercial enterprise to which it offers L2VPN service, if the operator intends to use BGP auto-discovery and LDP signaling of pseudowires at the CMTS. A cable operator may configure the same integer value in both VPNID and BGP VPNID Subtypes for operational simplicity. Please see Section 6.2.7.2.2 (BGP Auto-discovery) for more details.

6.2.2 Downstream Classifier L2VPN Encoding

A Downstream Classifier L2VPN Encoding is an L2VPN Encoding that appears in a Downstream Packet Classification Encoding [DOCSIS MAC]. 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 Downstream 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 Downstream User Priority Range subtype, the classifier applies only to encapsulated L2VPN packets received on the NSI with a user priority within the indicated range (inclusive). This allows high priority L2VPN traffic to be classified to downstream service flows with enhanced QoS.

The user priority value matched by a Downstream User Priority Range subtype is the user priority encoded in the (802.1Q or MPLS or L2TPv3) encapsulation header of the L2VPN packet received by the L2VPN forwarder on the NSI. Please refer to Section 6.7.2.1.1 for user priority description.

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+ standard [BPI+] 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 or REG-RSP-MP to the CM, adding the per-CM L2VPN Encoding to the REG-RSP or REG-RSP-MP 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 or REG-RSP-MP 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, TAIL, or SAIL 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 standard 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 standard 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 standard defines an NSI Encapsulation Subtype of an L2VPN Encoding, Section 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 standard requires CMTSs to implement only a single L2VPN NSI Encapsulation format: [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.

6.2.6.2 IEEE 802.1Q L2VPN Forwarding

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).

6.2.6.3 IEEE 802.1Q L2VPN Forwarding (formerly known as 802.1ad)

[802.1Q] describes a dual tagging approach (i.e., Q-in-Q) 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 802.1Q networking elements in the backbone.

6.2.6.3.1 Point-to-Point CMTS Forwarding with Point-to-Point 802.1Q Forwarding

In this scenario, the IEEE 802.1Q networking elements in the backbone simply forward point-to-point without learning MAC addresses. The outer 802.1Q 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 802.1Q 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 802.1Q frames are forwarded in the backbone network, the intermediate nodes only use the outer VLAN ID tag to make forwarding decisions. For example, 802.1Q 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.

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

IEEE 802.1Q 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 802.1Q L2VPN switch considers the outer VLAN ID tag to represent a separate virtual trunk interface, while the inner tag represents a logical switch. The 802.1Q 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 802.1Q L2VPN Switch, and each of these can have over 4000 cable modems/service flow associations at the CMTS.

6.2.6.4 IEEE 802.1Q L2VPN Forwarding (formerly known as 802.1ah)

[802.1Q] describes Provider Backbone Bridging (PBB) (i.e., MAC-in-MAC) which introduces a hierarchical sub-layer, by encapsulating the customer Ethernet frame within a service provider frame. PBB backbone edge switches append their own source address (B-SA) and destination address (B-DA), as well as a backbone VID (B-VID). A service ID (I-SID) field identifies a customer-specific service instance.

The NSI Encapsulation Subtype allows these values to be configured for each CM or SF performing L2VPN forwarding. The configuration of the tags depends on the L2VPN Forwarding Mode of the CMTS and the IEEE 802.1Q networking elements in the backbone.

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

The IETF has defined L2VPN framework [RFC 4664] by two types - multipoint L2VPN (VPLS) and point-to-point L2VPN (VPWS), using the notion of a Pseudowire (PW) [RFC 3985] to implement L2VPN over a Packet Switched Network (PSN) e.g., IP or MPLS network. The interoperation of DOCSIS L2VPN Forwarding with PW is required to allow seamless L2VPN forwarding over an MSO's IP/MPLS network.

Following the PW architecture [RFC 3985], the CMTS acts as a Provider Edge (PE) router having L2VPN Forwarder function, and does a simple mapping between the PW and Attachment Circuit (AC) based on local information, i.e., PW demultiplexer and incoming/outgoing logical/physical port. From the DOCSIS network standpoint, each CM with at least one upstream forwarding SF for an L2VPN corresponds to an AC at the CMTS. As described in Section 5.2.2, a cable AC to an L2VPN is considered to be the CM, not an individual service flow on the CM. Ethernet frames received over the L2VPN attachment circuits using either the MPLS or L2TPv3 NSI Encapsulation subtype are intended to be forwarded by the CMTS on PWs.

