Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.213

(11/2006)

SÉRIE J: RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Services interactifs pour la distribution de télévision numérique

Réseaux privés virtuels de couche 2 pour les systèmes de câblo-modem IP

Recommandation UIT-T J.213

Recommandation UIT-T J.213

Réseaux privés virtuels de couche 2 pour les systèmes de câblo-modem IP

Résumé

La Recommandation UIT-T J.213 décrit les exigences applicables à la fois aux systèmes CMTS et aux câblo-modems afin d'implémenter une capacité de réseau privé virtuel de couche 2 conformément à la spécification DOCSIS (réseaux L2VPN-DOCSIS). La capacité de réseau L2VPN permet aux câblo-opérateurs d'offrir aux entreprises commerciales un service transparent de réseau local (TLS, *transparent LAN service*) dans la couche 2.

Source

La Recommandation UIT-T J.213 a été approuvée le 29 novembre 2006 par la Commission d'études 9 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T J.213

Réseaux privés virtuels de couche 2 pour les systèmes de câblo-modem IP

1 Introduction

La présente Recommandation décrit les exigences applicables aussi bien aux systèmes CMTS qu'aux câblo-modems afin d'implémenter un réseau privé virtuel de couche 2 conformément à la spécification de service DOCSIS (L2VPN-DOCSIS).

La capacité de réseau L2VPN permet aux câblo-opérateurs d'offrir aux entreprises commerciales un service transparent de réseau local (TLS) dans la couche 2, ce qui est un des principaux objectifs de l'initiative concernant les services commerciaux par spécification DOCSIS (BSoD).

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[IEEE 802.1Q] IEEE Std 802.1Q-2005, *Virtual Bridged Local Area Networks* (Réseaux locaux virtuels routés).

[UIT-T J.122] Recommandation UIT-T J.122 (2002), *Systèmes de transmission de deuxième génération pour les services interactifs de télévision par câble – Câblo-modems pour protocole IP*.

[UIT-T J.125] Recommandation UIT-T J.125 (2004), *Confidentialité des liaisons pour les implémentations de câblo-modems*.

3 Définitions

La présente Recommandation utilise les termes suivants en plus de ceux qui sont définis dans [UIT-T J.122].

3.1 réseau ponté: ensemble de réseaux locaux conformes à la norme IEEE 802 et interconnectés par ponts de commande MAC selon la spécification IEEE 802.1D.

3.2 câblo-modem conforme: câblo-modem qui implémente la présente Recommandation dans les réseaux L2VPN-DOCSIS.

3.3 unité L2PDU-DOCSIS: unité PDU en paquets dans une trame de commande MAC-DOCSIS, c'est-à-dire l'unité L2PDU qui suit un en-tête de commande MAC ayant la valeur FC_TYPE=00. Cette définition signifie qu'un message de gestion MAC ayant la valeur FC_TYPE=11 *n*'est *pas* considéré comme étant une unité L2PDU-DOCSIS, même si la forme d'un en-tête de message de gestion MAC est la même que celle d'une unité L2PDU.

3.4 trame de commande MAC-DOCSIS: unité de transmission à l'interface RFI-DOCSIS entre câble et réseau radioélectrique, composée d'un en-tête de commande MAC et d'une unité PDU de données (éventuellement vide). Le champ FC_TYPE de l'en-tête de commande MAC identifie

l'unité PDU de données comme étant soit une unité PDU en paquet (FC_TYPE=00), ou une unité PDU propre à la commande MAC (FC_TYPE=11).

3.5 élargissement: fonctionnement d'un pont L2 lorsqu'il réplique, vers tous les ports de pont autres que le port d'insertion de l'unité L2PDU, une unité L2PDU adressée à une adresse MAC collective ou à une adresse MAC individuelle mais non acquise par un port d'entrée.

3.6 adresse MAC collective (GMAC): adresse MAC de 6 octets conforme à l'IEEE, dont le premier bit transmis (le bit indicateur d'adresse collective) est réglé à 1, indiquant que l'adresse se rapporte à un groupe de serveurs locaux de commande MAC. Dans la représentation canonique des adresses MAC servant à la transmission par réseau Ethernet le bit indicateur d'adresse collective est le bit de poids faible du premier octet. L'adresse MAC diffusée sous la forme d'une série de chiffres 1 est considérée comme étant une adresse MAC collective (GMAC).

3.7 adresse MAC individuelle: adresse MAC de 6 octets conforme à l'IEEE dont le premier bit transmis (le bit indicateur d'adresse collective) est réglé à 0, indiquant que l'adresse se rapporte à un unique serveur local de commandes MAC. Pour les adresses MAC d'un réseau Ethernet-DOCSIS, le bit indicateur d'adresse collective est le bit de poids faible du premier octet de l'adresse MAC.

3.8 réexpéditeur dans la couche 2: élément de réseau qui réexpédie des paquets de couche 2, d'une interface de couche 2 à une autre interface de couche 2. Un réexpéditeur dans la couche 2 peut fonctionner soit en mode de réexpédition point à point, c'est-à-dire en ne faisant suivre les paquets qu'entre deux interfaces, sans acquisition intelligente; ou en mode multipoint, en ne faisant suivre les paquets à destination unidiffusée que vers l'interface à partir de laquelle une adresse MAC a été acquise.

3.9 interface de couche 2: port d'interface physique ou circuit virtuel sur lequel une unité L2PDU est transmise. Les ports d'interface physique de couche 2 sont les suivants: une interface NSI avec un réseau Ethernet dans un système CMTS, ou le port d'interface CMCI dans un câblo-modem. Les interfaces de couche 2 avec un circuit virtuel sont les suivants: une interface NSI entre réseau et système de terminaison (CMTS), une ligne privée (PW), et une association de sécurité par interface BPI entre système CMTS et câblo-modem unitaire. Une interface de couche 2 peut se faire attribuer un indice d'interface: ifIndex.

