

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.213

(11/2006)

SERIES J: CABLE NETWORKS AND TRANSMISSION
OF TELEVISION, SOUND PROGRAMME AND OTHER
MULTIMEDIA SIGNALS

Interactive systems for digital television distribution

Layer 2 virtual private networks for IP cable modem systems

ITU-T Recommendation J.213



International
Telecommunication
Union

Documents
Document Sharing Hub

ITU-T Recommendation J.213

Layer 2 virtual private networks for IP cable modem systems

Summary

ITU-T Recommendation J.213 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.

Source

ITU-T Recommendation J.213 was approved on 29 November 2006 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2007

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Definitions	1
4	Abbreviations and acronyms	3
5	Conventions	4
5.1	Requirements.....	4
5.2	Conformance	4
6	Theory of operation (Informative).....	5
6.1	L2VPN features	5
6.2	CMTS layer-2 forwarding architecture	7
7	L2VPN operation.....	10
7.1	CMTS bridging model requirements.....	10
7.2	Configuring L2VPN forwarding	11
7.3	CMTS upstream L2VPN forwarding	19
7.4	CMTS downstream L2VPN forwarding	20
7.5	L2VPN isolation and privacy	22
7.6	CM and eSAFE exclusion	24
7.7	L2VPN quality of service.....	27
7.8	Stacked 802.1Q tags or tag-in-tag operation	29
7.9	Spanning tree and loop detection	29
8	Cable modem requirements	30
Annex A	– CMTS DOCS-L2VPN-MIB requirements	32
A.1	DOCS-L2VPN-MIB conformance	32
A.2	DOCS-L2VPN-MIB definitions.....	35
Annex B	– Parameter encodings	53
B.1	Capabilities	53
B.2	Downstream unencrypted traffic (DUT) filtering encoding.....	53
B.3	L2VPN encoding	54
B.4	Confirmation codes	60
B.5	L2VPN error encoding	60
B.6	CM interface mask classification criteria	62
Appendix I	– Example L2VPN encodings.....	63
I.1	Point-to-point example	63
I.2	Multipoint example	67
I.3	Upstream L2VPN classifier example	72

	Page
Appendix II – IEEE 802.1Q encapsulation.....	73
Appendix III – Embedded VLAN CM bridging model.....	74
III.1 IEEE 802.1Q and embedded VLAN model	75
III.2 Embedded bridge MAC domain service primitives	76
Appendix IV – L2VPN non-compliant CM restrictions.....	78
IV.1 Leaking through non-compliant CMs	78
Bibliography.....	80

ITU-T Recommendation J.213

Layer 2 virtual private networks for IP cable modem systems

1 Scope

This Recommendation 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.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[IEEE 802.1Q] IEEE Std 802.1Q-2005, *Virtual Bridged Local Area Networks*.

[ITU-T J.122] ITU-T Recommendation J.122 (2002), *Second-generation transmission systems for interactive cable television services – IP cable modems*.

[ITU-T J.125] ITU-T Recommendation J.125 (2004), *Link privacy for cable modem implementations*.

3 Definitions

This Recommendation defines the following terms and uses those defined in [ITU-T J.122].

3.1 bridged network: A set of IEEE 802 LANs interconnected by IEEE 802.1D MAC bridges.

3.2 compliant CM: A CM that implements this DOCSIS L2VPN Recommendation.

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

3.4 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).

3.5 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.

3.6 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.

3.7 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.

3.8 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.

3.9 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.

3.10 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.

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

3.12 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".

3.13 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.

3.14 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.

3.15 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.

3.16 non-compliant CM: A CM that does not implement this DOCSIS L2VPN Recommendation.

3.17 point-to-point L2 forwarding: Operation of an L2 forwarder between only two L2 networks with no source MAC address learning.

3.18 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 [ITU-T J.125] that includes a security association ID (SAID).

3.19 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.

3.20 tag header: A 16-bit tag protocol ID (0x8100) followed by a 16-bit tag control field. The tag control field consists of a 3-bit User Priority field, a 1-bit Canonical Format Indicator, and a 12-bit VLAN ID [IEEE 802.1Q].

3.21 transparent LAN service (TLS): A service offering of a cable operator that implements a private L2VPN among the CPE networks of the CMs of a single subscriber enterprise.

