Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.213

(11/2006)

SERIE J: REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, Y DE OTRAS SEÑALES MULTIMEDIA

Sistemas interactivos para distribución de televisión digital

Redes privadas virtuales de capa 2 para sistemas de módem de cable IP

Recomendación UIT-T J.213

UIT-T

ITU Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.213

Redes privadas virtuales de capa 2 para sistemas de módem de cable IP

Resumen

La Recomendación UIT-T J.213 describe los requisitos tanto de los CMTS como de los CM para implementar una característica de red privada virtual de capa 2 DOCSIS (L2VPN DOCSIS). La característica L2VPN permite a los operadores de cable ofrecer un servicio LAN transparente (TLS) de capa 2 a empresas comerciales.

Orígenes

La Recomendación UIT-T J.213 fue aprobada el 29 de noviembre de 2006 por la Comisión de Estudio 9 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Recomendación UIT-T J.213

Redes privadas virtuales de capa 2 para sistemas de módem de cable IP

1 Introducción

Esta Recomendación describe los requisitos tanto de los CMTS como de los CM para implementar una característica de red privada virtual de capa 2 DOCSIS (L2VPN DOCSIS).

La característica L2VPN permite a los operadores de cable ofrecer un servicio LAN transparente (TLS, *transparent LAN service*) de capa 2 a empresas comerciales, que es uno de los principales objetivos de la iniciativa de servicios de negocio mediante DOCSIS (BsoD, *business service over DOCSIS*).

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

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

[UIT-T J.122] Recomendación UIT-T J.122 (2002), *Sistemas de transmisión de segunda generación para los servicios interactivos de televisión por cable – Módems de cable para protocolo Internet*.

[UIT-T J.125] Recomendación UIT-T J.125 (2004), *Privacidad de enlace para la implementación de módems de cable*.

3 Términos y definiciones

Esta Recomendación define los términos siguientes y utiliza aquéllos definidos en [UIT-T J.122].

3.1 red puente: Un conjunto de LAN IEEE 802 interconectadas mediante puentes MAC IEEE 802.1D.

3.2 CM conforme: Un CM que implementa esta Recomendación L2VPN DOCSIS.

3.3 L2PDU DOCSIS: Una PDU de paquetes de una trama MAC DOCSIS, es decir, la L2PDU tras un encabezamiento MAC con un FC_TYPE=00. Esta definición significa que un mensaje de gestión MAC con FC_TYPE=11 *no* se considera una L2PDU DOCSIS, aunque el encabezamiento de mensaje de gestión MAC tenga la misma forma que el de una L2PDU.

3.4 trama MAC DOCSIS: Unidad de transmisión en una interfaz RF de cable DOCSIS, constituida por un encabezamiento MAC y una PDU de datos (probablemente nula). El campo FC_TYPE del encabezamiento MAC identifica la PDU de datos como una PDU de paquetes (FC_TYPE=00), o con una PDU específica MAC (FC_TYPE=11).

3.5 inundación: Operación de un puente L2 en el que replica una L2PDU dirigida a un MAC de grupo o a una dirección MAC individual no aprendida a todos los puertos puente distintos del puerto de entrada de la L2PDU.

3.6 dirección MAC de grupo (GMAC): Una dirección MAC de 6 bytes IEEE en la que el primer bit transmitido (bit de grupo) se fija a "1", lo que indica que la dirección se refiere a un grupo de anfitriones MAC. En la representación canónica de las direcciones MAC utilizadas para la transmisión Ethernet, el bit de grupo es el bit menos significativo del primer byte. La dirección MAC difundida como todo unos se considera que es una dirección GMAC.

3.7 dirección MAC individual: Una dirección MAC de 6 bytes IEEE en la que el primer bit transmitido (el bit de grupo) se fija a "0", lo que indica que la dirección se refiere a un único anfitrión MAC. Para las direcciones MAC Ethernet de DOCSIS, el bit de grupo es el bit menos significativo del primer byte de la dirección MAC.

3.8 retransmisor L2: Un elemento de red que retransmite paquetes de capa 2 desde una interfaz L2 hasta otra interfaz L2. El transmisor L2 puede funcionar en modo de retransmisión punto a punto o multipunto, es decir, retransmitiendo sólo entre dos interfaces sin aprendizaje o retransmitiendo paquetes para su difusión sólo a la interfaz en la que se aprendió la dirección MAC.

3.9 interfaz L2: Puerto o circuito virtual de interfaz física en el que se transmite una L2PDU. Los puertos de interfaz L2 física incluyen una NSI Ethernet en un CMTS o el puerto CMCI en un CM. Las interfaces L2 de circuito virtual incluyen un seudohilo (PW) de interfaz de sistema de red (NSI) CMTS y una asociación de seguridad BPI con un único CM CMTS. Una interfaz L2 puede o no tener asignado un índice ifIndex.

3.10 red privada virtual L2 (L2VPN): Conjunto de LAN y los retransmisores L2 situados entre ellas que permiten a los anfitriones vinculados a las LAN comunicar con unidades de datos de protocolo de capa 2 (L2PDU). Una única L2VPN retransmite las dos L2PDU basándose únicamente en las direcciones MAC de destino (DMAC) de la L2PDU, transparentes a cualquier dirección IP o de capa 3. Un dominio administrativo de operador soporta múltiples L2VPN, una para cada empresa de abonado a la que se ofrezca el servicio LAN transparente.

3.11 identificador L2VPN: Cadena de octetos que identifica de forma unívoca una L2VPN en un dominio administrativo de operador de cable, correspondiente a una única empresa suministradora.

3.12 retransmisor L3: Elemento de red que retransmite una PDU de capa 3 desde una interfaz de entrada a una o más interfaces de salida. También se denomina "encaminador" ("router").

3.13 unidad de datos de protocolo L2 (L2PDU): Secuencia de bytes que consta de una dirección MAC de destino (DMAC), una dirección MAC de origen (SMAC), encabezamiento(s) de rótulo (optativo), tipo/longitud Ethernet, cabida útil L2 y CRC.

3.14 aprendizaje: Operación de un puente de capa 2 mediante la que asocia la dirección MAC de origen (SMAC) de una L2PDU entrante con el puerto puente del que proviene.

3.15 retransmisión L2 multipunto: Operación de un retransmisor L2 entre múltiples redes L2 que retransmite paquetes individuales destinados a MAC sólo a la interfaz en la que se aprendió la dirección MAC de origen, y que difunde los paquetes destinados a MAC de grupo a todas las interfaces.

3.16 CM no conforme: Un CM que no implementa esta Recomendación L2VPN DOCSIS

3.17 retransmisión L2 punto a punto: Operación de un retransmisor L2 solo entre dos redes L2 sin aprendizaje de dirección MAC de origen.

3.18 asociación de seguridad (SA, *security association*): Una asociación entre el CMTS y un conjunto de CM en un dominio MAC que permite una comunicación criptada entre el CMTS y el conjunto de CM. Una SA de CM único es una asociación con un único CM que permite una conexión de red L2 punto a punto privada entre el CMTS y la LAN CPE del CM. Un descriptor de asociación de seguridad (SA-Descriptor) es un elemento de mensaje multipartito definido en la privacidad básica DOCSIS [UIT-T J.125] que incluye un ID de asociación de seguridad (SAID).

3.19 ID de asociación de seguridad (SAID, *security association ID*): Identificador de 14 bits que aparece en un encabezamiento ampliado BPI (BPI-EH) de un paquete de PDU DOCSIS para identificar la clave utilizada para criptar el paquete.

3.20 encabezamiento de rótulo: ID de protocolo de rótulo de 16 bits (0x8100) seguido de un campo de control de rótulo de 16 bits. El campo de control de rótulo está constituido por un campo de prioridad de usuario de 3 bits, un indicador de formato canónico de 1 bit y un ID VLAN de 12 bits [IEEE 802.1Q].

3.21 servicio LAN transparente (TLS, *transparent LAN service*): Capacidad de servicio de un operador de cable que implementa una L2VPN privada entre las redes CPE de los CM de una única empresa suministradora.

3.22 LAN virtual (VLAN, *virtual LAN*): *Subconjunto* de las LAN de una red puente IEEE 802.1 al que se asigna un identificador VLAN (VLAN ID). Una L2VPN puede estar constituida por diversas VLAN, cada una con diferentes VLAN ID e incluso de VLAN en diferentes redes puente IEEE 802.1 con el mismo VLAN ID.

3.23 identificador de LAN virtual (VLAN ID, *virtual LAN identifier*): Un VLAN ID IEEE 802.1 es un número de 12 bits que identifica una VLAN en una red puente IEEE 802.1. Un VLAN ID IEEE 802.1 apilado está constituido por un VLAN ID de servicio exterior de 12 bits y un VLAN ID de cliente interior de 12 bits.

3.24 L2VPN de aprovisionamiento: L2VPN para el tráfico anterior al registro de DHCP, ToD y TFTP que aprovisiona eCM y anfitriones eSAFE. Se puede combinar con una L2VPN de gestión.

3.25 L2VPN de gestión: L2VPN para el tráfico SNMP posterior al registro para dispositivos eCM o eSAFE. Puede estar combinada con una L2VPN de aprovisionamiento.

4 Abreviaturas, siglas o acrónimos

Esta Recomendación utiliza las siguientes abreviaturas, siglas o acrónimos.

BPI Interfaz de privacidad básica (*baseline privacy interface*)

BSoD Servicios de negocio por DOCSIS (*business services over DOCSIS*)

CMIM Máscara de interfaz CM (*CM interface mask*)

CRC Verificación por redundancia cíclica (*cyclic redundancy check*)

DIME Criptación de multidifusión IP en sentido descendente (*downstream IP multicast encryption*)

DMAC MAC de destino (*destination MAC*)

DUT Tráfico no criptado en sentido descendente (*downstream unencrypted traffic*)

eCM Módem de cable incorporado [UIT-T J.126] (*embedded cable modem*)

eMTA Adaptador terminal de medios incorporado [UIT-T J.167] (*embedded media terminal adapter*)

ePS Servicios de portal incorporados [UIT-T 192] (*embedded portal services*)

eSAFE Entidad funcional de servicio/aplicación incorporados [b-UIT-T J.126] (*embedded service/application functional entity*)

GMAC Dirección MAC de grupo (*group MAC address*)

L2 Capa 2 (*layer 2*)

L2VPN Red privada virtual de capa 2 (*layer 2 virtual private network*)

MAC Control de acceso a medios (*media access control*)

RPV Red privada virtual

SAID Identificador de asociación de seguridad (*security association identifier*)

SID Identificador de servicio (sentido ascendente) ((*upstream) service identifier*)

SMAC MAC de origen (*source MAC*)

TLS Servicio LAN transparente (*transparent LAN service*)

ToD Hora del día (*time of day*)

5 Convenios

5.1 Requisitos

En esta Recomendación, las palabras usadas para definir la importancia de determinados requisitos se escriben con mayúsculas. Estas palabras son:

DEBE(N) Esta palabra o el adjetivo o participio pasado "REQUERIDO" significan que se trata de un aspecto, elemento o comportamiento absolutamente obligatorio en esta Recomendación.

NO DEBE(N) Estas palabras significan que se trata de un aspecto, elemento o comportamiento que está absolutamente prohibido en esta Recomendación.

DEBERÍA(N) Esta palabra o el adjetivo o participio pasado "RECOMENDADO" significan que, en determinadas circunstancias, pueden existir razones válidas para no tener en cuenta un determinado aspecto, elemento o comportamiento, pero que, antes de tomar tal decisión, se deben comprender y analizar a fondo todas las implicaciones.

NO DEBERÍA(N) Estas palabras significan que, en determinadas circunstancias, pueden existir razones válidas para tener en cuenta o aplicar un determinado aspecto, elemento o comportamiento por considerarlo aceptable, o incluso útil, pero que, antes de tomar tal decisión, se deben comprender y analizar a fondo todas las implicaciones.

PUEDE(N) Esta palabra o el adjetivo "FACULTATIVO" significan que un determinado aspecto, elemento o comportamiento es verdaderamente facultativo. Por ejemplo, un suministrador puede optar por incluir un elemento porque se requiere en un mercado dado, o porque realza el producto, mientras que otro suministrador puede no incluirlo.

Algunas declaraciones normativas implican que un CMTS o un CM ignoren en silencio una condición que podría estar definida en una futura Recomendación. Un requisito para ignorar en silencio una condición implica que el CM o el CMTS:

- PUEDE incrementar una estadística propia del suministrador;
- NO DEBE generar un mensaje de registro cronológico; y
- DEBE en todo caso ignorar la condición y proseguir la operación como si la condición no se hubiera producido.

5.2 Conformidad

Un CMTS DOCSIS que pretenda implementar la característica L2VPN DOCSIS DEBE implementar las disposiciones normativas de esta Recomendación. Un CM DOCSIS que pretenda la conformidad para la característica L2VPN DOCSIS DEBE implementar los requisitos normativos de esta Recomendación.

Un CMTS o un CM que implemente esta Recomendación se dice que es conforme con L2VPN. En lo sucesivo en esta Recomendación todas las referencias a un CMTS se refieren a un CMTS conforme con L2VPN. Un CM que no ha implementado esta Recomendación se dice que es un CM no conforme con L2VPN.

Un CMTS conforme con L2VPN DEBE soportar un CM no conforme con L2VPN. Esto permite a un operador de cable ofrecer servicios de abonado L2VPN con los CM no conformes ya desplegados. El uso de CM no conformes implica ciertas limitaciones que se indican en el apéndice IV. La utilización de CM conformes para servicios de abonado L2VPN evita estas limitaciones. Los requisitos para que los CM cumplan esta Recomendación se resumen en la cláusula 8.

6 Modo de funcionamiento (informativo)

6.1 Características L2VPN

La capacidad de implementar redes privadas virtuales de capa 2 en conjuntos arbitrarios de CM admite algunas características DOCSIS importantes:

- Servicio LAN transparente.
- L2VPN con múltiples ISP.
- L2VPN de gestión.

6.1.1 Servicio LAN transparente

La interconexión de datos entre diferentes sucursales de empresas comerciales supone una oportunidad de negocio importante para los operadores de cable. Las redes de datos comerciales se implementan normalmente con conexiones de datos privadas punto a punto tales como relevadores de trama, RDSI o circuitos virtuales ATM, a menudo con equipos que proporcionan un suministro transparente de paquetes LAN Ethernet de capa 2. Un servicio que interconecta redes LAN de empresas suministradoras con transmisión de capa 2 se denomina servicio LAN transparente (TLS).

La norma de RFI DOCSIS [UIT-T J.122] se destinó originalmente a conexiones de abonados residenciales con la Internet pública. Esta Recomendación normaliza en DOCSIS el control y el funcionamiento en el plano de datos de los CMTS y los CM para ofrecer servicios LAN transparentes a empresas de abonados comerciales.

El término "TLS" se refiere a una determinada oferta de servicio a clientes de empresas comerciales. La tecnología que permite suministrar este servicio se denomina red privada virtual de capa 2 (L2VPN, *layer-2 virtual private network*). Un operador de cable ofrece TLS implementando una L2VPN para cada empresa comercial.

La figura 6-1 ofrece un ejemplo de servicio TLS comercial basado en DOCSIS:

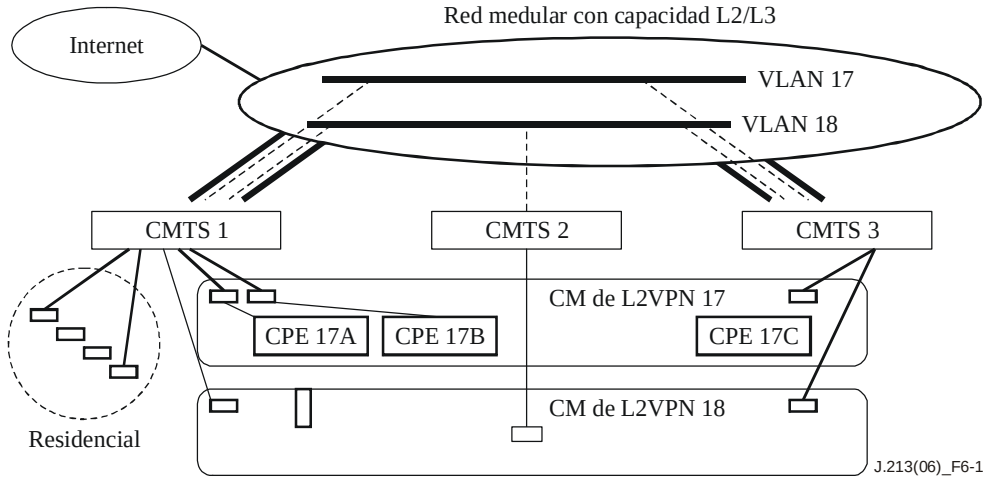

Figura 6-1 – Servicio LAN transparente

La figura 6-1 muestra un servicio LAN transparente que se ofrece a dos empresas comerciales; una indicada como L2VPN 17 y la otra como L2VPN 18. Todos los CMTS tienen el conjunto habitual de abonados residenciales, que están indicados solo como CMTS 1. CMTS 1 proporciona servicio L2VPN a dos CM en L2VPN 17 y a uno en L2VPN 18. CMTS 2 proporciona servicio L2VPN a un CM en L2VPN 18. CMTS 3 proporciona servicio a un CM en L2VPN 17 y a otro en L2VPN 18.

El ejemplo muestra que la red medular L2 del operador de cable implementa una única LAN virtual (VLAN, *virtual LAN*) para cada cliente. En esta Recomendación el término "VLAN" tiene un significado específico al referirse a la definición de IEEE 802.1Q, como un subconjunto de LAN con una red puente a la cuál se asigna un ID VLAN de 12 bits. En este ejemplo CMTS 1 encapsula directamente paquetes L2 en sentido ascendente de L2VPN 17 en un paquete Ethernet rotulado IEEE 802.1Q con un rótulo ID VLAN 17 y los envía por un puerto de interfaz de sistema de red (NSI, *network system interface*) Ethernet medular a la red modular del operador de cable.

En el ejemplo, CMTS 1 implementa una retransmisión L2 multipunto de forma que es responsable de trasladar paquetes entre sus dos CM vinculadas a L2VPN 17. Esto incluye aprender las direcciones MAC de origen (SMAC, *source MAC*) del CPE 17A y del CPE 17B y asociarlas con el CM a las que esos CPE están unidos.

CMTS 1 implementa únicamente un único circuito de enganche con VLAN 17 en la red medular. Cuando un paquete en sentido descendente proveniente de VLAN 17 llega a CMTS 1, busca la MAC de destino (DMAC, *destination MAC*) en su base de datos de aprendizaje y retransmite el paquete al CM correcto.

CMTS 3, sin embargo, sólo puede implementar retransmisiones L2 punto a punto, en las que retransmite de forma transparente todos los paquetes individuales y de grupo con destino MAC punto a punto entre el CM unido al CPE 17C y al ID VLAN 17 IEEE 802.1Q en su puerto Ethernet NSI a la red medular.

En la red medular, un puente de capa 2 de operador de cable conecta las diversas interfaces troncales Ethernet de los CMTS y establece puentes con cada VLAN. Este servicio TLS que ofrece el operador a L2VPN 17 aporta una conexión puente de capa 2 transparente entre los CPE 17A, 17B y 17C. Desde el punto de vista del cliente de la empresa, este tipo de CPE está gestionado y operado como si se encontrara en una LAN Ethernet privada. Normalmente, tendrán una dirección IP en la misma subred IP propiedad de la empresa. Normalmente la empresa designa la dirección IP a cada CPE y tiene su propio servidor DHCP para hacerlo. De hecho, cada empresa puede utilizar el

mismo espacio de subred IP privada. A diferencia de las tecnologías RPV de capa 3, el operador de cable no necesita coordinar la asignación de subred de dirección IP con los clientes de la empresa. Desde el punto de vista del operador, los abonados LAN de la empresa están completamente aislados en la capa 2 de todos los demás abonados residenciales y de cualquier otra L2VPN.

Un TLS de empresa puede incluir no sólo las LAN unidas a los CM sino también cualesquiera otras LAN conectadas con la VLAN de cliente en el puente IEEE 802.1Q de la red medular del operador de cable.

6.1.2 Redes L2VPN con múltiples ISP

La característica L2VPN permite a un operador de cable soportar múltiples proveedores de servicio de Internet (ISP, *Internet service providers*) proporcionando una L2VPN diferente para cada ISP. El operador de cable proporciona todo el aprovisionamiento CM y el fichero de configuración CM determina una L2VPN para transmitir todo el tráfico CPE. Cada ISP tiene asignado una L2VPN diferente. El ISP es responsable de proporcionar los servidores DHCP y las direcciones IP a todos los CPE en los CM incluidos en su L2VPN.

La ventaja de las L2VPN para funcionamiento con múltiples ISP es que separa totalmente la gestión del espacio de dirección IP y el encaminamiento IP del ISP del operador de cable. Por el contrario, las características de múltiples ISP basadas en adaptador terminal de capa 3 normalmente requieren coordinación de la asignación de direcciones IP y de la configuración de seguridad del encaminador entre los encaminadores de borde de proveedor MSO y de cliente ISP.

6.1.3 L2VPN de gestión

La característica L2VPN DOCSIS permite a un CMTS implementar una L2VPN exclusivamente para el suministro y la gestión de módems de cable incorporados (eCM, *embedded cable modems*) y entidades funcionales de servicio/aplicación incorporadas (eSAFE, *embedded service/application functional entities*) [b-UIT-T J.126], tales como un agente de transporte de medios incorporado (eMTA, *embedded media terminal adapter*) [b-UIT-T J.167] o una funcionalidad de servicios de portal incorporada (ePS, *embedded portal services*) [b-UIT-T J.192]. Al implementar una L2VPN diferente para el suministro y gestión de tráfico eCM y eSAFE, se aíslan estos dispositivos de Internet y del abonado, mejorando la seguridad.

Antes del registro, el CM transmite un SID temporal, y se toma todo este tráfico para su retransmisión por el retransmisor que no es L2VPN. Se podría implementar un CMTS para retransmitir tráfico antes del registro en una única L2VPN de aprovisionamiento. La RPV de aprovisionamiento estaría configurada por el propio suministrador.

Cuando un CM se registra, lee los códigos L2VPN de su fichero de configuración que pueden configurar sus dispositivos eCM y eSAFE para enviar una L2VPN. Esta L2VPN registrada con posterioridad se denomina una L2VPN de gestión, ya que el tráfico posterior al registro es fundamentalmente SNMP para la gestión del dispositivo.

6.1.4 Otras características permitidas en L2VPN

Algunas características requeridas por esta Recomendación son mejoras del funcionamiento global DOCSIS que no tienen relación con la RPV de capa 2:

- Clasificación basada en la interfaz.
- Filtrado DUT.
- Habilitación del control de indagación DHCP eSAFE.

La clasificación basada en la interfaz permite clasificar los paquetes en función de su interfaz de puerto puente interna o externa de CM, como se describe en 7.6.5. Esta característica se puede utilizar, por ejemplo, para clasificar paquetes hacia o desde la interfaz MTA incorporada, sin depender de una determinada subred IP en dicha interfaz.

El filtrado de tráfico no criptado en sentido descendente (DUT, *downstream unencrypted traffic*) se aplica al funcionamiento RPV de capa 3 específico del suministrador CMTS para impedir que el tráfico MAC de grupo, que se difundió a CM residenciales, se fugue hacia redes CPE supuestamente privadas de abonados RPV de capa 3. El filtrado DUT se describe en 7.5.2.1.

El control de indagación DHCP es un TLV explícito que autoriza al CMTS que aprenda automáticamente la dirección MAC de los anfitriones eSAFE incorporados, tales como eMTA, introduciéndose en su tráfico DHCP. Esto se puede utilizar junto con características propias del suministrador CMTS para transmitir DHCP u otros paquetes de los anfitriones eSAFE de una manera especial. La característica de habilitación de control de indagación DHCP eSAFE se describe en 7.6.4.1.

6.2 Arquitectura de la retransmisión de capa 2 CMTS

6.2.1 Retransmisión L2VPN y no L2VPN

Un CMTS se considera que tiene un retransmisor de paquetes totalmente separado para la retransmisión L2VPN y que difiere de los retransmisores no L2VPN para tráfico residencial, como se describe en la figura 6-2:

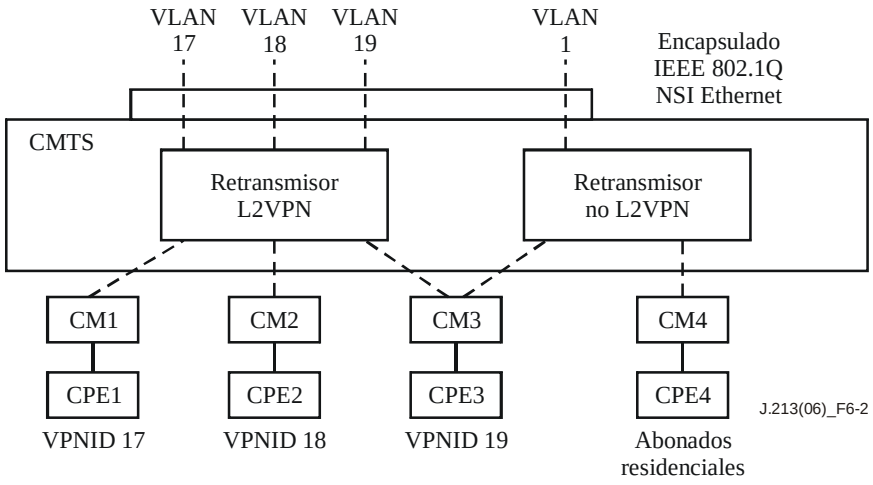

Figura 6-2 – Retransmisión de CMTS L2VPN y no L2VPN

Para soportar el funcionamiento L2VPN una interfaz de sistema de red (NSI, *network system interface*) del CMTS debe ser capaz de distinguir el tráfico en sentido descendente L2VPN del que no es L2VPN y de determinar la L2VPN del tráfico en sentido descendente. El formato del encapsulado del tráfico L2VPN en los puertos NSI de CMTS y los valores determinados del campo, en este encapsulado que distingue una determinada L2VPN, se denominan información de encapsulado L2VPN NSI. En el ejemplo anterior se utilizan rótulos ID VLAN IEEE 802.1Q como formatos de encapsulado L2VPN en un puerto NSI de Ethernet.

En general el tráfico L2VPN y el que no es L2VPN se mezcla en el mismo puerto NSI. En el ejemplo anterior, el CMTS implementa una interfaz de encaminador IP no L2VPN en el ID VLAN 1, que puede incluso ser la VLAN original, con un encapsulado sin rótulo. El tráfico residencial, como el CPE4 conectado a CM4, sigue siendo encaminado a través del retransmisor de encaminamiento IP del CMTS en la subinterfaz del encaminador en el ID VLAN 1. El otro CPE, sin embargo, tiene puentes con la capa 2 desde la interfaz Ethernet del CM hacia un ID VLAN 802.1Q configurado en el puerto NSI. En la figura 6-2, el CMTS implementa un modelo de retransmisión punto a punto en el que retransmite tráfico CPE desde CM1 al ID VLAN 17 802.1Q, tráfico CPE desde CM2 al ID VLAN 18 802.1Q y tráfico CPE proveniente de uno de los flujos de

servicio en sentido ascendente desde CM3 hacia el ID VLAN 19 802.1Q. El otro flujo de servicio en sentido ascendente de CM3 se transmite al retransmisor que no es L2VPN.

En el sentido ascendente, el CMTS distingue el tráfico L2VPN del tráfico que no es L2VPN, basándose en el flujo de servicio en sentido ascendente del que proviene el tráfico y en la dirección MAC de origen del tráfico. Algunos SF en sentido ascendente están configurados con codificaciones L2VPN de retransmisión que identifican una determinada L2VPN. La codificación L2VPN incluye una máscara de interfaz CM (CMIM, *CM interface mask*) que identifica qué anfitriones del extremo CM transmiten en sentido ascendente a la L2VPN. Por defecto, sólo los anfitriones CPE conectados a la interfaz CMCI de un CM retransmiten a una L2VPN. El CM y sus anfitriones internos eSAFE no retransmiten a una L2VPN.

Un SF configurado para transmitir tráfico CPE a una L2VPN se considera que es un circuito de anexión en el contexto del servicio de LAN privada virtual (VPLS, *virtual private LAN service*) EITF. Un retransmisor L2VPN VPLS CMTS es responsable de retransmitir paquetes entre circuitos de anexión y seudohilos en puertos NSI (por ejemplo, túneles MPLS o L2TPv3).

6.2.2 Modos de transmisión L2VPN punto a punto y multipunto

Esta Recomendación utiliza el término "retransmisión de capa 2" en lugar de "conexión puente", puesto que el servicio L2VPN comercial se puede ofrecer sin implementar necesariamente un puente de capa MAC de aprendizaje en el CMTS como se define en [IEEE 802.1Q]. El CMTS PUEDE implementar un modo de retransmisión de capa 2 punto a punto que retransmite paquetes entre un único puerto NSI y un único CM (o SF). Si el CMTS implementa un puente de capa MAC de aprendizaje entre interfaces NSI y RF, esta Recomendación lo denomina modo de retransmisión de capa 2 multipunto.

En el modo de transmisión L2VPN punto a punto, cada circuito conectado tiene un valor de encapsulado NSI diferente. Por ejemplo, con encapsulado IEEE 802.1Q, cada circuito de anexión (es decir, CM o SF) está configurado con un ID VLAN 802.1Q diferente. En el modo punto a punto, el retransmisor L2VPN transmite simplemente los datos en sentido descendente y en sentido ascendente entre un puerto NSI y un circuito de anexión, sin conocer las direcciones MAC de los paquetes CPE. El VPNID lógico al que se une un CM o un SF debería estar configurado con el circuito de anexión, pero su valor los ignora en otros casos el CMTS en el modo de retransmisión punto a punto. Un puente externo L2VPN en la red medular del operador de cable realiza realmente el aprendizaje de la dirección MAC de capa 2 para cada L2VPN y traslada paquetes entre los ID VLAN o entre seudohilos de los paquetes en su encapsulado NSI.