3.10 réseau privé virtuel dans la couche 2 (L2VPN): ensemble de réseaux locaux et de réexpéditeurs situés entre ces réseaux dans la couche 2, qui permet aux serveurs rattachés aux réseaux locaux de communiquer avec les unités de données de protocole de couche 2 (L2PDU). Un réseau L2VPN unique réexpédie les unités L2PDU sur la seule base de l'adresse MAC de destination (DMAC) de ces unités L2PDU, adresse qui reste transparente par rapport à toute adresse IP ou autre adresse de couche 3. Un domaine administratif de câblo-opérateur prend en charge de multiples réseaux L2VPN, un pour chaque entreprise d'abonnement à laquelle un service transparent de réseau local est offert.

3.11 identificateur de réseau L2VPN: chaîne d'octets qui identifie de façon unique un réseau L2VPN dans un domaine administratif de câblo-opérateur correspondant à une unique entreprise d'abonnement.

3.12 réexpéditeur dans la couche 3: élément de réseau qui réexpédie une unité PDU de couche 3, d'une interface avec le réseau d'insertion de flux jusqu'à une ou plusieurs interfaces avec le réseau d'extraction de flux. Cet élément est également appelé *routeur*.

3.13 unité de données protocolaire dans la couche 2 (L2PDU): séquence d'octets composée d'une adresse MAC de destination (DMAC), d'une adresse MAC d'origine (SMAC), (facultative) d'un ou plusieurs en-tête(s) contenant des balises, d'un champ indiquant le type de réseau Ethernet et sa longueur, d'une charge utile de couche 2, et du CRC.

3.14 acquisition intelligente: fonctionnement d'un pont de couche 2 lorsqu'il associe l'adresse MAC d'origine (SMAC) d'une unité L2PDU entrante au port de pont par lequel cette unité est arrivée.

3.15 réexpédition multipoint dans la couche: fonctionnement d'un réexpéditeur de couche 2 entre plusieurs réseaux de couche 2, qui ne réexpédie les paquets à adresse MAC de destination individuelle que vers l'interface à partir de laquelle une adresse MAC d'origine a été acquise et qui élargit les paquets à adresse MAC collective à toutes les interfaces.

3.16 câblo-modems non conformes: câblo-modem qui n'implémente pas la présente Recommandation dans les réseaux L2VPN-DOCSIS.

3.17 réexpédition point à point dans la couche 2: fonctionnement d'un réexpéditeur de couche 2 entre seulement deux réseaux de couche 2, sans aucune acquisition intelligente d'adresses MAC d'origine.

3.18 association de sécurité (SA, *security association*): association entre le système CMTS et un ensemble de câblo-modems situés dans un domaine de commande MAC, qui permet une communication chiffrée entre le système CMTS et l'ensemble des câblo-modems. Une association de sécurité à câblo-modem unique est réalisée avec un câblo-modem unique. Elle permet d'établir une connexion point à point privée dans la couche 2 d'un réseau, entre le système CMTS et le réseau local d'équipement CPE de ce câblo-modem. Un descripteur d'association de sécurité (ou "Descripteur-SA") est un élément de message à plusieurs parties qui est défini dans la confidentialité de base DOCSIS [UIT-T J.125] et qui contient un identificateur d'association de sécurité (SAID).

3.19 identificateur d'association de sécurité (SAID, *security association ID*): identificateur de 14 éléments binaires qui apparaît dans l'en-tête étendu d'interface BPI (BPI-EH) d'un paquet d'unité PDU-DOCSIS, afin d'identifier la clé servant à chiffrer le paquet.

3.20 en-tête contenant des balises: identificateur de protocole de balisage sur 16 éléments binaires (0x8100), suivi par un champ de commande de balisage sur 16 éléments binaires. Ce champ de commande de balisage se compose d'un champ de priorité d'utilisateur sur 3 éléments binaires, d'un fanion indicateur de format canonique et d'un identificateur de réseau local virtuel (VLAN) sur 12 éléments binaires [IEEE 802.1Q].

3.21 service transparent de réseau local (TLS, *transparent LAN service*): offre de service d'un câblo-opérateur qui met en œuvre un réseau privé L2VPN entre les réseaux par équipement CPE des câblo-modems d'une même entreprise d'abonnement.

3.22 réseau local virtuel (VLAN, *virtual LAN*): *sous-ensemble* des réseaux locaux d'un réseau ponté IEEE.802.1, auquel un identificateur de réseau local virtuel (VLAN) est attribué. Un réseau L2VPN peut se composer de plusieurs réseaux VLAN, chacun ayant un identificateur de réseau local virtuel différent; il peut même se composer de réseaux VLAN utilisant différents réseaux routés IEEE 802.1 avec le même identificateur de réseau local virtuel (VLAN).

3.23 identificateur de réseau local virtuel (VLAN-ID): un identificateur de réseau local virtuel (VLAN) selon la spécification IEEE 802.1Q est un nombre de 12 éléments binaires qui identifie un réseau VLAN à l'intérieur d'un réseau ponté IEEE.802.1. Un identificateur empilé de réseau local virtuel selon la spécification 802.1ah se compose d'un identificateur externe de réseau local virtuel de service selon la spécification 802.1ah codé sur 12 éléments binaires et d'un identificateur interne de réseau local virtuel de client codé sur 12 éléments binaires.

3.24 réseau L2VPN configurateur: réseau L2VPN pour le trafic de préinscription des protocoles DHCP, ToD et TFTP, qui configure les câblo-modems intégrés et les serveurs locaux d'entité eSAFE. Peut être combiné avec un réseau L2VPN gestionnaire.