A PW emulates the essential attributes of an L2VPN service (e.g., Ethernet) over a packet switched network (PSN) (e.g., IP or MPLS network). Simply put, a PW is a tunnel with either MPLS encapsulation or L2TPv3 encapsulation, which is used to carry the service-specific PDUs (e.g., Ethernet frames) through the PSN. An L2VPN instantiation means establishment of one or more pairs of PWs between two or more L2VPN Forwarders (i.e., PE routers) in the PSN.

In VPWS, an L2VPN Forwarder (i.e., PE router) binds a PW to a single AC, such that frames received on the one are sent on the other, and vice versa. VPWS involves two PE routers logically connected via a bidirectional PW.

In VPLS, an L2VPN Forwarder (i.e., PE router) binds a set of PWs to a set of ACs; when a frame is received from any member of that set, a MAC (Media Access Control) address table is consulted (and various 802.1d procedures executed) to determine the member or members of that set on which the frame is to be transmitted. VPLS involves two or more PE routers logically connected via distinct PWs.

PW can be set up on PE routers using one of two methods: (1) Static Configuration or (2) Dynamic Signaling, enforcing one of two data plane encapsulations. This is covered in detail in Section 6.2.7.2.

A PSN tunnel needs to be set up on PE routers for PWs to be useful. PSN tunnel data plane and control plane are discussed in Section 6.2.7.1.

6.2.7.1 PSN Tunnel – Control Plane and Data Plane Encapsulation

In order for Layer 2 VPN services to work in a PSN, a functioning IP or MPLS data plane between the PE routers having L2VPN Forwarder functions needs to exist. After all, the PW tunnels travel through PSN tunnels. The PSN tunnel may be an MPLS tunnel (i.e., MPLS Encapsulation) or IP tunnel (e.g., L2TPv3 Encapsulation or other encapsulation not defined in this standard). This means that a CMTS acting as a PE router in the PSN needs to support the corresponding tunnel data plane and control plane.

A CMTS **MUST** support MPLS data plane, as defined in [RFC 3031] and [RFC 3032]. That is, a CMTS **MUST** support MPLS packet forwarding (e.g., receiving and transmitting MPLS packets having ethertype=0x8847 and 0x8848) on its NSI ports. An MPLS packet is assumed to have one or more label stack entries.

A CMTS **MUST** support LDP as the MPLS control plane, as defined in [RFC 5036] and [ID LDPv6], on its NSI port. This is required to setup MPLS Label Switched Paths (LSPs) through dynamic label allocation and label exchange (for IGP prefixes) with other routers in PSN.

A CMTS **SHOULD** support BGP [RFC 3107] as the MPLS control plane to set up MPLS LSPs (for BGP prefixes identifying PE routers) with other routers in PSN. BGP is beneficial for higher scale.

A CMTS **MAY** support RSVP-TE [RFC 3209] as the MPLS control plane to setup MPLS LSPs for IGP prefixes. RSVP-TE is beneficial to construct path-constrained LSPs.

A CMTS **MUST** provide a mechanism to limit the advertisement of LDP Forward Equivalence Class of only host entries.

A CMTS **SHOULD** support TCP MD5 authenticity and integrity based on the use of the TCP MD5 Signature Option specified in [RFC 5925] per LDP neighbor.

A CMTS **MAY** support LDP Fast Reroute (FRR) as defined in a Basic Specification for IP Fast Reroute: Loop-Free Alternates [RFC 5286].

The usage of any other PSN Tunnel (i.e., IP Tunnel) not defined in this standard is not recommended for L2VPN packet forwarding.

6.2.7.2 PW – Control Plane and Data Plane Encapsulations

A PW needs to be set up between two PE routers participating in L2VPN. A PW can be established using one of two methods: (1) Static Provisioning or (2) Dynamic Signaling. The latter method is known as having a PW control plane.

The static method requires no protocol and relies on static assignment of PW encapsulation values (i.e., MPLS labels or L2TPv3 session ID) on CMTSs using either vendor-specific CMTS configuration or L2VPN vendor-specific Subtype parameters. Please note that the static method is not recommended.

The dynamic signaling method relies on the CMTS using a protocol to signal PW encapsulation values (i.e., MPLS label or L2TPv3 session ID) so as to set up PW with remote PE router(s). The following three signaling protocols are standardized by the IETF for PW establishment:

- LDP [RFC 4447] [RFC 4762]
- L2TPv3 [RFC 3931] [RFC 4667]
- BGP [RFC 4761] [RFC 6624] (See Note below)

NOTE: Usage of BGP as a signaling protocol is tied into the usage of BGP as the auto-discovery protocol.