En la figura 6-3 se muestra un ejemplo del modo de retransmisión punto a punto.

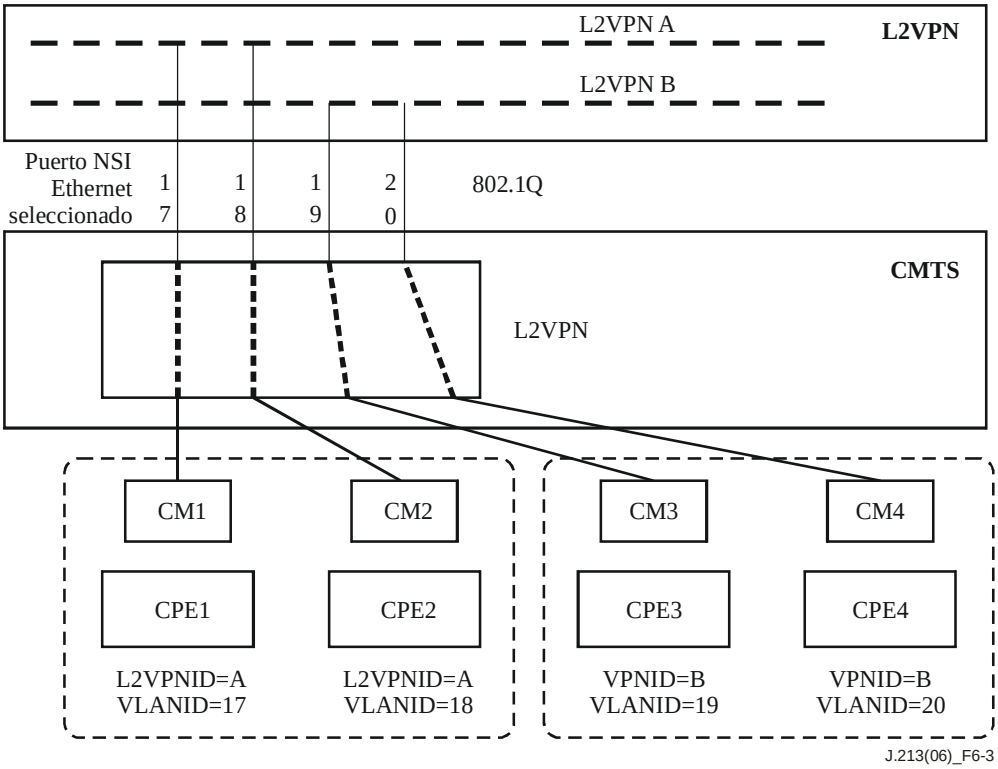

Figura 6-3 – Modo de retransmisión punto a punto

Se configuran cuatro CM para el funcionamiento L2VPN. Cada codificación L2VPN de CM incluye un VPNID lógico A o B, junto con un subtipo de encapsulado NSI configurado estáticamente para su utilización IEEE 802.1Q con un ID VLAN diferente para cada CM (ID VLAN 17 a 20). El retransmisor L2VPN de CMTS transmite tráfico del puerto NSI a esos ID VLAN de punto a punto, hacia y desde el CM configurado. Aunque el retransmisor L2VPN en el modo punto a punto no utiliza la configuración de VPNID, tiene que seguir configurado en cada codificación L2VPN de retransmisión aunque solo sea para información. Se configura un conmutador puente L2VPN de cada dos, externo al CMTS, para tratar los encapsulados NSI para los ID VLAN 17 y 18 como puertos puente lógicos separados para L2VPN A y para aprender direcciones MAC CPE en esos puertos puente. De la misma forma, el puente L2VPN externo se configura para tener en consideración los encapsulados con los ID VLAN 19 a 20, como puertos puente separados del dominio de difusión que es L2VPN B.

Con el modo de retransmisión punto a punto de encapsulado NSI IEEE 802.1Q, se limita el número de módems de abonado L2VPN soportados en un CMTS a 4.093 CM, debido al límite de 12 bits en un ID VLAN IEEE 802.1Q.

El modo de transmisión multipunto significa que el CMTS transmite paquetes L2VPN en sentido descendente a módems de cable que pueden ser múltiples. El CMTS construye una base de datos de retransmisión de capa 2 (FDB, *forwarding database*) de las direcciones MAC CPE que aprende en la dirección MAC de origen de los paquetes en sentido ascendente. Un retransmisor L2VPN multipunto utiliza esta FDB para seleccionar el CM para enviar tráfico L2VPN en sentido descendente. Si el destino es una dirección MAC de grupo o es una dirección MAC individual desconocida, un retransmisor L2VPN multipunto difunde el tráfico a todos los circuitos de anexión y a todos los puertos NSI salvo el puerto del que se recibió el paquete. Un retransmisor L2VPN multipunto también retransmite directamente paquetes entre circuitos de anexión (de CM o SF), configurados con la misma L2VPN lógica.

Con retransmisión multipunto solo se necesita un valor de encapsulado NSI para cada L2VPN lógica, y no para cada circuito de anexión. Esto permite soportar cualquier número de *módems* para el servicio L2VPN puesto que el ID VLAN IEEE 802.1Q de 12 bits, utilizado como un valor de encapsulado NSI, solo limitará el número de *redes* L2VPN de empresa.

En la figura 6-4 se muestra un ejemplo de modo de retransmisión multipunto.

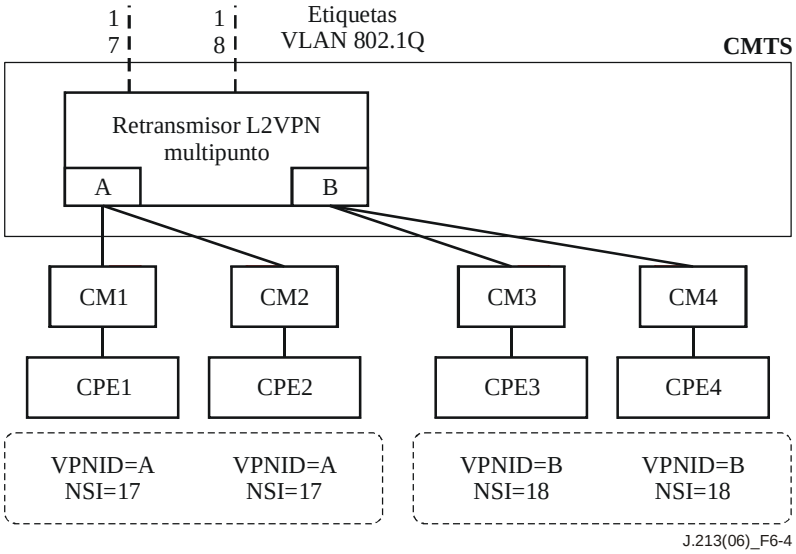

Figura 6-4 – Ejemplo de retransmisión L2VPN multipunto

En este ejemplo, tanto CM1 como CM2 están configurados para retransmitir L2VPN a VPNID A, y están configurados para utilizar un encapsulado NSI de ID VLAN 17 IEEE 802.1Q. El retransmisor L2VPN multipunto aprende las direcciones MAC de CPE1 y CPE2 para determinar hacia qué CM retransmitir el tráfico de difusión en sentido descendente recibido del puerto de red en el ID VLAN 17. De la misma forma, CM3 y CM4 están configurados con VPNID B y ambos están configurados para utilizar el ID VLAN 18 IEEE 802.1Q como su encapsulado NSI. El retransmisor L2VPN multipunto obtiene las direcciones MAC de CPE3 y CPE4 en L2VPN B. El retransmisor que no es L2VPN se muestra en la figura 6-4.

Esta Recomendación permite la calificación de los CMTS con modos de retransmisión punto a punto o multipunto. Se deben usar las pruebas de calificación DOCSIS para el modo de retransmisión indicado por la notificación PICS del suministrador para cada L2VPN. Esta Recomendación presupone que un CMTS selecciona un modo u otro para cada L2VPN. No existen requisitos, sin embargo, que impidan a un suministrador implementar modos de retransmisión diferentes para diferentes conjuntos de L2VPN.

7 Funcionamiento L2VPN

7.1 Requisitos del modelo puente CMTS

El CMTS DEBE retransmitir de forma transparente las L2PDU recibidas de un flujo de servicio en sentido ascendente configurado para recibir paquetes para una determinada L2VPN a puertos NSI configurados para encapsular paquetes para dicha L2VPN. El CMTS DEBE retransmitir de forma transparente los paquetes recibidos con un encapsulado NSI configurado para una determinada L2VPN a una L2PDU DOCSIS en sentido descendente criptada en un SAID único para la L2VPN y el CM a los que se retransmite el paquete.

Un CMTS DEBERÍA implementar una función puente con capacidad VLAN como se especifica en [b-IEEE 802.1s]. Para el cumplimiento de 802.1s, cada puerto puente implementado en una interfaz RF DEBERÍA considerarse como una interfaz 802.1Q totalmente rotulada para la que el ID VLAN entrante viene determinado por el SID en sentido ascendente y el ID VLAN saliente está rotulado con un SAID de BPI. Un CMTS conforme con L2VPN NO DEBE insertar un rótulo 802.1Q en los paquetes RF en sentido descendente.

El CMTS PUEDE restringir la configuración de un valor de multiplexación de servicio de encapsulado NSI (por ejemplo ID VLAN IEEE 802.1Q) a un único SF. En este modo de retransmisión punto a punto, el CMTS PUEDE omitir el aprendizaje de direcciones MAC CPE de una base de datos de retransmisión. Un CMTS punto a punto puede soportar múltiples codificaciones L2VPN por SF con el mismo subtipo de encapsulado NSI, siempre que se encuentren en el mismo CM.

Si el CMTS permite configurar más de un SF para alcanzar el mismo valor de multiplexación de servicio de encapsulado NSI, se dice que implementa el modo de retransmisión multipunto. En el modo de retransmisión multipunto, el CMTS DEBE asociar las direcciones MAC de origen CPE aprendidas con el CM del que las aprendió.

Un CMTS DEBE soportar las retransmisiones L2VPN y no L2VPN en el mismo dominio MAC RF. Un CMTS DEBE puentear de forma transparente tráfico CPE de los CM configurados con codificaciones L2VPN según esta Recomendación. Un CMTS DEBE retransmitir con sus algoritmos de retransmisión de paquetes normales que no sean L2VPN tráfico CPE proveniente de los CM con codificaciones no L2VPN, salvo cuando se especifique en esta Recomendación.

Un CMTS DEBE soportar la retransmisión L2VPN y no L2VPN de tráfico en sentido ascendente proveniente de diferentes flujos de servicio cuando se señalen sólo codificaciones L2VPN por SF.

7.2 Configuración de la retransmisión L2VPN

Un conjunto de una o más fijaciones de configuración de codificación L2VPN en un fichero de configuración CM controla sí y cómo el CMTS realiza la retransmisión L2VPN de paquetes CPE en sentido ascendente y en sentido descendente.

El parámetro de codificación L2VPN se codifica como un parámetro de ampliación de información general (GEI, *general extension information*), lo que significa que está codificado como un subtipo del parámetro de tipo 43 de información específica del suministrador mediante el ID de suministrador 0xFFFFFF (véase C.1.1.17 de [UIT-T J.122]). Al codificar la codificación L2VPN como un parámetro GEI, se puede incluir en el fichero de configuración de cualquier CM DOCSIS, incluidos los CM DOCSIS 1.0.

El parámetro de codificación L2VPN puede aparecer en las ubicaciones siguientes:

- En el nivel superior de un fichero de configuración CM, en cuyo caso, se denomina codificación L2VPN por CM.
- Como un subtipo de una GEI anidada en una codificación de flujo de servicio en sentido ascendente (tipo 24), en cuyo caso de denomina codificación L2VPN de retransmisión o por SF.
- Como un subtipo de una GEI anidada en una fijación de configuración de clasificación de paquetes en sentido ascendente (tipo 23), en cuyo caso de denomina codificación L2VPN de clasificador en sentido descendente.
- Como un subtipo de una GEI anidada en una fijación de configuración de clasificación de paquetes en sentido ascendente (tipo 22), en cuyo caso de denomina codificación L2VPN de clasificador en sentido ascendente.

El propio parámetro de codificación L2VPN se define como un parámetro multipartito con diversos parámetros de subtipo anidados. El cuadro 7-1 enumera cada uno de los subtipos y describe en qué ubicación se define el subtipo indicando si se requiere o es optativo para dicha ubicación.

Cuadro 7-1 – Resumen de ubicaciones de subtipos de codificación L2VPN

Número de subtipo	Parámetro de subtipo	Máximo nivel (por CM)	Flujo de servicio en sentido ascendente	Clasificador en sentido descendente	Clasificador en sentido ascendente
43.5.1	Identificador RPV	Requerido	Requerido	Requerido	
43.5.2	Encapsulado NSI	Opcional[c)]			
43.5.3	Habilita la indagación eSAFE DHCP	Opcional[a)]			
43.5.4	Máscara de interfaz CM	Opcional		Opcional[a)]	Opcional[a)]
43.5.5	ID de grupo de anexión	Opcional[c)]			
43.5.6	ID individual de anexión de origen	Opcional[c)]			
43.5.7	ID individual de anexión de objetivo	Opcional[c)]			
43.5.8	Prioridad de usuario entrante		Opcional		
43.5.9	Gama de prioridades de usuario			Opcional	
43.5.10	Descriptor de SA L2VPN	Requerido[b)]			
43.5.43	Específico del suministrador	Opcional	Opcional	Opcional	Opcional

[a)] El CMTS DEBE aceptar un parámetro identificado como opcional en este cuadro en una codificación L2VPN que no sea de retransmisión.

[b)] El CMTS inserta el subtipo SA-descriptor L2VPN en su primer mensaje al CM en cualquier mensaje de gestión MAC que incluya una codificación L2VPN de retransmisión; el subtipo SA-descriptor L2VPN no está configurado en un fichero de configuración CM.

[c)] Ésta es una configuración por L2VPN en el puerto NSI, definida en una codificación L2VPN por CM sólo en el modo de retransmisión punto a punto.

Si un subtipo no está definido como requerido u opcional en una ubicación, el CMTS DEBERÍA ignorarlo en silencio cuando aparezca en dicha ubicación. Si un subtipo no está definido como requerido u opcional en una ubicación, el módem de cable DEBERÍA ignorarlo en silencio cuando aparezca en dicha ubicación. Un CMTS DEBE ignorar en silencio subtipos no reconocidos en una codificación L2VPN. Un CM DEBE ignorar en silencio subtipos no reconocidos en una codificación L2VPN.

La codificación L2VPN de máximo nivel controla el comportamiento de CM y CMTS por L2VPN propio de una determinada L2VPN. La codificación L2VPN de flujo de servicio en sentido ascendente especifica qué flujo o flujos de servicio en sentido ascendente transportarán el tráfico L2VPN. Para un funcionamiento L2VPN adecuado se precisa que por lo menos un flujo de servicio en sentido ascendente esté configurado para la retransmisión de L2VPN.

Debido a que se pueden configurar múltiples flujos de servicio en sentido ascendente para retransmitir hacia la misma L2VPN, se codifican todos los parámetros por L2VPN comunes a la propia L2VPN en una única codificación L2VPN de máximo nivel en lugar de requerir o permitir que sean duplicados en múltiples codificaciones de flujo de servicio en sentido ascendente.

La retransmisión L2VPN en sentido ascendente se configura como por SF. El operador de cable puede configurar por lo menos un flujo de servicio en sentido ascendente en un fichero de configuración CM con una codificación L2VPN que define el identificador VPN hacia el que el CMTS retransmite tráfico en sentido ascendente por ese SF. Se requiere la codificación L2VPN por CM o de máximo nivel en un fichero de configuración CM sólo para el modo de retransmisión punto a punto, para definir el formato de encapsulado NSI para esa L2VPN de forma que el CMTS pueda determinar a qué CM retransmitir el tráfico L2VPN en sentido descendente. Con el modo de retransmisión multipunto para una L2VPN, se pueden retransmitir múltiples CM a múltiples encapsulados NSI, de forma que no esté definida ninguna configuración de encapsulado NSI por CM.

El fichero de configuración CM más sencillo para el funcionamiento L2VPN contiene:

- para el modo multipunto, una única codificación L2VPN por SF en la definición principal de SF en sentido ascendente; o
- para el modo punto a punto, una única codificación L2VPN por SF en la definición principal de SF en sentido ascendente y una única codificación L2VPN por CM con un subtipo de encapsulado NSI para dicha L2VPN.

En un mensaje de respuesta de registro, el CMTS siempre incluye una codificación L2VPN por CM (añadiendo otra codificación L2VPN por CM si es necesario) que proporciona por lo menos un SA-descriptor L2VPN para la criptación y etiquetado de paquetes en sentido descendente como tráfico L2VPN para CM. El CM PUEDE asignar más de un SAID a la misma L2VPN, en cuyo caso pueden aparecer múltiples subtipos SA-descriptor L2VPN en una codificación L2VPN de máximo nivel.

A menos que se configure de otra forma, el CMTS entrega tráfico L2VPN en sentido descendente a un único módem de cable en el flujo de servicio en sentido descendente principal del CM. El operador puede especificar una calidad de servicio (QoS, *quality of service*) mejorada para el tráfico L2VPN en sentido descendente con un flujo de servicio diferente en sentido descendente para la retransmisión L2VPN en el fichero de configuración del CM. El tráfico L2VPN en sentido descendente se puede clasificar para dicho flujo de servicio en sentido descendente definiendo un clasificador que incluya una codificación L2VPN de clasificador en sentido descendente que haga referencia al flujo de servicio.

El CMTS DEBE rechazar el registro de un CM con una codificación L2VPN no válida. Una configuración CM válida incluye cualquier número de codificaciones L2VPN por SF, codificaciones L2VPN de clasificador en sentido descendente y codificaciones L2VPN de clasificador en sentido ascendente. El CMTS DEBE aceptar una petición de registro CM que contenga múltiples codificaciones L2VPN por SF que retransmitan el mismo VPNID.

Una codificación L2VPN por SF válida aparece como un subtipo en la codificación de flujo de servicio en sentido ascendente (tipo 24) de un mensaje de fichero de configuración CM DOCSIS 1.1, REG-REQ, DSA-REQ o DSC-REQ. La codificación de retransmisión L2VPN por SF configura el CMTS para establecer la retransmisión puente L2VPN para todos los paquetes CPE recibidos en el flujo de servicio descrito. Una codificación de retransmisión L2VPN por SF contiene un subtipo ID L2VPN. El CMTS incluye una codificación L2VPN por CM en su REG-RSP. Tras el registro, un CM PUEDE incluir codificaciones L2VPN por CM en los mensajes de gestión MAC de servicio dinámico al máximo nivel que en otro caso añaden, cambian o suprimen codificaciones L2VPN por SF de retransmisión.

Para configurar determinadas direcciones MAC CPE para la retransmisión L2VPN, el CM se puede configurar con codificaciones de clasificación de paquetes que concuerden con la dirección MAC CPE de origen deseada. El CM clasifica el paquete con un flujo de servicio en sentido ascendente que esté configurado para retransmitir hacia una determinada L2VPN. La codificación de clasificación de paquetes en sentido ascendente que hace referencia a una codificación L2VPN de SF en sentido ascendente de retransmisión no contiene por sí misma el subtipo VPNID.

El CMTS DEBE considerar un flujo de servicio en sentido ascendente para su configuración para la retransmisión L2VPN por SF cuando REG-REQ, DSA-REQ o DSC-REQ contienen exactamente una codificación de retransmisión L2VPN por SF válida en la codificación de flujo de servicio en sentido ascendente. Una codificación de retransmisión L2VPN por SF válida contiene un subtipo VPNID. El CMTS DEBE rechazar una transacción de flujo de servicio que contenga más de una codificación L2VPN por SF.

El CMTS DEBE aceptar un DSC-REQ válido con una codificación L2VPN por SF válida y cambiar el tratamiento de la retransmisión en sentido ascendente de los paquetes recibidos en ese SF. Esto incluye, por ejemplo, añadir, cambiar o suprimir cualquier subtipo permitido de una codificación L2VPN por SF, incluido el subtipo VPNID.

El CMTS DEBE suprimir la retransmisión L2VPN por SF para un SF cuando se suprima el SF mediante una transacción de supresión de servicio dinámica (DSD, *dynamic service delete*) válida o una transacción de cambio de servicio dinámico (DSC, *dynamic service change*) completa que omita una codificación L2VPN por SF indicada con anterioridad.

El CMTS DEBE soportar múltiples codificaciones L2VPN por SF, cada una en un SF diferente, con el mismo valor de subtipo VPNID.

Un CMTS de retransmisión multipunto PUEDE aceptar los subtipos por RPV definidos sólo para el modo punto a punto, aunque no se ha definido el funcionamiento CMTS con diferentes valores de subtipos en diferentes CM.

7.2.1 Subtipo VPNID

El subtipo VPNID es una secuencia de bytes opaca que identifica una red privada virtual de capa 2 lógica. Todos los anfitriones conectados a la misma L2VPN lógica comunican entre ellos como si estuvieran conectados a la misma LAN privada. Una L2VPN es una red que retransmite paquetes basándose únicamente en información de capa 2 como las direcciones MAC de Ethernet y con cualesquiera rótulos ID VLAN encapsulando el paquete. El término "ID VLAN" debería utilizarse únicamente para describir el campo ID VLAN de 12 bits codificado en un par de rótulos IEEE 802.1Q o IEEE 802.1ad de un paquete L2VPN retransmitido en un puerto NSI.

Se espera que un operador de cable configure un único VPNID para cada empresa comercial a la cual ofrece servicio LAN transparente. El operador de cable puede elegir cualquier formato deseado para el VPNID, aunque debería ser globalmente único. Se sugiere seguir [b-IETF RFC 2685], que define un mecanismo para asignar globalmente identificadores RPV únicos de 7 bytes, basándose en una combinación de identificadores de organización únicos de 3 bytes para la organización que asigna el ID (por ejemplo, el propio operador de cable), con un VPNID de 4 bytes asignado por dicha organización. Otro planteamiento sugerido es el de [b-IETF RFC 2547], que describe un distinguidor de encaminamiento de 8 bytes que se puede utilizar como un VPNID único.

El CMTS DEBE ignorar una codificación L2VPN por SF que omita un subtipo VPNID o que contenga más de un subtipo VPNID. El CMTS DEBE soportar por lo menos cuatro (4) valores diferentes de VPNID por CM, señalados en cuatro o más codificaciones L2VPN por SF.

En una aplicación de servicio LAN privada virtual (VPLS) IETF, el VPNID está destinado para ser el ID de grupo de anexión (AGI, *attachment group ID*) señalado entre el CMTS y otros elementos de red VPLS.

7.2.2 Codificación L2VPN de clasificador en sentido descendente

Una codificación L2VPN de clasificador en sentido descendente es una codificación L2VPN que aparece en una codificación de clasificación de paquetes en sentido descendente (véase C.2.1.2 de [UIT-T J.122]. La presencia de una codificación L2VPN en una codificación de clasificación de paquetes en sentido descendente limita al clasificador a que aplique únicamente paquetes retransmitidos por el retransmisor L2VPN. Es más, sólo los clasificadores que contienen una clasificación L2VPN se aplican a paquetes retransmitidos por el retransmisor L2VPN. En otras palabras, los clasificadores en sentido descendente aplican a tráfico L2VPN o a tráfico que no es L2VPN, pero nunca a ambos.

Una codificación L2VPN de clasificador en sentido descendente puede contener ninguno o un subtipo VPNID y/o ninguno o un subtipo gama de prioridades de usuario. Puede que no incluya ningún subtipo (es decir, parámetro 43.5 de longitud 0), en cuyo caso, el clasificador aplica todos los paquetes en sentido descendente retransmitidos por L2VPN al CM, independientemente del VPNID o de la prioridad de usuario.

La presencia de un subtipo VPNID en una codificación L2VPN de clasificador en sentido descendente instruye al CMTS para que aplique el clasificador sólo al tráfico retransmitido por L2VPN en sentido descendente en la L2VPN indicada. Puesto que la L2VPN del tráfico retransmitido por L2VPN siempre está *implícita* en la interfaz RF DOCSIS, y no está presente explícitamente en el contenido del paquete, esta es la única forma de clasificar tráfico retransmitido por L2VPN en sentido descendente a un determinado flujo de servicio basándose en el propio VPNID.

Si el codificador L2VPN de clasificador en sentido descendente contiene un subtipo gama de prioridades de usuario, el clasificador aplica sólo a paquetes L2VPN retransmitidos en sentido descendente con una prioridad de usuario saliente en la gama indicada (inclusive). Esto permite clasificar tráfico L2VPN de alta prioridad para flujos de servicio en sentido descendente con QoS mejorada.

El valor de la prioridad de usuario saliente que corresponde a un subtipo de gama de prioridades de usuario es la prioridad transmitida de forma lógica por el retransmisor L2VPN en sentido descendente hacia la interfaz de capa MAC DOCSIS. Esto significa que es el valor *después* de cualquier regeneración del valor de prioridad de usuario por el retransmisor L2VPN. El suministrador CMTS PUEDE implementar mecanismos específicos del suministrador para determinar y regenerar las prioridades de usuario de paquetes retransmitidos por L2VPN en sentido descendente.

Un CMTS DEBE rechazar el registro de un CM con una codificación de clasificador de paquetes en sentido descendente que contenga más de una codificación L2VPN.

7.2.3 Subtipo SA-descriptor L2VPN

El subtipo SA-descriptor L2VPN es una codificación multipartita definida en la privacidad básica [UIT-T J.125] que proporciona:

- El identificador de asociación de seguridad (SAID, *security association identifier*) de privacidad básica (BPI, *baseline privacy*) que utiliza el CMTS para criptar tráfico L2VPN en sentido descendente para la L2VPN identificada en la codificación L2VPN;
- una serie criptográfica que identifica el algoritmo de criptación; y
- un tipo de asociación de seguridad (SA-Type).

El CMTS DEBE codificar el SA-descriptor L2VPN como un SA-Type dinámico (2). Un CM DEBE ignorar el SA-Type y considerarlo como un tipo dinámico (2).

El tráfico L2VPN en sentido ascendente siempre se cripta en el SAID primario del CM que transmite el tráfico en sentido ascendente. El subtipo SA-descriptor L2VPN no está indicado en un

fichero de configuración CM. Por el contrario, el CMTS añade uno o más subtipos SA-descriptor L2VPN a codificaciones L2VPN por CM de máximo nivel de su REG-RSP al CM, añadiendo la codificación L2VPN por CM al REG-RSP en caso necesario. Una vez que el CM completa la autenticidad BPI, inicia una transacción de clave de criptación de tráfico (TEK, *traffic encrypting key*) con el CMTS para cada SA-descriptor L2VPN en un mensaje REG-RSP.

El CMTS incluye un SAID L2VPN en una codificación de subtipo SA-descriptor L2VPN al máximo nivel de un mensaje DSA-REQ o DSC-REQ iniciado por el CMTS que define, en otro caso, un SF en sentido ascendente de retransmisión L2VPN. De la misma forma, el CMTS incluye un subtipo SA-descriptor L2VPN en una codificación L2VPN de máximo nivel en sus respuestas DSA-RSP o DSC-RSP al CM a la transacción de servicio dinámico iniciada por el CM, que define un flujo de servicio en sentido ascendente de retransmisión L2VPN. Un SAID señalado en una codificación de subtipo SA-descriptor L2VPN se denomina un SAID L2VPN. Un SAID conocido por el CM sólo a partir de mensajes distintos de un subtipo SA-descriptor L2VPN se denomina SAID no L2VPN. La cláusula 7.5 describe cómo la criptación BPI separa el tráfico L2VPN y tráfico no L2VPN en la red RF.

Una vez completada cualquier transacción de mensaje MAC de servicio dinámico que introduce un nuevo SAID al CM, el CM inicia una transacción TEK con el CMTS para obtener las claves para el nuevo SAID.

En el modo de retransmisión L2VPN punto a punto, el CMTS asigna un SAID L2VPN individual a cada CM. Si el CM retransmite más de una L2VPN, el CMTS asigna un SAID L2VPN individual diferente para cada L2VPN. En el modo de retransmisión L2VPN multipunto, el CMTS asigna un SAID L2VPN de grupo para todos los CM que retransmiten la L2VPN compartida.

7.2.4 Codificación L2VPN específica del suministrador

El subtipo codificación L2VPN específica del suministrador se acepta en cualquier ubicación de codificación L2VPN y proporciona información específica al suministrador del CMTS o del CM. Por ejemplo, puede indicar a un suministrador CMTS una subinterfaz de puerto NSI determinada por la que la L2VPN retransmite el tráfico en un modelo punto a punto. La codificación L2VPN específica del suministrador puede ser binaria o ASCII; su definición se deja al suministrador CMTS.

Una implementación CMTS PUEDE permitir una codificación L2VPN específica del suministrador para *sustituir* un VPNID que fuera necesario o un subtipo de encapsulado NSI, pero las codificaciones L2VPN específicas del suministrador NO DEBEN ser requeridas por un CMTS para las pruebas de certificación L2VPN.

7.2.5 Requisitos de error de configuración

Un CMTS de retransmisión multipunto DEBE rechazar – con un código de confirmación reject-multipoint-NSI – un registro o una transacción de servicio dinámica que pretenda configurar múltiples codificaciones L2VPN de retransmisión en sentido ascendente al mismo ID L2VPN pero con diferentes valores en los subtipos encapsulado NSI, AGI, TAII o SAII.