3.25 réseau L2VPN gestionnaire: réseau L2VPN envoyant le trafic de post-inscription SNMP à des dispositifs de câblo-modem intégré ou d'entité eSAFE. Peut être combiné avec un réseau L2VPN configurateur.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

BPI	interface avec la confidentialité de base (*baseline privacy interface*)
BSoD	services commerciaux DOCSIS (*business services over DOCSIS*)
CMIM	masque d'interface avec un câblo-modem (*CM interface mask*)
CRC	contrôle de redondance cyclique
DIME	chiffrement multidiffusé en voie IP descendante (*downstream IP multicast encryption*)
DMAC	adresse MAC de destination (*destination MAC*)
DUT	trafic descendant non chiffré (*downstream unencrypted traffic*)
eCM	câblo-modem intégré [UIT-T J.126] (*embedded cable modem*)
eMTA	adaptateur de terminal multimédia intégré [UIT-T J.167] (*embedded media terminal adapter*)
ePS	services de portail intégrés [UIT-T J.192] (*embedded portal services*)
eSAFE	entité fonctionnelle intégrée de service ou d'application [b-UIT-T J.126] (*embedded service/application functional entity*)
GMAC	adresse MAC collective (*group MAC address*)
L2	couche 2 (*layer 2*)
L2VPN	réseau privé virtuel de couche 2 (*layer 2 virtual private network*)
MAC	commande d'accès au support physique (*media access control*)
SAID	identificateur d'association de sécurité (*security association identifier*)
SID	identificateur de service (en voie montante) ((*upstream*) *service identifier*)
SMAC	adresse MAC d'origine (*source MAC*)
TLS	service transparent de réseau local (*transparent LAN service*)
ToD	heure (*time of day*)
VPN	réseau privé virtuel (*virtual private nework*)

5 Conventions

5.1 Exigences

Dans l'ensemble de la présente Recommandation, les termes employés pour définir l'importance d'une prescription particulière sont imprimés en majuscules. Ce sont les suivants:

"DOIT"	Ce mot signifie que l'élément est une exigence absolue de la présente Recommandation.
"NE DOIT PAS"	Cette phrase signifie que l'élément est une interdiction absolue de la présente Recommandation.

"DEVRAIT" Ce mot signifie que, dans des circonstances particulières, il peut exister des raisons valables d'ignorer cet élément; mais il faut en comprendre toutes les implications et étudier attentivement le cas avant de choisir une voie différente.

"NE DEVRAIT PAS" Cette phrase signifie que, dans des circonstances particulières, il peut exister des raisons valables de considérer le comportement indiqué comme acceptable ou même utile; mais il faut en comprendre toutes les implications et étudier attentivement le cas avant d'implémenter un quelconque comportement décrit avec cette mention.

"PEUT" Ce mot signifie que cet élément est véritablement facultatif. Un vendeur peut choisir d'inclure l'élément, par exemple parce qu'un marché particulier le requiert ou parce qu'il améliore le produit; un autre vendeur peut omettre le même élément.

Certaines déclarations normatives exigent qu'un câblo-modem ou système CMTS ignore de façon transparente une situation qui pourra être définie dans de futures Recommandations. Une prescription visant à ignorer de façon transparente une situation signifie que le câblo-modem ou système CMTS:

- PEUT incrémenter une statistique propre au vendeur;
- NE DOIT PAS produire de message de journalisation;
- DOIT par ailleurs ignorer la situation et continuer à fonctionner comme si la situation ne s'était pas produite.

5.2 Conformité

Un système CMTS conforme à la spécification DOCSIS, qui revendique l'implémentation de la capacité L2VPN-DOCSIS, DOIT implémenter les dispositions normatives de la présente Recommandation. Un câblo-modem conforme à la spécification DOCSIS, qui revendique la conformité à la capacité L2VPN-DOCSIS, DOIT implémenter les exigences normatives de la présente Recommandation.

Un système CMTS ou un câblo-modem implémentant la présente Recommandation est déclaré *compatible avec un réseau L2VPN*. Dans le reste de la présente Recommandation, toutes les références à un système CMTS désignent un système CMTS compatible avec un réseau L2VPN. Un câblo-modem qui n'a pas implémenté la présente Recommandation est déclaré *incompatible avec un réseau L2VPN*.

Un système CMTS compatible avec un réseau L2VPN DOIT prendre en charge un câblo-modem incompatible avec un réseau L2VPN. Cela permet à un câblo-opérateur d'offrir le service d'abonné L2VPN avec les câblo-modems non conformes qui sont actuellement déployés. L'emploi de câblo-modems non conformes implique certaines limitations qui sont détaillées dans l'Appendice IV. L'emploi de câblo-modems conformes pour le service d'abonné L2VPN évite ces limitations. Les exigences permettant aux câblo-modems d'être conformes à la présente Recommandation dans les réseaux L2VPN sont résumées dans le § 8.

6 Fonctionnement théorique (article informatif)

6.1 Caractéristiques des réseaux L2VPN

La capacité d'implémenter l'accès à un réseau privé virtuel de couche 2 vers des ensembles arbitraires de câblo-modems permet d'activer un certain nombre d'éléments de service DOCSIS:

- service transparent de réseau local;
- réseaux L2VPN à multiples fournisseurs ISP;

- réseaux L2VPN de gestion.

6.1.1 Service transparent de réseau local

L'accès à des réseaux de transmission de données entre de multiples sites d'entreprises commerciales représente une notable opportunité d'affaires pour les câblo-opérateurs. Les réseaux commerciaux de transmission de données sont habituellement implémentés avec des connexions privées de transmission de données point à point telles que par relais de trames, RNIS, ou circuits virtuels en mode ATM, souvent avec un équipement qui assure une livraison transparente des paquets de réseau local Ethernet en couche 2. Un service qui interconnecte des réseaux locaux d'entreprise d'abonnement avec une réexpédition dans la couche 2 est appelé *service transparent de réseau local* (TLS).

