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

L2VPN Development Guidelines Technical Report

CM-TR-L2VPN-DG-V01-080328

RELEASED

Notice

This DOCSIS technical report is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by CableLabs. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document.

Neither CableLabs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein.

Abstract

This technical report offers development phase guidance for the Business Services over DOCSIS L2VPN specification. The intended audience for this document includes operators designing new services and developers looking to implement the L2VPN specification in a phased manner.

This technical report contains the following information:

- A list of requirements with their phase priority;
- Special considerations for certain high-level features;
- A description of new L2VPN MAC aging behavior.

The L2VPN specification takes precedence over this technical report if the technical report contradicts any specification requirements.

Document Status Sheet

Document Control Number:	CM-TR-L2VPN-DG-V01-080328
Document Title:	L2VPN Development Guidelines Technical Report
Revision History:	V01 – Released 03/28/08
Date:	March 28, 2008

Trademarks:

Table of Contents

Tables

1 INTRODUCTION

This technical report offers guidelines to manufacturers as to how to phase the implementation of requirements defined in [L2VPN]. These guidelines are intended to improve time to market on those features that will allow operators to offer a Metro Ethernet Forum (MEF) compliant Layer 2 Transparent LAN Service (TLS) to commercial enterprises. Phase designations are only applicable to CMTS products. Cable modems are expected to support all required L2VPN features present in [L2VPN] in Phase 1.

Phase 1 designation is for those requirements desired by operators in the 2008 timeframe. These requirements will allow operators to offer a basic transparent LAN service supporting a single L2VPN per cable modem, bound to the cable modem's primary Ethernet interface.

Phase 2 is expected by operators in the late 2008-early 2009 timeframe. Phase 2 requirements include most of the remaining requirements in [L2VPN].

Phase 3 includes advanced features that operators would like to deploy in the future. Phase 3 features may require additional specification work beyond the current [L2VPN] specification.

2 REFERENCES

2.1 Normative References

There are no normative references in this technical report.

2.2 Informative References

This technical report uses the following informative references.

[L2VPN] Business Services over DOCSIS, Layer 2 Virtual Private Networks, CM-SP-L2VPN-I06-071206, December 6, 2007, Cable Television Laboratories, Inc.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027-9750; Phone +1 303-661-9100; Fax +1 303-661-9199; Internet: http://www.cablemodem.com/.

3 TERMS AND DEFINITIONS

This DOCSIS Technical Report uses the following terms and definitions:

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.
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 customer enterprise.

4 ABBREVIATIONS AND ACRONYMS

This DOCSIS Technical Report uses following abbreviations and acronyms:

CMCI Cable Modem Customer Interface

CMIM CM Interface Mask

CPE Customer Premises Equipment

DIME Downstream IP Multicast Encryption

eMTA Embedded Media Transport Agent

eSAFE Embedded Service/Application Functional Entity

L2VPN Layer 2 Virtual Private Network

MAC Media Access Control

MIB Management Information Base

VPNID Virtual Private Network Identifier

TLS Transparent LAN Service

5 SPECIAL SCOPE CHANGE CONSIDERATIONS

Section 5.3 details the phase priorities for CMTS L2VPN requirements. CMs are expected to implement all requirements specified in [L2VPN] beginning in Phase 1. Four changes to [L2VPN] require additional explanation. In particular, per-CM L2VPNs, support for L2VPN MIBs, CM Max CPE limits, and support for L2VPN MAC Aging are detailed below. This section describes those changes in more detail.

5.1 Per-CM L2VPNs

Phase 1 CMTSs will support a single L2VPN VPNID per cable modem. Cable modems will use per-CM L2VPN encodings. Multiple per-Service Flow L2VPN encodings and dynamic L2VPN service changes (using DSx messages) need not be supported until Phase 2. During Phase 1, 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 traffic to an L2VPN.

5.2 MIB support

The following MIB tables should be included in Phase 1. Additional MIB tables defined in [L2VPN] should be included in Phase 2.

- DocsL2vpnIdToIndex Table
- DocsL2vpnIndexToId Table
- DocsL2vpnVpnCmStats Table

5.3 Max CPE

L2VPN cable modems should support a Max CPE value of 64 in Phase 1, and 128 in Phase 2.

5.4 Modem support for CPE MAC Aging

In order to support Metro Ethernet Forum (MEF) functionality, L2VPNs should implement an aging mechanism for MAC addresses stored in the modem's bridging table. If the modem sees a new MAC address of a packet to be forwarded to the upstream RF interface and if the modem's bridging table is full (contains as many entries as specified by the Max CPE value), the CM will overwrite the bridging table entry for the MAC address of a device that has not transmitted a packet destined for the upstream RF interface for the longest amount of time. Such an aging mechanism will not overwrite any statically provisioned addresses in the bridging table. This functionality will override the DOCSIS requirements for CPE aging. When used for MEF certification, standard DOCSIS CM implementations would limit the total number of CPE devices that could attach to a particular modem. L2VPN MAC aging provides a simple way of working within the limits on the number of total clients supported in the CM bridging table, although the CM is subject to the Max CPE limitation on the number of simultaneous clients supported. This functionality is expected in Phase 1.