Un CMTS de retransmisión punto a punto DEBE rechazar – con un código de confirmación reject-VLAN-ID-in-use – un registro o una transacción de flujo de servicio con un subtipo de encapsulado NSI L2VPN que requiera retransmisión en el puerto seleccionado L2VPN con un ID VLAN ya asignado para fines distintos de L2VPN. Un CMTS de retransmisión punto a punto DEBE rechazar un intento de configurar un puerto seleccionado L2VPN con un ID VLAN ya asignado por una codificación de subtipo de encapsulado NSI L2VPN.

Un CMTS de retransmisión punto a punto DEBE rechazar – con un código de confirmación reject-multipoint-L2VPN – un registro o una transacción de flujo de servicio que intente configurar más de un circuito de anexión de cable (por ejemplo, CM) con el mismo valor de multiplexación de servicio de encapsulado NSI L2VPN.

7.2.6 Encapsulado de interfaz de sistema de red (NSI)

Los conmutadores y encaminadores LAN modernos implementan un amplio conjunto de características puente de capa 2 y el funcionamiento de L2VPN en amplias zonas mediante MPLS, y las redes medulares con túneles IP constituyen un campo en el que se están realizando innovaciones y normalizaciones. Esta Recomendación *no* especifica en su totalidad la retransmisión de capa 2 de paquetes Ethernet entre los CMTS. Intenta especificar la configuración de retransmisión L2VPN en un único CMTS y, en particular, entre un circuito de anexión de interfaz RF de un CM y una interfaz NSI. Se anima a los suministradores de CMTS que soporten los protocolos y características de puentes de futuras redes medulares de capa 2 cuando retransmitan tráfico de capa 2 hacia y desde una interfaz MAC RFI DOCSIS.

7.2.6.1 Subtipo encapsulado NSI

Aunque esta Recomendación especifica principalmente el funcionamiento L2VPN en la interfaz RF DOCSIS, también especifica en menor grado el funcionamiento en una interfaz NSI por las razones siguientes:

- para normalizar la configuración L2VPN para pruebas de certificación; y
- para normalizar entre suministradores de CMTS un conjunto útil de capacidades L2VPN.

Esta Recomendación define un subtipo encapsulado NSI de una codificación L2VPN (véase B.3.2). para describir como opción cómo se encapsulan los paquetes de la L2VPN en un único puerto NSI seleccionado. La implementación del suministrador CMTS puede permitir que este puerto NSI seleccionado cambie en el caso de un fallo de puerto o de otros eventos. Un suministrador de CMTS PUEDE utilizar el subtipo encapsulado NSI para otros casos y PUEDE utilizar subtipos específicos del suministrador de encapsulado NSI para soportar las correspondencias específicas del suministrador entre circuitos de anexión y seudohilos medulares o instancias de conmutación virtual externas.

Esta Recomendación requiere a los CMTS que implementen sólo un único formato de encapsulado NSI L2VPN: rótulos IEEE 802.1Q, con un valor de ID VLAN de 12 bits configurado de forma estática como el valor de multiplexación de servicio. Si el CMTS implementa otros formatos de encapsulado L2VPN en un puerto NSI debería utilizar la codificación del subtipo encapsulado NSI si ese código de formato en particular está definido para el subtipo.

Cuando un ID VLAN de encapsulado NSI está configurado de forma estática, se supone que aplica sólo al puerto Ethernet seleccionado. La selección de una determinada interfaz NSI para retransmitir una determinada L2VPN o un circuito de anexión depende del suministrador. El subtipo L2VPN específico del suministrador se puede utilizar para estos fines.

Un CMTS de retransmisión punto a punto DEBE rechazar un registro CM o una transacción de flujo de servicio con una codificación L2VPN que omita el subtipo encapsulado NSI o un subtipo específico del suministrador que identifique el valor de multiplexación de servicio NSI. Un CMTS de retransmisión multipunto no requiere un subtipo encapsulado NSI en una codificación L2VPN, aunque DEBE aceptar e implementar el subtipo si está especificado. Un CMTS en cualquier modo de retransmisión DEBE rechazar un registro CM o una transacción de flujo de servicio con una codificación L2VPN que incluya un subtipo encapsulado NSI para un VPNID que difiera del subtipo encapsulado NSI para dicho VPNID en cualquier otra codificación L2VPN aceptada.

En el encapsulado NSI IEEE 802.1Q, los valores de ID VLAN 0, 1 y 4095 no están permitidos como ID VLAN configurados. El ID VLAN 0 se reserva para rótulos sólo de prioridad en [IEEE 802.1Q]. El ID VLAN 1 se reserva como el ID VLAN por defecto basado en puertos [IEEE 802.1Q]. Si se permite a las L2VPN de abonado configurar el ID VLAN 1, existe el riesgo de retransmitir sin querer en la capa 2 el tráfico de gestión fuera de banda en dicha L2VPN de abonado. El ID VLAN 4095 (todo '1') está reservado por el IEEE.

Que el CMTS acepte o no tráfico L2VPN en un puerto LSI con un rótulo IEEE 802.1Q sólo de prioridad (es decir, con ID VLAN 0) depende de las implementaciones propias del suministrador.

7.2.6.2 Retransmisión L2VPN IEEE 802.1ad

[b-IEEE 802.1ad] describe un planteamiento de rotulado dual para la retransmisión L2VPN en una red medular. Un paquete tiene un rótulo exterior ID VLAN de 12 bits y un rótulo interior ID VLAN de 12 bits. El subtipo encapsulado NSI permite configurar el par de rótulos ID VLAN de 12 bits para cada CM o SF que realice la retransmisión L2VPN. La configuración de rótulos duales depende del modo de retransmisión L2VPN del CMTS y de los elementos de red IEEE 802.1ad en la red medular.

7.2.6.2.1 Retransmisión CMTS punto a punto con retransmisión 802.1ad punto a punto

En este escenario, los elementos de red IEEE 802.1ad en la red medular retransmiten simplemente punto a punto sin aprendizaje de direcciones MAC. El rótulo 802.1ad exterior identifica un elemento de red de destino que realiza las funciones de puente L2VPN del aprendizaje de direcciones MAC en un puerto puente y la retransmisión/difusión entre esos puertos puente. El rótulo 802.1ad interior identifica un determinado puerto puente en ese elemento puente L2VPN externo.

El CMTS no está configurado con la dirección o la identidad IP del nodo de destino en este caso. Está configurado sólo con los dos rótulos ID VLAN para usarlos en el encapsulado de puerto NSI.

Cuando se retransmiten tramas 802.1ad con doble rótulo en una red básica, los nodos intermedios sólo utilizan el rótulo ID VLAN exterior para tomar decisiones de retransmisión. Por ejemplo, 802.1ad soporta el aprovisionamiento de tramas de retransmisión basándose en el valor del rótulo exterior sin una dirección MAC.

El puente L2VPN considerado por el rótulo ID VLAN exterior está configurado por separado en función de la L2VPN de cliente lógica a la que esté conectado cada puerto puente con rótulo interno.

7.2.6.2.2 Retransmisión CMTS punto a punto con elemento de red puente L2VPN

[b-IEEE 802.1ad] se puede utilizar para construir un elemento de red medular, generar la función de conmutación L2VPN de aprendizaje de capa MAC y la retransmisión/difusión entre circuitos de anexión pertenecientes a la misma L2VPN.

En este escenario, el rótulo ID VLAN interno representa a la L2VPN lógica y el rótulo ID VLAN externo representa a un circuito de anexión individual con dicha L2VPN lógica. El conmutador L2VPN IEEE 802.1ad considera que el rótulo ID VLAN exterior representa a una base de datos de retransmisión basándose en las direcciones MAC que obtiene de cada interfaz troncal virtual, y retransmite/difunde paquetes entre esas interfaces troncales virtuales. De esta forma, proporciona la retransmisión de conmutadores L2VPN entre todos los circuitos de anexión de una L2VPN. Utilizando esta técnica, se pueden soportar más de 4000 ejemplares de servicio L2VPN entre un CMTS y el conmutador L2VPN IEEE 802.1ad y cada uno de estos puede tener más de 4000 asociaciones entre módems de cable y flujos de servicio en el CMTS.

7.2.7 Servicio LAN privado virtual (VPLS) y servicio de cable privado virtual.

7.2.7.1 Encapsulado NSI MPLS y L2TPv3

Los formatos de encapsulado NSI MPLS y L2TPv3 están diseñados para soportar el interfuncionamiento de la retransmisión L2VPN DOCSIS con normas de servicio de cable privado virtual (VPWS, *virtual private wire service*) y servicio LAN privado virtual (VPLS) del IETF. El modelo IETF está basado en circuitos de anexión a entidades de retransmisor L2VPN. Cada CM con por lo menos un SF de retransmisión en sentido ascendente para una L2VPN se corresponde con un circuito de anexión con la L2VPN. Debido a que la característica L2VPN DOCSIS permite

múltiples flujos de servicio para la misma L2VPN, y que no asocia determinados flujos de servicio en sentido descendente a flujos de servicio en sentido ascendente, se considera que un circuito de anexión de cable con una L2VPN es el CM y no un flujo de servicio individual en el CM.

Los paquetes de capa 2 se retransmiten en seudohilos a través de un puerto NSI, siendo un seudohilo un trayecto MPLS o una sesión túnel L2TPv3. Un determinado seudohilo se identifica a la entrada a un punto extremo con una pila de una o más etiquetas MPLS o un ID de sesión L2TPv3. Los protocolos L2VPN IETF se destinan a soportar la selección dinámica de estos valores de encapsulado túnel negociando la creación de seudohilos entre puntos extremos que implementen la misma L2VPN lógica. Ésta es la razón fundamental para que se configure un subtipo VPNID único globalmente para cada codificación de retransmisión L2VPN por SF. Para puntos extremos que implementen protocolos de creación de túnel dinámicos compatibles, sólo los campos VPNID y protocolo de encapsulado NSI precisan ser configurados para un CM o SF DOCSIS.

En el caso en que los valores de encapsulado de seudohilo (es decir, etiqueta MPLS o valores ID de sesión L2TPv3) no puedan ser negociados de forma dinámica, se pueden configurar mediante parámetros de subtipo específicos del suministrador L2VPN o mediante otra configuración CMTS propia del suministrador.

7.2.7.2 Configuración VPLS/VPWS

La señalización del plano de control para VPLS utiliza tres campos configurables para identificar las L2VPN y los circuitos de anexión:

- ID de grupo de anexión;
- ID individual de anexión de origen (SAII, *source attachment individual ID*); e
- ID individual de anexión de objetivo (TAII, *target attachment individual ID*).

Para establecer la norma de configuración DOCSIS de estos campos en un fichero de configuración CM, esta Recomendación define un subtipo de una codificación L2VPN para cada campo.

El subtipo ID de grupo de anexión (AGI) de una codificación L2VPN se define actualmente sólo en codificaciones L2VPN de retransmisión por SF. Proporciona el valor del campo AGI cuando se establece un MPLS de red básica NSI o un seudohilo L2TPv3 para un circuito de anexión de cable. Sólo se aplica para retransmisiones punto a punto entre el circuito de anexión y el seudohilo. Para una descripción de la arquitectura de la emulación de seudohilo véase [b-IETF RFC 3985].

El subtipo individual ID de anexión de origen (SAII) se define sólo en una codificación L2VPN de retransmisión por SF. Indica el valor señalado dinámicamente por el retransmisor L2VPN como el campo SAII, cuando advierte un valor de multiplexación de servicio de encapsulado NSI tal como una etiqueta MPLS o un identificador de sesión L2TPv3. Este campo sólo se utiliza para aplicaciones L2VPN IETF tales como el servicio LAN privado virtual (VPLS) o el servicio alámbrico privado virtual (VPWS) cuando el CMTS funciona en el modo de retransmisión punto a punto entre seudohilos NSI y circuitos de anexión CM/SF. El SAII configurado se corresponde con el ID individual de objetivo (TAII) de una petición de establecimiento de seudohilo dinámica entrante.

El subtipo ID individual de anexión de objetivo (TAII) se define sólo para una codificación L2VPN de retransmisión por SF. Proporciona el valor señalado de forma dinámica por el retransmisor L2VPN como el campo TAII cuando se inicia el establecimiento de un seudohilo L2VPN IETF en una interfaz NSI. Este campo se utiliza sólo para aplicaciones L2VPN IETF tales como VPLS o VPWS cuando el CMTS está iniciando un seudohilo con un elemento de red distante que esté implementando una retransmisión punto a punto. El TAII concuerda con el SAII de uno de los circuitos de anexión del elemento de red distante.

El CMTS DEBERÍA utilizar cualquier subtipo ID de grupo de anexión (AGI), ID individual de anexión de origen (SAII) o ID individual de anexión de objetivo (TAII) configurados en una

codificación L2VPN de retransmisión, para los valores de los campos correspondientes con protocolos especificados por IETF que pretendan establecer un seudohilo NSI conmutado a un circuito de anexión.

7.3 Retransmisión L2VPN en sentido ascendente de CMTS

El CMTS NO DEBE interpretar un rótulo 802.1Q que ya ha aparecido en un paquete en sentido ascendente como si proporcionara la prioridad o el identificador L2VPN para el puente de retransmisión L2VPN. Esto incluye un rótulo sólo de prioridad. El CMTS DEBE retransmitir de forma transparente cualquier rótulo 802.1Q proporcionado por el abonado. Si el paquete rotulado por el abonado se retransmite en un puerto Ethernet NSI 802.1Q, el CMTS DEBE añadir un rótulo 802.1Q exterior delante del rótulo interior proporcionado por el abonado.

El CMTS DEBE ser capaz de enviar y recibir para su retransmisión L2VPN por todas las interfaces un paquete de 1522 bytes que incluye un rótulo de abonado apilado, además de cualquier información L2VPN que delimite el servicio en la interfaz. Por ejemplo, en una interfaz NSI Ethernet que acepte rótulos 802.1Q para encapsulado NSI L2VPN, el CMTS acepta y retransmite un paquete Ethernet de 1526 bytes. Este tipo de paquete se retransmite al dominio MAC RF en sentido descendente como un paquete de 1522 bytes constituido por un paquete Ethernet nominal de longitud máxima 1518 bytes con un rótulo de cuatro bytes que no delimita el servicio de abonado.

El CMTS NO DEBE contar direcciones MAC CPE L2VPN aprendidas obtenidas de los paquetes en sentido ascendente hacia cualquier fijación docsSubMgtCpeControlMaxCPEIp en vigor para el CM (véase C.1.1.18.1 de [UIT-T J.122]). Esta fijación sólo aplica a direcciones IP de abonado aprendidas que se retransmiten de forma distinta a L2VPN. Los CMTS en modo multipunto tienen un requisito diferenciado para limitar el número de direcciones MAC de origen obtenidas en cada L2VPN.

El CMTS NO DEBE aplicar filtrado de gestión de abonado (véase C.1.1.18 de [UIT-T J.122]) a paquetes retransmitidos por L2VPN en sentido ascendente.

El CMTS NO DEBE realizar funciones de sobreescritura ToS (véase C.2.2.6.10 de [UIT-T J.122]) para paquetes retransmitidos por L2VPN en sentido ascendente.

Un retransmisor L2VPN mantiene una prioridad de usuario de 3 bits fuera de banda asociada con cada paquete retransmitido. El CMTS DEBE utilizar el campo prioridad de usuario de 3 bits de los rótulos IEEE 802.1Q como su prioridad de usuario cuando acepte paquetes retransmitidos L2VPN con un encapsulado NSI IEEE 802.1Q. El CMTS DEBE utilizar su prioridad de usuario cuando clasifique paquetes en sentido descendente. El CMTS DEBE codificar el valor entrante de la prioridad de usuario como se haya especificado para el formato de encapsulado NSI (por ejemplo, en los bits de prioridad de usuario de un rótulo en IEEE 802.1Q). El CMTS DEBERÍA proporcionar correspondencias entre las prioridades de usuario entrantes y las clases de tráfico de transmisión de puerto NSI según se especifica en [b-IEEE 802.1s]. El número de clases de tráfico de transmisión de puerto NSI depende del suministrador. Si una codificación L2VPN de flujo de servicio en sentido ascendente omite el subtipo prioridad de usuario IEEE 802.1, el CMTS DEBE por defecto retransmitir esos paquetes a un puerto NSI con encapsulado NSI IEEE 802.1Q con una prioridad de usuario cero. El CMTS PUEDE retransmitir valores de prioridad de usuario por defecto distintos de cero con configuraciones propias del suministrador.

El CMTS DEBE soportar tanto retransmisiones L2VPN como no L2VPN de tráfico en sentido ascendente desde un flujo de servicio L2VPN de retransmisión, basándose en la comprobación de la dirección MAC de origen frente a una máscara de interfaz CM configurada para el SF. El CMTS DEBE dirigir paquetes provenientes de las direcciones MAC de origen indicadas con un '1' en la máscara de interfaz CM hacia el retransmisor L2VPN. El CMTS NO DEBE dirigir al retransmisor L2VPN paquetes provenientes de eCM y de por lo menos otra dirección MAC de origen eSAFE, incluso cuando se recibieran en un flujo de servicio en sentido ascendente de retransmisión L2VPN,

cuando las interfaces correspondientes a esas direcciones MAC de origen estén indicadas con un '0' en la máscara de interfaz CM.

Un CMTS PUEDE reconocer cuando las máscaras de interfaz CM en el conjunto de codificaciones L2VPN de clasificador de paquetes en sentido ascendente de una CM conforme permiten evitar la comprobación de direcciones MAC en sentido ascendente y retransmitir en su lugar paquetes en sentido ascendente a los retransmisores L2VPN y no L2VPN, basándose únicamente en el flujo de servicio en sentido ascendente.

El CMTS DEBE reconocer un criterio de máscara de interfaz CM en una codificación L2VPN de clasificador de paquetes en sentido descendente independientemente de si la codificación clasifica tráfico L2VPN o no L2VPN. El CMTS DEBE clasificar la dirección MAC de destino de un paquete en sentido descendente en tres clases:

1) una dirección MAC CM;

2) una dirección MAC CPE; o

3) una dirección MAC eSAFE de un determinado tipo de anfitrión eSAFE.

El CMTS DEBE considerar el criterio elegido cuando la dirección MAC de destino de un paquete de capa 2 en sentido descendente es una dirección MAC CM o una dirección MAC eSAFE que corresponde a un tipo anfitrión con un '1' en una máscara de interfaz CM. El CMTS DEBE considerar el criterio de correspondencia cuando la dirección MAC de destino es una dirección MAC CPE y la máscara de interfaz CPE tiene *cualquier* conjunto de bits de tipo anfitrión CPE, es decir, cualquier bit 1 ó 1-15. El CMTS DEBE considerar el criterio de no correspondencia cuando la dirección MAC de destino es una dirección MAC CM o eSAFE y el único bit de la máscara de interfaz CM correspondiente a ese tipo anfitrión tiene un '0'. El CMTS DEBE considerar el criterio de no concordancia cuando la dirección MAC de destino es una dirección MAC CPE y la máscara de interfaz CM tiene un bit cero en todas las posiciones del tipo anfitrión CPE, es decir tiene un bit cero en las posiciones 1 y 5-15.

El CMTS DEBE rechazar cualquier intento (es decir, registro o transacción DSx) para configurar múltiples codificaciones L2VPN de clasificador en sentido ascendente que clasifiquen al mismo flujo de servicio en sentido ascendente pero con subtipos VPNID diferentes. El CMTS utiliza el SF en sentido ascendente para determinar un único VPNID para la retransmisión L2VPN.

7.4 Retransmisión L2VPN en sentido descendente de CMTS

El CMTS DEBE rechazar cualquier REG-REQ con una codificación L2VPN, si la BPI no está también habilitada en el REG-REQ. El CMTS DEBE rechazar cualquier DSA-REQ o DSC-REQ con una codificación L2VPN, si la BPI no está también habilitada para el CM.

El CMTS NO DEBE aplicar filtros de gestión de abonado (véase C.1.1.18 de [UIT-T J.122]) a tráfico retransmitido por L2VPN en sentido descendente.

El CMTS DEBE aceptar una única codificación L2VPN de clasificador en sentido descendente en una codificación de clasificación de paquetes en sentido descendente de un mensaje REG-REQ, DSA-REQ o DSC-REQ. Un CMTS DEBE aplicar reglas de clasificación que contengan una codificación L2VPN sólo a paquetes retransmitidos por el retransmisor L2VPN. Es más, sólo se pueden aplicar clasificadores que contengan una clasificación L2VPN al tráfico retransmitido por L2VPN en sentido descendente.

- El CMTS DEBE rechazar el registro de módems de cable con codificaciones de clasificación de paquetes en sentido descendente no válidas.
- Una codificación L2VPN de clasificación en sentido descendente válida contiene cero o un subtipo VPNID, cero o un subtipo gama de prioridades de usuario y cualquier cantidad de subtipos parámetro L2VPN específico del suministrador. El CMTS DEBE ignorar en silencio todos los subtipos de codificación L2VPN no válidos.

- El CMTS DEBE aceptar como válido e ignorar en silencio cualquier subtipo de codificación L2VPN no reconocido.
- El CMTS DEBE aceptar múltiples fijaciones de configuración de clasificación en sentido descendente con una codificación L2VPN de clasificador en sentido descendente que clasifique diferentes ID VPN L2VPN con el mismo flujo de servicio referenciado.
- El CMTS DEBE soportar las mismas opciones del criterio de clasificador para codificaciones L2VPN de clasificador en sentido descendente de la misma forma que para codificaciones L2VPN de clasificador en sentido descendente no L2VPN.
- El CMTS DEBE interpretar una codificación de clasificador de paquetes en sentido descendente que no contenga otros criterios que el de una codificación L2VPN de clasificador para que concuerde con *todos* los paquetes retransmitidos en sentido descendente en la L2VPN identificada mediante el VPNID de la codificación L2VPN de clasificador, y clasificar todos estos paquetes con el flujo de servicio referenciado.
- El CMTS PUEDE aceptar múltiples codificaciones L2VPN de clasificador en sentido descendente con los mismos paquetes de clasificación VPNID para diferentes flujos de servicio. El funcionamiento no está definido cuando más de un clasificador en sentido descendente concuerda con un determinado paquete en sentido descendente.
- El CMTS DEBE rechazar una petición de transacción de flujo de servicio que contenga una codificación L2VPN de clasificador en sentido descendente no válida.
- Si la codificación L2VPN contiene un subtipo gama de prioridades de usuario, el CMTS DEBE hacer corresponder el clasificador sólo con paquetes retransmitidos por L2VPN con una prioridad de usuario entrante en la gama indicada. En otro caso, el clasificador aplica a todas las prioridades de usuario entrantes.

Con la aceptación de una codificación L2VPN de clasificador en sentido descendente, el retransmisor L2VPN del CMTS DEBE retransmitir en el flujo de servicio referenciado del clasificador todo el tráfico en sentido descendente de un único CM destinado al CPE anexado a dicho CM. Para el modo punto a punto esto implica a todo el tráfico en sentido descendente en la L2VPN. Para el modo multipunto esto implica el tráfico unidifundido destinado a las direcciones MAC CPE obtenidas del tráfico en sentido ascendente desde el CM. Si el tráfico retransmitido por L2VPN en sentido descendente no está clasificado a un determinado flujo de servicio en sentido descendente, el CMTS DEBE retransmitir tráfico de un único CM en el flujo de servicio en sentido descendente principal del CM.

El CMTS DEBE clasificar paquetes de capa 2 según aparezcan en la interfaz RFI, es decir, SIN incluir ningún rótulo 802.1Q que delimite el servicio y que haya aparecido en el puerto NSI CMTS. Esto significa que las codificaciones de clasificación de paquetes 802.1Q (véase C.2.1.7 de [UIT-T J.122]) aplican únicamente al rótulo 802.1Q de abonado privado o interno y no al ID VLAN del paquete retransmitido por L2VPN.

Un CMTS NO DEBE aplicar filtros de gestión de abonado (véase C.1.1.18 de [UIT-T J.122]) al tráfico L2VPN en sentido descendente.

Un CMTS DEBE retransmitir paquetes retransmitidos por L2VPN en sentido descendente para diferentes L2VPN en diferentes flujos de servicio en sentido descendente. Esto proporciona aislamiento de QoS para el servicio L2VPN.

A menos que esté configurado explícitamente para combinar la base de datos de retransmisión de diferentes L2VPN, el retransmisor L2VPN CMTS DEBE mantener la separación entre el sentido ascendente y el sentido descendente del tráfico retransmitido por L2 entre circuitos de anexión configurados con diferente VPNID. El número de CM o SF soportados por la retransmisión L2VPN depende del suministrador CMTS. El número de VPNID únicos soportados por un CMTS depende del suministrador.

7.4.1 Retransmisión multipunto en sentido descendente

El CMTS DEBE rechazar (con un código de confirmación reject-permanent) un registro o una transacción de flujo de servicio que pudiera requerir la definición de SAID L2VPN que exceda la capacidad SAID en sentido descendente del CM (véase C.1.3.1.7 de [UIT-T J.122]).

Un CMTS en el modo de retransmisión multipunto DEBE aprender las direcciones MAC de origen del tráfico CPE en sentido ascendente y asociarlas con un determinado CM en esa L2VPN.

Un CMTS de retransmisión multipunto DEBE limitar el número de direcciones MAC permitidas para su aprendizaje en una única L2VPN a un valor configurable que aplique a todas las L2VPN. El CMTS DEBERÍA permitir la configuración de un número máximo de direcciones MAC por L2VPN para cada L2VPN.

Un CMTS de retransmisión multipunto DEBE retransmitir paquetes en sentido descendente criptados en diferentes SAID L2VPN sobre diferentes flujos de servicio.

7.5 Aislamiento y privacidad L2VPN

Un objetivo fundamental de esta Recomendación es *separar* el tráfico entre abonados L2VPN y abonados no L2VPN, así como entre diferentes abonados L2VPN. Los abonados no L2VPN (es decir, residenciales) no deberían ser capaces de ver el tráfico retransmitido a abonados L2VPN, y los abonados L2VPN, además, no deberían ver el tráfico destinado a abonados residenciales no L2VPN.

7.5.1 Protección del tráfico L2VPN

Esta Recomendación utiliza criptación BPI para aislar al tráfico L2VPN del tráfico no L2VPN en sentido descendente. Esto requiere que un operador de cable configure los CM que dan servicio L2VPN para permitir el funcionamiento de la interfaz de privacidad básica (BPI). Se espera que el operador de cable configure todos los CM con y sin retransmisión L2VPN, para habilitar la BPI, de forma que todos estos CM puedan recibir tráfico IP multidifundido y criptado.

El CMTS DEBE rechazar cualquier intento (es decir, un registro o una transacción DSx) de configurar una codificación L2VPN de retransmisión cuando el CM no esté también configurado para soportar el funcionamiento BPI.

Un CMTS DEBE asignar por lo menos un SAID L2VPN para la retransmisión en sentido descendente para cada L2VPN retransmitida por el CMTS en un canal en sentido descendente. Un SAID L2VPN único asignado para todos los CM en la misma L2VPN se denomina SAID L2VPN de grupo. El CMTS PUEDE asignar valores SAID L2VPN que sean diferentes para la misma L2VPN en diferentes canales en sentido descendente. Un CMTS PUEDE asignar múltiples SAID L2VPN a la misma L2VPN en el mismo canal en sentido descendente, por ejemplo, para asignar un SAID L2VPN individual a cada CM en el modo de retransmisión punto a punto. El CMTS DEBE asignar un SAID L2VPN de grupo o individual que difiera de cualquier otro SAID primario asignado en dicho canal. Un CMTS PUEDE asignar múltiples SAID a la misma L2VPN en el mismo CM.

Un CMTS DEBE añadir a la codificación L2VPN de retransmisión de sus mensajes REG-RSP y de servicio dinámico hacia un CM conforme con L2VPN uno o más subtipos SA-descriptor L2VPN para sus SAID L2VPN asignados para la retransmisión en sentido descendente a dicha L2VPN en el canal en sentido descendente del CM. El CMTS DEBE codificar codificaciones separadas L2VPN de máximo nivel para cada ID L2VPN diferente. Un CMTS PUEDE añadir subtipos SA-descriptor L2VPN en mensajes a los CM no conformes, aunque serán ignorados por el CM. El CMTS DEBE describir los SAID L2VPN con un tipo de SA dinámica en una codificación SA-descriptor L2VPN.

Un CMTS NO incluye descriptores SA para todos los SAID L2VPN que asignó para un módem de registro en su respuesta inicial de autorización BPI al CM tras el registro.

Un CMTS DEBE criptar todo el tráfico retransmitido por L2VPN en sentido descendente en un SAID L2VPN asignado a la L2VPN.

El CMTS NO DEBE retransmitir tráfico L2VPN en sentido descendente a un CM hasta que dicho CM haya completado la autorización BIP y la negociación TEK para el SAID L2VPN en el que se debe criptar el tráfico.

Un CMTS de retransmisión punto a punto DEBERÍA asignar el mismo SAID L2VPN de grupo a diferentes CM en el mismo dominio MAC anexado al mismo identificador L2VPN, aunque PUEDE elegir asignar un SAID L2VPN individual único para el CM.

Un CMTS de retransmisión multipunto DEBE asignar por lo menos un SAID L2VPN de difusión a todos los CM en el mismo dominio MAC anexado al mismo identificador L2VPN. El CMTS de retransmisión multipunto DEBE retransmitir paquetes de difusión en sentido descendente de la L2VPN criptados en ese SAID L2VPN de difusión.

Un CMTS PUEDE soportar configuraciones específicas del suministrador para iniciar o detener de forma dinámica la retransmisión L2VPN a través de un CM registrado. Un CMTS que interrumpe la retransmisión L2VPN a través de un CM DEBE suprimir de forma dinámica todos los flujos de servicio en sentido ascendente que estén retransmitiendo hacia esa L2VPN, y DEBE señalar una codificación L2VPN de máximo nivel al CM que omita todos los descriptores SA para dicha L2VPN. Esto indica al CM que interrumpa la descriptación en sentido descendente para todos los SAID L2VPN asociados con la L2VPN.