L'interface RFI normalisée selon DOCSIS [UIT-T J.122] était initialement destinée à la connexion d'abonnés résidentiels au réseau IP public. La présente Recommandation normalise, sur la base de la spécification DOCSIS, le fonctionnement des systèmes CMTS et des câblo-modems dans les plans de commande et de données afin d'offrir un service transparent de réseau local à des entreprises commerciales d'abonnement.

Le terme de *service TLS* se rapporte à une offre de service particulière, faite aux clients d'une entreprise commerciale. La technologie particulière qui fournit ce service est appelée *réseau privé virtuel dans la couche 2* (L2VPN). Un câblo-opérateur offre le service TLS en implémentant un seul réseau L2VPN pour chaque entreprise commerciale.

Un exemple de service TLS commercial fondé sur la spécification DOCSIS est décrit dans la Figure 6-1 ci-après:

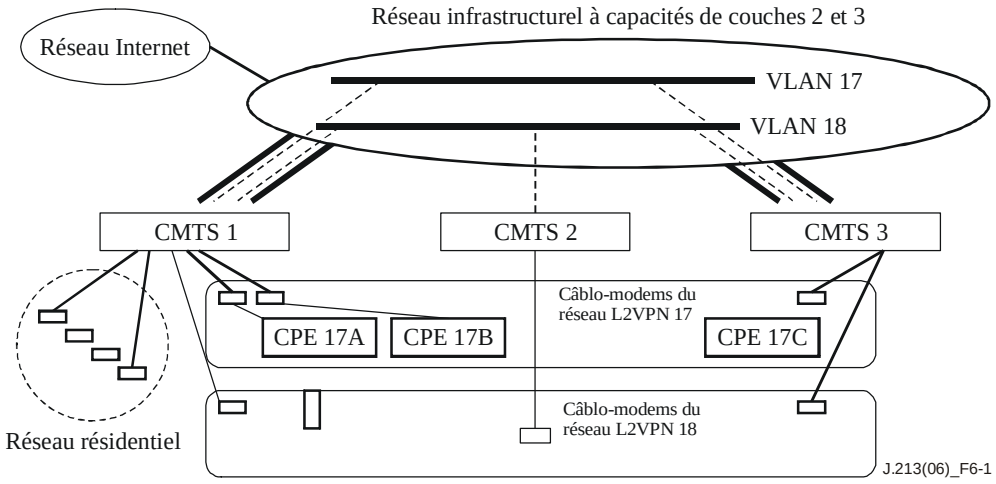

Figure 6-1 – Service transparent de réseau local

La Figure 6-1 décrit un service transparent de réseau local offert à deux entreprises commerciales: le premier est désigné par le terme de *réseau L2VPN 17* et le second par le terme de *réseau L2VPN 18*. Tous les systèmes CMTS ont l'ensemble habituel d'abonnés résidentiels, qui ne sont décrits que dans le système CMTS 1, lequel fournit le service de réseau L2VPN à deux câblo-modems dans le réseau L2VPN 17 et à un seul câblo-modem dans le réseau L2VPN 18. Le système CMTS 2 fournit le service de réseau L2VPN à un seul câblo-modem situé dans le réseau L2VPN. Le système CMTS 3 fournit ce service à un seul câblo-modem dans le réseau L2VPN 17 et à un autre dans le réseau L2VPN 18.

L'exemple montre que le réseau infrastructurel de couche 2 du câblo-opérateur implémente un unique réseau local virtuel (VLAN, *virtual LAN*) pour chaque client. Dans la présente Recommandation, le terme *réseau VLAN* possède une signification spécifique, dans la mesure où il

se rapporte à la définition de la spécification IEEE 802.1Q en tant que sous-ensemble de réseaux locaux situés à l'intérieur d'un réseau ponté, auquel est assigné un identificateur de 12 bits de réseau local virtuel (VLAN). Dans cet exemple, le système CMTS 1 encapsule directement dans un paquet Ethernet à balises IEEE 802.1Q, en leur attribuant une balise 17 d'identificateur de réseau local virtuel (VLAN), les paquets issus de la couche 2 du réseau L2VPN 17 en voie montante avant de les réexpédier vers le réseau infrastructurel du câblo-opérateur par un port de terminaison réseau d'une interface entre réseau Ethernet et système de terminaison (NSI, *network system interface*).

Dans cet exemple, le système CMTS 1 implémente la réexpédition multipoint dans la couche 2, de sorte qu'il est chargé du routage des paquets entre ses deux câblo-modems rattachés au réseau L2VPN 17. Cela implique l'acquisition intelligente des adresses MAC d'origine (SMAC, *source MAC*) des équipements CPE 17A et CPE 17B et leur association au câblo-modem auquel ces équipements CPE sont rattachés.

Le système CMTS 1 n'implémente qu'un seul circuit de rattachement au réseau VLAN 17 situé dans le réseau infrastructurel. Quand un paquet unidiffusé en voie descendante à partir du réseau VLAN 17 arrive au système CMTS 1, celui-ci recherche par exploration l'adresse MAC de destination (DMAC) dans sa base de données à acquisition intelligente puis réexpédie le paquet au câblo-modem correct.

Le système CMTS 3 ne peut implémenter que la réexpédition point à point dans la couche 2, lorsqu'il réexpédie en mode point à point transparent vers le réseau infrastructurel tous les paquets à adresse MAC individuelle ou collective, entre le câblo-modem rattaché à l'équipement CPE 17C et l'identificateur de réseau VLAN-IEEE 802.1Q 17, par son port de terminaison Ethernet à l'interface NSI.