6 PHASED L2VPN REQUIREMENTS

Table 1 lists the L2VPN requirements present in [L2VPN] and assigns them into phases, as defined in Section 1. These requirements should be implemented as-written in the L2VPN specification unless noted in Section 5 of this document.

Table 1: Phased Requirements

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1286	A DOCSIS CMTS that claims to implement the DOCSIS L2VPN feature MUST implement the normative provisions of this document.	CMTS	MUST	1
REQ1287	A DOCSIS CM that claims conformance for DOCSIS L2VPN feature MUST implement the normative requirements of this document.	CM	MUST	1
REQ1288	An L2VPN-compliant CMTS MUST support an L2VPN non-compliant CM.	CMTS	MUST	1
REQ1289	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.	CMTS	MUST	1
REQ1290	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.	CMTS	MUST	1
REQ1291	A L2VPN compliant CMTS MUST NOT insert an 802.Q tag on downstream RF packets.	CMTS	MUST NOT	1
REQ1292	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.	CMTS	MUST	2
REQ1293	In Multipoint forwarding mode, the CMTS MUST associate learned CPE source MAC addresses with the particular CM from which they were learned.	CMTS	MUST	1
REQ1294	A CMTS MUST support both L2VPN and non-L2VPN forwarding on the same RF MAC domain.	CMTS	MUST	1
REQ1295	A CMTS MUST transparently bridge CPE traffic from CMs configured with L2VPN Encodings according to this specification.	CMTS	MUST	1
REQ1296	A CMTS MUST forward with its normal, non-L2VPN packet forwarding algorithms CPE traffic from CMs with no L2VPN Encodings, except as specified in this specification.	CMTS	MUST	1
REQ1297	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.	CMTS	MUST	2
REQ1298	The CMTS MUST accept a parameter identified as optional(1) in Table 6-1 in a non-forwarding L2VPN Encoding.	CMTS	MUST	1
REQ1299	A CMTS MUST silently ignore unrecognized subtypes in an L2VPN Encoding.	CMTS	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1300	A CM MUST silently ignore unrecognized subtypes in an L2VPN Encoding.	CM	MUST	1
REQ1301	The CMTS MUST reject the registration of a CM with an invalid L2VPN Encoding.	CMTS	MUST	1
REQ1302	The CMTS MUST accept a CM registration request that contains multiple per-SF L2VPN Encodings that forward to the same VPN ID.	CMTS	MUST	1
REQ1303	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.	CMTS	MUST	2
REQ1304	The CMTS MUST reject a service flow transaction that contains more than one per-SF L2VPN Encoding.	CMTS	MUST	2
REQ1305	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.	CMTS	MUST	2
REQ1306	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.	CMTS	MUST	2
REQ1307	The CMTS MUST support multiple per-SF L2VPN Encodings, each on a separate SF, with the same VPNID Subtype value.	CMTS	MUST	2
REQ1308	The CMTS MUST ignore a per-SF L2VPN encoding that omits a VPNID subtype or that contains more than one VPNID subtype.	CMTS	MUST	2
REQ1309	The CMTS MUST support at least four (4) different values of VPNID per CM, signaled in four or more per-SF L2VPN Encodings.	CMTS	MUST	2
REQ1310	A CMTS MUST reject the registration of a CM with a Downstream Packet Classifier Encoding that contains more than one L2VPN Encoding.	CMTS	MUST	2
REQ1311	A CMTS MUST encode the L2VPN SA-Descriptor as a Dynamic(2) SA-Type.	CMTS	MUST	1
REQ1312	A CM MUST ignore the SA-Type and consider it to be of type Dynamic(2).	CM	MUST	1
REQ1313	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.	CMTS	MAY	1
REQ1314	A Multipoint forwarding CMTS MUST reject--with a reject-multipoint-NSI confirmation code--a registration or dynamic service transaction that attempts to configure multiple upstream forwarding L2VPN Encodings to the same L2VPN ID but with different values of the NSI Encapsulation, AGI, TAII, or SAII subtypes.	CMTS	MUST	2
REQ1315	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.	CMTS	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1316	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.	CMTS	MUST	1
REQ1317	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.	CMTS	MUST	1
REQ1318	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.	CMTS	MUST	1
REQ1319	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.	CMTS	MUST	1
REQ1320	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.	CMTS	MUST	1
REQ1321	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.	CMTS	MUST NOT	1
REQ1322	The CMTS MUST transparently forward any subscriber-provided 802.1Q tag.	CMTS	MUST	1
REQ1323	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.	CMTS	MUST	1
REQ1324	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.	CMTS	MUST	1
REQ1325	The CMTS MUST NOT count learned L2VPN CPE MAC addresses learned from upstream packets towards any enforced docsSubMgtCpeControlMaxCPEIp setting for the CM [RFI 2.0] C.1.1.18.1.	CMTS	MUST NOT	1
REQ1326	The CMTS MUST NOT apply subscriber management filtering [RFI 2.0] C.1.1.18 to upstream L2VPN forwarded packets.	CMTS	MUST NOT	1
REQ1327	The CMTS MUST NOT perform the TOS Overwrite function [RFI 2.0] C.2.2.6.10 for upstream L2VPN-forwarded packets.	CMTS	MUST NOT	1
REQ1328	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.	CMTS	MUST	1
REQ1329	The CMTS MUST use this user priority when classifying downstream packets.	CMTS	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1330	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).	CMTS	MUST	1
REQ1331	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.	CMTS	MUST	1