3.22 virtual LAN (VLAN): A *subset* of the LANs of an IEEE 802.1 bridged network to which a VLAN identifier (VLAN ID) is assigned. An L2VPN may consist of several VLANs, each with different VLAN IDs, and even of VLANs on different IEEE 802.1 bridged networks with the same VLAN ID.

3.23 virtual LAN identifier (VLAN ID): An IEEE 802.1Q VLAN ID is a 12-bit number that identifies a VLAN within an IEEE 802.1 bridged network. An IEEE 802.1ah stacked VLAN ID consists of an outer service 12-bit VLAN ID and an inner customer 12-bit VLAN ID.

3.24 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.

3.25 management L2VPN: An L2VPN for the post-registration SNMP traffic to eCM or eSAFE devices. May be combined with a provisioning L2VPN.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BPI	Baseline Privacy Interface
BSoD	Business Services over DOCSIS
CMIM	CM Interface Mask
CRC	Cyclic Redundancy Check
DIME	Downstream IP Multicast Encryption
DMAC	Destination MAC
DUT	Downstream Unencrypted Traffic
eCM	embedded Cable Modem [ITU-T J.126]
eMTA	embedded Media Terminal Adapter [ITU-T J.167]
ePS	embedded Portal Services [ITU-T J.192]
eSAFE	embedded Service/Application Functional Entity [b-ITU-T J.126]
GMAC	Group MAC address
L2	Layer 2
L2VPN	Layer 2 Virtual Private Network
MAC	Media Access Control
SAID	Security Association Identifier
SID	(Upstream) Service Identifier
SMAC	Source MAC
TLS	Transparent LAN Service
TOD	Time of Day
VPN	Virtual Private Network

5 Conventions

5.1 Requirements

Throughout this Recommendation, 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 Recommendation.
MUST NOT	This phrase means that the item is an absolute prohibition of this Recommendation.
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 behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour 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 Recommendations. 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.

5.2 Conformance

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

A CMTS or CM implementing this Recommendation is said to be L2VPN compliant. For the remainder of this Recommendation, all references to a CMTS refer to an L2VPN-compliant CMTS. A CM that has not implemented this Recommendation 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 Recommendation are summarized in clause 8.

6 Theory of operation (Informative)

6.1 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.

6.1.1 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 [ITU-T J.122] was originally intended for residential subscriber connection to the public Internet. This Recommendation 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 6-1:

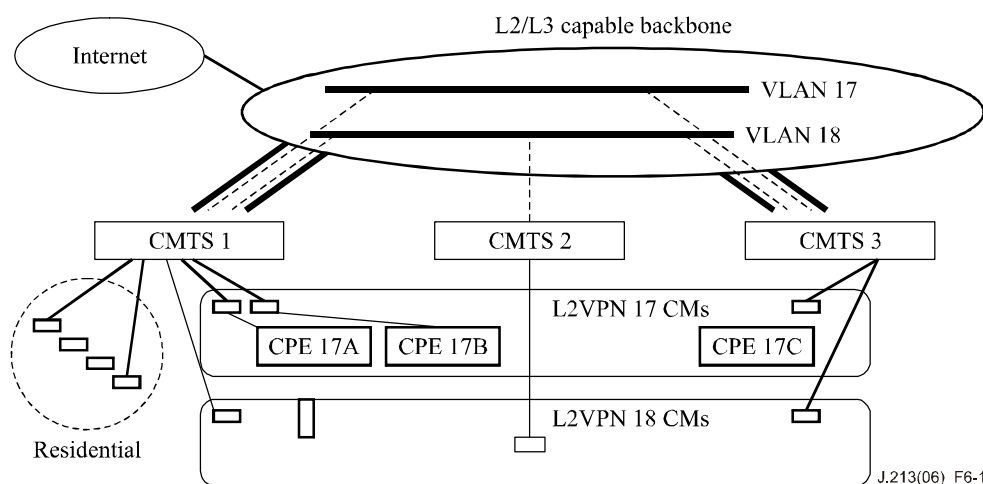


Figure 6-1 – Transparent LAN service

Figure 6-1 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 Recommendation, the term "VLAN" has a specific meaning as referring to the IEEE 802.1Q definition, as a subset of LANs, within a bridged network, to which is

assigned a 12-bit VLAN ID. In this example, 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. This includes learning the source MAC (SMAC) addresses of CPE 17A and CPE 17B, and associating them with the CM, from which those CPE attach.