7.5.2 Cómo evitar la fuga de tráfico no L2VPN

Un problema con el funcionamiento L2VPN es el tráfico de capa 2 no L2VPN en sentido descendente hacia una dirección MAC de grupo (GMAC, *group MAC*), es decir, una difusión o multidifusión de capa 2. El tráfico de difusión no L2VPN en sentido descendente incluye ARP originados en el CMTS hacia el CPE no L2VPN y avisos del encaminador CMTS para RIP o OSPF. Por defecto, *todos* los módems de cable – L2VPN y no L2VPN – retransmitirán a su interfaz CPE tráfico de difusión en sentido descendente que *no* está criptado. Es más, el tráfico GMAC no L2VPN *no* criptado hacia la misma dirección de destino Ethernet de multidifusión, utilizado por una L2VPN privada, se retransmitiría también por un CM L2VPN hacia su interfaz CPE. Si no se tiene cuidado, el tráfico GMAC no L2VPN en sentido descendente se fugará por la red CPE supuestamente privada del abonado L2VPN.

Esta Recomendación resuelve el problema de las fugas GMAC no L2VPN con el mecanismo siguiente:

- Filtrado del tráfico no criptado en sentido descendente (DUT).
- Criptación de multidifusión IP en sentido descendente (DIME, *downstream IP multicast encryption*).

7.5.2.1 Filtrado del tráfico no criptado en sentido descendente (DUT)

Un operador de cable puede evitar la fuga de tráfico no L2VPN de texto en claro a través de los CM conformes con L2VPN, permitiendo la codificación de filtrado de tráfico no criptado (DUT) en sentido descendente. Cuando se admite filtrado DUT se define una máscara de interfaz CM DUT (CMIM DUT) para limitar la retransmisión de tráfico no criptado en sentido descendente a únicamente las interfaces con un bit '1' para dicha interfaz en la CMIM. La DUT CMIM por defecto contiene solo bits '1' para las interfaces de anfitriones eCM y eSAFE, que requieren que el CM impida la retransmisión de ese tráfico hacia las interfaces CMCI en el CM. El filtrado DUT por sí solo evita la fuga GMAC no L2VPN hacia una red CPE de abonado L2VPN.

7.5.2.2 Criptación de multidifusión IP en sentido descendente (DIME)

Los CM por defecto deben habilitar la retransmisión libre de GMAC para el funcionamiento de L2VPN y en la mayoría de los CM DOCSIS 2.0 o anteriores, esto hace que todo el tráfico GMAC

no criptado se entregue al soporte lógico CM. Aunque el filtrado DUT del soporte lógico CM evita realmente que este tráfico se fugue por la interfaz CPE, si este es importante, puede afectar a las características de retransmisión del tráfico L2VPN deseado a través del CM. Es deseable permitir que los CM L2VPN utilicen sus propios filtros SAID para suprimir el tráfico GMAC no L2VPN de gran volumen.

En la mayoría de los desarrollos CMTS se espera que el tráfico de multidifusión IP sea la fuente más importante de tráfico GMAC en sentido descendente de gran volumen. Es deseable criptar este tráfico en un SAID desconocido por los CM L2VPN, de forma que sus circuitos filtren los paquetes antes de entregarlos al soporte lógico L2VPN.

Un CMTS DEBE implementar una opción configurable para habilitar o inhabilitar la criptación de multidifusión IP en sentido descendente (DIME). Con el DIME habilitado, el CMTS DEBE criptar todo el tráfico de multidifusión IP en sentido descendente no L2VPN que esté vinculado estáticamente con el BPI+ MIB o dinámicamente con las peticiones SA-MAP en sentido ascendente provenientes de un CM. El DIME no requiere que el CMTS cripte multidifusiones IP *desvinculadas* en sentido descendente no L2VPN (por ejemplo, multidifusiones RIPv2 u OSPF).

Al criptar tráfico de multidifusión IP no L2VPN vinculado en un SAID no L2VPN, el tráfico de multidifusión no L2VPN en sentido descendente de probable gran volumen debe ser filtrado por los CM DOCSIS 2.0 que implementan esta Recomendación.

Puesto que el tráfico GMAC no L2VPN está criptado en un SAID desconocido para el CM L2VPN, el CM filtra el tráfico en sentido descendente y evita su fuga hacia la red CPE privada.

7.5.2.3 Mezcla de retransmisión L2VPN y no L2VPN en el mismo CM

La característica L2VPN soporta la mezcla de retransmisiones L2VPN y no L2VPN para diferentes anfitriones CPE conectados al mismo CM. En este caso, el tráfico L2VPN y el tráfico no L2VPN por supuesto no están aislados en las redes CMCI del CM, tanto en el sentido ascendente como en el sentido descendente. Para soportar la mezcla de tráfico L2VPN y no L2VPN, el operador de cable puede configurar clasificadores L2VPN en sentido ascendente en el CM con una regla que identifique el tipo particular de tráfico que hay que retransmitir en la L2VPN (por ejemplo, tráfico con la dirección MAC de origen de un determinado CPE).

Esta Recomendación no requiere que el CM restringa la retransmisión entre anfitriones CPE L2VPN y no L2VPN cuando están conectados en diferentes puertos CMCI del CM. El modelo VLAN incorporado (eVLAN) de retransmisión CM, si está implementado en el CM, puede lograr este aislamiento (véase el apéndice III).

No se debería permitir el filtrado DUT cuando se mezclan anfitriones CPE L2VPN y no L2VPN en el mismo CM, puesto que es necesario que los CPE no L2VPN sigan recibiendo ARP en sentido descendente y difusiones DHCP. Con el filtrado DUT inhabilitado, sin embargo, todo el tráfico GMAC no criptado en sentido descendente pasará a la red mixta de CPE.

7.6 Exclusión de CM y eSAFE

Esta Recomendación utiliza el término "incluido" para indicar el tráfico retransmitido a través del retransmisor L2VPN y "excluido" para indicar cualquier otro tráfico no L2VPN.

El servicio LAN transparente de abonado requiere que se incluya todo el tráfico CPE en la retransmisión L2VPN mientras que el tráfico proveniente de los CM incorporados y de cualesquiera otros anfitriones incorporados en la misma ubicación que el CM se excluya de la retransmisión L2VPN.

La característica L2VPN se puede configurar, sin embargo, de forma que el tráfico eCM y eSAFE se pueda retransmitir en redes L2VPN separadas si así se desea.

7.6.1 Modelo de retransmisión para anfitriones CM y eSAFE

La figura 7-1 describe el modelo de retransmisión L2VPN de CMTS y de CM global para los anfitriones CM y eSAFE.

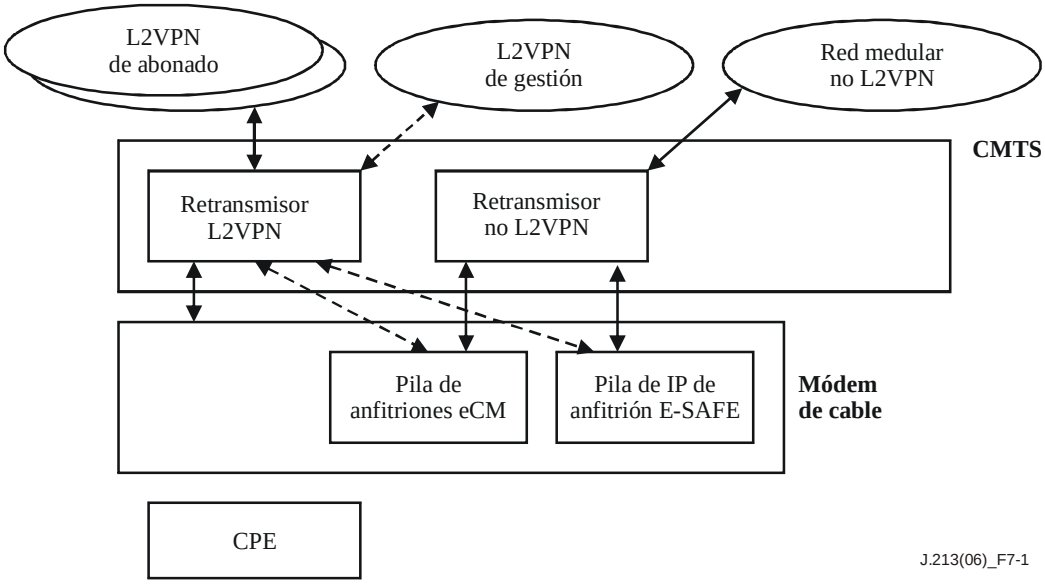

Figura 7-1 – Retransmisión de CM, eMTA y CPE

Para el servicio TLS, se excluye el tráfico hacia y desde la pila de IP de anfitrión eCM y eSAFE de la retransmisión L2VPN y se retransmite con el retransmisor no L2VPN normal del CMTS como se indica mediante la línea continua de la figura 7-1.

Con la característica L2VPN de gestión, el tráfico tras el registro del eCM se clasifica hacia un flujo de servicio de retransmisión L2VPN y se incluye para la retransmisión L2VPN (línea de puntos). Cualquier tráfico eCM anterior al registro no puede utilizar la característica L2VPN puesto que el criptado en un SAID L2VPN no es posible antes del registro.

El tráfico de gestión desde y hacia un anfitrión eSAFE puede utilizar la misma L2VPN de gestión que el eCM, o su propia L2VPN de gestión diferente, como desee.

7.6.2 Máscaras de interfaz puente MAC de módem de cable

De conformidad con el modelo de puente MAC descrito en [b-UIT-T J.126], se considera que un CM que cumpla esta Recomendación implementa un conjunto de interfaces puente MAC como se resume a continuación.

Cuadro 7-2 – Interfaces puente MAC de módem de cable

ifIndex	Descripción
(0)	(eCM: interfaz de anfitrión propia)
1	Interfaz CPE primaria, también ePS: servicios de portal incorporados J.192
2	Interfaz RF
16	eMTA: interfaz de anfitrión de adaptador de terminal de medios incorporado IPCablecom
17	eSTB-IP: Interfaz de anfitrión IP de adaptador incorporado OpenCable
18	eSTB-DSG: interfaz de pasarela DOCSIS de adaptador incorporado OpenCable

Esta Recomendación introduce el convenio de que ifIndex 0 se considera que aplica a la interfaz de anfitrión interna con la pila IP de gestión CM o su interfaz propia.

La retransmisión de capa 2 L2VPN en un CM se considera que se produce únicamente sobre una lista explícita de las anteriores interfaces puente MAC. Por ejemplo, el servicio LAN transparente implica el establecimiento de un puerto sólo entre la interfaz MAC RF (ifIndex 2) y la interfaz CPE primaria (ifIndex 1). No se permite el acceso de TLS a la interfaz propia del eCM o a cualquier otra interfaz de anfitrión eSAFE.

Para cada L2VPN retransmitida en un CM, se configura un parámetro de máscara de interfaz de CM (CMIM) con un conjunto de interfaces puente MAC que tienen autorización para retransmitir paquetes hacia y desde esa L2VPN. A cada interfaz puente MAC se le asigna una posición de bit en la máscara CMIM que corresponde a su valor ifIndex. La interfaz de anfitrión eCM tiene asignada la posición de bit cero de la CMIM.

El parámetro CMIM para una L2VPN se codifica en la misma codificación L2VPN por SF que define el VPNID L2VPN. Si el subtipo CMIM se omite de una retransmisión de codificación L2VPN, su valor por defecto es el adecuado para el servicio TLS (es decir, con un único conjunto con los bits de interfaz RF (ifIndex 2) y de interfaz CPE primaria (ifIndex 1)). El parámetro CMIM se codifica de la misma forma que las reglas de codificación básicas de un tipo de objeto BITS SNMP. En un TLV de subtipo CMIM, la máscara de bits se codifica como una cadena de octetos de longitud variable en la que la posición de bit 0 es el bit más significativo del primer octeto; la posición 1 es el siguiente bit más significativo; la posición 7 es el bit menos significativo del primer octeto y la posición de bit 8 es el bit más significativo del segundo octeto. Por ejemplo, el valor CMIM por defecto, con el conjunto de posiciones de bit 1 y 2, se puede codificar como un único octeto con el valor 0x60.

7.6.3 Exclusión de anfitrión incorporado

Cuando una máscara CMIM tiene un valor cero en una posición de interfaz puente MAC, todo el tráfico proveniente de esa interfaz se configura para ser excluido de la retransmisión L2VPN. En particular, la interfaz de anfitrión propia de eCM (posición de bit 0 de la interfaz CMIM) está excluida de las L2VPN de servicio LAN transparente. Cuando la interfaz de anfitrión propia de eCM está excluida de un subtipo CMIM para un SF en sentido ascendente de retransmisión L2VPN, el CMTS DEBE excluir de la retransmisión L2VPN en sentido ascendente todo el tráfico que contenga un MAC de origen que concuerde con la dirección MAC de anfitrión CM.

Puesto que los CM no conformes son incapaces de distinguir el tráfico L2VPN en sentido ascendente del tráfico no L2VPN, un CMTS DEBE soportar la retransmisión L2VPN y no L2VPN de tráfico en sentido ascendente desde un flujo de servicio L2VPN de retransmisión de un CM no conforme, basándose en la comprobación de la dirección MAC de origen en una máscara de interfaz CM configurada por el SF. El CMTS DEBE dirigir paquetes desde los tipos de anfitrión incluidos hacia el retransmisor L2VPN. El CMTS NO DEBE entregar tráfico proveniente de tipos de anfitrión excluidos hacia el retransmisor L2VPN.

El CMTS DEBE soportar la exclusión de la dirección MAC de CM y de por lo menos otra dirección MAC eSAFE en todos los flujos de servicio de retransmisión L2VPN, tanto desde los CM no conformes como desde los CM conformes. Los CM no conformes pueden tener como mucho una dirección MAC eSAFE verificada de esta manera. Esta Recomendación no soporta la retransmisión L2VPN desde un CM no conforme con más de un anfitrión eSAFE. Esta Recomendación soporta la retransmisión L2VPN desde los CM conformes con más de un anfitrión eSAFE únicamente configurando codificaciones de clasificación de paquetes en sentido ascendente que clasifiquen explícitamente el tráfico eSAFE de retransmisión no L2VPN hacia flujos de servicio en sentido ascendente de retransmisión no L2VPN.

7.6.4 Aprendizaje de direcciones MAC de anfitrión incorporado CMTS

Un CMTS DEBE aprender la dirección MAC de un CM incorporado a partir de una dirección MAC de origen del mensaje inicial de petición de medición de distancia del CM e incluirlo en la tabla docsDevCmCmtsStatusTable.

El CMTS utiliza dos técnicas para aprender la dirección MAC de anfitriones eSAFE:

- Para los CM conformes con L2VPN, el CMTS DEBE aprender las direcciones MAC eSAFE (véase B.1.2) de codificaciones de capacidad de anfitrión eSAFE cuando se registra el CM.
- Para los CM no conformes con L2VPN, el CMTS DEBE buscar paquetes DHCP en sentido ascendente para determinar las direcciones MAC eSAFE.

7.6.4.1 Subtipo habilitación de indagación DHCP eSAFE

El CMTS DEBE habilitar la indagación DHCP para determinar las direcciones MAC eSAFE en un CM no conforme cuando esté presente un subtipo habilitación de indagación DHCP eSAFE en cualquier codificación L2VPN por SF (véase B.3.3). El valor de la codificación es una máscara de bits que permite buscar determinados anfitriones eSAFE. El CMTS NO DEBE permitir la indagación DHCP cuando el subtipo habilitación de indagación DHCP eSAFE esté ausente de todas las codificaciones L2VPN por SF o no tenga un bit '1' para un determinado tipo de anfitrión eSAFE cuando esté presente. Esto se hace para evitar la intervención de eSAFE por CPE no autorizadas y no incorporadas.

Cuando se habilita la indagación DHCP eSAFE, el CMTS DEBE soportar la detección de un tipo de anfitrión eSAFE en una dirección MAC a partir de la subcadena inicial de la opción 60 del paquete DHCP DISCOVER de difusión proveniente del anfitrión eSAFE que está vinculado al CMTS cuando la opción 60 está presente. Cuando se habilita la indagación DHCP eSAFE, el CMTS DEBE soportar la detección del tipo anfitrión eSAFE en una dirección MAC a partir del subtipo 2 de la opción 43 de un paquete DHCP DISCOVER proveniente del anfitrión eSAFE que está vinculado al CMTS cuando está presente el subtipo 2 de la opción 43. El cuadro 7-3 proporciona los valores de estas opciones DHCP para cada tipo de anfitrión eSAFE definido actualmente.

Cuadro 7-3 – Subcadenas de indagación DGCP eSAFE

Tipo de anfitrión eSAFE	Subcadena de la opción 60 DHCP	Subcadena de la subopción 2 de la opción 43 DHCP
Adaptador de terminal de medios incorporado [b-UIT-T J.167]	pktc	EMTA
Servicios de portal incorporados [b-UIT-T J.192]	CableHome	EPS

El CMTS DEBE aprender la dirección MAC del eSAFE en el campo identificador del soporte físico del cliente del paquete DHCP DISCOVER indagado.

Una vez que el CMTS aprende las direcciones MAC de los anfitriones eSAFE, el CMTS excluye de la retransmisión L2VPN a todo el tráfico en sentido ascendente proveniente de esa dirección MAC de anfitrión DOCSIS.

7.6.5 Clasificación basada en interfaces

El dominio MAC RF implementa los clasificadores de paquetes DOCSIS en sentido ascendente que clasifican una L2PDU unida a la interfaz de dominio MAC en un flujo de servicio en sentido ascendente.

En una codificación de clasificación de paquetes en sentido ascendente el subtipo CMIM representa una regla que concuerda con el puerto puente de ingreso de la L2PDU. Esto permite a los clasificadores clasificar tráfico CPE, eCM y eSAFE de forma genérica por tipo de anfitrión, en lugar de requerir clasificadores estáticos basados en la dirección IP asignada o la dirección MAC real del anfitrión.

La capacidad de clasificación de anfitrión resulta más útil cuando se implementan las L2VPN de gestión para aislar el tráfico de gestión CM y eSAFE del tráfico de cabida útil en una red medular de capa 2. Permite a los clasificadores de CM direccionar tráfico eCM y/o eSAFE en sentido ascendente hacia un flujo de servicio en sentido ascendente de retransmisión L2VPN separado para la L2VPN de gestión.

7.7 Calidad de servicio L2VPN

7.7.1 Separación del flujo de servicio

Un aspecto importante del servicio L2VPN prestado por un operador es el aislamiento, no sólo de la retransmisión de tráfico, sino también de la calidad de servicio. Con tráfico excesivo no debería ser posible que un flujo de servicio L2VPN (o incluso un flujo de tráfico no L2VPN) afectara de forma significativa a la QoS recibida en cualesquiera otros flujos L2VPN. Por lo tanto, esta Recomendación, requiere que el tráfico en sentido descendente para cada L2VPN esté aislado entre ellas y del tráfico no L2VPN situando el tráfico en un flujo de servicio (SF, *service flow*) separado. En el caso de retransmisión en modo punto a punto, esto se produce automáticamente puesto que cada CM ya dispone de un flujo de servicio primario en sentido descendente. En el caso de retransmisión en modo multipunto, esta Recomendación requiere que cada L2VPN tenga un flujo de servicio separado para su tráfico MAC de grupo difundido en sentido descendente y para el tráfico con destino MAC individual y desconocido.

7.7.2 Prioridad de usuario IEEE 802.1

El modelo de puente de capa 2 IEEE 802.1 utiliza el concepto de prioridad de usuario con 8 valores posibles para indicar la QoS que se debe considerar cuando se retransmite una L2PDU [IEEE 802.1Q]. Este campo se utiliza para proporcionar una QoS diferenciada para cada flujo de tráfico *dentro de la misma* L2VPN.

Cuando una L2PDU se retransmite con un rótulo IEEE 802.1 en una interfaz NSI Ethernet troncal, la prioridad de usuario del paquete se codifica en los tres bits superiores de un valor de control de rótulo 802.1Q. El apéndice II proporciona detalles sobre el encapsulado IEEE 802.1Q.

Un CMTS DEBE aceptar los bits de prioridad de un rótulo 802.1Q, que delimite el servicio a la entrada del puerto NSI, como el atributo de prioridad de usuario entrante L2VPN del paquete. El CMTS DEBE mantener la prioridad de usuario del paquete en el retransmisor L2VPN (probablemente regenerándolo mediante la configuración específica del suministrador), y utilizar el valor de salida de la prioridad de usuario para que concuerde con el subtipo gama de prioridades de usuario de las codificaciones L2VPN del clasificador en sentido descendente.

En el sentido ascendente, esta Recomendación requiere que la prioridad de usuario del tráfico L2VPN en sentido ascendente se configure de forma explícita como el subtipo prioridad de usuario entrante de una codificación L2VPN de retransmisión. Requiere que el retransmisor L2VPN mantenga esa prioridad de usuario (probablemente regenerada) cuando se codifique el rótulo IEEE 802.1Q para extraerlo de un puerto NSI. Si se omite el subtipo prioridad de usuario entrante, el CMTS supone que la prioridad de usuario entrante es cero. Al requerir que la prioridad de usuario esté configurada de forma explícita en la codificación L2VPN de retransmisión, se evita que el CPE entregue paquetes L2VPN con una prioridad de usuario arbitraria en la red medular L2VPN del operador de cable.

7.7.3 Clasificación de la gama de prioridades de usuario en sentido descendente

Esta Recomendación define un subtipo gama de prioridades de usuario para una codificación L2VPN que aparece como un nuevo criterio de concordancia de reglas en una codificación de clasificador de paquetes de flujo de servicio en sentido descendente. El subtipo gama de prioridades de usuario se describe en B.3.9. Cuando un subtipo gama de prioridades de usuario está presente en una codificación de clasificador de paquetes de flujo de servicio en sentido descendente, el CMTS DEBE equiparar este clasificador sólo con paquetes retransmitidos por L2VPN con una prioridad de usuario en la gama indicada.

7.7.4 Prioridad de usuario entrante en sentido ascendente

Esta Recomendación propone que el CMTS asocie una prioridad de usuario configurada para un flujo de servicio de retransmisión L2VPN en sentido ascendente basándose en un subtipo configurado prioridad de usuario entrante de la codificación L2VPN por SF que definió el SF. El subtipo prioridad de usuario entrante se define en B.3.8.

Un CMTS PUEDE implementar configuraciones específicas del suministrador para seleccionar la prioridad de usuario entrante de paquetes L2VPN en sentido ascendente. El modelo de puente particular implementado por el CMTS (por ejemplo, [b-IEEE 802.1s] o [b-IEEE 802.1ad]) PUEDE proporcionar la regeneración de una prioridad de usuario entrante en sentido ascendente a una prioridad de usuario diferente para el paquete en el CMTS.

El CMTS NO DEBE utilizar ningún rótulo sólo de prioridad aplicado por el CPE para determinar la prioridad de usuario entrante de un paquete en sentido ascendente. Si es necesario, el CM se puede configurar para que clasifique el paquete con rótulo CPE sólo de prioridad en sentido ascendente para un flujo de servicio que esté configurado con un subtipo prioridad de usuario entrante explícito. Si el CMTS implementa un retransmisor puente IEEE 802.1ad, el CMTS PUEDE equiparar el rótulo de prioridad de usuario de cliente interno al rótulo de prioridad de usuario de servicio externo.

Hay que destacar que el parámetro prioridad de usuario de un paquete L2VPN define sólo la prioridad de la retransmisión del paquete a través de puentes de la red medular L2; no afecta a la retransmisión de paquetes en sentido ascendente o en sentido descendente en la interfaz RF DOCSIS. Sólo el conjunto de parámetros QoS del flujo de servicio en el que está clasificado el paquete define la prioridad para la retransmisión del paquete en una interfaz RF DOCSIS.

7.7.5 QoS de red medular de capa 2

En una red puenteada de una red medular L2, la prioridad de puenteo de un paquete L2VPN se puede indicar de distintas formas:

- En los bits de prioridad de usuario de un rótulo IEEE 802.1 externo.
- En los bits experimentales EXP de una etiqueta de seudohilo MPLS.
- En los bits DSCP de un encapsulado de seudohilo L2TPv3.

El CMTS DEBE transmitir un paquete en sentido ascendente L2VPN en un puerto NSI con la prioridad de usuario entrante codificada como adecuada para su encapsulado NSI. La correspondencia de la prioridad de usuario entrante con los bits EXP MPLS o los valores DSCP está fuera del ámbito de esta Recomendación.

Para el encapsulado NSI de seudohilo IETF del tráfico L2VPN, está fuera del ámbito de esta Recomendación la determinación de la prioridad de usuario entrante en sentido descendente y la codificación de la prioridad de usuario saliente en sentido ascendente en los bits EXP MPLS o en los valores DSCP L2TPv3.

7.8 Rótulos 802.1Q apilados o funcionamiento de rótulo en rótulo

La selección de una determinada L2VPN para el tráfico puente en sentido ascendente siempre viene indicada por el subtipo VPNID de la codificación L2VPN. Esta Recomendación no considera la interpretación de rótulos 802.1Q aplicados por el CPE y recibidos por el puerto Ethernet de un CM para la retransmisión en sentido ascendente. Estos rótulos se consideran no delimitadores de servicio y siempre son ignorados en la selección de L2VPN por el CMTS DOCSIS. Estos rótulos no delimitadores de servicio se retransmiten como parte de la cabida útil CPE. Los CMTS DOCSIS y CM DOCSIS conformes con esta Recomendación soportan la retransmisión de paquetes Ethernet de longitud máxima con un rótulo 802.1Q no delimitador de servicio de abonado único. Esto significa que un CM que soporte esta Recomendación es capaz de retransmitir paquetes de 1522 bytes entre sus interfaces RF y CPE y un CMTS es capaz de retransmitir paquetes de 1526 bytes por su puerto NSI Ethernet con rótulos 802.1Q.

Cuando un paquete con un rótulo no delimitador de servicio interno suministrado por el CPE se retransmite por un puerto NSI que también utiliza encapsulado IEEE 802.1Q, el CMTS añade un rótulo delimitador de servicio externo con el ID VLAN de encapsulado NSI configurado. Esto se denomina rotulado 802.1Q apilado o rótulo en rótulo. Los criterios de codificación de clasificación de paquetes IEEE 802.1P/Q de C.2.1.7 de [UIT-T J.122] aplican únicamente a rótulos 802.1Q no delimitadores de servicio suministrados por el CPE cuando el paquete aparece en la interfaz RF y no al valor del rótulo delimitador de servicio exterior al aparecer el paquete en un puerto NSI. Por ejemplo, el CM puede otorgar paquetes CPE en sentido ascendente a un flujo de servicio en particular, basándose en los bits de prioridad del rótulo aplicado por el CPE.

Para evitar abusos del CPE en las prioridades de usuario L2 de la red medular, el CMTS NO DEBE interpretar un rótulo sólo de prioridad aplicado por el CPE como si definiera la prioridad de usuario entrante en sentido ascendente de una paquete L2VPN. La prioridad de usuario de un paquete en sentido ascendente está definida únicamente por el subtipo prioridad de usuario IEEE 802.1 configurado en la codificación L2VPN de retransmisión por SF que aplica al paquete. Un rótulo sólo de prioridad aplicado por el CPE se considera un rótulo no delimitador de servicio y se apila como un rótulo interno cuando lo retransmite el CMTS. Si se desea que un rótulo de prioridad aplicada por el CPE seleccione la prioridad de usuario entrante en sentido ascendente, el CM debería estar configurado para otorgar el paquete a un flujo de servicio con un subtipo prioridad de usuario entrante explícito. Esto permite al operador de cable controlar la prioridad de los paquetes retransmitidos por L2 en la red medular.

En el sentido descendente, los criterios de codificación de clasificación de paquetes IEEE 802.1P/Q de C.2.1.7 de [UIT-T J.122] aplican únicamente a cualquier rótulo no delimitador de servicio interno en el paquete según aparece en la interfaz RF. Hay que destacar que los CMTS no precisan implementar estos criterios de capa 2 en el sentido descendente. Lo que normalmente se desea, sin embargo, es clasificar el tráfico en sentido descendente siguiendo la prioridad o el ID VLAN del rótulo delimitador de servicio exterior cuando el paquete *aparece en la interfaz NSI*. Esta Recomendación define codificaciones L2VPN de clasificador en sentido descendente para permitir la clasificación basada en el VPNID del paquete y en la prioridad de usuario como se indica en su encapsulado NSI.

7.9 Árbol abarcante y detección de bucle

[UIT-T J.122] describe el protocolo de árbol abarcante DOCSIS (DSTP, *DOCSIS spanning tree protocol*). Desgraciadamente, pocos CM implementan DSTP, de forma que este protocolo no se puede utilizar para evitar bucles puente L2VPN. Se espera que un operador configure las redes L2VPN de abonado sin bucles, o se base en el propio equipo del abonado para implementar el protocolo de árbol abarcante IEEE para abrir cualquier bucle puente en una L2VPN de abonado. Esta cláusula describe los requisitos CMTS para evitar que la L2VPN deniegue el servicio cuando un abonado configura accidentalmente o intencionadamente un bucle puente.

El CMTS DEBE retransmitir de forma transparente el protocolo de árbol abarcante IEEE (STP, *spanning tree protocol*) en la RPV de capa 2 del abonado.

Un CMTS PUEDE implementar el protocolo de árbol abarcante DOCSIS y transmitir las BPDU DSTP por todas las interfaces NSI y RF configuradas para el funcionamiento L2VPN. El CMTS DEBE transmitir paquetes con protocolo de árbol abarcante DOCSIS sin rótulo por una interfaz NSI IEEE 802.1Q y criptados en una SAID suministrado al CM L2VPN por una interfaz RF de dominio MAC CMTS. Una interfaz CMTS PUEDE implementar un SAID de árbol abarcante DOCSIS (DST) específicamente para la retransmisión DST a los puertos CPE de todos los puertos CM L2VPN.