REQ1332	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.	CMTS	MUST	1
REQ1333	The CMTS MUST direct packets from the source MAC addresses indicated with a '1' in the CM Interface Mask to the L2VPN forwarder.	CMTS	MUST	2
REQ1334	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.	CMTS	MUST NOT	1
REQ1335	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.	CMTS	MUST	1
REQ1336	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.	CMTS	MUST	1
REQ1337	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.	CMTS	MUST	2
REQ1338	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.	CMTS	MUST	2
REQ1339	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.	CMTS	MUST	2
REQ1340	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.	CMTS	MUST	2
REQ1341	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.	CMTS	MUST	2
REQ1342	The CMTS MUST reject any REG-REQ with an L2VPN Encoding if BPI is not also enabled in the REG-REQ.	CMTS	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1343	The CMTS MUST reject any DSA-REQ or DSC-REQ with an L2VPN Encoding if BPI is not also enabled for the CM.	CMTS	MUST	2
REQ1344	The CMTS MUST NOT apply subscriber management filters ([RFI 2.0] section C.1.1.18) to downstream L2VPN forwarded traffic.	CMTS	MUST NOT	1
REQ1345	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.	CMTS	MUST	2
REQ1346	A CMTS MUST apply classifier rules that contain an L2VPN Encoding only to packets forwarded by the L2VPN Forwarder.	CMTS	MUST	1
REQ1347	The CMTS MUST reject the registration of cable modems with invalid Downstream Packet Classification Encodings.	CMTS	MUST	1
REQ1348	The CMTS MUST silently ignore all invalid L2VPN Encoding subtypes.	CMTS	MUST	1
REQ1349	The CMTS MUST accept as valid and silently ignore any unrecognized L2VPN Encoding subtypes.	CMTS	MUST	1
REQ1350	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.	CMTS	MUST	2
REQ1351	The CMTS MUST support the same Classifier criteria options for Downstream Classifier L2VPN Encodings as it does for non-L2VPN Downstream Classifier L2VPN Encodings.	CMTS	MUST	2
REQ1352	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.	CMTS	MUST	2
REQ1353	The CMTS MUST reject a service flow transaction request containing an invalid Downstream Classifier L2VPN Encoding.	CMTS	MUST	2
REQ1354	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.	CMTS	MUST	1
REQ1355	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.	CMTS	MUST	2
REQ1356	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.	CMTS	MUST	1
REQ1357	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.	CMTS	MUST	3
REQ1358	A CMTS MUST NOT apply Subscriber Management filters [RFI 2.0] C.1.1.18 to downstream L2VPN traffic.	CMTS	MUST NOT	1
REQ1359	A CMTS MUST forward downstream L2VPN-forwarded packets for different L2VPNs on different downstream service flows.	CMTS	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1360	Unless explicitly configured to combine the forwarding data base of different L2VPNs, the CMTS L2VPN Forwarder MUST maintain upstream and downstream separation of L2 forwarded traffic between attachment circuits configured with different VPNIDs.	CMTS	MUST	1
REQ1361	The CMTS MUST reject (with a reject-permanent confirmation code) a registration or service flow transaction that would require defining L2VPN SAIDs exceeding the CM's Downstream SAID capability ([RFI 2.0] C.1.3.1.7).	CMTS	MUST	1
REQ1362	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.	CMTS	MUST	1
REQ1363	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.	CMTS	MUST	1
REQ1364	A Multipoint forwarding CMTS MUST forward downstream packets encrypted on different L2VPN SAIDs on different service flows.	CMTS	MUST	1
REQ1365	The CMTS MUST reject an attempt (i.e., a registration or DSx transaction) to configure a forwarding L2VPN Encoding if the CM is not also configured to support BPI operation.	CMTS	MUST	1
REQ1366	A CMTS MUST assign at least one L2VPN SAID for downstream forwarding to each separate L2VPN forwarded by the CMTS on a downstream channel.	CMTS	MUST	1
REQ1367	The CMTS MUST assign a Group or Individual L2VPN SAID that differs from any other Primary SAID assigned on that channel.	CMTS	MUST	1
REQ1368	A CMTS MUST add to the forwarding L2VPN Encoding of its REG-RSP and Dynamic Service messages to an L2VPN-compliant CM one or more L2VPN SA-Descriptor Subtypes for its assigned L2VPN SAID(s) for downstream forwarding to that L2VPN on the CM's downstream channel.	CMTS	MUST	1
REQ1369	The CMTS MUST encode separate top-level L2VPN encodings for each separate L2VPN ID.A CMTS MAY add L2VPN SA-Descriptor Subtypes in messages to non-compliant CMs, but they will be ignored by the CM.	CMTS	MUST	1
REQ1370	The CMTS MUST describe the L2VPN SAIDs with an SA-Type of Dynamic in an L2VPN SA-Descriptor Encoding.	CMTS	MUST	1
REQ1371	A CMTS MUST encrypt all downstream L2VPN forwarded traffic in an L2VPN SAID assigned to the L2VPN.	CMTS	MUST	1
REQ1372	The CMTS MUST NOT forward downstream L2VPN traffic to a CM until that CM has completed BPI Authorization and TEK negotiation for the L2VPN SAID in which the traffic is to be encrypted.	CMTS	MUST NOT	1
REQ1373	A Multipoint forwarding CMTS MUST assign at least one broadcast L2VPN SAID to all CMs on the same MAC Domain attaching to the same L2VPN Identifier.	CMTS	MUST	1