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 L2VPN 17 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 coordinate 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.

6.1.2 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 coordination of IP address assignment and router security configuration between the MSO Provider Edge and ISP Customer Edge routers.

6.1.3 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) [b-ITU-T J.126], such as an embedded Media Terminal Adapter (eMTA) [b-ITU-T J.167], or embedded Portal Services functionality (ePS) [ITU-T J.192]. 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.

6.1.4 Other L2VPN-enabled features

Some features required by this Recommendation 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 clause 7.6.5. 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 clause 7.5.2.1.

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 clause 7.6.4.1.

6.2 CMTS layer-2 forwarding architecture

6.2.1 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 6-2:

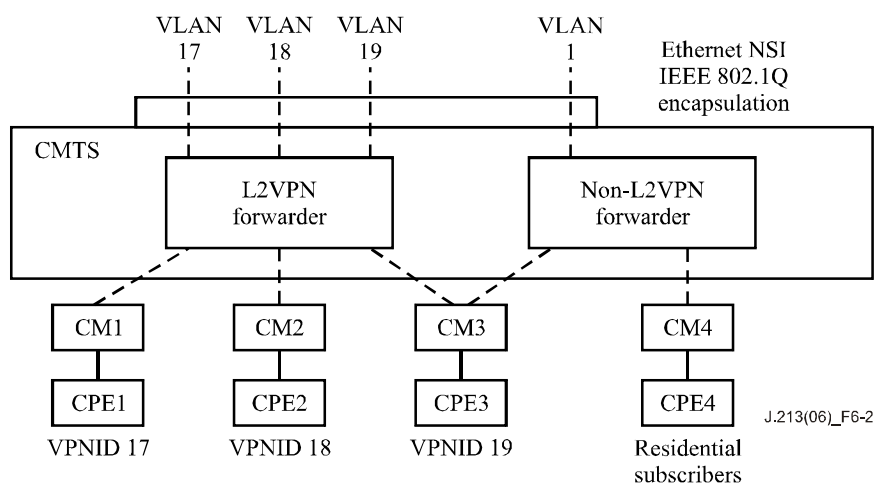


Figure 6-2 – CMTS L2VPN and non-L2VPN forwarding

To support L2VPN operation, a CMTS's network system interface (NSI) must be capable of distinguishing L2VPN from non-L2VPN downstream traffic, and determining the L2VPN of the downstream traffic. The encapsulation format of L2VPN traffic on a CMTS's 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 CPEs, 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 6-2, 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).

6.2.2 Point-to-point and multipoint L2VPN forwarding modes

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

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

An example of point-to-point forwarding mode is depicted in Figure 6-3:

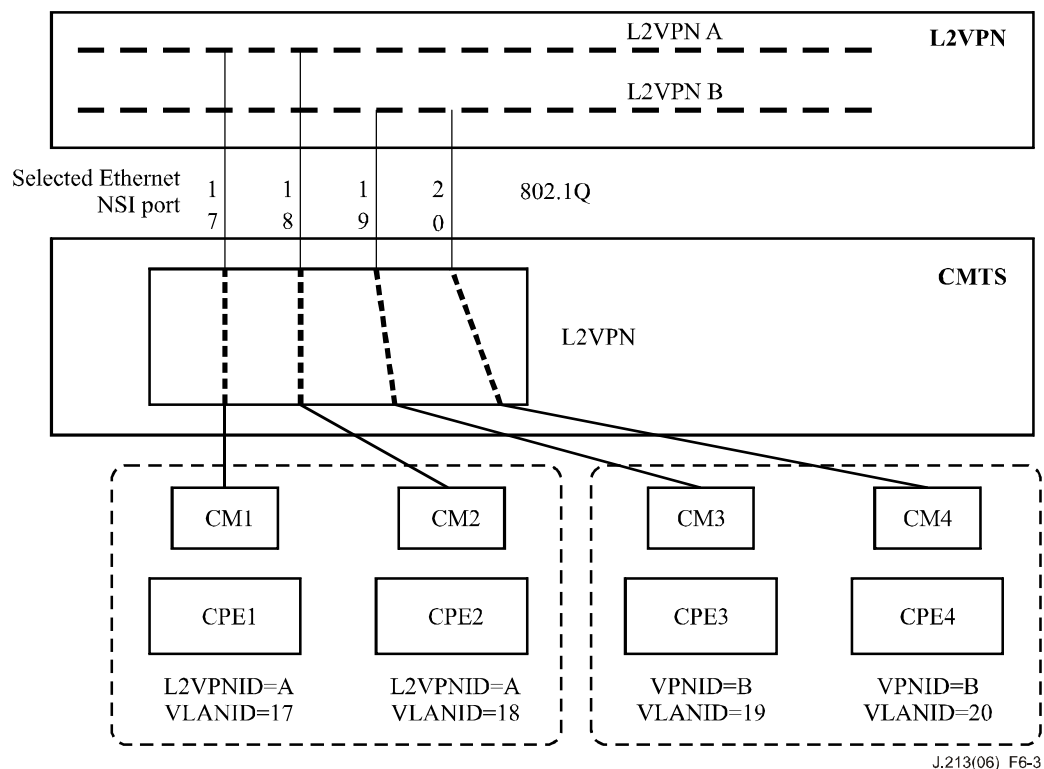


Figure 6-3 – Point-to-point forwarding mode

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

With IEEE 802.1Q NSI encapsulation point-to-point forwarding mode, 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 6-4.

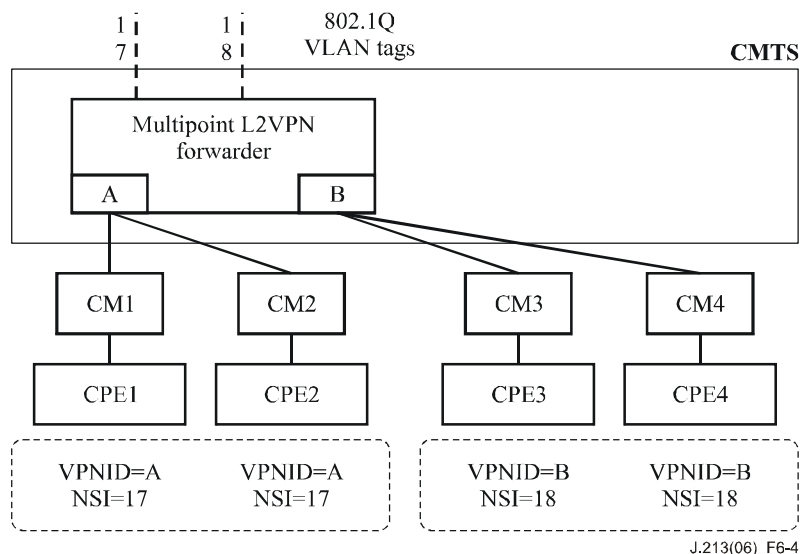


Figure 6-4 – Multipoint L2VPN forwarding mode example

In this example, both CM1 and CM2 are configured for L2VPN forwarding to VPNID A, and configured to use an NSI encapsulation of IEEE 802.1Q VLAN ID 17. The multipoint L2VPN forwarder learns the MAC addresses of CPE1 and CPE2 in order to determine to which CM to forward downstream unicast traffic received from the network port on VLAN ID 17. Likewise CM3 and CM4 are configured with VPNID B and both are configured to use IEEE 802.1Q VLAN ID 18 as their NSI encapsulation. The multipoint L2VPN forwarder learns the MAC addresses of CPE3 and CPE4 on L2VPN B. The non-L2VPN forwarder is not shown in Figure 6-4.

This Recommendation permits qualification of CMTSs with either point-to-point or multipoint forwarding modes. DOCSIS qualification testing shall use the forwarding mode indicated by the vendor's PICS submission for all L2VPNs. This Recommendation 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.

7 L2VPN operation

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

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

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

A CMTS MUST support both L2VPN and non-L2VPN forwarding on the same RF MAC domain. A CMTS MUST transparently bridge CPE traffic from CMs configured with L2VPN encodings according to this Recommendation. 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 Recommendation.