Un CMTS DEBE impedir que un bucle puente para una L2VPN deniegue la retransmisión o difusión de tráfico en cualquier otra L2VPN sin bucle. Un CMTS PUEDE requerir la configuración de velocidades de retransmisión máximas de flujo de servicio en sentido descendente y en sentido ascendente para cumplir este requisito, siempre que estos límites no sean inferiores al 10% de la capacidad de enlace.

8 Requisitos de módem de cable

Un CM DEBE aceptar uno o más subtipos SA-descriptor L2VPN añadidos por un CMTS a cualquier codificación L2VPN de retransmisión en un mensaje REG-RSP o DSx-RSP al CM. El CM asocia los SAID de los descriptores SA en la codificación L2VPN con la única L2VPN identificada en la codificación L2VPN. El CM DEBE ser capaz de asociar cualquier número de sus SAID disponibles a una L2VPN. El CM DEBE ser capaz de asociar más de un SAID a una única L2VPN. Un CM que recibe de una codificación L2VPN con un subtipo SA-descriptor L2VPN para un SAID no establecido previamente en ese CM DEBE iniciar una transacción TEK BPKM para establecer el nuevo SAID L2VPN [UIT-T J.125]. Un CM que recibe un subtipo SA-descriptor L2VPN en un REG-RSP DEBE esperar que esté completa la autorización BPI antes de iniciar el TEK BPKM. El CM determina que se debe retransmitir un paquete en sentido descendente en una L2VPN cuando el paquete está criptado con un SAID L2VPN. Un CM DEBE sustituir el conjunto de SAID L2VPN de una L2VPN cuando reciba una codificación L2VPN de máximo nivel en un mensaje de gestión MAC que identifique esa L2VPN. El CM DEBE interrumpir la descriptación en sentido descendente de un SAID L2VPN cuando reciba en un mensaje de flujo de servicio dinámico una codificación L2VPN de máximo nivel para un ID L2VPN que omite el subtipo SA-descriptor con SAID.

Un CM DEBE retransmitir todo el tráfico destinado al MAC de grupo (GMAC) en sentido descendente que esté criptado en un SAID L2VPN señalado al CM, independientemente del destino GMAC del paquete.

El CM NO DEBE aplicar el filtrado multidifusión o las reglas de retransmisión de 5.3.1.3.1 de [UIT-T J.122] al tráfico GMAC en sentido descendente criptado en un SAID L2VPN. Un CM DEBE continuar implementando reglas de retransmisión MAC de grupo DOCSIS 2.0 para todos los paquetes descriptados y los paquetes criptados en un SAID no L2VPN.

Un CM NO DEBE implementar las reglas de retransmisión multidifusión IGMP de 5.3.1.3.1 de [UIT-T J.122] a ningún paquete en sentido ascendente (por ejemplo, informes de pertenencia IGMP) otorgado a un flujo de servicio L2VPN de retransmisión. El CM DEBE continuar implementando reglas de retransmisión multidifusión IGMP DOCSIS para informes de pertenencia IGMP en sentido ascendente no otorgados a un flujo de servicio L2VPN de retransmisión.

Un CM conforme DEBE restringir la retransmisión puente de paquetes en sentido descendente criptados en un SAID L2VPN únicamente a las interfaces puente indicadas con un bit '1' en la máscara de interfaz CM (CMIM) configurada para esa L2VPN. Por ejemplo, el CM no entrega tráfico L2VPN en sentido descendente al eCM o a ningún anfitrión interno eSAFE cuando la CMIM omite esa interfaz de anfitrión (es decir, contiene un bit '0') para esa interfaz, aunque el

paquete esté dirigido a una dirección MAC de destino individual para el anfitrión. De la misma forma, el CM no entrega tráfico destinado al MAC de grupo (GMAC) con etiqueta L2VPN a anfitriones internos cuando esa CMIM de L2VPN omite la interfaz de anfitrión interna.

Un CM DEBE soportar un criterio de regla de clasificación señalado mediante una máscara de interfaz CM (CMIM) en una codificación L2VPN de una codificación de clasificador de paquetes en sentido ascendente, si esa codificación clasifica o no a un flujo de servicio L2VPN de retransmisión. El CM DEBE considerar el criterio que ha de aplicar cuando la dirección MAC de origen de un paquete en sentido ascendente es para un tipo anfitrión con un bit '1' en la máscara de interfaz CM. El CM DEBE considerar que el criterio no concuerda y, en consecuencia, retransmitir o suprimir un paquete, cuando la dirección MAC de origen es para un tipo anfitrión con un bit '0' en la máscara de interfaz CM.

Un CM DEBE soportar el filtrado de tráfico no criptado en sentido descendente (DUT) como se describe en B.2 e indicarlo en una codificación de capacidad de filtrado DUT (véase B.1.3). Cuando se habilita el filtrado DUT un CM DEBE restringir la retransmisión puente de tráfico no encriptado en sentido descendente únicamente a las interfaces indicadas en la máscara de interfaz DUT CM (DUT CMIM) implicada o configurada por la codificación de de filtrado DUT.

Puesto que la posición de bit 1 de la CMIM (correspondiente al ifIndex 1 de puente CM) representa el *conjunto* de *todas* las interfaces CPE en la retransmisión L2VPN, del filtrado DUT y de las codificaciones de clasificador en sentido ascendente, un CM conforme que implemente más de una interfaz CPE PUEDE asignar una posición de bit CMIM entre 5 y 15 para representar su única interfaz CPE primaria. De esta forma, los valores de CMIM (y otros filtros propios de interfaces DOCSIS) pueden representar a la propia interfaz CPE primaria, independiente del conjunto de las restantes interfaces CPE. El CM DEBE seguir indicando únicamente ifIndex 1 como su interfaz CPE primaria.

Un CM DEBE retransmitir paquetes en sentido ascendente y en sentido descendente con tamaños de hasta 1522 bytes, lo que proporciona un único rótulo 802.1Q de abonado en un paquete Ethernet de máxima longitud.

Un CM DEBE indicar el subtipo capacidad L2VPN de la codificación de capacidades de módem (véase B.1.1) de su petición de registro.

Un CM con anfitriones eSAFE incorporados DEBE indicarlos al CMTS en un mensaje petición de registro con una codificación (véase B.1.2) de capacidad de anfitrión eSAFE para cada anfitrión eSAFE.

Un CM DEBE ignorar en silencio una codificación L2VPN en cualquier contexto TLV que no se mencione en esta Recomendación. Un CM DEBE ignorar en silencio cualquier subtipo de codificación L2VPN no reconocido y procesar normalmente todas las codificaciones L2VPN reconocidas.

Anexo A

Requisitos DOCS-L2VPN-MIB CMTS

Un CMTS DEBE implementar DOCS-L2VPN-MIB. Un CM no implementa DOCS-L2VPN-MIB.

A.1 Conformidad DOCS-L2VPN-MIB

Leyenda:

M	Obligatorio
NA	No aplicable
RO	Sólo lectura
RC	Lectura-creación

DOCS-L2VPN-MIB				
DocsL2vpnIdToIndexTable (Punto a punto y multipunto)				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnIdToIndexIdx	NA	NA	M	RO
docsL2vpnIndexToIdTable (Punto a punto y multipunto)				
Objeto	CM	Acceso	CMTS	Acceso
DocsL2vpnIndexToIdId	NA	NA	M	RO
docsL2vpnCmTable				
docsL2vpnCmCompliantCapability	NA	NA	M	RO
docsL2vpnCmDutFilteringCapability	NA	NA	M	RO
docsL2vpnCmDutCMIM	NA	NA	M	RO
docsL2vpnCmDhcpSnooping	NA	NA	M	RO
docsL2vpnVpnCmTable				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnVpnCmDhcpSnooping	NA	NA	M	RO
docsL2vpnVpnCmCMIM	NA	NA	M	RO
docsL2vpnVpnCmVendorSpecific	NA	NA	M	RO

DOCS-L2VPN-MIB				
docsL2vpnVpnCmStatsTable (Punto a punto y multipunto)				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnVpnCmStatsUpstreamPkts	NA	NA	M	RO
docsL2vpnVpnCmStatsUpstreamDiscards	NA	NA	M	RO
docsL2vpnVpnCmStatsDownstreamPkts	NA	NA	M	RO
docsL2vpnVpnCmStatsDownstreamDiscards	NA	NA	M	RO
docsL2vpnPortStatusTable (Punto a punto y multipunto)				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnPortStatusSAID	NA	NA	M	RO
docsL2vpnSfStatusTable (Punto a punto y multipunto)				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnSfStatusL2vpnId	NA	NA	M	RO
docsL2vpnSfStatusIngressUserPriority	NA	NA	M	RO
docsL2vpnSfStatusVendorSpecific	NA	NA	M	RO
docsL2vpnPktClassTable (Punto a punto y multipunto)				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnPktClassL2vpnId	NA	NA	M	RO
docsL2vpnPktClassUserPriRangeLow	NA	NA	M	RO
docsL2vpnPktClassUserPriRangeHigh	NA	NA	M	RO
docsL2vpnPktClassCmim	NA	NA	M	RO
docsL2vpnPktClassVendorSpecific	NA	NA	M	RO
docsL2vpnCmNsiTable (sólo punto a punto)				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnCmNsiEncapSubtype	NA	NA	M	RO
docsL2vpnCmNsiEncapValue	NA	NA	M	RO
docsL2vpnCmNsiAGI	NA	NA	M	RO
docsL2vpnCmNsiSAII	NA	NA	M	RO
docsL2vpnCmVpnCpeTable (sólo multipunto)				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnCmVpnCpeMacAddress	NA	NA	M	RO

DOCS-L2VPN-MIB				
docsL2vpnVpnCmCpeTable (sólo multipunto)				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnVpnCmCpeMacAddress	NA	NA	M	RO
docsL2vpnDot1qTpFdbExtTable (sólo multipunto)				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnDot1qTpFdbExtTransmitPkts	NA	NA	M	RO
docsL2vpnDot1qTpFdbExtReceivePkts	NA	NA	M	RO
docsL2vpnDot1qTpGroupExtTable (sólo multipunto)				
Objeto	CM	Acceso	CMTS	Acceso
docsL2vpnDot1qTpGroupExtTransmitPkts	NA	NA	M	RO
docsL2vpnDot1qTpGroupExtReceivePkts	NA	NA	M	RO

A.2 Definiciones DOCS-L2VPN-MIB

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

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

    TEXTUAL-CONVENTION,
    TruthValue,
    MacAddress              FROM SNMPv2-TC

    MODULE-COMPLIANCE,
    OBJECT-GROUP            FROM SNMPv2-CONF

    ifIndex                 FROM IF-MIB

    dot1dBasePort           FROM BRIDGE-MIB

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

    docsIfCmtsCmStatusIndex FROM DOCS-IF-MIB

    docsQosServiceFlowId,
    docsQosPktClassId       FROM DOCS-QOS-MIB

    clabProjDocsis          FROM CLAB-DEF-MIB;

docsL2vpnMIB MODULE-IDENTITY
    LAST-UPDATED  "200603280000Z"  -- March 28, 2006
    ORGANIZATION  "CableLabs"
    CONTACT-INFO
        "Postal: Cable Television Laboratories, Inc.
        858 Coal Creek Circle
        Louisville, Colorado 80027-9750
```

```
        U.S.A.
        Phone:  +1 303-661-9100
        Fax:   +1 303-661-9199
        E-mail: mibs@cablelabs.com"
    DESCRIPTION
        "MIB de gestión para dispositivos conformes con la
        Característica L2VPN DOCSIS."
    REVISION "200603280000Z"
    DESCRIPTION
        "Versión inicial."
    ::= { clabProjDocsis 8 }

----------------------------------------------------------
--
-- Convenios textuales
--
DocsL2vpnIdentifier ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "255a"
    STATUS      current
    DESCRIPTION
            "Cadena de octetos administrada externamente que identifica una
            L2VPN. Una implementación DEBE soportar una longitud de por lo menos
            16 octetos. La cadena de octetos se utiliza como un índice. Como tal,
            el CMTS considera que los objetos del tipo DocsL2vpnIdentifier
            son únicos en cada CMTS. Se anima a los MSO a que definan valores
            DocsL2vpnIdentifier como globalmente únicos."
    SYNTAX      OCTET STRING (SIZE(1..16))

DocsL2vpnIndex ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "Valor entero generado localmente por el agente para cada identificador
            administrativo DocsL2vpnIdentifier conocido. Está destinado para su uso
            como índice corto para tablas en este módulo MIB en lugar de como objeto
            del tipo DocsL2vpnIdentifier."
    SYNTAX      Unsigned32 (0..4294967295)

DocsNsiEncapSubtype ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "Número entero enumerado que define el encapsulado por
            defecto de puertos NSI de un paquete retransmitido por L2VPN.
            Una implementación CMTS DEBE soportar ieee802.1q(2).
            Un CMTS PUEDE omitir el soporte para todos los encapsulados NSI
            Que no sean ieee802.1q(2)."
    SYNTAX      INTEGER {
        other(1),
        ieee8021q(2),
        ieee8021ad(3),
        mpls(4),
        l2tpv3(5)
    }

DocsNsiEncapValue ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "Valor de encapsulado para los paquetes retransmitidos por L2VPN en
            puertos NSI. El valor de un objeto de este tipo depende del valor de
            un objeto asociado del tipo DocsEncapSubtype:

            other(1): específico del suministrador,
            ieee8021q(2): rótulo 802.1Q con un ID VLAN en los 12 bits inferiores,
            ieee8021ad(3): par de valores de 16 bits con proveedor de servicio en
            los 12 bits inferiores del primer valor de 16 bits e ID VLAN de cliente
            en los 12 bits inferiores del segundo valor de 16 bits,
            mpls(4): debe ser una cadena de longitud cero,
            l2tpv3(5): debe ser una cadena de longitud cero."

    SYNTAX      OCTET STRING

-- Lista de interfaces de módem de cable
```

```
DocsL2vpnIfList ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "Un objeto de este tipo indica un conjunto de interfaces puente
            CM MAC, codificado como sintaxis BITS con un bit ?1?
            para cada interfaz incluida en el conjunto.

            La posición de bit eCM(0) representa una interfaz conceptual con
            el MAC anfitrión 'self' interna del propio eCM. Todas las demás
            posiciones de bit K corresponden a índices de interfaz de puerto
            puente MAC CM con un valor ifIndex K.

            Un objeto BITS está codificado como una CADENA DE OCTETOS, que puede
            tener longitud cero. La posición de bit 0 se codifica en el bit más
            significativo del primer octeto, hasta la posición de bit 7 que está
            en el bit menos significativo. La posición de bit 8 se codifica en
            el bit más significativo del segundo octeto, y así sucesivamente.

            En un CM, el valor de ifIndex 1 corresponde a la interfaz CPE primaria.
            En dispositivos CableHome, esta interfaz se asigna a la interfaz de
            anfitrión de servicios de portal incorporados (ePS), que proporciona
            un portal a la interfaz CPE física primaria. En muchos contextos de
            una DocsL2VpnIfList, un '1' en la posición de bit 1 corresponde
            a 'cualesquiera' o a 'todas' las interfaces CPE cuando el CM contiene
            más de una interfaz CPE.

            El valor ifIndex 2 corresponde a la interfaz MAC RF
            docsCableMacLayer

            Los valores ifIndex 3 y 4 corresponden a las interfaces docsCableDownstream
            y docsCableUpstream respectivamente, que no son interfaces de puerto puente
            MAC separadas. Las posiciones de bit 3 y 4 no se utilizan en este tipo;
            se deben guardar e indicar como configuradas, e ignorarse en otro caso.

            Los valores 5 a 15 de ifIndex se reservan para interfaces CPE individuales
            para dispositivos que implementan más de una interfaz CPE. En estos
            dispositivos, la posición de bit 1 de DocsL2vpnIfList corresponde al
            conjunto de todas las interfaces CPE. Un CM con más de una interfaz CPE
            PUEDE asignar una posición de bit DocsL2vpnIfList entre 5 y 15 para hacer
            referencia a una única interfaz CPE primaria.

            El valor 16 de ifIndex se asigna a cualquier adaptador de terminal
            de multimedia incorporado (eMTA) como se define en IPCablecom.

            El valor 17 de ifIndex se asigna a la interfaz de anfitrión de gestión IP
            de un adaptador incorporado (eSTB). El valor 18 de ifIndex se reserva el
            tráfico de pasarela Set-top DOCSIS (DSG) entregado a una eSTB.

            Los valores de ifIndex 19 a 31 se reservan para futuras aplicaciones
            de servicio incorporadas."
    SYNTAX      BITS {
        eCm(0),
        cmci(1),
        docsCableMacLayer(2),
        docsCableDownstream(3),
        docsCableUpstream(4),
        -- 5..15 reservados para otras interfaces CPE
        eMta(16),
        eStbIp(17),
        eStbDsg(18)
        -- 19..31 reservados para otras interfaces eSAFE
    }

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

-- Emplazamiento para notificaciones
--
docsL2vpnMIBNotifications OBJECT IDENTIFIER ::= { docsL2vpnMIB 0 }

--  Ninguno definido
```

```
--
-- Objetos MIB L2VPN
--

docsL2vpnMIBObjects OBJECT IDENTIFIER ::= { docsL2vpnMIB 1 }

-----------------------------------------------------------------------
--
-- Punto a punto y punto a multipunto
--
-- Se requieren los objetos siguientes para el funcionamiento
-- punto a punto y punto a multipunto.
--

-------------------------------------------------------------
--
-- Identificador L2VPN para la tabla de correspondencias de índices L2VPN.
--
docsL2vpnIdToIndexTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnIdToIndexEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Tabla indexada por la cadena de octetos DocsL2vpnIdentifier que
            proporciona el valor docsL2vpnIdx asignado internamente por el
            agente local para ese valor DocsL2vpnIdentifier. La correspondencia
            de DocsL2vpnIdentifier con docsL2vpnIdx es 1-1. El agente debe
            ejemplificar una fila tanto en docsL2vpnIndexToIdTable como en
            docsL2vpnIdToIndexTable para cada identificador L2VPN conocido."
    ::= { docsL2vpnMIBObjects 1 }

docsL2vpnIdToIndexEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnIdToIndexEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Hace corresponder una cadena de octetos DocsL2vpnIdentifier con el valor
            docsL2vpnIdx asignado localmente por el agente local."
    INDEX { docsL2vpnId }
    ::= { docsL2vpnIdToIndexTable 1 }

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

docsL2vpnId OBJECT-TYPE
    SYNTAX      DocsL2vpnIdentifier
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Cadena de octetos configurada externamente que identifica una L2VPN."
    ::= { docsL2vpnIdToIndexEntry 1 }

docsL2vpnIdToIndexIdx OBJECT-TYPE
    SYNTAX      DocsL2vpnIndex
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Valor de índice asignado internamente para una L2VPN conocida."
    ::= { docsL2vpnIdToIndexEntry 2 }

-------------------------------------------------------------
--
-- Índice L2VPN para tablas de correspondencia de identificadores L2VPN
--
docsL2vpnIndexToIdTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnIndexToIdEntry
    MAX-ACCESS  not-accessible
```

```
    STATUS      current
    DESCRIPTION
            "Tabla indexada por el docsL2vpnIdx local del agente que proporciona
            el identificador L2VPN global. La correspondencia de docsL2vpnIdx con
            DocsL2vpnIdentifier es 1-1. El agente debe ejemplificar r una fila
            tanto en docsL2vpnIndexToIdTable como en docsL2vpnIdToIndexTable para
            cada L2VPN conocida."
    ::= { docsL2vpnMIBObjects 2 }

docsL2vpnIndexToIdEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnIndexToIdEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Proporciona el identificador L2VPN para cada índice
            L2vpn asignado localmente."
    INDEX { docsL2vpnIdx }
    ::= { docsL2vpnIndexToIdTable 1 }

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

docsL2vpnIdx OBJECT-TYPE
    SYNTAX      DocsL2vpnIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Valor de índice asignado internamente para una L2VPN conocida."
    ::= { docsL2vpnIndexToIdEntry 1 }

docsL2vpnIndexToIdId OBJECT-TYPE
    SYNTAX      DocsL2vpnIdentifier
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Cadena de octetos administrada que identifica externamente una
            L2VPN."
    ::= { docsL2vpnIndexToIdEntry 2 }

--------------------------------------------------------------------------
--
-- Tabla CM L2VPN
--  Modo punto a punto y multipunto
--
docsL2vpnCmTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnCmEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla describe información L2VPN por CM que es común
            a todas las L2VPN para el CM, independientemente del
            modo de retransmisión."
    ::= { docsL2vpnMIBObjects 3 }

docsL2vpnCmEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnCmEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "El índice de módem de cable indexa un dato de entrada que describe
            información L2VPN para un único CM que es común a todas las L2VPN
            implementadas por el CM, independientemente del modo de
            retransmisión L2VPN.