REQ1374	The Multipoint forwarding CMTS MUST forward downstream broadcast packets of the L2VPN encrypted on such a broadcast L2VPN SAID.	CMTS	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1375	A CMTS that discontinues L2VPN forwarding through a CM MUST dynamically delete all upstream service flows forwarding to that L2VPN, and MUST signal a top-level L2VPN encoding to the CM that omits all SA-Descriptors for that L2VPN.	CMTS	MUST	1
REQ1376	A CMTS MUST implement a configurable option to enable or disable Downstream IP Multicast Encryption (DIME).	CMTS	MUST	2
REQ1377	With DIME enabled, the CMTS MUST encrypt all non-L2VPN downstream IP Multicast traffic that is either statically joined with the BPI+ MIB or dynamically joined with upstream SA-MAP requests from a CM.	CMTS	MUST	2
REQ1378	When the eCM self host interface is excluded from a CMIM subtype for an L2VPN forwarding upstream SF, the CMTS MUST exclude from upstream L2VPN forwarding all traffic that contains a source MAC that matches the CM host's MAC address.	CMTS	MUST	2
REQ1379	Because non-compliant CMs are unable to classify L2VPN from non-L2VPN upstream traffic, a CMTS MUST support both L2VPN and non-L2VPN forwarding of upstream traffic from a Forwarding L2VPN service flow of a non-compliant CM based on checking the source MAC address against a CM Interface Mask configured for the SF.	CMTS	MUST	1
REQ1380	The CMTS MUST direct packets from included host types to the L2VPN forwarder.	CMTS	MUST	1
REQ1381	The CMTS MUST NOT deliver traffic from excluded host types to the L2VPN Forwarder.	CMTS	MUST NOT	1
REQ1382	A CMTS MUST support exclusion of the CM MAC address and at least one other eSAFE MAC address on all L2VPN forwarding service flows from both non-compliant CMs and compliant CMs.	CMTS	MUST	1
REQ1383	A CMTS MUST learn the MAC address of an embedded CM from the Source MAC address of the CM's initial ranging request message and include it in the docsDevCmCmtsStatusTable.	CMTS	MUST	1
REQ1384	For L2VPN-compliant CMs, the CMTS MUST learn the eSAFE MAC addresses from the eSAFE Host Capability encodings section A.3.2 when the CM registers;	CMTS	MUST	1
REQ1385	For non-L2VPN-compliant CMs, the CMTS MUST snoop upstream DHCP packets to determine the eSAFE MAC addresses.	CMTS	MUST	1
REQ1386	The CMTS MUST enable DHCP snooping to determine eSAFE MAC addresses from a non-compliant CM when an Enable eSAFE DHCP Snooping subtype is present in any per-SF L2VPN Encoding A.5.3.	CMTS	MUST	1
REQ1387	The CMTS MUST NOT enable DHCP snooping when the Enable eSAFE DHCP Snooping subtype is absent from all per-SF L2VPN encodings or does not have a '1' bit for the particular eSAFE host type when it is present.	CMTS	MUST NOT	1
REQ1388	When eSAFE DHCP snooping is enabled, the CMTS MUST support detection of the eSAFE host type of a MAC address, from the initial substring of option 60 of the broadcast DHCP DISCOVER packet, from the eSAFE host that is relayed by the CMTS, when option 60 is present.	CMTS	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1389	When eSAFE DHCP snooping is enabled, the CMTS MUST support detection of the eSAFE host type of a MAC address from option 43, subtype 2 of a DHCP DISCOVER packet from the eSAFE host that is relayed by the CMTS, when option 43, subtype 2 is present.	CMTS	MUST	1
REQ1390	The CMTS MUST learn the eSAFE's MAC address from the client hardware identifier field of the snooped DHCP-DISCOVER packet.	CMTS	MUST	1
REQ1391	A CMTS MUST accept the priority bits of a service-delimiting 802.1Q tag on NSI port input as the L2VPN ingress user priority attribute of the packet.	CMTS	MUST	1
REQ1392	The CMTS MUST maintain the user priority of the packet within the L2VPN forwarder (possibly regenerating it via vendor-specific configuration), and use the egress value of user priority for matching against the User Priority Range subtype of Downstream Classifier L2VPN Encodings.	CMTS	MUST	1
REQ1393	When a User Priority Range subtype is present in a Downstream Service Flow Packet Classifier Encoding, the CMTS MUST match the classifier only to L2VPN forwarded packets with a user priority within the indicated range.	CMTS	MUST	1
REQ1394	The CMTS MUST NOT use any priority only tag applied by CPE to determine the ingress user priority of an upstream packet.	CMTS	MUST NOT	1
REQ1395	The CMTS MUST transmit an L2VPN upstream packet on an NSI port with the egress user priority encoded as appropriate for its NSI encapsulation.	CMTS	MUST	1
REQ1396	In order to prevent CPE abuse of backbone L2 user priorities, the CMTS MUST NOT interpret a priority-only tag applied by the CPE as defining the upstream ingress user priority of an L2VPN packet.	CMTS	MUST NOT	1
REQ1397	The CMTS MUST transparently forward the IEEE Spanning Tree Protocol (STP) on the subscriber's layer2 VPN.	CMTS	MUST	1
REQ1398	The CMTS MUST transmit DOCSIS Spanning Tree Protocol packets as untagged on an IEEE 802.1Q NSI interface and encrypted in a SAID provided to the L2VPN CMs on a CMTS MAC domain RF interface.	CMTS	MUST	1
REQ1399	A CMTS MUST prevent a bridging loop for one L2VPN from denying all forwarding or flooding of traffic on any other non-looped L2VPN.	CMTS	MUST	1
REQ1400	A CM MUST accept one or more L2VPN SA-Descriptor Subtypes added by a CMTS to any forwarding L2VPN Encoding in a REG-RSP or DSx-RSP message to the CM.	CM	MUST	1
REQ1401	The CM MUST be capable of associating any number of its available SAIDs to an L2VPN.	CM	MUST	1
REQ1402	The CM MUST be capable of associating more than one SAID to a single L2VPN.	CM	MUST	1