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

7.2 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 (see clause C.1.1.17 of [ITU-T J.122]). 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 subtype 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 subtype 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. Table 7-1 lists each of the subtypes and describes in which location the subtype is defined, as required or optional for that location.

Table 7-1 – 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 ^{c)}			
43.5.3	Enable eSAFE DHCP Snooping	Optional ^{a)}			
43.5.4	CM Interface Mask	Optional		Optional ^{a)}	Optional ^{a)}
43.5.5	Attachment Group ID	Optional ^{c)}			
43.5.6	Source Attachment Individual ID	Optional ^{c)}			
43.5.7	Target Attachment Individual ID	Optional ^{c)}			
43.5.8	Ingress User Priority		Optional		
43.5.9	User Priority Range			Optional	
43.5.10	L2VPN SA-Descriptor	Required ^{b)}			
43.5.43	Vendor-specific	Optional	Optional	Optional	Optional
^{a)} The CMTS MUST accept a parameter identified as Optional in this table in a non-forwarding L2VPN encoding. ^{b)} 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. ^{c)} This is a per-L2VPN configuration on the NSI port that is defined in a per-CM L2VPN encoding only for point-to-point forwarding mode.					

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

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

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

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

The simplest CM configuration file for L2VPN operation contains:

- for multipoint mode, a single per-SF L2VPN encoding within the primary upstream SF definition; or
- for point-to-point mode, a 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 labelling downstream packets as L2VPN traffic for the CM. The CMTS MAY assign more than one SAID to the same L2VPN, in which case multiple L2VPN SA-descriptor subtypes may appear in a top-level L2VPN encoding.

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

The CMTS MUST reject the registration of a CM with an invalid L2VPN encoding. A valid CM configuration contains any number of per-SF L2VPN encodings, downstream classifier L2VPN encodings and upstream classifier L2VPN encodings. The CMTS MUST accept a CM registration request that contains multiple per-SF L2VPN encodings that forward to the same VPN ID.

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

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

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

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

7.2.1 VPNID subtype

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

A cable operator is expected to configure a unique VPNID for each commercial enterprise to which it offers transparent LAN service. The cable operator may choose any format desired for the VPNID, but it should be globally unique. One suggested approach is [b-IETF 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 VPNID assigned by that organization. Another suggested approach is [b-IETF RFC 2547], which describes an 8-byte route distinguisher that may be used as a globally-unique VPNID.

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

In an IETF virtual private LAN service (VPLS) application, the VPNID is intended to be the attachment group ID (AGI) signalled between the CMTS and other VPLS network elements.

7.2.2 Downstream classifier L2VPN encoding

A downstream classifier L2VPN encoding is an L2VPN encoding that appears in a downstream packet classification encoding (see clause C.2.1.2 of [ITU-T J.122]). 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 VPNID subtype and/or zero or one user priority range subtype. 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 VPNID or user priority.

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

If the downstream classifier L2VPN encoding contains a user priority range subtype, the classifier applies only to L2VPN packets forwarded downstream with an egress user priority within the indicated range (inclusive). This allows high priority L2VPN traffic to be classified to downstream service flows with enhanced QoS.

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

A CMTS MUST reject the registration of a CM with a downstream packet classifier encoding that contains more than one L2VPN encoding.

7.2.3 L2VPN SA-descriptor subtype

The L2VPN SA-descriptor subtype is a multiple-part encoding defined in the baseline privacy [ITU-T J.125] 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 signalled in a CM configuration file. Instead, the CMTS adds one or more L2VPN SA-descriptor subtypes to top-level per-CM L2VPN encodings of its REG-RSP to the CM, adding the per-CM L2VPN encoding to the REG-RSP if necessary. After a CM completes BPI authentication, it initiates a traffic encrypting key (TEK) transaction with the CMTS for each L2VPN SA-descriptor in a REG-RSP message.

The CMTS includes an L2VPN SAID in an L2VPN SA-descriptor subtype encoding at the top level of a CMTS-initiated DSA-REQ or DSC-REQ message that otherwise defines a L2VPN forwarding upstream SF. Likewise, the CMTS includes an L2VPN SA-descriptor subtype in a top-level L2VPN encoding in its DSA-RSP or DSC-RSP responses to a CM-initiated dynamic service transaction, defining an L2VPN forwarding upstream service flow. A SAID signalled 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. Clause 7.5 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.