Each of the above three signaling protocols require the CMTS (i.e., PE router) to have the following information per PW per L2VPN for successful PW setup with a remote PE:

- 1) Remote PE Identifier (e.g., IP address of each remote PE)
- 2) PW Identifier
- 3) Other Parameters (e.g., MTU)

This information can be either encoded using L2VPN encodings, or dynamically formulated by the CMTS based on auto-discovery mechanism (e.g., BGP). The next two sub-sections focus on specifying the usage of PW signaling protocols with or without auto-discovery.

The CMTS **SHOULD** support the PW Control Word for use within a MPLS Network as defined in [RFC 4385] and [RFC 4448].

6.2.7.2.1 PW Signaling without Auto-Discovery

If the NSI Encapsulation subtype of MPLS or L2TPv3 is included for any L2VPN and the BGP Attribute sub TLV (43.5.21) is NOT included, the CMTS **MUST NOT** initiate the usage of any auto-discovery procedures for that L2VPN, irrespective of the auto-discovery protocol enabled on the CMTS.

When the NSI Encapsulation subtype is present, the CMTS uses the encapsulation protocol (e.g., MPLS or L2TPv3) that is specified on a per L2VPN basis in the data plane, along with the corresponding signaling protocol (e.g., LDP or L2TPv3) in the control plane to set up the PW with the remote PE router whose IP address is specified in NSI Encapsulation subtype field.

A CMTS **MUST** support NSI Encapsulation subtype of MPLS. The CMTS **MAY** support NSI Encapsulation subtype of L2TPv3.

Using MPLS encapsulation implicitly means that a CMTS MUST support MPLS encapsulation of Ethernet Frames, as per [RFC 4448]. The CMTS would encapsulate the upstream Ethernet frames received on cable attachment circuit (e.g., SF) into an Ethernet over MPLS PW [RFC 4448] and forward them via the NSI port. Similarly, the CMTS decapsulates the downstream MPLS packets received on NSI port and forwards the resulting Ethernet frames to the CM via the downstream service flow (e.g., SF).

Using MPLS encapsulation implicitly means that a CMTS MUST support LDP for PW signaling, as per [RFC 4447] and [RFC 4762]. Specifically, the CMTS MUST use PwID FEC Element to establish the PW using LDP. The value of PwID is learned from the Pseudowire ID Encoding. The CMTS SHOULD NOT use Generalized PwID FEC Element (e.g., SAIL in B.3.6 and TAIL in B.3.7) to establish the PW using LDP, as it is meant to be used with auto-discovery by CMTS.

A CMTS MAY support L2TPv3 for PW signaling and L2TPv3 Encapsulation, as per [RFC 3931].

If LDP is used for PW establishment, the PSN tunnel is to be an MPLS tunnel (e.g., an MPLS data plane on the NSI of CMTS).

6.2.7.2.2 PW Signaling with Auto-Discovery

Auto-discovery of PE routers participating in a given L2VPN is done using Multi-Protocol BGP extensions for the L2VPN address-family.

If the NSI Encapsulation subtype and the BGP Attribute sub TLV (43.5.21) are included for an L2VPN, then the CMTS MUST initiate MP-BGP based auto-discovery procedures for that L2VPN. The MPLS PW ID, MPLS Peer IP address and L2TPv3 TLV values will be ignored by the CMTS in this case. If the NSI Encapsulation is not included the CMTS will assume MPLS NSI Encapsulation and will initiate MP-BGP auto-discovery procedures accordingly.

The CMTS MAY use vendor-specific configuration to dynamically select and learn the Service Multiplexing value for an L2VPN Encoding from the CMTS's L2VPN peers.

The CMTS could signal the PW setup using LDP or L2TPv3 immediately after the auto-discovery is completed (using BGP), as specified in [RFC 6074], or signal the PW setup using BGP at the same time as that of auto-discovery (using BGP), as specified in [RFC 4761] and [RFC 6624]. While both approaches could be utilized, they result in using either two protocols (BGP and LDP) or one protocol (BGP).

A CMTS MUST support BGP for auto-discovery and LDP for PW signaling, as per [RFC 6074] [RFC 4447].