REQ1403	A CM receiving an L2VPN SA-Descriptor Subtype in a REG-RSP MUST wait for BPI Authorization to complete before initiating the BPKM TEK.	CM	MUST	1
REQ1404	A CM MUST replace the set of L2VPN SAIDs of an L2VPN when receiving a top-level L2VPN Encoding in a MAC Management message that identifies that L2VPN.	CM	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1405	The CM MUST discontinue downstream decryption of an L2VPN SAID when it receives in a dynamic service flow message a top-level L2VPN Encoding for an L2VPN ID that omits the SA-Descriptor subtype with that SAID.	CM	MUST	1
REQ1406	A CM MUST promiscuously forward all downstream group MAC (GMAC) destined traffic that is encrypted in an L2VPN SAID signaled to the CM, regardless of the GMAC destination of the packet.	CM	MUST	1
REQ1407	The CM MUST NOT apply the multicast filtering or forwarding rules of [RFI 2.0] section 5.3.1.3.1 to downstream GMAC traffic encrypted in an L2VPN SAID.	CM	MUST NOT	1
REQ1408	A CM MUST continue to implement downstream DOCSIS 2.0 group MAC forwarding rules for all unencrypted packets and packets encrypted in a non-L2VPN SAID.	CM	MUST	1
REQ1409	A CM MUST NOT implement the IGMP Multicast Forwarding rules of [RFI 2.0] section 5.3.1.3.1 for any upstream packets (e.g., IGMP Membership Reports) classified to a forwarding L2VPN service flow.	CM	MUST NOT	1
REQ1410	The CM MUST continue to implement DOCSIS IGMP Multicast Forwarding rules for upstream IGMP Membership Reports not classified to a forwarding L2VPN service flow.	CM	MUST	1
REQ1411	A compliant CM MUST restrict bridge forwarding of downstream packets encrypted in an L2VPN SAID to only the bridge interfaces indicated with a '1' bit in the CM Interface Mask (CMIM) configured for that L2VPN.	CM	MUST	1
REQ1412	A CM MUST support a classification rule criterion signaled with a CM Interface Mask (CMIM) in an L2VPN Encoding of an Upstream Classifier Packet Encoding, whether or not that Encoding classifies to a Forwarding L2VPN service flow.	CM	MUST	1
REQ1413	The CM MUST consider the criterion to be matched when the source MAC address of an upstream packet is for a host type with a '1' bit in the CM Interface Mask.	CM	MUST	1
REQ1414	The CM MUST consider the criterion to be unmatched and forward or drop a packet accordingly, when the source MAC address is for a host type with a '0' bit in the CM Interface Mask.	CM	MUST	1
REQ1415	A CM MUST support the Downstream Unencrypted Traffic (DUT) Filtering feature as described in B.2, and advertise this in a DUT Filtering Capability Encoding B.1.3.	CM	MUST	1
REQ1416	When DUT Filtering is enabled, a CM MUST restrict bridge forwarding of downstream unencrypted traffic to only the interfaces indicated in the DUT CM Interface Mask (DUT CMIM) implied or configured by the DUT Filtering Encoding.	CM	MUST	1
REQ1417	The CM MUST continue to report only ifIndex 1 as its primary CPE interface.	CM	MUST	1
REQ1418	A CM MUST forward upstream and downstream packets as large as 1522 bytes, which provides for a single subscriber 802.1Q tag on a maximum length Ethernet packet.	CM	MUST	1
REQ1419	A CM MUST advertise the L2VPN Capability subtype of the Modem Capabilities Encoding A.3.1 of its Registration Request.	CM	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1420	A CM with embedded eSAFE hosts MUST advertise them to the CMTS in a Registration Request message with an eSAFE Host Capability Encoding A.3.2 for each eSAFE host.	CM	MUST	1
REQ1421	A CM MUST silently ignore an L2VPN Encoding in any TLV context not mentioned in this specification.	CM	MUST	1
REQ1422	A CM MUST silently ignore any unrecognized L2VPN Encoding subtype and process all recognized L2VPN Encodings normally.	CM	MUST	1
REQ1423	A CMTS MUST implement the DOCS-L2VPN-MIB.	CMTS	MUST	2
REQ1424	An implementation MUST support a length of at least 16 octets.	CMTS	MUST	1
REQ1425	A CMTS implementation MUST support IEEE 802.1Q.	CMTS	MUST	1
REQ1426	A CM capable of DUT filtering MUST discard DUT to interfaces with a '0' in the DUT CMIM.	CM	MUST	1
REQ1427	If the CMTS does not allocate an individual SAID for multipoint forwarding (as is recommended),it MUST report this object as zero."	CMTS	MUST	1
REQ1428	If the DUT Filtering Encoding is present and the DUT Filtering bit is set to "1", the CM MUST restrict forwarding of downstream unencrypted traffic (for both individual and group MAC destinations) to only the set of interfaces indicated in a DUT CM Interface Mask (DUT CMIM) configured or implied by the encoding.	CM	MUST	1
REQ1429	A CMTS performing Multipoint L2VPN Forwarding MUST perform transparent learning layer 2 forwarding between 802.1Q bridge ports, cable modems, and service flows configured with the same VPNID.	CMTS	MUST	1
REQ1430	The CMTS MUST support configuration of VPNID values of at least 16 octets, and no more than 255 octets.	CMTS	MUST	1
REQ1431	When a Selected Ethernet Port is identified, the CMTS MUST accept the IEEE 802.1Q NSI Encapsulation Format Code in Forwarding L2VPN Encodings and MAY accept the other codes.	CMTS	MUST	1
REQ1432	In this case, the CMTS MUST enforce that L2VPN Encodings with the same VPN Identifier subtype that include an NSI Encapsulation Subtype MUST all have the same NSI Encapsulation Subtype encoding value.	CMTS	MUST	1
REQ1433	If the NSI Encapsulation Subtype or an L2VPN Vendor Specific Subtype does not statically configure a Service Multiplexing value, the CMTS MUST dynamically select and learn the Service Multiplexing value for a forwarding L2VPN Encoding from the CMTS's L2VPN peers across the NSI interface.	CMTS	MUST	1