Dans le réseau infrastructurel, un pont de câblo-opérateur dans la couche 2 connecte les diverses interfaces de jonction Ethernet du côté des systèmes CMTS et interconnecte chaque réseau VLAN. Le service TLS offert par l'opérateur au réseau L2VPN 17 assure le pontage d'une connexion en transparence dans la couche 2 entre les équipements CPE 17A, 17B et 17C. Du point de vue d'un client d'entreprise, de tels équipements CPE sont gérés et exploités comme s'ils étaient sur un réseau local de client privé. Habituellement, ils auront une adresse IP dans le sous-réseau IP dont l'entreprise est propriétaire. L'entreprise attribue habituellement l'adresse IP à chaque équipement CPE et charge normalement son propre serveur DHCP d'effectuer cette tâche. En fait, chaque entreprise peut utiliser en superposition le même espace de sous-réseau IP privé. Contrairement aux technologies des réseaux VPN de couche 3, le câblo-opérateur n'a pas besoin de coordonner, avec les clients de l'entreprise, l'attribution en sous-réseau des adresses IP. Du point de vue de l'opérateur, les abonnés au réseau local d'entreprise sont complètement isolés, dans la couche 2, de tous les autres abonnés résidentiels et de chaque autre réseau L2VPN.

Un service TLS d'entreprise peut comprendre non seulement les réseaux locaux rattachés aux câblo-modems, mais également tous les autres réseaux locaux pontés vers le réseau VLAN du client dans le pont IEEE 802.1Q situé à l'intérieur du réseau infrastructurel du câblo-opérateur.

6.1.2 Réseaux L2VPN à multiples fournisseurs ISP

La capacité de réseau L2VPN permet à un câblo-opérateur de prendre en charge de multiples fournisseurs de services IP (fournisseurs ISP) en offrant un réseau L2VPN distinct à chaque fournisseur ISP. Le câblo-opérateur assure la préconfiguration de tous les câblo-modems et le fichier de configuration du câblo-modem détermine un réseau L2VPN afin de réexpédier tout le trafic des équipements CPE. Chaque fournisseur ISP reçoit l'assignation d'un réseau L2VPN distinct. Le fournisseur ISP est chargé de fournir les serveurs de protocole DHCP et l'adressage IP relatif à tous les équipements CPE, dans les câblo-modems rattachés au réseau L2VPN de ces équipements.

L'avantage des réseaux L2VPN en exploitation à fournisseurs ISP multiples est que ces réseaux séparent complètement la gestion de l'espace d'adressage IP et le routage IP des fournisseurs ISP,

par rapport à ceux du câblo-opérateur. En revanche, les capacités de fournisseurs ISP multiples, utilisant des réseaux VPN de couche 3, nécessitent habituellement la coordination de la configuration d'attribution d'adresse IP et de la sécurité des routeurs situés entre l'extrémité fournisseur d'un opérateur MSO et l'extrémité client d'un fournisseur ISP.

6.1.3 Réseaux L2VPN de gestion

La capacité L2VPN-DOCSIS permet à un système CMTS de n'implémenter un réseau L2VPN que pour la configuration et la gestion de câblo-modems intégrés (eCM) et d'entités fonctionnelles intégrées de service/d'application (eSAFE) [b-UIT-T J.126] telles qu'un adaptateur de terminal multimédia incorporé (eMTA) [b-UIT-T J.167] ou des fonctionnalités de services de portail intégrés (ePS) [b-UIT-T J.192]. L'implémentation d'un réseau L2VPN distinct pour la configuration et la gestion du trafic d'un câblo-modem intégré et d'une entité eSAFE isole ces dispositifs par rapport au réseau IP et à l'abonné, ce qui augmente la sécurité.

Avant son inscription, le câblo-modem émet un identificateur SID temporaire et tout le trafic de ce type est considéré comme étant réexpédié par le réexpéditeur de flux non L2VPN. Un système CMTS pourra être implémenté de façon à réexpédier le trafic de préinscription vers un unique réseau L2VPN configurateur, lequel sera configuré de façon spécifique par le vendeur.

Quand un câblo-modem s'inscrit, il lit dans son fichier de configuration les codages L2VPN qui peuvent configurer les dispositifs câblo-modem intégré et eSAFE de façon à assurer la réexpédition dans un réseau L2VPN. Ce réseau L2VPN de post-inscription est appelé *réseau L2VPN gestionnaire* parce que le trafic de post-inscription est essentiellement en protocole SNMP afin de gérer le dispositif.

6.1.4 Autres capacités activées dans un réseau L2VPN

Certains éléments de service requis par la présente Recommandation apportent des améliorations à l'exploitation mondiale de la spécification DOCSIS, sans autre rapport avec les réseaux VPN de couche 2:

- classification fondée sur l'interface;
- filtrage du trafic DUT;
- activation de la commande de surveillance du trafic DHCP par entité eSAFE.

La classification fondée sur l'interface permet de classifier les paquets conformément à l'interface avec le port interne ou externe du pont de câblo-modem. Elle est décrite dans le § 7.6.5. Cet élément de service peut par exemple servir à classifier des paquets à destination ou en provenance de l'interface avec l'agent MTA intégré, sans dépendre du sous-réseau IP particulier de cette interface.

Le filtrage du trafic descendant non chiffré (DUT, *downstream unencrypted traffic*) est applicable au fonctionnement d'un réseau L3VPN propre au vendeur du système CMTS afin d'empêcher que le trafic d'adresses MAC collectives, qui est diffusé vers les câblo-modems résidentiels, ne s'échappe vers les réseaux, censés être privés, des équipements CPE d'abonnés au réseau L3VPN. Le filtrage du trafic DUT est décrit dans le § 7.5.2.1.