            Se crea un dato de entrada en esta tabla para cada CM que se registra
            con una codificación L2VPN de retransmisión."
    INDEX { docsIfCmtsCmStatusIndex }
    ::= { docsL2vpnCmTable 1 }
```

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

docsL2vpnCmCompliantCapability OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto indica si un CM que retransmite una L2VPN
            cumple la especificación L2VPN DOCSIS, como se indica en la
            codificación de capacidad L2VPN en el mensaje de petición
            de registro del CM.

            Si se omitiera la codificación de capacidad, este objeto debe
            indicar el valor falso(2)."
    ::= { docsL2vpnCmEntry 1 }

docsL2vpnCmDutFilteringCapability OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto indica si un CM de retransmisión L2VPN es capaz de  filtrar
            tráfico no criptado en sentido descendente (DUT), como se indica en el
            mensaje de petición de registo.
            Si se omite la codificación de capacidad, este objeto debe indicar el valor
            falso (2)."


    ::= { docsL2vpnCmEntry 2 }

docsL2vpnCmDutCMIM OBJECT-TYPE
    SYNTAX      DocsL2vpnIfList
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto indica el valor configurado en una codificación L2VPN por CM
            para la máscara de interfaz de módem de cable (CMIM) del tráfico no criptado
            en sentido descendente (DUT).

            La CMIM DUT es una cadena de bits con un '1' para cada posición de bit K
            para una interfaz CM interna o externa con ifIndex K al que el CM permite
            retransmitir DUT. Un CM capaz de filtrar DUT DEBE descartar DUT en interfaces
            con un '0' en la CMIM DUT.

            Si una codificación L2VPN de petición de registro de máximo nivel del CM
            no contiene ningún subtipo CMIM DUT, este objeto se indica con su valor
            por defecto como un '1' en la posición de bit 0 (correspondiente al propio
            anfitrión 'self' del eCM) y con un valor '1' en cada posición de bit K en la
            que exista una interfaz eSAFE en el ifIndex K. En otras palabras, el valor
            por defecto DUT CMIM incluye el eCM y todas las interfaces eSAFE.

            Este valor se indica independientemente de que el CM sea realmente capaz
            de realizar el filtrado DUT."
    ::= { docsL2vpnCmEntry 3 }

docsL2vpnCmDhcpSnooping OBJECT-TYPE
    SYNTAX      DocsL2vpnIfList
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto indica el valor del subtipo habilitación de indagación DHCP
            de una codificación L2VPN de máximo nivel.
```

```
            Tiene la sintaxis de un máscara de bits de lista de interfaz CM y representa
            a un conjunto de interfaces puente MAC CM correspondientes a anfitriones
            eSAFE para los que  el CMTS está habilitado para indagar tráfico DHCP y
            aprender la dirección MAC de anfitrión eSAFE en esa interfaz.

            Solo los bits correspondientes a direcciones  MAC de anfitrión eSAFE
            se pueden fijar en este objeto, incluido el cpe(1) para ePS y las
            interfaces eSAFE en las posiciones de bit 16 a 31."
    ::= { docsL2vpnCmEntry 4 }

--------------------------------------------------------------------
--
-- Tabla L2VPN/CM
--  Modo punto a punto y multipunto
--

docsL2vpnVpnCmTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnVpnCmEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla describe el funcionamiento de la retransmisión
            L2VPN en cada CM."
    ::= { docsL2vpnMIBObjects 4 }

docsL2vpnVpnCmEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnVpnCmEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Un dato de entrada es indexado por el ID VPN y por el índice de módem
            de cable que describe la operación de retransmisión L2VPN para una
            única L2VPN en un único CM."
    INDEX { docsL2vpnIdx, docsIfCmtsCmStatusIndex }
    ::= { docsL2vpnVpnCmTable 1 }

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

docsL2vpnVpnCmCMIM OBJECT-TYPE
    SYNTAX      DocsL2vpnIfList
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Una máscara de interfaz de módem de cable representa un conjunto
            de interfaces puente MAC en el CM. Este objeto representa la CMIM
            en una codificación L2VPN por SF de retransmisión que especifica
            un conjunto de interfaces puente MAC de CM al que está restringida
            la retransmisión L2VPN.

            Si el subtipo CMIM se omite en una codificación por SF de retransmisión,
            su valor por defecto incluye únicamente cpePrimary(1) y cableMac(2),
            que se pueden codificar mediante un único octeto con el valor 0x60."
    ::= { docsL2vpnVpnCmEntry 1 }

docsL2vpnVpnCmIndividualSAId OBJECT-TYPE
    SYNTAX      Integer32 (0..16383)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "ID de asociación de seguridad BPI+ en el que se retransmite el tráfico
            destinado a retransmisiones punto a punto a través de un CM individual.

            Si el CMTS no asigna un SAID individual para la retransmisión multipunto
            (como se recomienda), DEBE indicar este objeto como cero."
    ::= { docsL2vpnVpnCmEntry 2 }
```

```
docsL2vpnVpnCmVendorSpecific OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto codifica la concatenación de todos las codificaciones de subtipo
            específicas de suministrador que aparecieron en cualquier codificación L2VPN
            por CM de registro asociada con este dato de entrada."
    ::= { docsL2vpnVpnCmEntry 3 }

-------------------------------------------------------------------
--
-- Tabla de estadística L2VPN/CM
--  Modo punto a punto y multipunto
--
docsL2vpnVpnCmStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnVpnCmStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla contiene estadísticas para la retransmisión de paquetes hacia
            y desde un CM a cada RPV."
    ::= { docsL2vpnMIBObjects 5 }

docsL2vpnVpnCmStatsEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnVpnCmStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Un dato de entrada se indexa mediante el ID y el índice de módem de cable."
    INDEX { docsL2vpnIdx, docsIfCmtsCmStatusIndex }
    ::= { docsL2vpnVpnCmStatsTable 1 }

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

docsL2vpnVpnCmStatsUpstreamPkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Número de paquetes retransmitidos por L2VPN recibidos desde este módem
            de cable del ejemplar en esta L2VPN del ejemplar."
    ::= { docsL2vpnVpnCmStatsEntry 1 }

docsL2vpnVpnCmStatsUpstreamBytes OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Número de bytes retransmitidos por L2vpn recibidos desde este módem
            de cable del ejemplar en esta L2VPN del ejemplar."
    ::= { docsL2vpnVpnCmStatsEntry 2 }

docsL2vpnVpnCmStatsUpstreamDiscards OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Número de paquetes retransmitidos por L2 descartados de este módem
            de cable del ejemplar en esta RPV del ejemplar."
    ::= { docsL2vpnVpnCmStatsEntry 3 }
```

```
docsL2vpnVpnCmStatsDownstreamPkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Número de paquetes retransmitidos por L2 transmitidos a este módem
            de cable del ejemplar en esta RPV del ejemplar."
    ::= { docsL2vpnVpnCmStatsEntry 4 }

docsL2vpnVpnCmStatsDownstreamBytes OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Número de bytes retransmitidos por L2 transmitidos a este módem de cable
            del ejemplar en esta RPV del ejemplar."
    ::= { docsL2vpnVpnCmStatsEntry 5 }

docsL2vpnVpnCmStatsDownstreamDiscards OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Número de paquetes retransmitidos por L2 que se descartaron antes
            de que pudieran ser transmitidos a este módem de cable del ejemplar
            en esta RPV del ejemplar."
    ::= { docsL2vpnVpnCmStatsEntry 6 }

-------------------------------------------------------------------------
--
-- Tabla de estados de puerto RPV
--  (Modo punto a punto y multipunto)
--
docsL2vpnPortStatusTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnPortStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla presenta información resumida sobre el estado temporal
            de cada RPV que está funcionando en cada puerto puente."
    ::= { docsL2vpnMIBObjects 6 }

docsL2vpnPortStatusEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnPortStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Información específica para el funcionamiento de la retransmisión L2VPN
            en un determinado 'puerto puente' CMTS. Un 'puerto puente' CMTS lo
            puede definir el suministrador CMTS, pero es preferentemente un único
            dominio MAC DOCSIS."
    INDEX { dot1dBasePort, docsL2vpnIdx }
    ::= { docsL2vpnPortStatusTable 1 }

DocsL2vpnPortStatusEntry ::= SEQUENCE {
        docsL2vpnPortStatusGroupSAId   Integer32
    }

docsL2vpnPortStatusGroupSAId OBJECT-TYPE
    SYNTAX      Integer32 (0..16383)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "SAID de grupo asociado con esta RPV en un determinado dominio MAC CMTS.
            Este SAID se utiliza para criptar todo el tráfico puente difundido en
            sentido descendente, enviado a los CM en esta RPV y por este puerto puente
            de dominio MAC CMTS.

            Un valor de '0' significa que no hay SAID de grupo asociado para esta RPV
            y este puerto puente, es decir, si la L2VPN utiliza SAID individuales punto
            a punto solo para retransmisión.
```

```
            Un puerto puente que no es un dominio MAC CMTS indicará un valor '0'."
    ::= { docsL2vpnPortStatusEntry 1 }

-------------------------------------------------------------------------
--
-- Tabla de estados de flujos de servicio L2VPN
--  (Modo punto a punto y multipunto)
--
-- Esta tabla tiene una fila para cada SF en sentido ascendente con una
-- codificación L2VPN por SF.
--

docsL2vpnSfStatusTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnSfStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
           "Esta tabla muestra el estado de retransmisión L2VPN específica de SF
            para cada flujo de servicio en sentido ascendente configurado con una
            codificación L2VPN por SF.

            Los objetos que se indican en una codificación L2VPN por SF pero
            aplican a todo el CM se muestran en docsL2vpnVpnCmTable."
    ::= { docsL2vpnMIBObjects 7 }

docsL2vpnSfStatusEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnSfStatusEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Información del estado de retransmisión L2VPN específica de SF para
            cada flujo de servicio en sentido ascendente configurado con una
            codificación L2VPN por SF. El ifIndex es del tipo docsCableMacLayer(127)."
    INDEX { ifIndex, docsQosServiceFlowId }
    ::= { docsL2vpnSfStatusTable 1 }

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

docsL2vpnSfStatusL2vpnId OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto representa el valor del subtipo identificador L2VPN
            de una codificación L2VPN por SF."
    ::= { docsL2vpnSfStatusEntry 1 }

docsL2vpnSfStatusIngressUserPriority OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto proporciona el subtipo prioridad de usuario entrante configurado
            de una codificación L2VPN por SF para este CM. Si el subtipo se omitiera,
            el valor de este objeto sería cero."
    ::= { docsL2vpnSfStatusEntry 2 }

docsL2vpnSfStatusVendorSpecific OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto proporciona el conjunto de subtipos específicos de suministrador
            configurados en una codificación L2VPN por SF para un CM. Si no se
            especificara ningún subtipo específico de suministrador, este objeto sería
            una cadena de octetos de longitud cero. Si se especifica uno o más parámetros
```

```
            de subtipo específicos del suministrador, este objeto representa la
            concatenación de todos estos subtipos."
    ::= { docsL2vpnSfStatusEntry 3 }

-------------------------------------------------------------------
--
-- Tabla de clasificador L2VPN
--  (Modo punto a punto y multipunto)
--

docsL2vpnPktClassTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnPktClassEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla proporciona los objetos específicos de L2VPN para clasificadores
            de paquetes que aplican sólo a tráfico L2VPN. Los índices de esta tabla son
            un subconjunto de los índices de clasificadores en docsQosPktClassTable."
    ::= { docsL2vpnMIBObjects 8 }

docsL2vpnPktClassEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnPktClassEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Un dato de entrada en esta tabla amplia una única fila
            de docsQosPktClassTable para una regla que aplica únicamente a
            paquetes retransmitidos por L2VPN en sentido descendente.
            El índice ifIndex es un ifType de docsCableMaclayer(127)."
    INDEX {
        ifIndex,
        docsQosServiceFlowId,
        docsQosPktClassId
    }
    ::= { docsL2vpnPktClassTable 1 }

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

docsL2vpnPktClassL2vpnId OBJECT-TYPE
    SYNTAX      DocsL2vpnIdentifier
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Índice L2VPN asignado localmente correspondiente al subtipo
            identificador RPV de una codificación L2VPN de clasificador
            en sentido descendente."
    ::= { docsL2vpnPktClassEntry 1 }

docsL2vpnPktClassUserPriRangeLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Prioridad más baja del subtipo gama de prioridades de usuario
            de una codificación L2VPN de clasificador en sentido descendente.
            Si se omitiera el subtipo, este objeto tendría el valor 0."
    ::= { docsL2vpnPktClassEntry 2 }

docsL2vpnPktClassUserPriRangeHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Mayor prioridad del subtipo gama de prioridades de usuario
            de una codificación L2VPN de clasificador en sentido descendente.
```

```
            Si se omitiera el subtipo, este objeto tendría el valor 7."
    ::= { docsL2vpnPktClassEntry 3 }

docsL2vpnPktClassCMIM OBJECT-TYPE
    SYNTAX      DocsL2vpnIfList
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Máscara de interfaz de módem de cable (CMIM) indicada en una
            codificación de clasificador de paquetes. En una codificación
            de clasificador de paquetes en sentido descendente, un valor CMIM
            especificado restringe al clasificador la equiparación de paquetes con una
            dirección MAC de destino correspondiente a las interfaces indicadas
            en la máscara CMIM. El propio eCM y cualesquiera bits de interfaz eSAFE
            corresponden a direcciones MAC de anfitrión eCM y eSAFE individuales.

            En una codificación de clasificador de paquetes en sentido ascendente,
            un valor CMIM especificado restringe al clasificador la equiparación
            de paquetes con una interfaz de puerto puente entrante que corresponda
            a los bits en el valor CMIM.

            Si se omite el subtipo CMIM, este objeto debería indicarse como
            una cadena de octetos de longitud cero."
    ::= { docsL2vpnPktClassEntry 4 }

docsL2vpnPktClassVendorSpecific OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto proporciona un conjunto de subtipos específicos
            del suministrador configurados en una codificación de clasificador
            de paquetes para un CM. Si no se especifica ningún subtipo específico
            de suministrador, este objeto es una cadena de octetos de longitud cero.
            Si se especifican uno o más parámetros del subtipo específico de
            suministrador, este objeto representa la concatenación de todo este tipo
            de subtipos."
    ::= { docsL2vpnPktClassEntry 5 }

--------------------------------------------------------------------------
--
-- Tabla NSI CM L2VPN
--  Sólo punto a punto
--
docsL2vpnCmNsiTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnCmNsiEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla describe la configuración NSI para un único
            CM cuando funciona en el modo de retransmisión punto a punto para una
            L2VPN."
    ::= { docsL2vpnMIBObjects 9 }

docsL2vpnCmNsiEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnCmNsiEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Dato de entrada indexado por el ID RPV y el índice de módem de cable que
            describe la retransmisión punto a punto entre un único encapsulado
            NSI y un único CM. Esta tabla se implementa únicamente para un
            CM que retransmita una L2VPN punto a punto. Está asociada con una
            única codificación L2VPN por CM."
    INDEX { docsL2vpnIdx, docsIfCmtsCmStatusIndex }
    ::= { docsL2vpnCmNsiTable 1 }

DocsL2vpnCmNsiEntry ::= SEQUENCE {
        docsL2vpnCmNsiEncapSubtype        DocsNsiEncapSubtype,
        docsL2vpnCmNsiEncapValue          DocsNsiEncapValue,
        docsL2vpnCmNsiAGI                 OCTET STRING,
```

```
        docsL2vpnCmNsiSAII                OCTET STRING,
        docsL2vpnCmNsiTAII                OCTET STRING
    }

docsL2vpnCmNsiEncapSubtype OBJECT-TYPE
    SYNTAX      DocsNsiEncapSubtype
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Subtipo información de encapsulado general (GEI) del encapsulado
            de interfaz de sistema de red (NSI) configurado para el
            CM."
    ::= { docsL2vpnCmNsiEntry 1 }

docsL2vpnCmNsiEncapValue OBJECT-TYPE
    SYNTAX      DocsNsiEncapValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Valor de encapsulado para los paquetes retransmitidos por L2VPN
            en puertos NSI."
    ::= { docsL2vpnCmNsiEntry 2 }

docsL2vpnCmNsiAGI OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto es la configuración de cualquier subtipo identificador
            de grupo de anexión en la codificación L2VPN por SF representada
            por esta fila. Si el subtipo se omite, el valor de este objeto
            es una cadena de longitud cero."
   ::= { docsL2vpnCmNsiEntry 3 }

docsL2vpnCmNsiSAII OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto es la configuración de cualquier subtipo ID individual de
            anexión de origen en la codificación L2VPN representada por esta fila.
            Si el subtipo se omite, el valor de este objeto es una cadena de
            longitud cero."
    ::= { docsL2vpnCmNsiEntry 4 }

docsL2vpnCmNsiTAII OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Este objeto es la configuración de cualquier subtipo ID individual
            de anexión de objetivo en la codificación L2VPN representada por esta fila.
            Si el subtipo se omite, el valor de este objeto es una cadena de
            longitud cero."
    ::= { docsL2vpnCmNsiEntry 5 }

-------------------------------------------------------------------------
--
-- Sólo punto a multipunto
--
-- Los siguientes objetos sólo se requieren para el funcionamiento
-- punto a multipunto.
--
-------------------------------------------------------------------------
--
-- Tabla módem de cable/Vpn/CPE
--  (Sólo punto a multipunto)
--
```

```
docsL2vpnCmVpnCpeTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnCmVpnCpeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla es una lista de CPE, indexados mediante las RPV en un módem
            de cable."
    ::= { docsL2vpnMIBObjects 10 }

docsL2vpnCmVpnCpeEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnCmVpnCpeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla es una lista de CPE, indexados mediante las RPV en un módem
            de cable."
    INDEX { docsIfCmtsCmStatusIndex,
        docsL2vpnIdx,
        docsL2vpnCmVpnCpeMacAddress }
    ::= { docsL2vpnCmVpnCpeTable 1 }

DocsL2vpnCmVpnCpeEntry ::= SEQUENCE {
        docsL2vpnCmVpnCpeMacAddress   MacAddress
    }

docsL2vpnCmVpnCpeMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Dirección Mac de equipo en las instalaciones del cliente (CPE) que se
            anexa a este módem de cable de ejemplares y sirve de puente a este Id RPV
            de ejemplar."
    ::= { docsL2vpnCmVpnCpeEntry 1 }

--------------------------------------------------------------------
--
-- Tabla RPV/Módem de Cable/CPE Table
--  (Sólo punto a multipunto)
--
docsL2vpnVpnCmCpeTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnVpnCmCpeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla contiene una lista de CPE puente, indexados mediante el
            índice L2VPN y los correspondientes CM en esa RPV."
    ::= { docsL2vpnMIBObjects 11 }

docsL2vpnVpnCmCpeEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnVpnCmCpeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla contiene una lista de CPE puente, indexados mediante el
            índice RPV y los correspondientes CM en esa RPV."
    INDEX  { docsL2vpnIdx,
        docsIfCmtsCmStatusIndex,
        docsL2vpnVpnCmCpeMacAddress }
    ::= { docsL2vpnVpnCmCpeTable 1 }

DocsL2vpnVpnCmCpeEntry ::= SEQUENCE {
        docsL2vpnVpnCmCpeMacAddress   MacAddress
    }

docsL2vpnVpnCmCpeMacAddress OBJECT-TYPE
    SYNTAX      MacAddress
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "Dirección Mac de equipo en las instalaciones del cliente (CPE) que se anexa
            a este módem de cable de ejemplares y sirve de puente a este índice L2vpn
            de ejemplar."
    ::= { docsL2vpnVpnCmCpeEntry 1 }

-------------------------------------------------------------------
--
-- dot1qTpFdbTable Extension
--  (Point-to-Multipoint only)
--
docsL2vpnDot1qTpFdbExtTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnDot1qTpFdbExtEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla contiene contadores de paquetes para direcciones MAC
            de unidifusión en una RPV."
    ::= { docsL2vpnMIBObjects 12 }

docsL2vpnDot1qTpFdbExtEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnDot1qTpFdbExtEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Este cuadro amplía dot1qTpFdbTable sólo para datos de entrada de puerto
            puente de red RF. Está implementada mediante un agente sólo si el agente
            implementa dot1qTpFdbTable para puertos puente de red RF."
    INDEX { dot1qFdbId, dot1qTpFdbAddress }
    ::= { docsL2vpnDot1qTpFdbExtTable 1 }

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

docsL2vpnDot1qTpFdbExtTransmitPkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Número de paquetes en el que la dirección MAC de destino concordaba con
            este ejemplar dot1qTpFdbAddress y el paquete estaba puenteado en una RPV,
            en la que el ID RPV concuerda con este dot1qFdbId de ejemplar."
    ::= { docsL2vpnDot1qTpFdbExtEntry 1 }

docsL2vpnDot1qTpFdbExtReceivePkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Número de paquetes en el que la dirección MAC de origen concordaba con
            este ejemplar dot1qTpFdbAddress y el paquete estaba puenteado en una RPV,
            en la que docsL2vpnIdx concordaba con este dot1qFdbId de ejemplar."
    ::= { docsL2vpnDot1qTpFdbExtEntry 2 }

-------------------------------------------------------------------
--
-- Ampliación de dot1qTpGroupTable
--  (Sólo punto a multipunto)
--
docsL2vpnDot1qTpGroupExtTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnDot1qTpGroupExtEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla contiene contadores de paquetes para direcciones MAC
            de multidifusión en una RPV."
    ::= { docsL2vpnMIBObjects 13 }
```

```
docsL2vpnDot1qTpGroupExtEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnDot1qTpGroupExtEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Esta tabla amplía dot1qTpGroupTable sólo para datos de entrada de puerto
            puente de red RF.  La implementa un agente sólo cuando el agente implementa
            dot1qTpGroupTable para puertos puente de red RF."
    INDEX { dot1qVlanIndex, dot1qTpGroupAddress }
    ::= { docsL2vpnDot1qTpGroupExtTable 1 }

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

docsL2vpnDot1qTpGroupExtTransmitPkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Número de paquetes en el que la dirección MAC de destino concuerda
            con esta dot1qTpGroupAddress de ejemplar y el paquete estaba puenteado
            en una RPV, en la que docsL2vpnIdx concordaba con este dot1qVlanIndex
            de ejemplar."
    ::= { docsL2vpnDot1qTpGroupExtEntry 1 }

docsL2vpnDot1qTpGroupExtReceivePkts OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Número de paquetes en el que la dirección MAC de origen concordaba con
            esta dot1qTpGroupAddress de ejemplar y el paquete estaba puenteado en
            una RPV, en la que docsL2vpnIdx concordaba con este dot1qVlanIndex
            de ejemplar."
    ::= { docsL2vpnDot1qTpGroupExtEntry 2 }

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

--
-- Definiciones de conformidad
--
docsL2vpnConformance  OBJECT IDENTIFIER ::= { docsL2vpnMIB 2 }
docsL2vpnCompliances  OBJECT IDENTIFIER ::= { docsL2vpnConformance 1 }
docsL2vpnGroups       OBJECT IDENTIFIER ::= { docsL2vpnConformance 2 }

docsL2vpnCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "Declaración de conformidad para sistemas de terminación de
            módem de cable que implementan la característica L2VPN DOCSIS."

    MODULE    -- docsL2vpn
      -- Grupos obligatorios condicionados
    GROUP docsL2vpnBaseGroup
    DESCRIPTION
            "Obligatorio en todos los CMTS."

    GROUP docsL2vpnPointToPointGroup
    DESCRIPTION
            "Obligatorio en todos los CMTS que implementan la retransmisión L2VPN
            punto a punto."

    GROUP docsL2vpnMultipointGroup
    DESCRIPTION
            "Obligatorio en todos los CMTS que implementan el modo de retransmisión
            L2VPN multipunto para cualquier L2VPN."

    ::= { docsL2vpnCompliances 1 }
```

```
docsL2vpnBaseGroup OBJECT-GROUP
    OBJECTS {
        docsL2vpnIdToIndexIdx,
        docsL2vpnIndexToIdId,

        docsL2vpnCmCompliantCapability,
        docsL2vpnCmDutFilteringCapability,
        docsL2vpnCmDutCMIM,
        docsL2vpnCmDhcpSnooping,

        docsL2vpnVpnCmCMIM,
        docsL2vpnVpnCmVendorSpecific,
        docsL2vpnVpnCmIndividualSAId,

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

        docsL2vpnPortStatusGroupSAId,

        docsL2vpnSfStatusL2vpnId,
        docsL2vpnSfStatusIngressUserPriority,
        docsL2vpnSfStatusVendorSpecific,

        docsL2vpnPktClassL2vpnId,
        docsL2vpnPktClassUserPriRangeLow,
        docsL2vpnPktClassUserPriRangeHigh,
        docsL2vpnPktClassCMIM,
        docsL2vpnPktClassVendorSpecific
    }
    STATUS      current
    DESCRIPTION
            "Colección de objetos común tanto para la retransmisión
            L2VPN punto a punto como multipunto."
    ::= { docsL2vpnGroups 1 }

docsL2vpnPointToPointGroup OBJECT-GROUP
    OBJECTS {
        docsL2vpnCmNsiEncapSubtype,
        docsL2vpnCmNsiEncapValue,
        docsL2vpnCmNsiAGI,
        docsL2vpnCmNsiSAII,
        docsL2vpnCmNsiTAII
    }
    STATUS      current
    DESCRIPTION
            "Colección de objetos común para cualquier modo
            de retransmisión punto a punto."
    ::= { docsL2vpnGroups 2 }

docsL2vpnMultipointGroup OBJECT-GROUP
    OBJECTS {
        docsL2vpnCmVpnCpeMacAddress,

        docsL2vpnVpnCmCpeMacAddress,

        docsL2vpnDot1qTpFdbExtTransmitPkts,
        docsL2vpnDot1qTpFdbExtReceivePkts,

        docsL2vpnDot1qTpGroupExtTransmitPkts,
        docsL2vpnDot1qTpGroupExtReceivePkts
    }
    STATUS      current
    DESCRIPTION
            "Colección de objetos necesaria sólo para el modo de
            retransmisión multipunto."
    ::= { docsL2vpnGroups 3 }
END
```

Anexo B

Codificaciones de parámetros

B.1 Capacidades

B.1.1 Capacidad L2VPN

Esta capacidad indica si el CM cumple los requisitos de red privada virtual de capa 2 para un CM especificado en la cláusula 8. El funcionamiento L2VPN se puede seguir realizando con los CM que no implementan estos requisitos, aunque con posibles limitaciones.

Tipo	Longitud	Valor
5.17	1	0 CM no conforme con la cláusula 8 de L2VPN DOCSIS (por defecto) 1 CM conforme con la cláusula 8 de L2VPN DOCSIS

B.1.2 Capacidad de anfitrión de entidad funcional de aplicación/servicio incorporado (eSAFE)

Esta codificación de capacidad indica al CMTS el tipo y la dirección MAC de un anfitrión eSAFE incorporado en el CM. Esto es necesario para que el CMTS garantice una retransmisión adecuada IPv4 e IPv6 (futura) del tráfico en sentido ascendente desde un anfitrión eSAFE. Se requiere una codificación de capacidad de anfitrión eSAFE separada para cada anfitrión eSAFE incorporado en el CM.

Tipo	Longitud	Valor
5.18	7	ifIndex eSAFE (1 byte), dirección MAC eSAFE (6 bytes) ifIndex eSAFE: 1 ePS 15 eMTA 17 eSTB-IP 18 eSTB-DSG

B.1.3 Filtrado de tráfico no criptado en sentido descendente

Esta capacidad indica si el CM soporta la característica de filtrado DUT descrita en 7.5.2.1.

Tipo	Longitud	Valor
5.19	1	0 Filtrado DUT no soportado (por defecto) 1 Filtrado DUT soportado

B.2 Codificación de filtrado de tráfico no criptado en sentido descendente (DUT)

El parámetro filtrado DUT se destina a los CM que implementan redes privadas virtuales de capa 2 o de capa 3. En estas redes, el tráfico en sentido descendente destinado a la red privada siempre se cripta mediante BPI. Aunque las señales RF en sentido descendente se difunden a todos los CM, sin embargo, el tráfico MAC de grupo no criptado destinado a *otros* CM se fugará por puertos CMCI de CM VPN a menos que se filtre en el CM VPN. Este parámetro permite a los CM RPV filtrar todo el tráfico no criptado en sentido descendente, tanto para destinos MAC individuales como de grupo.

Codificación TLV de máximo nivel para filtrado DUT:

Tipo	Longitud	Valor
45	1..N	Byte 1 (Control DUT) Bit 0 = 0: Inhabilita el filtrado DUT (por defecto) Bit 0 = 1: Habilita el filtrado DUT Bits 1..7: Reservados Bytes 2..N (CMIM DUT, opcional) Máscara de interfaz de CM (CMIM) que limita las interfaces de salida del tráfico DUT. Si se omite la CMIM DUT su valor por defecto incluye el eCM y todas las interfaces eSAFE implementadas, pero ninguna interfaz CPE.

Si se omite la codificación de filtrado DUT, o el valor del byte de control de codificación de filtrado es cero, entonces el CM puentea el tráfico no criptado en sentido descendente, recibido desde su interfaz RF (ifIndex 2), de conformidad con las especificaciones DOCSIS correspondientes, es decir, retransmitiendo el tráfico MAC unidifundido al puerto puente interno (eCM/eSAFE) o externo (CPE) desde el cuál se conoció o se configuró el MAC de origen y retransmitiendo el tráfico MAC de grupo (GMAC) obtenido de IGMP o configurado a todos los demás puertos puente internos y externos.

Si está presente la codificación de filtrado DUT y está fijado el bit de habilitación del filtrado DUT, el CM DEBE restringir la retransmisión del tráfico no criptado en sentido descendente (para los destinos MAC individuales y de grupo) a sólo el conjunto de interfaces indicado en una máscara de interfaz de CM DUT (CMIM DUT) configurada o implícita en la codificación. Una CMIM DUT explícita sigue al byte de control DUT y tiene el formato definido en B.3.4. Hay que destacar que las posiciones de bit de la CMIM, al ser una cadena BITS, están numeradas de izquierda (bit más significativo) a derecha (bit menos significativo) en la secuencia de octetos que representa la cadena BITS.

Si al byte de control DUT no le sigue ningún otro byte (es decir, la codificación de filtrado DUT tiene una longitud de un solo byte), la CMIM DUT incluye el eCM (posición de bit 0 de la CMIM) y todas las interfaces eSAFE implementadas en el CM (posiciones de bit de la CMIM 16 y superiores) pero excluye todas las interfaces CPE. Esta CMIM DUT implícita permite a un operador de cable configurar una codificación de filtrado DUT que sea genérica para todos los tipos de dispositivos CM que ofrecen un servicio LAN transparente.

B.3 Codificación L2VPN

El parámetro codificación L2VPN es una codificación multipartita que configura cómo establece el CMTS el puente de red privada virtual de capa 2 para paquetes CPE. El funcionamiento L2VPN se especifica en la cláusula 7.

Una codificación L2VPN se denomina codificación L2VPN por SF cuando aparece como un subtipo de una codificación de flujo de servicio (tipo 24) en sentido ascendente. La codificación es una codificación L2VPN de clasificador en sentido descendente cuando aparece en una fijación de configuración de clasificación de paquetes en sentido descendente (tipo 23). Se denomina codificación L2VPN de clasificador en sentido ascendente cuando aparece en una fijación de configuración de clasificación de paquetes en sentido ascendente (tipo 22).

Una codificación L2VPN de retransmisión es aquella que contiene un subtipo VPNID L2VPN que configura la retransmisión de paquetes en una determinada L2VPN.

La codificación L2VPN se codifica como información de ampliación general (GEI) (véase C.1.1.17 de [UIT-T J.122]) como una codificación específica del suministrador con un ID de suministrador 0xFFFFFF. El subtipo 5 GEI se asigna a codificaciones L2VPN.

GEI encapsulado Codificación L2VPN:

Tipo	Longitud	Valor
43.5	n	Tupla subtipo/longitud/valor L2VPN

La propia codificación L2VPN contiene una o más codificaciones de subtipo L2VPN.

B.3.1 Identificador RPV

La codificación del subtipo identificador RPV (VPNID) es un identificador de cadenas de octetos opaco que asocia un circuito de anexión (es decir, un CM o un SF de un CM) o un clasificador en sentido descendente a una determinada red privada virtual de capa 2. Los valores de VPNID se configuran preferentemente como cadenas ASCII imprimibles. Los valores VPNID son únicos en un único CMTS. Los valores VPNID se configuran preferentemente como únicos en *todos* los CMTS dentro de un dominio administrativo del operador de cable que explota el CMTS. Los valores VPNID se pueden configurar para que sean *globalmente* únicos para facilitar la retransmisión L2VPN entre dominios.

Para que sean comparables, un operador de cable puede configurar cadenas VPNID para que se correspondan de forma algorítmica con cadenas de octetos binarios globalmente únicas. Al ser cadenas de octetos binarios globalmente únicas para las RPV, incluyen el formato VPNID de 7 bytes descrito en [b-IETF RFC 2685] y el discriminador de encaminamiento de 8 bytes descrito en [b-IETF RFC 2547]. En codificaciones L2VPN de retransmisión válidas está presente un único subtipo VPNID.

En general, múltiples circuitos de anexión (es decir, CM/SF) pueden estar conectados a la misma L2VPN y estarían así configurados con el mismo valor de subtipo VPNID. Si el CMTS realiza sólo retransmisión L2VPN punto a punto para la L2VPN indicada hacia un puerto NSI, es obligatorio que la codificación L2VPN también incluya un subtipo de encapsulado NSI.

Un CMTS que realiza retransmisiones L2VPN multipunto DEBE realizar retransmisiones de capa 2 de aprendizaje transparente entre puertos puente 802.1Q, módems de cable y flujos de servicio configurados con el mismo VPNID.

En codificaciones L2VPN por SF, el VPNID identifica la L2VPN en la que se retransmitirá el tráfico en sentido ascendente. En codificaciones L2VPN de clasificador en sentido descendente en una fijación de clasificación de paquetes en sentido descendente, el VPNID configura el clasificador para que aplique sólo a tráfico en sentido descendente retransmitido por la L2VPN en la L2VPN identificada mediante el VPNID.

Un CMTS DEBERÍA utilizar el valor del VPNID con cualesquiera protocolos de señalización que determinen de forma dinámica los valores del campo de multiplexación de servicio en paquetes L2VPN encapsulados en un puerto NSI. El VPNID se destina para ser (o para corresponder con) el identificador de grupo de gestión (AGI) para los protocolos de señalización de grupo de la L2VPN IETF.

El CMTS DEBE soportar la configuración de valores VPNID de por lo menos 16 octetos y de no más de 255 octetos. El número de valores VPNID únicos soportados por el CMTS depende del suministrador.

Subtipo	Longitud	Valor
43.5.1	1..N	Cadena de octetos opaca que identifica una red privada virtual de capa 2. N depende del suministrador, pero debe estar entre 16 y 255.

B.3.2 Subtipo encapsulado NSI

Como mínimo, se requiere que este subtipo especifique cómo el CMTS encapsula paquetes retransmitidos por la L2VPN punto a punto en un único puerto NSI Ethernet seleccionado, principalmente para pruebas de certificación de las características L2VPN. Se pretende, sin embargo, normalizar también la configuración de operador de cable de la emulación de seudohilos IETF [b-IETF RFC 3985] de cada circuito de anexión de cable (CM o SF) en la red principal NSI.

En el modo Ethernet seleccionado, el CMTS está configurado para retransmitir todo el tráfico L2VPN a través de un único puerto NSI Ethernet en todo momento. Cuando se identifica un puerto Ethernet seleccionado, el CMTS DEBE aceptar el código del formato de encapsulado NSI IEEE 802.1Q en codificaciones L2VPN de retransmisión y PUEDE aceptar los demás códigos.

Aunque el subtipo encapsulado NSI está destinado principalmente para modos de retransmisión punto a punto, el CMTS PUEDE aceptarlo en el modo multipunto (incluido en el modo Ethernet seleccionado). En este caso, el CMTS DEBE imponer que las codificaciones L2VPN con el mismo subtipo identificador RPV, que incluyan un subtipo encapsulado NSI, tengan todas el mismo valor de codificación del subtipo encapsulado NSI.

El valor del subtipo encapsulado NSI es una única tupla código de formato-longitud-valor que identifica un código de formato de encapsulado NSI y probablemente, un valor de multiplexado de servicio de encapsulado NSI.

Subtipo	Longitud	Valor
43.5.2	n	Una única tupla código de formato/longitud/valor de encapsulado NSI

Si el subtipo encapsulado NSI o un subtipo específico del suministrador L2VPN no configuran de forma estática un valor de multiplexación de servicio, el CMTS DEBE de forma dinámica seleccionar y aprender el valor de multiplexación de servicio para una codificación L2VPN de retransmisión en los pares de L2VPN del CMTS a través de la interfaz NSI. Los valores de multiplexación de servicio obtenidos de forma dinámica pueden ser diferentes en diferentes puertos NSI.

Código de formato de encapsulado NSI	Longitud	Valor de multiplexación de servicio
43.5.2.1	0	*Other*: El formato de encapsulado NIS L2VPN es distinto de los especificados a continuación. En este caso, las codificaciones de subtipo específicas del suministrador L2VPN (subtipo 5.43 de GEI) DEBEN proporcionar el formato de encapsulado NSI y cualesquiera valores deseados de multiplexación de servicio estáticos.
43.5.2.2	2	*IEEE 802.1Q*. El valor es el rótulo IEEE 802.1Q de 16 bits (con el byte más significativo en primer lugar) que incluye, en sus 12 bits menos significativos, un ID VLAN utilizado para reconocer paquetes para la L2VPN en el puerto NSI Ethernet seleccionado. Los 4 bits más significativos del valor de rótulo de 16 bits están reservados. El CMTS DEBERÍA ignorar los 4 bits más significativos del valor de rótulo IEEE 802.1Q del encapsulado NSI de 16 bits. El número máximo de valores ID VLAN únicos aceptado por un CMTS depende del suministrador. Un CMTS DEBE aceptar toda la gama de valores ID VLAN de 12 bits para los valores únicos que acepta.