REQ1434	A CM MUST silently ignore CMIM bit positions for unimplemented interfaces.	CM	MUST	1
REQ1435	Unless the L2VPN forwarder is otherwise configured, CMTS MUST transmit the ingress priority signaled with this subtype as the user priority bits of an IEEE 802.1Q tag when it forwards the packet to an NSI port with IEEE 802.1Q encapsulation.	CMTS	MUST	1
REQ1436	The CM MUST include an L2VPN Error Encoding in its MAC management response when it rejects an L2VPN Encoding in a REG-RSP, DSA-REQ, DSA-RSP, DSC-REQ or DSC-RSP.	CM	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1437	In an Upstream Classifier Encoding, a CM MUST silently ignore bit positions for unimplemented interfaces.	CM	MUST	1
REQ1438	A CMTS SHOULD implement a VLAN-capable bridging function as specified by [IEEE802.1Q].	CMTS	SHOULD	1
REQ1439	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.	CMTS	SHOULD	1
REQ1440	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.	CMTS	SHOULD	1
REQ1441	The CMTS SHOULD provide mapping of egress user priority to NSI port transmission traffic class as specified by [IEEE802.1Q].	CMTS	SHOULD	1
REQ1442	A CMTS SHOULD use the value of the VPNID with any signaling protocols that dynamically determine Service Multiplexing field values on L2VPN packets encapsulated on an NSI port.	CMTS	SHOULD	1
REQ1443	The CMTS SHOULD ignore the most significant 4 bits of the 16-bit NSI Encapsulation IEEE 802.1Q tag value.	CMTS	SHOULD	1
REQ1444	The CMTS SHOULD dynamically select and learn the label stack for incoming and outgoing label stacks, respectively.	CMTS	SHOULD	2
REQ1445	The CMTS SHOULD dynamically select and learn the local and remote session IDs for each tunnel.	CMTS	SHOULD	2
REQ1446	If present, the CMTS SHOULD use this subtype value as the Attachment Group ID (AGI) signaling element, associated with a VPN Identifier, when dynamically establishing an NSI pseudowire for Point-to-Point forwarding of the attachment circuit.	CMTS	SHOULD	2
REQ1447	If present, the CMTS SHOULD use this subtype value as the source attachment individual identifier (SAII) signaling element associated with the local pseudowire attachment when establishing an NSI backbone pseudowire for the cable attachment circuit.	CMTS	SHOULD	2
REQ1448	If present, the CMTS SHOULD use this subtype value as the target attachment individual identifier (TAII) signaling element associated with the remote pseudowire attachment when establishing an NSI PseudoWire for the attachment circuit.	CMTS	SHOULD	2
REQ1449	If the reason for rejection is due to a particular subtype of the L2VPN Encoding, the CM SHOULD include additional bytes in the L2VPN Error Parameter type string to identify the particular subtype of the L2VPN Encoding that it rejected.	CM	SHOULD	1
REQ1450	A CM SHOULD include this parameter in an L2VPN Error Encoding.	CM	SHOULD	1
REQ1451	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).	CMTS	MAY	1
REQ1452	The CMTS MAY restrict configuration of an NSI Encapsulation service multiplexing value (e.g., IEEE 802.1Q VLAN ID) to a single SF.	CMTS	MAY	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1453	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.	CMTS	MAY	1
REQ1454	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.	CM	MAY	1
REQ1455	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.	CMTS	MAY	1
REQ1456	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.	CMTS	MAY	1
REQ1457	The CMTS MAY accept multiple Downstream Classifier L2VPN Encodings with the same VPNID classifying packets to different service flows.	CMTS	MAY	1
REQ1458	The CMTS MAY assign L2VPN SAID values to be different for the same L2VPN on different downstream channels.	CMTS	MAY	1
REQ1459	A CMTS MAY implement vendor-specific configuration to select the ingress user priority of upstream L2VPN packets.	CMTS	MAY	1
REQ1460	If the CMTS implements an IEEE 802.1ad bridge forwarder, the CMTS MAY map the inner customer user priority tag to the outer service user priority tag.	CMTS	MAY	1
REQ1461	A CMTS MAY require configuration of both downstream and upstream service flow maximum forwarding rates to meet this requirement, as long as such limits are no less than 10% of link capacity.	CMTS	MAY	1
REQ1462	Because CMIM bit position 1 (corresponding to CM bridge ifIndex 1) represents the set of all CPE interfaces in L2VPN Forwarding, DUT Filtering, and Upstream Classifier Encodings, a compliant CM that implements more than one CPE interface MAY assign a CMIM bit position in the range of 5..15 to represent its single primary CPE interface.	CM	MAY	1
REQ1463	A CMTS MAY omit support for all NSI encapsulations other than IEEE802.1Q(2)."	CMTS	MAY	1
REQ1464	A CM with more than one CPE interface MAY assign a DocsL2vpnIfList bit position within the range of 5..15 to refer to the single primary CPE interface.	CM	MAY	1
REQ1465	The CMTS MAY use Vendor Specific L2VPN Subtypes to statically configure the ingress and egress label stacks.	CMTS	MAY	2
REQ1466	The CMTS MAY use Vendor Specific L2VPN Subtypes to statically configure session IDs, L2TPv3 peer network addresses, and other information as required by the vendor.	CMTS	MAY	2
REQ1467	A CMTS MAY signal that a CMIM value represents all possible CPE interfaces with the CMIM value for positions 1 and 5-15, i.e., the CMIM value 0x47 FF.	CMTS	MAY	2