La commande de surveillance du trafic DHCP est un nuplet TLV explicite qui autorise le système CMTS à acquérir automatiquement l'adresse MAC des serveurs locaux intégrés dans les entités eSAFE, comme les agents eMTA, par intrusion dans leur trafic DHCP. Cette commande peut être utilisée dans le cadre des éléments de service propres au vendeur du système CMTS qui réexpédient d'une façon particulière des paquets DHCP ou d'autres paquets issus des serveurs locaux d'entité eSAFE. L'élément de service de commande d'activation de la surveillance du trafic DHCP par entité eSAFE est décrit dans le § 7.6.4.1.

6.2 Architecture de réexpédition par un système CMTS dans la couche 2

6.2.1 Réexpédition par réseaux L2VPN et par réseaux non L2VPN

Un système CMTS est considéré comme ayant un réexpéditeur de paquets entièrement distinct pour la réexpédition L2VPN: ce dispositif diffère du réexpéditeur de flux non L2VPN pour le trafic résidentiel, comme décrit dans la Figure 6-2 ci-dessous:

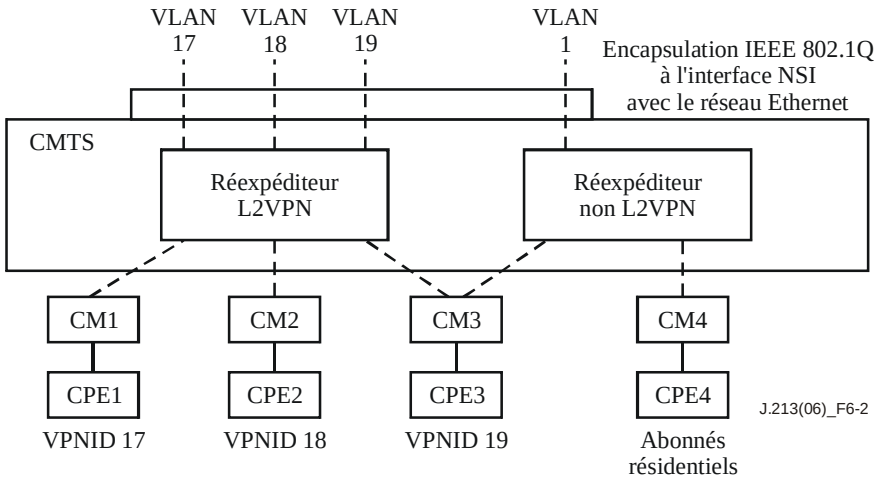

Figure 6-2 – Réexpédition par réseaux L2VPN et par réseaux non L2VPN

Afin de prendre en charge le fonctionnement d'un réseau L2VPN, une interface entre réseau et système CMTS (interface NSI) doit être capable de distinguer le trafic en voie descendante d'un réseau L2VPN du trafic en voie descendante d'un réseau non L2VPN. Elle doit également être capable de déterminer le réseau L2VPN acheminant le trafic en voie descendante. Le format d'encapsulation du trafic d'un réseau L2VPN aux ports d'interface NSI d'un système CMTS et les valeurs de champ particulières qui distinguent, dans cette encapsulation, un réseau L2VPN particulier, sont appelés *informations d'encapsulation du trafic d'un réseau L2VPN à l'interface NSI*. Dans l'exemple qui précède, les balises d'identificateur de réseau VLAN-IEEE 802.1Q sont utilisées comme format d'encapsulation du trafic d'un réseau L2VPN à un port d'interface NSI avec un réseau Ethernet.

En général, les trafics L2VPN et non L2VPN sont multiplexés au même port d'interface NSI. Dans l'exemple qui précède, le système CMTS implémente une interface avec un routeur IP non L2VPN au niveau de l'identificateur de réseau VLAN 1, qui peut même être le réseau VLAN initial, avec une encapsulation non balisée. Le trafic résidentiel, comme l'équipement CPE4 connecté au câblo-modem CM4, continue à être routée au moyen du réexpéditeur de routage IP du système CMTS vers la sous-interface du routeur situé au niveau de l'identificateur de réseau VLAN 1. Les autres équipements CPE, cependant, sont pontés dans la couche 2 à partir de l'interface du câblo-modem avec le réseau Ethernet vers un identificateur configuré de réseau VLAN-802.1Q au niveau du port d'interface NSI. Dans la Figure 6-2 ci-dessus, le système CMTS implémente un modèle de réexpédition point à point lorsqu'il réexpédie: le trafic d'équipement CPE à partir du câblo-modem CM1 vers l'identificateur 17 de réseau VLAN-802.1Q, le trafic d'équipement CPE à partir du câblo-modem CM2 vers l'identificateur 18 de réseau VLAN-802.1Q, et le trafic d'équipement CPE à partir d'un des flux de service en voie montante du câblo-modem CM3 vers l'identificateur 19 de réseau VLAN-802.1Q. L'autre flux de service en voie montante du câblo-modem CM3 est renvoyé au réexpéditeur de flux non L2VPN.

En voie montante, le système CMTS différencie le trafic L2VPN du trafic non L2VPN sur la base du flux de service en voie montante par lequel le trafic arrive et sur la base de l'adresse MAC d'origine de ce trafic. Certains flux de service en voie montante sont configurés avec des codages de

réexpédition L2VPN qui identifient un réseau L2VPN particulier. Le codage L2VPN contient un masque d'interface avec un câblo-modem (CMIM) qui identifie les serveurs locaux du côté câblo-modem qui réexpédient en voie montante vers le réseau L2VPN. Par défaut, seuls les serveurs locaux d'équipement CPE rattachés à l'interface CMCI d'un câblo-modem réexpédient vers un réseau L2VPN; le câblo-modem et ses serveurs locaux intégrés dans une entité eSAFE ne réexpédient pas vers un réseau L2VPN.