A CMTS MAY support BGP for PW signaling and auto-discovery, as per [RFC 4761] and [RFC 6624], by implementing the MP-BGP L2VPN address-family. Specifically, a CMTS MAY support [RFC 4761] for Multipoint L2VPN and [RFC 6624] for Point-to-Point L2VPN.

A CMTS MAY support BGP for auto-discovery and L2TPv3 for PW signaling, as per [RFC 6074] and [RFC 4667].

When implementing BGP, the CMTS MAY implement BGP Support for Four-octet AS Number Space [RFC 4893]. The CMTS MUST support the co-existence of two-octet and four-octet BGP autonomous system numbers (ASN). The CMTS MUST support Route Refresh Capability for BGP-4 [RFC 2918].

The CMTS MAY support the TCP Authentication Option for BGP [RFC 5925].

When implementing BGP auto-discovery, the CMTS treats the L2VPN as a Point-to-Point L2VPN, unless it receives the Virtual Switch Instance encoding (Section B.3.20), in which case it treats the L2VPN as a Multipoint L2VPN.

The CMTS MUST deploy one of the two PW signaling with auto-discovery methods as follows:

- If the BGP VPN ID TLV (43.5.21.1) is included then LDP PW signaling with BGP auto-discovery [RFC 6074] will be deployed.
- If the BGP CE-ID/VE-ID TLV (43.5.21.5) is included then auto-discovery and PW signaling with BGP [RFC 4761] and [RFC 6624] will be deployed.

Once the CMTS has instantiated a particular L2VPN, the CMTS invokes BGP to advertise the availability of the L2VPN site, as per [RFC 6074] or [RFC 4761] and [RFC 6624].

When BGP auto-discovery with LDP signaling is used [RFC 6074], the CMTS auto-generates Route Distinguisher (RD), Route-Target (RT), L2VPN Extended Community and L2VPN NLRI that are encoded in a BGP UPDATE message using the 4-byte BGP VPNID (Section B.3.21.1) and using local information such as BGP Router-ID, as described below.

- 1) The L2VPN Extended Community value is calculated by combining 2-byte BGP ASN with 4-byte BGP VPNID in this format ASN:BGP VPNID.
Note that the BGP VPNID is assumed to be an AS-wide unique number.
- 2) The RD value is the same as that of L2VPN Extended Community.
- 3) The RT value is the same as that of L2VPN Extended Community (and used as both import RT and export RT values), unless CM conveys import and export RT to CMTS via TLV 43.5.21.3 and 43.5.21.4.
- 4) The L2VPN NLRI is calculated by combining the RD (calculated above) with a 4-byte number formatted as follows: RD: POOL_NUMBER, where the 4-byte CMTS BGP Router-ID is used as the POOL_NUMBER.

According to [RFC 4761] and [RFC 6624], when BGP auto-discovery and PW signaling is used for a L2VPN, the CMTS will encode in a BGP UPDATE message a specific L2VPN/VPLS NLRI, Route-Targets and an additional Layer 2 Info Extended Community, as described below:

- 1) The L2VPN NLRI will be generated by the CMTS as follows:
 - a. The RD value is the same as that of the Route Distinguisher TLV (43.5.21.2).
 - b. The VE ID value is the same as that of the BGP CE-ID/VE-ID TLV (43.5.21.5). Please note that if the L2VPN instance is a Virtual Switch Instance and multiple local CMs are part of this VSI then the NLRI might have multiple VE-IDs/CE-IDs.
 - c. The rest of the L2VPN/VPLS NLRI fields (VE Block Offset, VE Block Size and Label Base) will be generated by the CMTS based on internal variables.
- 2) The RT value is the same as that of the RD (and used as both import RT and export RT values), unless CM conveys import and export RT to CMTS via TLV 43.5.21.3 and 43.5.21.4.
- 3) The L2 Info Extended Community will be generated by the CMTS as follows:
 - a. Encapsulation Type will be set to point-to-point Ethernet RAW Mode (5), unless a different value is conveyed by the CM via the MPLS PW Type TLV (43.5.2.4.3). Acceptable values: Ethernet Tagged Mode (4), RAW Mode (5) and VPLS(19),
 - b. The rest of the fields (Control Flags and Layer2 MTU) will be generated by the CMTS based on internal variables.