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1468	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.	CMTS	SHOULD	1
REQ1469	In this Point-to-Point forwarding mode, the CMTS MAY omit learning of CPE MAC addresses into a Forwarding Database.	CMTS	MAY	1
REQ1470	A CMTS vendor MAY implement vendor-specific mechanisms to determine and regenerate the user priority of downstream L2VPN forwarded packets.	CMTS	MAY	1
REQ1471	The CMTS MAY forward with non-zero default user priority values with vendor-specific configuration.	CMTS	MAY	1
REQ1472	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.	CMTS	MAY	1
REQ1473	The CMTS SHOULD permit configuration of the maximum number of MAC addresses per L2VPN on a per-L2VPN basis.	CMTS	SHOULD	2
REQ1474	A CMTS MAY assign multiple L2VPN SAIDs to the same L2VPN on the same downstream channel, e.g., to assign an Individual L2VPN SAID to each CM in Point-to-Point forwarding mode.	CMTS	MAY	1
REQ1475	A CMTS MAY assign multiple SAIDs to the same L2VPN on the same CM.	CMTS	MAY	1
REQ1476	A Point-to-Point forwarding CMTS SHOULD assign the same Group L2VPN SAID to different CMs on the same MAC domain attaching to the same L2VPN Identifier, but MAY choose to assign an Individual L2VPN SAID unique for the CM.	CMTS	SHOULD	1
REQ1477	A CMTS MAY support vendor-specific configuration to dynamically start or discontinue L2VPN forwarding through a registered CM.	CMTS	MAY	1
REQ1478	The particular bridging model implemented by the CMTS (e.g., [IEEE802.1Q] or [IEEE 802.1ad]) MAY provide for the regeneration of an upstream ingress user priority to a different internal user priority for the packet in the CMTS.	CMTS	MAY	1
REQ1479	A CMTS MAY implement the DOCSIS Spanning Tree protocol and transmit DSTP BPDUs on all NSI and RF interfaces configured for L2VPN operation.	CMTS	MAY	1
REQ1480	A CMTS MAY implement a DOCSIS Spanning Tree (DST) SAID specifically for DST forwarding to the CPE ports of all L2VPN CMs.	CMTS	MAY	1
REQ1481	A CM receiving an L2VPN Encoding with an L2VPN SA-Descriptor Subtype for a SAID not previously established on that CM MUST initiate a BPKM TEK transaction to establish the new L2VPN SAID [BPI-PLUS].	CM	MUST	1
REQ1482	In this case, L2VPN Vendor Specific Subtype Encodings (GEI Subtype 5.43) MUST provide the NSI Encapsulation Format and any desired static Service Multiplexing values.	CMTS	MUST	1