7.2.4 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.

7.2.5 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.

7.2.6 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 Recommendation 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.

7.2.6.1 NSI encapsulation subtype

Although this Recommendation 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 Recommendation defines an NSI encapsulation subtype of an L2VPN encoding (see clause B.3.2) to optionally describe how 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 pseudowires or internal virtual switch instances.

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

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

A point-to-point forwarding CMTS MUST reject a CM registration or service flow transaction with an L2VPN encoding that omits the NSI encapsulation subtype or a vendor-specific subtype that identifies the NSI service multiplexing value. A multipoint forwarding CMTS does not require an NSI encapsulation subtype in an L2VPN encoding, but MUST accept and implement the subtype if

it is specified. A CMTS in either forwarding mode MUST reject a CM registration or service flow transaction with an L2VPN encoding that contains an NSI encapsulation subtype for a VPNID that differs from the NSI encapsulation subtype for that VPNID within any other accepted L2VPN encoding.

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

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

7.2.6.2 IEEE 802.1ad L2VPN forwarding

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

7.2.6.2.1 Point-to-point CMTS forwarding with point-to-point 802.1ad forwarding

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

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

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

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

7.2.6.2.2 Point-to-point CMTS forwarding with L2VPN bridging network element

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

In this scenario, the inner VLAN ID tag represents the logical L2VPN, and the outer VLAN ID tag represents an individual attachment circuit to that logical L2VPN. The IEEE 802.1ad L2VPN switch considers the outer VLAN ID tag to represent a separate virtual trunk interface, while the inner tag represents a logical switch. The 802.1ad L2VPN switch builds an L2 forwarding database based on the MAC addresses it learns from each virtual trunk interface, and forwards/floods packets among those virtual trunk interfaces. In this manner, it provides L2VPN switch forwarding between all attachment circuits of an L2VPN. Using this technique, over 4'000 L2VPN service instances can be supported between one CMTS and the IEEE 802.1ad L2VPN switch, and each of these can have over 4'000 cable modems/service flow associations at the CMTS.

7.2.7 Virtual private LAN service (VPLS) and virtual private wire service

7.2.7.1 MPLS and L2TPv3 NSI encapsulation

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

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

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

7.2.7.2 VPLS/VPWS configuration

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

- attachment group ID;
- source attachment individual ID (SAII); and
- target attachment individual ID (TAII).

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

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

The source attachment individual ID (SAII) subtype is defined only in a per-SF forwarding L2VPN encoding. It indicates the value dynamically signalled by the L2VPN forwarder as the SAII field when advertising an NSI encapsulation service multiplexing value such as an MPLS label or L2TPv3 session identifier. This field is used only for IETF L2VPN applications such as virtual private LAN service (VPLS) or virtual private wire service (VPWS) when the CMTS operates in point-to-point forwarding mode between NSI pseudowires and CM/SF attachment circuits. The configured SAII is intended to match the target attachment individual ID (TAII) of an incoming dynamic pseudowire establishment request.

The target attachment individual ID (TAII) subtype is defined only in a per-SF forwarding L2VPN encoding. It provides the value dynamically signalled by the L2VPN forwarder as the TAI field when initiating the establishment of an IETF L2VPN pseudowire on an NSI interface. This field is used only for IETF L2VPN applications such as VPLS or VPWS when the CMTS is initiating a

pseudowire to a remote network element that is implementing point-to-point forwarding. The TAI is intended to match the SAI of one of the attachment circuits of the remote network element.

A CMTS SHOULD use any configured attachment group ID (AGI) subtype, source attachment individual ID (SAII) subtype or target attachment individual ID (TAII) subtypes configured in a forwarding L2VPN encoding for the values of the corresponding fields with IETF-specified protocols that attempt to establish an NSI pseudowire switched to an attachment circuit.

7.3 CMTS upstream L2VPN forwarding

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

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

The CMTS MUST NOT count learned L2VPN CPE MAC addresses learned from upstream packets towards any enforced docsSubMgtCpeControlMaxCPEIp setting for the CM (see clause C.1.1.18.1 of [ITU-T J.122]). 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 (see clause C.1.1.18 of [ITU-T J.122]) to upstream L2VPN forwarded packets.