Código de formato de encapsulado NSI	Longitud	Valor de multiplexación de servicio
43.5.2.3	4	*IEEE 802.1ad*. El valor es un par de valores de 16 bits (con el byte más significativo en primer lugar) en el que el primer campo de 16 bits incluye un ID VLAN de proveedor de servicio en los 12 bits menos significativos y el segundo campo de 16 bits incluye el ID VLAN de cliente en los 12 bits menos significativos. Los 4 bits más significativos de cada valor de 16 bits están reservados. El número máximo de valores ID VLAN de proveedor de servicio y de cliente que acepta el CMTS depende del suministrador, pero el CMTS DEBE aceptar toda la gama de valores ID VLAN de 12 bits.
43.5.2.4	5 ó 17	*MPLS Peer*. El valor es un InetAddressTypeCode (ipv4(1) o ipv6(2)) de 1 byte seguido por una InetAddress IPv4 o IPv6. El tráfico L2VPN del circuito de anexión se destina para retransmitir por un trayecto conmutado de etiqueta MPLS hacia el par. El CMTS DEBERÍA de forma dinámica seleccionar y aprender la pila de etiquetas para las pilas de etiquetas entrantes y salientes, respectivamente. El CMTS PUEDE utilizar subtipos L2VPN específicos de suministrador para configurar de forma estática las pilas de etiquetas entrantes y salientes. El CMTS PUEDE limitar de forma estática los valores de etiqueta MPLS configurados a una gama definida por el suministrador.
43.5.2.5	5 ó 17	*L2TPv3 Peer*. El valor es un InetAddressTypeCode (ipv4(1) o ipv6(2)) de un byte seguido por una InetAddress IPv4 o IPv6. El tráfico L2VPN del circuito de anexión se destina para la retransmisión por un túnel L2TPv3 hacia el par considerado. El CMTS DEBERÍA de forma dinámica seleccionar y aprender los ID de sesión local y distante para cada túnel. El CMTS PUEDE utilizar subtipos L2VPN específicos de suministrador para configurar de forma estática los ID de sesión, las direcciones de red par L2TPv3 y la información requerida por el suministrador. El CMTS PUEDE limitar de forma estática los valores de ID de sesión u otros valores de multiplexión de servicio configurados a una gama determinada por el suministrador.

B.3.3 Indagación DHCP eSAFE

Este parámetro se define únicamente en una codificación L2VPN de retransmisión por SF. El parámetro es una máscara de bits con las posiciones de los bits definidas para cada posible tipo de anfitrión eSAFE. Un '1' en la posición de bit del tipo anfitrión eSAFE permite al CMTS detectar automáticamente la dirección MAC de dicho anfitrión eSAFE analizando el tráfico DHCP retransmitido entre el CM y un servidor DHCP. Las posiciones de los bits en el parámetro indagación DHCP eSAFE concuerdan con los de la máscara de interfaz CM (CMIM) para la interfaz asociada con el tipo anfitrión eSAFE.

Subtipo	Longitud	Valor
43.5.3	1..N	Máscara de bits de los anfitriones de eSAFE habilitados para indagación DHCP Bit 1 (0x40 00 00): Servicios de portal incorporados (ePS) Bit 16 (0x00 00 80): IPCablecom-EMTA Bit 17 (0x00 00 40): eSTB-IP Bit 18 (0x00 00 20): eSTB-DSG Bits 19..31 (0x00 00 1F FF): otras interfaces eSAFE

B.3.4 Subtipo máscara de interfaz CM (CMIM)

Este parámetro es una máscara de bits que describe un conjunto de índices de interfaz eCM [b-UIT-T J.126]. En una codificación L2VPN de retransmisión, el subtipo máscara de interfaz CM describe el conjunto de interfaces de puerto puente en el que el CM retransmite paquetes de la L2VPN.

Cada bit de la CMIM corresponde a una interfaz de puerto puente lógica de un puente de capa 2 MAC implementado en el CM de un módem de cable. El parámetro se codifica como una cadena de octetos de la codificación reglas de codificación básicas de una cadena de bits BITS SNMP. La posición de bit K en la codificación BITS corresponde a la interfaz puente MAC eDOCSIS K. Por convenio, la posición de bit 0 corresponde a la interfaz de anfitrión propia del eCM. La dirección MAC propia del eCM se indica como si estuviera en un ifIndex de interfaz de puerto puente cero (0) incluso aunque no exista realmente esta interfaz.

Subtipo	Longitud	Valor
43.5.4	N	BITS SNMP mapa de bits codificado en el que la posición de bit K representa el valor del índice de interfaz lógica eCM K. La posición de bit 0 representa el anfitrión propio del eCM. La posición de bit 0 es el bit más significativo del primer octeto. Para las asignaciones de los últimos índices de la interfaz lógica véase [b-UIT-T J.126]. Bit 0 (0x80): interfaz de anfitrión propia del eCM Bit 1 (0x40): interfaz CPE primaria (también ePS) Bit 2 (0x20): interfaz RF Bits 3,4 reservados Bits 5..15 (0x07 FF): otras interfaces CPE Bits 16-31: interfaces lógicas incorporadas. Las interfaces actualmente definidas incluyen: Bit 16 (0x00 00 80): IPCablecom-EMTA Bit 17 (0x00 00 40): eSTB-IP Bit 18 (0x00 00 20): eSTB-DSG Bits 19..31 (0x00 00 1F FF): otras interfaces eSAFE

Si el subtipo máscara de interfaz CM no está presente en una codificación L2VPN de retransmisión, su valor por defecto es solo para la interfaz CPE primaria (índice 1) y para la interfaz RF de cable (índice 2), es decir, un valor 0x60 de CMIM. Un CM DEBE ignorar en silencio las posiciones de bit de la CMIM para interfaces no implementadas. Un CMTS PUEDE indicar que un valor CMIM representa todas las interfaces CPE posibles con el valor CMIM para las posiciones 1 y 5-15, es decir, el valor 0x47 FF de la CMIM.

B.3.5 ID de grupo de anexión

Si está presente, el CMTS DEBERÍA utilizar este valor de subtipo como el elemento de señalización del ID de grupo de anexión (AGI) asociado con un identificador RPV, cuando establezca de forma dinámica un seudohilo NSI para la retransmisión punto a punto del circuito de anexión. Sólo se aplica junto con el encapsulado MPLS o NSI L2TPv3 y a la retransmisión punto a punto entre el circuito de anexión y el seudohilo.

Subtipo	Longitud	Valor
43.5.5	0..16	Cadena de bytes opaca que identifica el CM o el SF como un circuito de anexión para protocolos de señalización RPV de capa 2 IETF.

B.3.6 ID individual de anexión de fuente

Si está presente, el CMTS DEBERÍA utilizar este valor de subtipo como el elemento de señalización de identificador individual de anexión de fuente (SAII) asociado con la anexión de seudohilo local cuando se establece un seudohilo de red medular NSI para el circuito de anexión de cable. Sólo se aplica junto con un subtipo MPLS o de encapsulado NSI L2TPv3 y para la retransmisión punto a punto entre el circuito de anexión de cable y el seudohilo.

Subtipo	Longitud	Valor
43.5.6	0..16	Cadena de bytes opaca indicada como circuito SAII para protocolos de señalización RPV de capa 2 IETF.

B.3.7 ID individual de anexión de objetivo

Si está presente, el CMTS DEBERÍA utilizar este valor de subtipo como el elemento de señalización de identificador individual de anexión de objetivo (TAII) asociado con la anexión de seudohilo distante cuando se establece un seudohilo NSI para el circuito de anexión. Se aplica sólo junto con un subtipo MPLS o de encapsulado NSI L2TPv3 y para la retransmisión punto a punto entre el circuito de anexión de cable y el seudohilo.

Subtipo	Longitud	Valor
43.5.7	0..16	Cadena de bytes opaca que identifica al CM o el SF como un circuito de anexión para protocolos de señalización RPV de capa 2 IETF.

B.3.8 Prioridad de usuario entrante

Los protocolos puente IEEE 802.1 requieren la detección o generación, la regeneración opcional y la señalización de un atributo prioridad de usuario para todos los paquetes con puentes. El subtipo prioridad de usuario entrante se utiliza para configurar la prioridad de usuario IEEE 802.1 entrante de paquetes L2VPN en sentido ascendente. Se define sólo en codificaciones L2VPN de retransmisión por SF en sentido ascendente.

A menos que se configure de otra forma el retransmisor L2VPN, el CMTS DEBE transmitir la prioridad de entrada señalada con este subtipo como bits de prioridad de usuario de un rótulo IEEE 802.1Q cuando retransmite el paquete a un puerto NSI con encapsulado IEEE 802.1Q. Si se omite este subtipo en una codificación L2VPN de retransmisión, el CMTS considera que la prioridad de usuario entrante es cero (0). Este subtipo no aparece más de una vez en una codificación L2VPN de retransmisión válida.

Subtipo	Longitud	Valor
43.5.8	1	Valor de prioridad de usuario IEEE 802.1 de entrada en la gama 0..7 codificado en los tres bits menos significativos. Valores mayores indican una mayor prioridad.

B.3.9 Gama de prioridades de usuario

En una codificación de clasificación de paquetes en sentido descendente, la presencia de una codificación L2VPN con este subtipo restringe al clasificador sólo a paquetes retransmitidos en sentido descendente con la gama indicada de valores de prioridad de usuario (inclusive). La prioridad de usuario clasificada es como la transmitida en la interfaz de capa MAC DOCSIS, y así se considera *después* de cualquier selección de prioridad de usuario por defecto entrante o de cualquier regeneración de prioridad de usuario realizada por el retransmisor L2VPN. Este subtipo puede aparecer sólo en una codificación L2VPN de clasificador en sentido descendente y, como

mucho, una vez en una única codificación L2VPN. Si se omite este subtipo, el clasificador se aplica a todos los valores de prioridad de usuario salientes.

Subtipo	Longitud	Valor
43.5.9	2	Prioridad baja, prioridad alta. El valor de prioridad de usuario más bajo de la gama de prioridades de usuario se codifica en los tres bits menos significativos del primer byte y el valor más alto de la gama se codifica en los tres bits menos significativos del segundo byte.

B.3.10 Subtipo SA-descriptor L2VPN

El CMTS añade este subtipo a la respuesta de registro en sentido descendente y en los mensajes de servicio dinámico que tengan codificaciones L2VPN de retransmisión para indicar a un CM conforme con L2VPN los valores SAID con los que el CMTS criptará el tráfico en sentido descendente retransmitido a esa L2VPN a través del CM. Una codificación L2VPN válida puede tener múltiples subtipos SA-descriptor L2VPN.

Subtipo	Longitud	Valor
43.5.10	N	Codificación SA-descriptor especificada en [UIT-T J.125] que proporciona el valor SAID con el que el CMTS cripta el tráfico en sentido descendente retransmitido a una L2VPN. El tipo SA del SA-descriptor debe ser dinámico.

B.3.11 Subtipo L2VPN específica del suministrador

Este subtipo es interpretado por el CMTS como decida el suministrador. Un ejemplo de uso consiste en configurar la subinterfaz NSI o el circuito virtual hacia los que se encaminan los paquetes en sentido ascendente provenientes del CM o del SF en un modo punto a punto. El contenido del subtipo específico del suministrador puede ser datos codificados en binario o ASCII.

Tipo GEI	Longitud	Valor
43.5.43	N	08, 3, ID de suministrador, seguido de tuplas tipo/longitud/valor específicas del suministrador.

B.4 Códigos de confirmación

Esta cláusula define nuevos códigos de confirmación para el funcionamiento L2VPN. Amplía la lista de códigos de confirmación de C.4 de [UIT-T J.122].

Los códigos de confirmación adicionales definidos para la característica L2VPN DOCSIS incluyen:

- reject-VLAN-ID-in-use(26): indica que un VLAN-ID IEEE 802.1Q o IEEE 802.1ad requerido para el encapsulado NSI de tráfico L2VPN está ya asignado para su uso por tráfico no L2VPN, véase 7.2.5.
- reject-multipoint-L2VPN(27): indica que el modo de retransmisión L2VPN no está soportado y que un CM está intentado configurar más de un circuito de anexión L2VPN en la misma L2VPN, véase 7.2.5.
- reject-multipoint-NSI(28): indica que una L2VPN de retransmisión multipunto contenía múltiples codificaciones L2VPN con diferentes valores de encapsulado NSI.

B.5 Codificación de error L2VPN

Esta codificación proporciona información adicional del CM cuando rechaza una codificación L2VPN indicada por el CMTS. El CM DEBE incluir una codificación de error L2VPN en su

respuesta de gestión MAC cuando rechace una codificación L2VPN en un REG-RSP, DSA-RSP, DSC-REQ o DSC-REP.

Tipo GEI	Longitud	Valor
43.5.254	N	Codificación de error L2VPN constituida por exactamente una codificación de parámetro con error L2VPN, exactamente una codificación de código de error L2VPN, y ninguna o una codificación de mensaje de error L2VPN.

B.5.1 Parámetro con errores L2VPN

Este parámetro proporciona una secuencia de tipos y subtipos que identifica la ubicación y el subtipo de la codificación L2VPN rechazada. Una codificación de error L2VPN válida contiene exactamente una cadena del tipo parámetro con errores L2VPN.

Tipo GEI	Longitud	Valor
43.5.254.1	N	Secuencia de tipos y subtipos

La secuencia de tipos y subtipos se inicia en el nivel superior de las codificaciones TLV del mensaje de gestión MAC que incluye la codificación L2VPN. Esta secuencia depende de la ubicación de la codificación L2VPN como se describe en 7.2. En particular:

- Una cadena de parámetros de error L2VPN para una codificación L2VPN de máximo nivel se inicia con dos bytes para el código de tipo GEI para la codificación L2VPN o (43.5);
- Una cadena de parámetros de error L2VPN para una codificación de flujo de servicio en sentido ascendente se inicia con el código de tipo para esa codificación (24) seguido de un tipo GEI de codificación L2VPN o (24.43.5);
- Una cadena de parámetros de error L2VPN para una fijación de configuración de clasificación de paquetes en sentido descendente se inicia con el tipo de esa codificación (23) seguido de un tipo GEI de codificación L2VPN o (23.43.5);
- Una cadena de parámetros de error L2VPN para una fijación de configuración de clasificación de paquetes en sentido ascendente se inicia con el tipo para esa codificación (22) seguido de un tipo GEI de codificación L2VPN o (22.43.5);

Si se rechaza la totalidad de la codificación L2VPN, el CM PUEDE incluir en la cadena de tipos parámetro de error L2VPN sólo los dos o tres bytes que identifican la ubicación de una codificación L2VPN completa. Si el rechazo se debe a un determinado subtipo de codificación L2VPN, el CM DEBERÍA incluir bytes adicionales en la cadena de tipos de parámetro de error L2VPN para identificar el subtipo de la codificación L2VPN rechazada. Una razón para rechazar una codificación L2VPN completa es que se exceda el número máximo de L2VPN soportadas por el CM. Una razón para rechazar un determinado subtipo, por ejemplo, la codificación subtipo SA-descriptor L2VPN es que se exceda el número de SAID soportados por el CM.

B.5.2 Código de error L2VPN

Este parámetro proporciona un código de confirmación definido según C.4 de [UIT-T J.122] para identificar el motivo por el que se rechazó la codificación o el subtipo L2VPN. Una codificación de error L2VPN contiene exactamente un código de confirmación L2VPN.

Tipo GEI	Longitud	Valor
43.5.254.2	1	Código de confirmación.

B.5.3 Mensaje de error L2VPN

Este parámetro, si está presente, proporciona un mensaje para presentar en la consola CMTS una razón del rechazo. Un CM DEBERÍA incluir este parámetro en una codificación de error L2VPN. Una codificación de error L2VPN contiene cero o un subtipo mensaje de error L2VPN.

Tipo GEI	Longitud	Valor
43.5.254.2	N	Cadena terminada en cero de caracteres ASCII.

B.6 Criterios de clasificación de máscaras de interfaz CM

Esta Recomendación define un mecanismo genérico para la clasificación del tráfico en sentido ascendente y en sentido descendente basándose en los puertos de interfaz lógicos de entrada o de salida en el CM.

En una codificación de clasificador de paquetes en sentido ascendente (tipo 22) el subtipo de máscara de interfaz CM define un criterio regulado para equiparar la interfaz de entrada de una L2PDU.

En una codificación de clasificador de paquetes en sentido descendente (tipo 23), el subtipo de máscara de interfaz CM define un criterio regulado para hacer equiparar una dirección MAC de destino en sentido descendente unidifundida. En cualquier caso, la codificación de un subtipo CMIM en una codificación de clasificador de paquetes aplica tanto al tráfico L2VPN como al tráfico no L2VPN.

Cada bit de CMIM corresponde a una interfaz de puerto puente lógica de un puente de capa 2 MAC implementado en el eCM de un módem de cable. El parámetro se codifica como una cadena de octetos de la codificación regla de codificación básica de una cadena de bits BITS SNMP. La posición de bit K en la codificación BITS corresponde a la interfaz puente MAC eDOCSIS K. Por convenio, la posición de bit 0 corresponde a la interfaz de anfitrión propia del eCM (es decir, la pila IP del CM). La dirección MAC propia del eCM se indica como si estuviera en un índice de interfaz de puerto puente cero (0), incluso aunque no exista realmente esa interfaz.

Subtipo	Longitud	Valor
[22/23].13	N	BITS SNMP mapa de bits codificados en el que la posición de bit K representa el valor del índice de interfaz lógica eCM K. La posición de bit 0 representa al anfitrión propio del eCM. La posición de bit 0 es el bit más significativo del primer octeto. La especificación de DOCSIS incorporado [b-UIT-T J.126] define las asignaciones de los índices de interfaz. Para información, las asignaciones actuales incluyen: Bit 0 (0x80): interfaz de anfitrión propia del eCM Bit 1 (0x40): interfaz CPE primaria (también ePS) Bit 2 (0x20): interfaz RF Bits 3,4: reservados Bits 5..15 (0x07 FF): otras interfaces CPE Bits 16-31: interfaces CPE lógicas para anfitriones eSAFE. Las asignaciones actuales incluyen: Bit 16 (0x00 00 80): IPCablecom-EMTA Bit 17 (0x00 00 40): eSTB-IP Bit 18 (0x00 00 20): eSTB-DSG Bits 19..31 (0x00 00 1F FF): otras interfaces eSAFE

En una codificación de clasificador en sentido ascendente, un CM DEBE ignorar en silencio las posiciones de bit para interfaces no implementadas. Por ejemplo, un criterio de clasificador CMIM en sentido ascendente destinado a equiparar sólo interfaces CPE externas de un CM tiene los bits 1 y 5-15 de fijación del valor de máscara CMIM, es decir, una codificación 0x47 FF.

En una codificación de clasificador en sentido descendente, que incluye un criterio CMIM, el CMTS comprueba la dirección MAC de destino para determinar si es una dirección MAC de anfitrión propia del CM o una dirección MAC de anfitrión propia de la eSAFE reconocida. Cualquier otra dirección MAC difundida se considera que es una dirección MAC CPE. El CMTS no sabe en qué interfaz CPE ha aprendido el CM una dirección MAC CPE. El CMTS considera sólo el bit 1 de la CMIM para incorporar una dirección MAC CPE en una codificación de clasificador de paquetes en sentido descendente. El número máximo de direcciones MAC de destino eSAFE reconocidas por un CMTS depende del suministrador.

Apéndice I

Ejemplo de codificaciones L2VPN

La codificación L2VPN siempre está encapsulada utilizando una codificación de información de ampliación general (GEI), que utiliza el código tipo 43 con el ID de suministrador reservado 0xFFFFFF.

I.1 Ejemplo de punto a punto

Esta cláusula describe codificaciones L2VPN para tres CM que por defecto realizan la retransmisión L2VPN punto a punto de todo el tráfico en su flujo de servicio en sentido ascendente. Dos de los CM están conectados externamente con puentes a la misma empresa (ID L2VPN 0234560001) y uno de los CM lo está a una empresa diferente (ID L2VPN 0234560002). El ejemplo se muestra en la figura I.1:

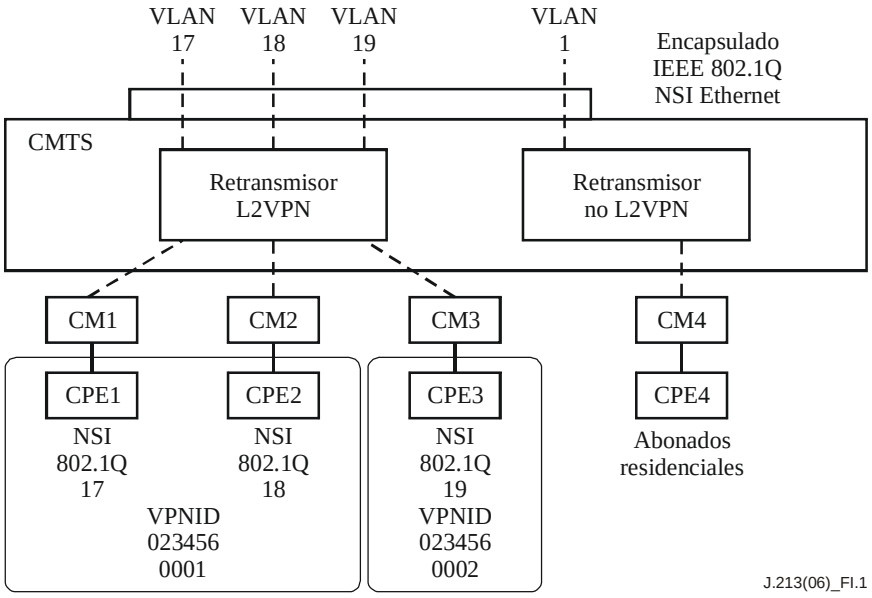

Figura I.1 – Ejemplo de retransmisión de tráfico L2VPN punto a punto

Cuadro I.1 – Codificación L2VPN CM1 punto a punto

Fichero de configuración CM1 punto a punto				
43				Codificación L2VPN por CM
20				Longitud total
	08 03 FFFFFF			ID de suministrador: 0xFFFFFF para GEI
	05			GEI 43.5 para codificación L2VPN
	13			Longitud del subtipo GEI.5
		01 05 x0234560001		Subtipo VPNID
		02		Subtipo encapsulado NSI
		04		Longitud del subtipo GEI.5.2
			02	Subtipo formato IEEE 802.1Q
			02	Longitud del subtipo GEI.5.2.2
			0x0011	VLAN ID 17
24				Codificación de flujo de servicio en sentido ascendente
19				Longitud
	6			Subtipo tipo conjunto de parámetros QoS
	1			
		0x07		
	43			Subtipo específico del suministrador:
	14			Longitud total
		08 03 FFFFFF		ID de suministrador para GEI
		05		GEI 43.5 para codificación L2VPN
		7		Longitud del subtipo GEI.5
			01 05 x0234560001	Subtipo VPNID
45				Filtrado DUT:
01				Longitud total
	01			Filtrado DUT habilitado

Cuadro I.2 – Codificación L2VPN CM2 punto a punto

Fichero de configuración CM2 punto a punto				
43				Codificación L2VPN por CM
20				Longitud total
	08 03 FFFFFF			ID de suministrador : 0xFFFFFF para GEI
	05			GEI 43.5 para codificación L2VPN
	13			Longitud del subtipo GEI.5
		01 05 x0234560001		Subtipo VPNID
		02		Subtipo encapsulado NSI
		04		Longitud del subtipo GEI.5.2
			02	Subtipo formato IEEE 802.1Q
			02	Longitud del subtipo GEI.5.2.2
			0x0012	VLAN ID 18
24				Codificación de flujo de servicio en sentido ascendente
19				Longitud
	6			Subtipo tipo conjunto de parámetros QoS
	1			
		0x07		
	43			Subtipo específico del suministrador:
	14			Longitud total
		08 03 FFFFFF		ID de suministrador para GEI
		05		GEI 43.5 para codificación L2VPN
		7		Longitud de subtipo GEI.5
			01 05 x0234560001	Subtipo VPNID
45				Filtrado DUT:
01				Longitud total
	01			Filtrado DUT habilitado

CPE2 está conectado externamente a la misma L2VPN que CPE1 (VPNID x0234560001), pero toda la retransmisión L2VPN para CPE2 se produce en el ID VLAN 18 IEEE 802.1Q NSI.

Cuadro I.3 – Codificación L2VPN CM3 punto a punto

Fichero de configuración CM3 punto a punto				
43				Codificación L2VPN por CM
20				Longitud total
	08 03 FFFFFF			ID de suministrador: 0xFFFFFF para GEI
	05			GEI 43.5 para codificación L2VPN
	13			Longitud del subtipo GEI.5
		01 05 x0234560002		Subtipo VPNID
		02		Subtipo encapsulado NSI
		04		Longitud del subtipo GEI.5.2
			02	Subtipo formato IEEE 802.1Q
			02	Longitud del subtipo GEI.5.2.2
			0x0013	VLAN ID 19
24				Codificación de flujo de servicio en sentido ascendente
19				Longitud
	6			Subtipo tipo conjunto de parámetros QoS
	1			
		0x07		
	43			Subtipo específico del suministrador:
	14			Longitud total
		08 03 FFFFFF		ID de suministrador para GEI
		05		GEI 43.5 para codificación L2VPN
		7		Longitud del subtipo GEI.5
			01 05 x0234560002	Subtipo VPNID
45				Filtrado DUT:
01				Longitud total
	01			Filtrado DUT habilitado

I.2 Ejemplo multipunto

Esta cláusula proporciona un ejemplo de codificaciones L2VPN para retransmisión multipunto como se indica a continuación. Para la retransmisión multipunto el encapsulado NSI para una L2VPN se puede configurar de una de las dos formas siguientes:

- como una codificación específica del suministrador CMTS o;
- en el fichero de configuración de CM de uno o más CM en la L2VPN.

En el ejemplo de la figura I.2, el encapsulado NSI para cada L2VPN aparece en el fichero de configuración CM para todos los CM.

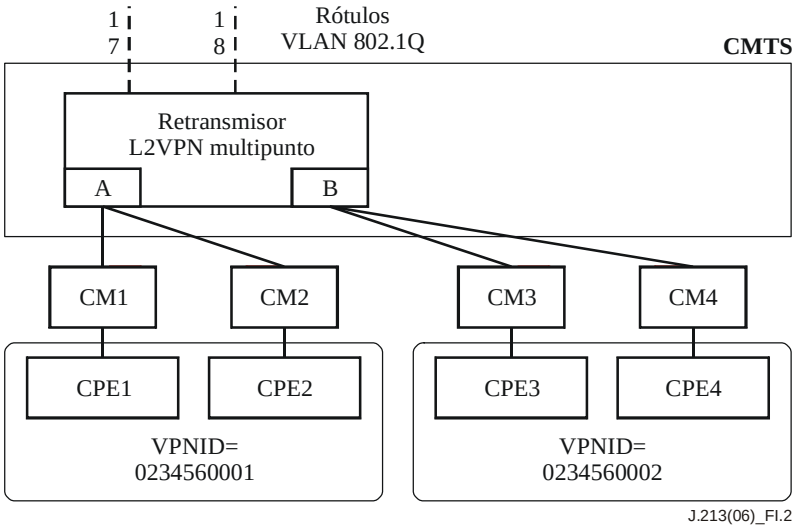

Figura I.2 – Ejemplo de retransmisión del tráfico L2VPN multipunto

Cuadro I.4 – Codificación L2VPN CM1 multipunto

Fichero de configuración CM1 multipunto				
43				Codificación L2VPN por CM
20				Longitud total
	08 03 FFFFFF			ID de suministrador: 0xFFFFFF para GEI
	05			GEI 43.5 para codificación L2VPN
	13			Longitud del subtipo GEI.5
		01 05 x0234560001		Subtipo VPNID
		02		Subtipo encapsulado NSI
		04		Longitud del subtipo GEI.5.2
			02	Subtipo formato IEEE 802.1Q
			02	Longitud del subtipo GEI.5.2.2
			0x0011	VLAN ID 17
24				Codificación de flujo de servicio en sentido ascendente
19				Longitud
	6			Subtipo tipo conjunto de parámetros QoS
	1			
		0x07		
	43			Subtipo específico del suministrador:
	14			Longitud total
		08 03 FFFFFF		ID de suministrador para GEI
		05		GEI 43.5 para codificación L2VPN
		7		Longitud del subtipo GEI.5
			01 05 x0234560001	Subtipo VPNID

Cuadro I.4 – Codificación L2VPN CM1 multipunto

Fichero de configuración CM1 multipunto				
45				Filtrado DUT:
01				Longitud total
	01			Filtrado DUT habilitado

Cuadro I.5 – Codificación L2VPN CM2 multipunto

Fichero de configuración CM2 multipunto				
43				Codificación L2VPN por CM
20				Longitud total
	08 03 FFFFFF			ID de suministrador: 0xFFFFFF para GEI
	05			GEI 43.5 para codificación L2VPN
	13			Longitud del subtipo GEI.5
		01 05 x0234560001		Subtipo VPNID
		02		Subtipo encapsulado NSI
		04		Longitud del subtipo GEI.5.2
			02	Subtipo formato IEEE 802.1Q
			02	Longitud del subtipo GEI.5.2.2
			0x0011	VLAN ID 17
24				Codificación de flujo de servicio en sentido ascendente
19				Longitud
	6			Subtipo tipo conjunto de parámetros QoS
	1			
		0x07		
	43			Subtipo específico de suministrador:
	14			Longitud total
		08 03 FFFFFF		ID de suministrador para GEI
		05		GEI 43.5 para codificación L2VPN
		7		Longitud del subtipo GEI.5
			01 05 x0234560001	Subtipo VPNID
45				Filtrado DUT:
01				Longitud total
	01			Filtrado DUT habilitado
NOTA – Las codificaciones L2VPN para CM2 multipunto son exactamente las mismas que para CM1.				