Following [RFC 6074] or [RFC 4761]/[RFC 6624] upon receiving a BGP UPDATE message from any of the remote PE routers, the CMTS checks for the matching RT value (e.g., checks the received RT value with the local RT value that was auto-generated). If a match is found, then the CMTS concludes to have discovered the remote PE router for that L2VPN. The CMTS invokes LDP to setup the PW with that remote PE router (identified by its IP address that was in BGP NEXT_HOP attribute), as per [RFC 6074] or, in the [RFC 4761]/[RFC 6624] case, starts using the information in the L2VPN/VPLS NLRI and the L2 Info Extended Community to setup the PW.

If CMTS instantiated a P2P L2VPN, then CMTS SHOULD setup the PW with only one remote PE using LDP signaling [RFC 4447] or BGP signaling [RFC 6624]. If CMTS instantiated a multipoint L2VPN, then CMTS SHOULD setup the PW with one or more remote PEs using LDP signaling [RFC 4447] or BGP signaling [RFC 4761], as/when they get discovered using MP-BGP.

If the CMTS discovers more than one remote PE router for an L2VPN that is locally marked P2P L2VPN, then the CMTS MUST tear down any pre-established PW for that L2VPN. In such case, the CMTS SHOULD generate an

error (e.g., syslog). This helps to avoid any misconfiguration of remote PE routers and avoids possible L2VPN leakage. Note that there is nothing in BGP that identifies a given advertisement as P2P or Multipoint L2VPN.

A CMTS MUST support LDP for PW signaling, as per [RFC 4447]. Specifically, the CMTS MUST use Generalized PWid FEC Element (e.g., AGI, SAIL, TAIL) to establish the PW using LDP, as per [RFC 6074]. This means that AGI = L2VPN Extended Community Value, SAIL = Local POOL_NUMBER and TAIL = Remote POOL_NUMBER.

A CMTS MUST support MPLS Encapsulation, as per [RFC 4448]. In data plane, the CMTS encapsulates the upstream Ethernet frames received on an L2VPN Service Flow into an Ethernet over MPLS PW [RFC 4448]. Similarly, the CMTS decapsulates the downstream MPLS packets received on NSI port and forwards the resulting Ethernet frames to the CM via the downstream service flow.

If LDP is used for PW establishment, the PSN tunnel is an MPLS tunnel (e.g., an MPLS data plane on the NSI of CMTS).

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 independent of the NSI encapsulation. If the subscriber-tagged packet is forwarded with 802.1Q NSI Encapsulation on an 802.1Q NSI Ethernet port, the CMTS MUST prepend an outer 802.1Q tag before the inner subscriber-provided tag.

A CMTS MUST be able to send and receive for L2VPN forwarding on all interfaces packets as large as the maximum supported packet PDU length as defined in [DOCSIS MAC]. The maximum packet PDU length supported in a pre-3.1 DOCSIS CMTS is 1522 bytes and in a DOCSIS 3.1 CMTS is 2000 bytes.

For example, on an Ethernet NSI interface accepting 802.1Q tags for L2VPN NSI Encapsulation, the CMTS accepts and forwards a 1526 byte (pre-3.1 DOCSIS) or a 2004 byte (DOCSIS 3.1) Ethernet packet. For pre-3.1 DOCSIS, 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. For DOCSIS 3.1 such a packet is forwarded to the downstream RF MAC domain as a 2000 byte packet consisting of a nominal maximum length 1996 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 [DOCSIS MAC]. 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 [DOCSIS MAC] to upstream L2VPN forwarded packets.

The CMTS MUST NOT perform the TOS Overwrite function [DOCSIS MAC] for upstream L2VPN-forwarded packets.

An L2VPN forwarder maintains an out-of-band 3-bit user priority, as defined in Section 6.7.2.2, associated with each forwarded packet. 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 or in the Traffic Class bits of an MPLS header). The CMTS SHOULD provide mapping of upstream user priority to NSI port transmission traffic class as specified for the NSI Encapsulation format. The number of NSI port transmission traffic classes is vendor-specific. If an upstream service flow L2VPN Encoding omits the Upstream User Priority subtype, the CMTS MUST by default forward such packets to an NSI port with a user priority of zero. The CMTS MAY forward with non-zero default user priority values with vendor-specific configuration. The CMTS MAY also use this out-of-band 3-bit user priority of received NSI encapsulated packets for downstream classification (e.g., in the case of multipoint L2VPN forwarding).

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 or REG-REQ-MP with an L2VPN Encoding if BPI is not also enabled in the REG-REQ or REG-REQ-MP. 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 ([DOCSIS MAC]) 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, REG-REQ-MP, 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.