The CMTS MUST NOT perform the ToS overwrite function (see clause C.2.2.6.10 of [ITU-T J.122]) for upstream L2VPN-forwarded packets.

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

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

A CMTS MAY recognize when the CM interface masks in the set of upstream packet classifier L2VPN encodings of a compliant CM permit it to avoid checking upstream source MAC addresses

and instead forward upstream packets to the L2VPN or non-L2VPN forwarder solely on the basis of the upstream service flow.

The CMTS MUST recognize a CM interface mask criterion in a downstream packet classifier L2VPN encoding regardless of whether the encoding classifies L2VPN or non-L2VPN traffic. The CMTS MUST classify the destination MAC address of a downstream packet as one of three classes:

- 1) A CM MAC address;
- 2) a CPE MAC address; or
- 3) an eSAFE MAC address of a particular eSAFE host type.

The CMTS MUST consider the criterion to be matched when the destination MAC address of the downstream layer-2 packet is a CM MAC address or eSAFE MAC address that corresponds to a host type with a '1' in the CM interface mask. The CMTS MUST consider the criterion to be matched when the destination MAC address is a CPE MAC address and the CM interface mask has *any* CPE host type bit set, i.e., any of bits 1 or 5-15 set. The CMTS MUST consider the criterion to be unmatched when the destination MAC address is a CM or eSAFE MAC address and the single CM Interface mask bit corresponding to that host type has a '0' bit. The CMTS MUST consider the criterion to be unmatched when the destination MAC address is a CPE MAC address and the CM Interface Mask has a zero bit in all CPE host type positions, i.e., has a zero bit in positions 1 and 5-15.

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

7.4 CMTS downstream L2VPN forwarding

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

The CMTS MUST NOT apply subscriber management filters (see clause C.1.1.18 of [ITU-T J.122]) to downstream L2VPN forwarded traffic.

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

- The CMTS MUST reject the registration of cable modems with invalid downstream packet classification encodings.
- A valid downstream classification L2VPN encoding contains zero or one VPNID subtypes, zero or one User Priority Range subtype, and any number of vendor-specific L2VPN parameter subtypes. The CMTS MUST silently ignore all invalid L2VPN encoding subtypes.
- The CMTS MUST accept as valid and silently ignore any unrecognized L2VPN encoding subtypes.
- The CMTS MUST accept multiple downstream classification configuration settings with a downstream classifier L2VPN encoding that classify different L2VPN VPN IDs to the same referenced service flow.
- The CMTS MUST support the same classifier criteria options for downstream classifier L2VPN encodings as it does for non-L2VPN downstream classifier L2VPN encodings.

- The CMTS MUST interpret a downstream packet classifier encoding containing no other criteria than a classifier L2VPN encoding as matching *all* packets forwarded downstream on the L2VPN identified by the VPNID of the classifier L2VPN encoding, and classify all such packets to the referenced service flow.
- The CMTS MAY accept multiple downstream classifier L2VPN encodings with the same VPNID classifying packets to different service flows. Operation is undefined when more than one downstream classifier matches a particular downstream packet.
- The CMTS MUST reject a service flow transaction request containing an invalid downstream classifier L2VPN encoding.
- If the L2VPN encoding contains a user priority range subtype, the CMTS MUST match the classifier only to L2VPN forwarded packets with an egress user priority within the indicated range. Otherwise, the classifier applies to all egress user priorities.

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

The CMTS MUST classify layer-2 packets as they appear on the RFI interface, that is, NOT including any service-delimiting 802.1Q tag that appeared on the CMTS NSI port. This means that the 802.1Q packet classification encodings (see clause C.2.1.7 of [ITU-T J.122]) apply only to the subscriber-private or inner 802.1Q tag, and not the VLAN ID of the L2VPN-forwarded packet.

A CMTS MUST NOT apply subscriber management filters (see clause C.1.1.18 of [ITU-T J.122]) to downstream L2VPN traffic.

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

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

7.4.1 Multipoint downstream forwarding

The CMTS MUST reject (with a reject-permanent confirmation code) a registration or service flow transaction that would require defining L2VPN SAIDs exceeding the CM's downstream SAID capability (see clause C.1.3.1.7 of [ITU-T J.122]).

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

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

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