Cuadro I.6 – Codificación L2VPN CM3 multipunto

Fichero de configuración CM3 multipunto				
43				Codificación L2VPN por CM
20				Longitud total
	08 03 FFFFFF			ID de suministrador: 0xFFFFFF para GEI
	05			GEI 43.5 para codificación L2VPN
	13			Longitud del subtipo GEI.5
		01 05 x0234560002		Subtipo VPNID
		02		Subtipo encapsulado NSI
		04		Longitud del subtipo GEI.5.2
			02	Subtipo formato IEEE 802.1Q
			02	Longitud del subtipo GEI.5.2.2
			0x0012	VLAN ID 18
24				Codificación de flujo de servicio en sentido ascendente
19				Longitud
	6			Subtipo tipo conjunto de parámetros QoS
	1			
		0x07		
	43			Subtipo específico del suministrador:
	14			Longitud total
		08 03 FFFFFF		ID de suministrador para GEI
		05		GEI 43.5 para codificación L2VPN
		7		Longitud del subtipo GEI.5
			01 05 x0234560002	Subtipo VPNID
45				Filtrado DUT:
01				Longitud total
	01			Filtrado DUT habilitado

Cuadro I.7 – Codificación L2VPN CM4 multipunto

Fichero de configuración CM4 multipunto				
43				Codificación L2VPN por CM
20				Longitud total
	08 03 FFFFFF			ID de suministrador: 0xFFFFFF para GEI
	05			GEI 43.5 para codificación L2VPN
	13			Longitud del subtipo GEI.5
		01 05 x0234560002		Subtipo VPNID

Cuadro I.7 – Codificación L2VPN CM4 multipunto

Fichero de configuración CM4 multipunto				
		02		Subtipo encapsulado NSI
		04		Longitud del subtipo GEI.5.2
			02	Subtipo formato IEEE 802.1Q
			02	Longitud del subtipo GEI.5.2.2
			0x0012	VLAN ID 18
24				Codificación de flujo de servicio en sentido ascendente
19				Longitud
	6			Subtipo tipo conjunto de parámetros QoS
	1			
		0x07		
	43			Subtipo específico del suministrador:
	14			Longitud total
		08 03 FFFFFF		ID de suministrador para GEI
		05		GEI 43.5 para codificación L2VPN
		7		Longitud del subtipo GEI.5
			01 05 x0234560002	Subtipo VPNID
45				Filtrado DUT:
01				Longitud total
	01			Filtrado DUT habilitado
NOTA – Las codificaciones L2VPN para CM4 multipunto son exactamente las mismas que para CM3.				

I.3 Ejemplo de clasificador L2VPN en sentido ascendente

Este ejemplo muestra el tráfico en sentido ascendente de clasificación desde un CPE1 específico a un flujo de servicio L2VPN en sentido ascendente, en el que todos los CPE anexados al CM retransmiten al retransmisor no L2VPN, como se muestra en el cuadro I.8.

Cuadro I.8 – Codificación de clasificador LSVPN en sentido ascendente

Fichero de configuración de módem de cable clasificador LSVPN en sentido ascendente				
43				Codificación L2VPN por CM
20				Longitud total
	08 03 FFFFFF			ID de suministrador: 0xFFFFFF para GEI
	05			GEI 43.5 para codificación L2VPN
	13			Longitud del subtipo GEI.5

Cuadro I.8 – Codificación de clasificador LSVPN en sentido ascendente

Fichero de configuración de módem de cable clasificador LSVPN en sentido ascendente				
		01 05 x0234560003		Subtipo VPNID
		02		Subtipo encapsulado NSI
		04		Longitud del subtipo GEI.5.2
			02	Subtipo formato IEEE 802.1Q
			02	Longitud del subtipo GEI.5.2.2
			0x0019	VLAN ID 18
24				Codificación de flujo de servicio en sentido ascendente por defecto
07				Longitud
	01 02 0001			Referencia de flujo de servicio 0001
	06 01 07			Subtipo tipo conjunto de parámetros QoS
24				Codificación de flujo de servicio L2VPN en sentido ascendente
19				Longitud
	06 01 07			Subtipo tipo conjunto de parámetros QoS
	43			Subtipo específico de suministrador
	14			Longitud total
		08 03 FFFFFF		ID de suministrador: para GEI
		05		GEI 43.5 para codificación L2VPN
		7		Longitud del subtipo GEI.5
			01 05 x0234560003	Subtipo VPNID
22				Codificación de clasificador en sentido ascendente
14				Longitud
	03 02 0001			Referencia de flujo de servicio a 0001
	10			Clasificación de paquetes Ethernet/LLC
		02		Dirección MAC de origen
		6		Longitud
			x0001020000AA	Dirección MAC del CPE1
45				Filtrado DUT:
01				Longitud total
	01			Filtrado DUT habilitado

Apéndice II

Encapsulado IEEE 802.1Q

Este apéndice proporciona información básica sobre el formato de los rótulos IEEE 802.1Q en interfaces NSI del extremo Ethernet. Es un mecanismo normalizado para indicar la VLAN de un paquete con puente en una interfaz Ethernet. Se requiere un CMTS conforme con esta Recomendación para soportar el reconocimiento del encapsulado IEEE 802.1Q en una interfaz Ethernet cuando esté configurado para ello.

Debido a que el CMTS interpreta el ID VLAN del rótulo 802.1Q más alejado de un paquete entrante en una NSI, el rótulo se denomina rótulo delimitador de servicio.

El retransmisor L2VPN *detecta* el rótulo IEEE 802.1Q delimitador de servicio en un paquete Ethernet cuando lo retransmite en sentido descendente e *inserta* el rótulo IEEE 802.1Q delimitador de servicio cuando retransmite paquetes en sentido ascendente. La VLAN a la que pertenece un paquete L2VPN se indica explícitamente en una interfaz Ethernet encapsulada 802.1Q y siempre se incluye cuando se retransmite en la interfaz MAC RF DOCSIS.

Esta detección e inserción de los rótulos IEEE 802.1Q se muestra en la figura II.1:

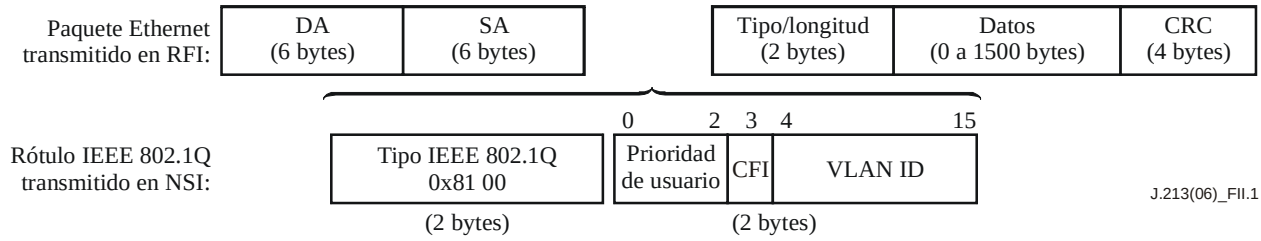

Figura II.1 – Rótulos Ethernet 802.1Q

Un paquete Ethernet se rotula con un rótulo IEEE 802.1Q insertando 4 bytes entre su dirección de fuente original (SA, *source address*) y el campo longitud/tipo original. El código tipo Ethernet de dos bytes 0x8100 indica que sigue un rótulo IEEE 802.1Q de 16 bits. El valor del rótulo está constituido por un campo de prioridad de usuario de 3 bits en los 3 bits más significativos, un bit indicador de formato canónico (CFI, *canonical format indicator*) y un ID VLAN de 12 bits en los bits menos significativos. El funcionamiento del bit CFI está definido en el IEEE, y es cero para direcciones MAC Ethernet. Todos los campos con múltiples bytes se transmiten con el byte más significativo en primer lugar.

El campo prioridad de usuario indica una prioridad de retransmisión de tráfico en la gama de 0 a 7, indicando los valores más altos la mayor prioridad.

Esta Recomendación permite, pero no requiere, que el CMTS utilice encapsulados de puerto NSI diferentes de los de IEEE 802.1Q para indicar la L2VPN o el circuito de anexión para un paquete retransmitido por L2VPN. El encapsulado NSI específico utilizado para la retransmisión L2VPN se ha de configurar en el subtipo encapsulado NSI de una codificación L2VPN.

Apéndice III

Modelo de puente CM VLAN incorporado

Este apéndice propone un modelo VLAN incorporado para la retransmisión puente interna CM de paquetes para su consideración por la comunidad DOCSIS. Actualmente no es un requisito para la certificación L2VPN en un CM.

La especificación L2VPN utiliza el concepto de máscara de interfaz CM (CMIM) para definir el conjunto de interfaces puente internas y externas al que el CM puede destacar tráfico en sentido descendente. La CMIM, por ejemplo, define el dominio de difusión del tráfico en sentido descendente dirigido al MAC de grupo como al individual. Un dominio de difusión es una interpretación de una LAN virtual, de forma que la CMIM define una VLAN interna de los puertos internos y externos hacia la que se retransmite tráfico DUT y L2VPN.

El modelo VLAN incorporado amplía el puente MAC del modelo eDOCSIS para llegar a ser un puente MAC con capacidad VLAN con dominios de retransmisión MAC VLAN incorporada (eVLAN) separados. Utilizando el concepto de eVLAN, el CM es capaz de aislar los anfitriones eCM y eSAFE de los dominios de difusión MAC de las L2VPN privadas de cliente.

La figura III.1 describe el modelo VLAN incorporada para los CM conformes con L2VPN.

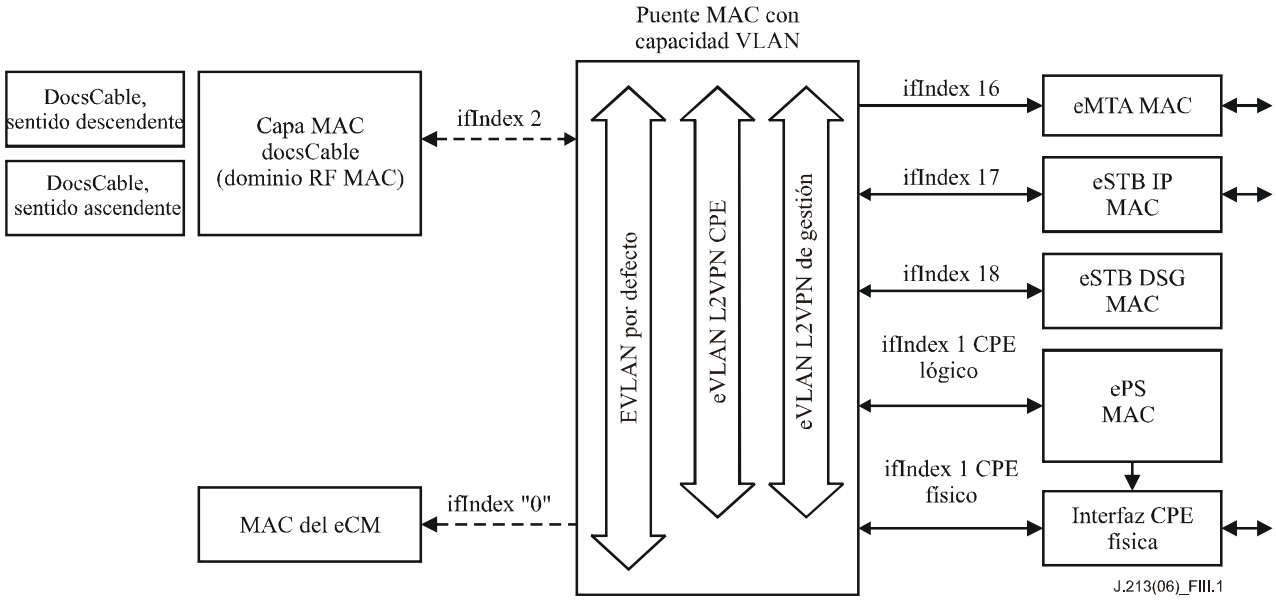

Figura III.1 – Modelo VLAN incorporada (eVLAN) L2VPN

El puente MAC de un CM incorporado se considera que tiene una interfaz de puerto puente con la interfaz de dominio RF MAC como ifIndex 2 y una interfaz de puerto puente CPE primaria como ifIndex 1. DOCSIS define el funcionamiento de la retransmisión CPE mediante un CM residencial como función puente MAC de capa 2 entre la interfaz RF y la interfaz CPE. En eDOCSIS, la dirección MAC propia del eCM (su MAC propia) se considera interna al puente MAC y alcanzable por todas las interfaces de puerto puente.

La especificación eDOCSIS define una entidad funcional de servicio/aplicación incorporada (eSAFE) como una entidad ubicada en el mismo lugar que un módem de cable incorporado (eCM) que contiene su propia MAC y dirección IP [b-UIT-T J.126]. Actualmente las eSAFE definidas incluyen:

- Anfitrión MTA incorporado IPCablecom (eMTA).
- Anfitrión de servicios de portal incorporados (ePS).
- Adaptador de ESTB incorporado.

Cada uno de estos dispositivos eSAFE se considera que tiene una interfaz CPE lógica diferente con el puente MAC, y se asigna a un índice de interfaz (ifIndex) diferente para fines de gestión y de control. En la arquitectura eDOCSIS, el puente MAC eCM se supone que implementa una única base de datos de retransmisión, asociando direcciones MAC a cada interfaz CPE lógica y retransmitiendo unidades de datos de protocolo de capa 2 (L2PDU) entre todos los puertos del puente MAC, de conformidad con la dirección MAC de destino (DMAC) de la L2PDU. La interfaz RF, las interfaces CPE, MAC eCM y todas las interfaces MAC eSAFE se considera que están en el mismo dominio de difusión MAC de capa 2 (es decir, en una única LAN).

La especificación L2VPN ampliará esta arquitectura introduciendo el concepto de VLAN incorporada (eVLAN) en el puente MAC del eCM, en el que las VLAN tienen diferentes conjuntos de puertos CPE lógicos. Para controlar el acceso a la dirección MAC propia del eCM (por ejemplo, para aislarlo del acceso L2VPN del cliente), el MAC eCM se considera que reside en una interfaz con su propio puerto puente.

La arquitectura L2VPN introduce el concepto de máscara de interfaz de módem de cable (CMIM) con una posición de bit para cada puerto puente lógico en el puente MAC con capacidad VLAN del eCM. Cada eVLAN en el puente MAC contiene un valor de CMIM que representa los puertos puente lógicos que pertenecen a la eVLAN. La CMIM está representada como una codificación de objeto BITS SNMP en la que la posición de bit K corresponde al ifIndex K de la interfaz de puerto puente. En una máscara CMIM al puerto puente lógico se le asigna la posición de bit 0 (es decir, como si tuviera un ifIndex de valor 0). No se crea ningún dato de entrada ifStack para la interfaz de puerto propio, puesto que cero es un valor no válido para un valor de ifIndex.

En el puente MAC eCM todas las retransmisiones no L2VPN se considera que están puenteadas a una eVLAN que tiene una CMIM, con todos los bits de interfaz fijados a '1'. Esto corresponde a la retransmisión normal de puente MAC con una única LAN definido anteriormente en este documento L2VPN.

Sin embargo, se pueden definir diferentes eVLAN con subconjuntos de interfaces de puerto puente eCM para una retransmisión de capa 2 independiente. En particular, se implementa el servicio LAN transparente (TLS) de cliente definiendo una VLAN para la L2VPN del abonado que contiene sólo la interfaz RF y la interfaz CPE. No se permite que una L2VPN TLS de cliente acceda a ningún anfitrión eCM o eSAFE.

El modelo eVLAN permite a un operador de cable implementar redes L2VPN de gestión para el tráfico eCM y eSAFE, definiendo una L2VPN con una CMIM que puentea únicamente la interfaz RF y las interfaces puente lógicas eSAFE y/o propia del eCM.

III.1 IEEE 802.1Q y el modelo VLAN incorporada

La operación y gestión de un puente de capa MAC con múltiples VLAN está normalizado mediante la especificación [IEEE 802.1Q]. [IEEE 802.1Q] se normalizó en primer lugar en 1998 y tiene una MIB de normalización [b-IETF RFC 2674]. La CMIM de una L2VPN se puede considerar que define la máscara de bits dot1qVlanCurrentEgressPorts de [b-IETF RFC 2674]. Si se adopta el concepto eVLAN como modelo de retransmisión de capa 2 CM DOCSIS, [b-IETF RFC 2674] ya define un amplio conjunto de objetos para indicar y controlar el funcionamiento de capa 2 CM.

La especificación [IEEE 802.1Q] se actualizó en 2003 incluyendo muchas ampliaciones IEEE 802.1 interinas (incluida [b-IEEE 802.1p]). La MIB para la ampliación IEEE 802.1Q se da en [b-IETF RFC 4363].

La adopción del modelo de retransmisión eVLAN permite a futuras especificaciones DOCSIS separar con claridad el funcionamiento de la interfaz RF de filtrado de capa 2, de la retransmisión y de la réplica de las diversas interfaces físicas internas y externas en dispositivos DOCSIS basados en CM.

[IEEE 802.1Q] tiene un propósito muy general y complejo y, por lo tanto, también resulta extraordinariamente compleja. La especificación tiene 327 páginas y su proyecto de MIB [b-IETF RFC 4363] tiene 106 páginas. La inclusión sólo de las funciones mínimas especificadas para el cumplimiento de la especificación [IEEE 802.1Q] o los objetos mínimos necesarios para [b-IETF RFC 2547] resulta demasiado funcional y de control y no es apropiada para el puente MAC incorporado de un CM conforme con L2VPN.

Aún así, las amplias capacidades y las MIB desarrolladas por el IEEE para establecer puentes entre múltiples VLAN pueden y deberían servir como modelo para la futura ampliación de la especificaciones de retransmisión de capa 2 CM. El concepto eVLAN tiene la capacidad de representar todos los modelos de retransmisión eDOCSIS actuales y puede representar con claridad los modelos de retransmisión L2 para futuras especificaciones DOCSIS, para la retransmisión IPv6 y para mejoras en la multidifusión IP. [IEEE 802.1Q], por ejemplo, define objetos de gestión normalizados para realizar clasificaciones VLAN basadas en el protocolo IP e incluso una clasificación VLAN basada en MAC de origen individual.

Esta Recomendación, por lo tanto, utiliza [IEEE 802.1Q] y [b-IETF RFC 2674] sólo como directriz conceptual para información sobre la funcionalidad requerida de un CM conforme con L2VPN (y un CMTS de hecho). Futuras versiones de esta y de otras especificaciones pueden añadir funciones de retransmisión de capa 2 adicionales y [IEEE 802.1Q] y [b-IETF RFC 4363] deberían servir como guía para definir esas funciones.

Por ejemplo, las actuales especificaciones L2VPN tratan únicamente con paquetes sin rótulos en las interfaces de puerto puente lógico del eCM. En la interfaz RF, la L2VPN particular (o como lo indica [IEEE 802.1Q], la VLAN particular) para una L2PDU siempre está *implícita* en el dominio MAC de ingreso CMTS o CM mediante el flujo de servicio en sentido ascendente o el SAID en sentido descendente. Futuras versiones de esta Recomendación pueden introducir el concepto de rótulos limitadores de servicio [IEEE 802.1Q] en la interfaz RF y/o en la interfaz CPE del puente MAC eCM. En este caso, la futura Recomendación debería utilizar conceptos y objetos MIB como los ya normalizados por la industria mediante [IEEE 802.1Q] y el IETF.

III.2 Primitivas de servicio de dominio MAC de puente incorporado

Debido a las capacidades de flujo de servicio de un dominio MAC RF DOCSIS, se define un puente MAC de eCM para proporcionar el siguiente servicio conceptual al dominio MAC RF:

- Sentido descendente (dominio MAC RF a puente):
  M_UNITDATA.request (
  L2PDU,
  eVLAN,
  user_priority)
- Sentido ascendente (puente a dominio RF MAC):
  M_UNITDATA.indication (
  L2PDU,
  eVLAN,
  user_priority,
  ingress_port)

donde:

- L2PDU es una PDU Ethernet (sin rótulos) con DMAC, SMAC, EtherType y con 0 a 1500 bytes de cabida útil L2;
- eVLAN es un identificador local para una determinada eVLAN;
- user_priority es una prioridad de 8 puntos para la retransmisión de capa 2 de la L2PDU, según se define en [IEEE 802.1Q];
- ingress_port es el valor del ifIndex lógico del puente desde el que se recibió la L2PDU.

La retransmisión de paquetes puente eCM en sentido descendente se realiza de la forma siguiente:

1) El subcomponente dominio MAC del CM (CM-MD) recibe una PDU DOCSIS de su interfaz docsCableDownstream que contiene una L2PDU de gestión no MAC. La PDU DOCSIS puede contener un encabezamiento ampliado BPI o un encabezamiento ampliado de servicio en sentido descendente.
2) Si el paquete estaba criptado con un SAID L2VPN, el CM-MD asigna la eVLAN puente solicitada a la que generó para la L2VPN; en otro caso, el CM-MD asigna la eVLAN requerida a la eVLAN por defecto.
3) Si el paquete incluía un ID en sentido descendente (DSID) que identifica el flujo de servicio en sentido descendente, el CM-MD fija la prioridad de usuario al parámetro de prioridad de tráfico de la SF DS; en otro caso, el CM-MD fija la prioridad de usuario a cero (0).
4) El CM-MD solicita al puente MAC que retransmita la L2PDU en la eVLAN requerida con la prioridad de usuario requerida.
5) El puente MAC retransmite el paquete a un puerto puente lógico de entrada de conformidad con los puertos de ingreso permitidos indicados en la CMIM para la eVLAN. Puede distribuir el paquete a múltiples puertos puente.
6) Si el puente MAC retransmite la L2PDU a un puerto puente de interfaz física CPE, implementa por lo menos dos clases de tráfico IEEE 802.1Q, para proporcionar la retransmisión de paquetes de capa 2 con prioridades de QoS. Los CM pueden implementar de dos a ocho (8) clases de tráfico.
7) Si el puente MAC retransmite la L2PDU a los servicios de portal J.192 internos (ePS) con una prioridad de usuario derivada de una prioridad de tráfico de flujo de servicio DS, el ePS utiliza este valor como el número de importancia de tráfico del paquete. Esto impide una reclasificación de ePS del paquete con su MIB cabhQos2PolicyTable.

La retransmisión de paquetes puente eCM en sentido ascendente se realiza de la forma siguiente:

1) La interfaz física CPE recibe una L2PDU. La interfaz física CPE solicita al puente MAC eCM que retransmita el paquete con prioridad de usuario 0 y la eVLAN por defecto.
2) Alternativamente, un dispositivo eSAFE interno puede solicitar al puente MAC que retransmita una L2PDU con una prioridad de usuario explícita y un valor eVLAN explícito.
3) El puente MAC indica que se transmita una L2PDU al subcomponente dominio MAC CM (CM-MD) con una eVLAN, una interfaz de ingreso y una prioridad de usuario.
4) El CM-MD utiliza la eVLAN para seleccionar un conjunto de clasificadores de paquetes en sentido ascendente; la eVLAN por defecto seleccionará los clasificadores no L2VPN, mientras que cualquier eVLAN seleccionará los clasificadores de paquetes en sentido ascendente L2VPN sólo para la L2VPN correspondiente.
5) El CM-MD utiliza el puerto de ingreso indicado para comparar las reglas de clasificador CMIM y utiliza la prioridad de usuario indicada para adaptar las reglas de clasificador a un criterio de gama de prioridades de usuario. Estos criterios aplican tanto a codificación L2VPN como a codificación no L2VPN.

6) El CM-MD asigna la L2PDU a un flujo de servicio en sentido ascendente y retransmite el paquete a la interfaz docsCableUpstream.

En este momento, la Recomendación L2VPN requiere que se consideren estos paquetes como si tuvieran una prioridad de usuario recibida cero (0). Futuras versiones de esta Recomendación pueden implementar diversos mecanismos [IEEE 802.1Q] para señalar de forma explícita (con rótulos sólo de prioridad), configurar de forma implícita (con prioridad de usuario de ingreso por defecto) y regenerar la prioridad de usuario entrante.

En lugar de realizar un modelo de ePS saliendo directamente al CPE físico, el modelo debería modificarse para que el ePS transmita a una eVLAN CPE J.192 diferente que incluya sólo el ePS y los puertos puente CPE físicos. El número de importancia de tráfico determinado por el ePS se convierte en la prioridad de usuario de la petición de ePS para transmitir en la eVLAN CPE J.192. Este modelo deja claro cómo J.192 (y cualquier otro futuro retransmisor CPE de capa 3) puede compartir el puerto CPE físico con otros retransmisores al puerto CPE físico en el eCM, manteniendo las prioridades QoS.

Apéndice IV

Restricciones de CM no conforme con L2VPN

El servicio L2VPN está implementado principalmente en el CMTS. Un operador puede desplegar servicios L2VPN utilizando un CMTS conforme y unos CM no conformes. Las restricciones cuando se utilizan CM no conformes son:

- Los abonados L2VPN con DOCSIS 1.1 no conforme y CM posteriores pueden no disponer de retransmisión transparente de multidifusiones IP. Esto es particularmente molesto cuando no se retransmiten avisos OSPF y RIPv2 a los encaminadores de las instalaciones del abonado. Los CM no conformes con DOCSIS 1.1 y 2.0 siguen cumpliendo las reglas de retransmisión de multidifusión IP por lo que bloquearán la retransmisión en sentido descendente de grupos de multidifusión IP disjuntos. No obstante, los CM DOCSIS 2.0 que implementan el parámetro MAC de multidifusión estática pueden programarse para retransmitir el tráfico de multidifusión deseado. Los CM no conformes con DOCSIS 1.0 no perderán este tráfico de multidifusión. Algunos suministradores de CM también ofrecen configuraciones propias para retransmitir todas las multidifusiones IP en sentido descendente.
- Las transmisiones que no son de difusión de capa 2 ni L2VPN no criptado escaparán por las redes CPE L2VPN. Para una descripción de este problema véase IV.1.
- Los CM no conformes pueden no retransmitir paquetes de tamaño máximo con un rótulo de abonado; es decir, con una longitud de 1522 bytes. El funcionamiento apilado o rótulo en rótulo puede no ser posible con estos CM.
- Los CM no conformes no pueden impedir que el tráfico L2VPN en sentido descendente alcance pilas IP y los anfitriones eSAFE incorporados de la CM L2VPN.

NOTA – El tráfico en *sentido ascendente* desde los eCM y (normalmente) los anfitriones eSAFE se bloquea, evitando el acceso bidireccional no autorizado.

- Los CM no conformes no pueden unir las L2VPN de forma dinámica, es decir, mediante mensajes de flujo de servicio dinámicos iniciados por el CMTS tras el registro. Los CM no conformes deben configurarse de forma estática para unir todas las L2VPN requeridas, basándose en las codificaciones L2VPN configuradas en su fichero de configuración CM o en el CMTS.

IV.1 Pérdidas a través de CM no conformes

Esta Recomendación no especifica ningún mecanismo para evitar las pérdidas de tráfico no criptado que no es L2VPN a través de CM *no conformes* configurados para la retransmisión L2VPN. El cuadro IV.1 resume las condiciones en las que transmisiones sentido descendente que no son de difusión ni L2VPN pueden perderse en una red de CPE de abonado, cuando un CM no conforme se configura para la retransmisión L2VPN.

Cuadro IV.1 – Pérdidas no L2VPN a través de CM no conformes configurados para L2VPN

Tipo de tráfico en sentido descendente	DIME	
	Habilitado	**Inhabilitado**
Difusiones Arp/DHCP (no criptadas)	Fuga	Fuga
Multidifusiones IP desunidas, por ejemplo, RIPv2, OSPF (no criptadas)	DOCSIS 1.0 CM: Fuga DOCSIS 1.1 CM: Bloqueado	DOCSIS 1.0 CM: Fuga DOCSIS 1.1 CM: Bloqueado
Multidifusión IP unida (criptada cuando DIME habilitado)	Bloqueado	DOCSIS 1.0 CM: Fuga DOCSIS 1.1 CM: Bloqueado
DSG (siempre sin criptar)	DOCSIS 1.0 CM: Fuga DOCSIS 1.1 CM: Bloqueado	DOCSIS 1.0 CM: Fuga DOCSIS 1.1 CM: Bloqueado

NOTA – Las fugas del tráfico de difusión no L2VPN no criptada (ARP y DHCP) en una red de abonado L2VPN normalmente no son un problema fundamental para el abonado ya que este tipo de tráfico es relativamente escaso. El tráfico de gran volumen de multidifusión IP unida se bloquea incluso a través de los CM no conformes cuando está criptado. Incluso las pérdidas de multidifusión no criptada a través de CM no conformes DOCSIS 1.0 se pueden evitar con filtros IP adecuados en el fichero de configuración del CM DOCSIS 1.0.

Bibliografía

[b-UIT-T J.126] Recomendación UIT-T J.126 (2004), *Especificación de dispositivos módem de cable incorporados*.

[b- UIT-T J.167] Recomendación UIT-T J.167 (2005), *Requisitos del aprovisionamiento de un dispositivo adaptador de terminal de medios para la entrega de servicios en tiempo real por redes de televisión por cable que utilizan módems de cable*.

[b- UIT-T J.192] Recomendación UIT-T J.192 (2005), *Pasarela residencial para soportar la entrega de servicios de datos por cable*.

[b-IETF RFC 2547] IETF RFC 2547 (1999), *BGP/MPLS VPNs*.

[b-IETF RFC 2674] IETF RFC 2674 (1999), *Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions*.

[b-IETF RFC 2685] IETF RFC 2685 (1999), *Virtual Private Network Identifier*.

[b-IETF RFC 3985] IETF RFC 3985 (2005), *Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*.

[b-IETF RFC 4363] IETF RFC 4363 (2006), *Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions*.

[b-IEEE 802.1D] IEEE Std 802.1D, *MAC bridges*.

[b-IEEE 802.1ah] IEEE Std 802.1ah, *Provider Backbone Bridges*.

[b-IEEE 802.1ad] IEEE Std 802.1ad, *Provider Bridges*.

[b-IEEE 802.1p] IEEE Std 802.1p, *Traffic Class Expediting and Dynamic Multicast Filtering*. (published in 802.1D-1998)

[b-IEEE 802.1s] IEEE Std 802.1s, *Multiple Spanning Trees*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	**Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia**
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2007