REQ Tag	Requirement text	Device Under Test	Requirement Category	Phase
REQ1483	A CMTS MUST accept the full 12-bit range of VLAN ID values for the unique values it does accept.	CMTS	MUST	1
REQ1484	The maximum number of Service Provider and Customer VLAN ID values the CMTS accepts is vendor specific, but the CMTS MUST accept the full 12-bit range of VLAN ID values.	CMTS	MUST	1
REQ1485	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.	CM	SHOULD	1
REQ1486	Although the NSI Encapsulation Subtype is intended primarily for Point-to-Point forwarding modes, the CMTS MAY accept it in Multipoint mode (including in the Selected Ethernet mode).	CMTS	MAY	1
REQ1487	The CMTS MAY limit statically configured MPLS label values to a vendor-specific range.	CMTS	MAY	1
REQ1488	The CMTS MAY limit statically configured session ID or other Service Multiplexing values to a vendor-specific range.	CMTS	MAY	1
REQ1489	If the entire L2VPN Encoding is rejected, the CM MAY include in the L2VPN Error Parameter type string only the two or three bytes that identify the location of a full L2VPN Encoding.	CM	MAY	1

Appendix I Acknowledgements

This Technical Report was developed and influenced by numerous individuals representing many different vendors and organizations. CableLabs hereby wishes to thank everybody who participated directly or indirectly in this effort.

CableLabs wishes to recognize the following individuals for their significant involvement and contributions to this Technical Report:

Michael Patrick, Motorola
Steve Muller, Broadcom
Margo Dolas, Broadcom
Victor Hou, Broadcom
Satish Kumar, Texas Instruments
Prasanna Mucharikar, Cisco
Dan Torbet, ARRIS
Troy Rawson, SMC
Brian Rose, Cox
Darren Wolner, Time Warner Cable
Kirk Erichsen, Time Warner Cable
Pierre Roy, Vidéotron
Omar Baceski, Vidéotron
Rahul Sethi, Charter Business
Charles Bergren, CableLabs
Chris Donley, CableLabs