Un flux de service configuré de façon à réexpédier le trafic d'équipement CPE vers un réseau L2VPN est considéré comme étant un circuit de rattachement dans le contexte du service IETF de LAN privé virtuel (VPLS). Un réexpéditeur L2VPN d'un service VPLS dans un système CMTS est chargé de faire suivre les paquets entre circuits de rattachement et lignes privées par des ports d'interface NSI (p. ex. par commutation MPLS ou par tunnels L2TPv3).

6.2.2 Modes de réexpédition par réseaux L2VPN point à point et multipoint

La présente Recommandation utilise le terme *réexpédition dans la couche 2* plutôt que *pontage* parce que le service commercial de réseau L2VPN peut être offert sans nécessairement implémenter un pont de couche MAC d'acquisition intelligente dans le système CMTS comme défini par la spécification IEEE 802.1Q. Le système CMTS PEUT implémente un mode de réexpédition point à point dans la couche 2 qui réexpédie les paquets entre un unique port d'interface NSI et un câblo-modem (ou flux de service) unique. Si le système CMTS implémente effectivement un pont de couche MAC d'acquisition intelligente entre interfaces NSI et RFI, la présente Recommandation le désigne par le terme de *mode de réexpédition multipoint dans la couche 2*.

Dans le mode de réexpédition point à point par réseau L2VPN, chaque circuit de rattachement possède une valeur différente d'encapsulation du trafic à l'interface NSI. Par exemple, avec une encapsulation IEEE 802.1Q, chaque circuit de rattachement (c'est-à-dire chaque câblo-modem ou flux de service) est configuré avec un identificateur différent de réseau VLAN-802.1Q. En mode point à point, le réexpéditeur L2VPN réexpédie simplement les données en voie montante et en voie descendante entre un port d'interface NSI et un circuit de rattachement, sans acquisition intelligente des adresses MAC des paquets d'équipement CPE. L'identificateur logique VPNID auquel un câblo-modem ou un flux de service se rattache devrait être configuré avec le circuit de rattachement, mais sa valeur est par ailleurs ignorée par le système CMTS en mode de réexpédition point à point. Un pont L2VPN externe situé dans le réseau infrastructurel du câblo-opérateur exécute effectivement l'acquisition intelligente d'adresses MAC dans la couche 2 pour chaque réseau L2VPN puis il ponte les paquets entre les identificateurs de réseau VLAN ou entre les pseudo-circuits des paquets contenus dans leur encapsulation à l'interface NSI.

Un exemple de mode de réexpédition point à point est décrit dans la Figure 6-3 ci-dessous:

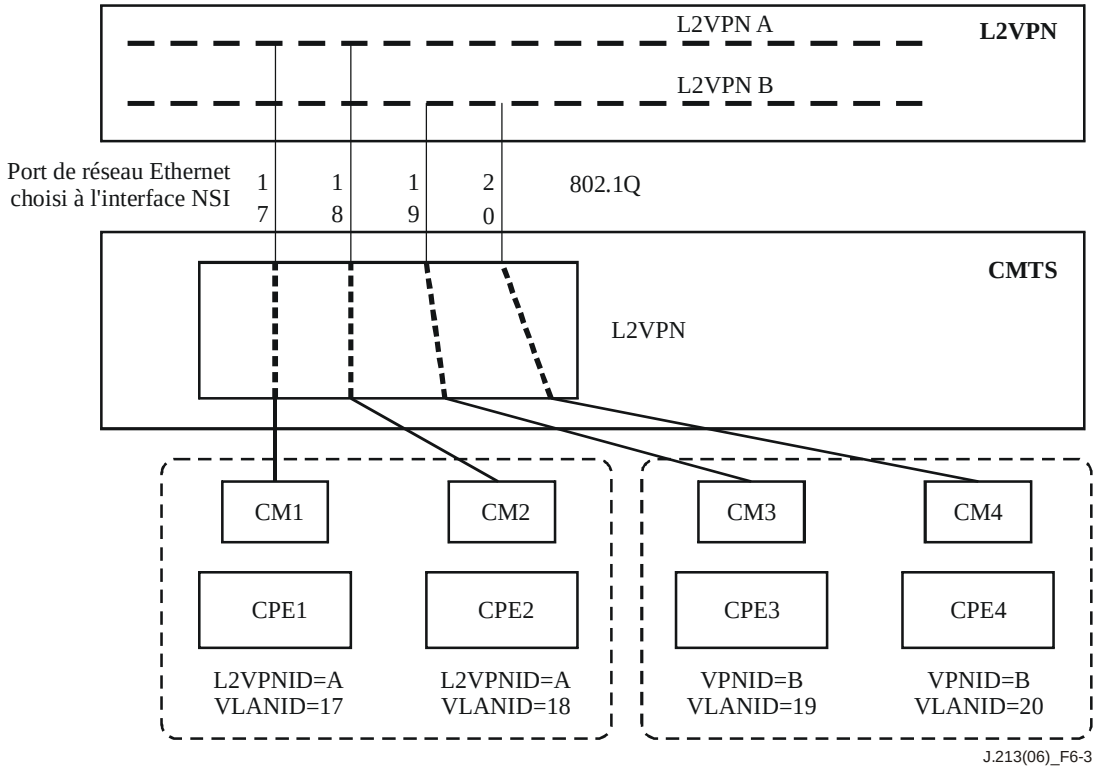

Figure 6-3 – Mode de réexpédition point à point

Quatre câblo-modems sont configurés pour fonctionner en réseau L2VPN. Chaque codage L2VPN dans un câblo-modem contient un identificateur logique VPNID A ou B, assorti d'un sous-type d'encapsulation de flux à l'interface NSI configuré statiquement, qui configure l'utilisation de la spécification IEEE 802.1Q avec un identificateur de réseau VLAN différent pour chaque câblo-modem (identificateurs de réseau VLAN de 17 à 20). Le réexpéditeur L2VPN du système CMTS réexpédie le trafic à partir du port d'interface NSI sur ces identificateurs de réseau VLAN en mode point à point, à destination et en provenance du câblo-modem configuré. Bien que le réexpéditeur L2VPN en mode point à point n'utilise pas la configuration de l'identificateur VPNID, il doit cependant être configuré dans chaque codage de réexpédition L2VPN à titre d'information minimale. Un commutateur de pont L2VPN, extérieur au système CMTS, est configuré dans la couche 2 afin de traiter les encapsulations de flux à l'interface NSI pour les identificateurs de réseau VLAN 17 et 18 en tant que ports logiques de pont distincts pour le réseau L2VPN A et afin d'acquérir des adresses MAC d'équipement CPE sur ces ports de pont. De même, le pont L2VPN externe est configuré de façon à considérer les encapsulations avec les identificateurs de réseau VLAN 19 et 20 comme étant des ports de pont distincts du domaine de diffusion qui est le réseau L2VPN B.

Le mode de réexpédition point à point des encapsulations IEEE 802.1Q à l'interface NSI limite à 4093 le nombre de câblo-modems d'abonné L2VPN pris en charge par un système CMTS, en raison de la longueur limitée à 12 éléments binaires d'un identificateur de réseau VLAN-IEEE 802.1Q.

Le mode de réexpédition multipoint signifie que le système CMTS réexpédie les paquets L2VPN en voie descendante vers des câblo-modems pouvant être multiples. Le système CMTS construit une base de données de réexpédition dans la couche 2 (base FDB) contenant les adresses MAC d'équipement CPE qu'il acquiert à partir de l'adresse MAC d'origine des paquets en voie montante. Un réexpéditeur multipoint L2VPN utilise cette base FDB afin de sélectionner le câblo-modem qui sera chargé de réexpédier le trafic L2VPN en voie descendante. Si la destination est une adresse MAC collective, ou est une adresse MAC individuelle inconnue, un réexpéditeur multipoint L2VPN élargit le trafic à tous les circuits de rattachement et ports d'interface NSI autres que celui par lequel

le paquet a été reçu. Un réexpéditeur multipoint L2VPN réexpédie directement les paquets entre les circuits de rattachement (câblo-modems ou flux de service) configurés avec le même réseau L2VPN logique.

Avec la réexpédition multipoint, une valeur d'encapsulation du trafic à l'interface NSI n'est requise que pour chaque réseau L2VPN logique et non pour chaque circuit de rattachement. Cela permet la prise en charge d'un nombre quelconque de *modems* par le service de réseau L2VPN, parce que l'identificateur de 12 bits de réseau VLAN-IEEE 802.1Q, utilisé comme valeur d'encapsulation du trafic à l'interface NSI, ne limitera que le nombre de *réseaux* L2VPN d'entreprise.

Un exemple du mode de réexpédition multipoint est décrit dans la Figure 6-4 ci-dessous.

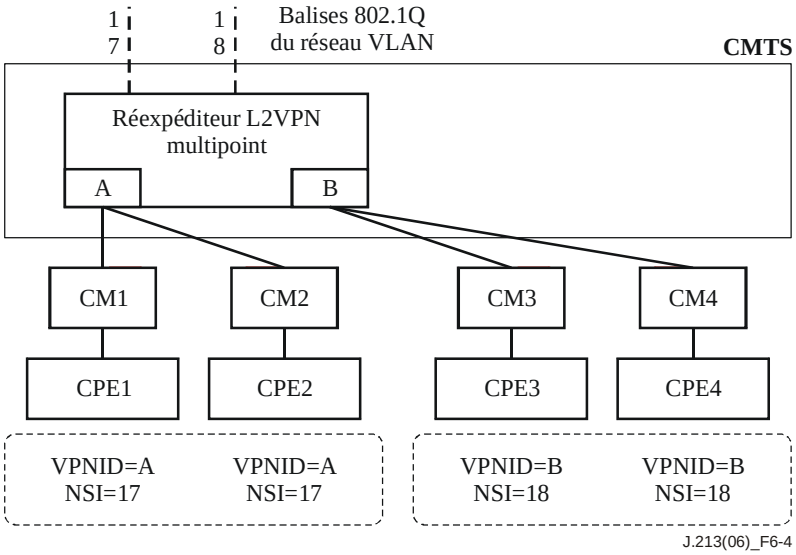

Figure 6-4 – Exemple de mode de réexpédition multipoint L2VPN

Dans cet exemple, les câblo-modems CM1 et CM2 sont tous les deux configurés pour la réexpédition L2VPN vers l'identificateur VPNID A et sont configurés de façon à utiliser une encapsulation de flux à l'interface NSI désignée par l'identificateur 17 de réseau VLAN-IEEE 802.1Q. Le réexpéditeur multipoint L2VPN acquiert les adresses MAC des équipements CPE1 et CPE2 afin de déterminer à quel câblo-modem il convient de réexpédier le trafic undiffusé en voie descendante et reçu du port correspondant à l'identificateur de réseau VLAN 17. De même, les câblo-modems CM3 et CM4 sont configurés avec l'identificateur VPNID B de façon à utiliser l'identificateur 18 de réseau VLAN-IEEE 802.1Q comme représentant leur encapsulation de flux à l'interface NSI. Le réexpéditeur multipoint L2VPN acquiert les adresses MAC des équipements CPE3 et CPE4 dans le réseau L2VPN B. Le réexpéditeur de flux non L2VPN n'est pas représenté dans la Figure 6-4.

La présente Recommandation permet la qualification des systèmes CMTS avec les modes de réexpédition point à point ou multipoint. Les essais de qualification DOCSIS doivent utiliser le mode de réexpédition indiqué par la soumission PICS du vendeur pour tous les réseaux L2VPN. La présente Recommandation est rédigée en supposant qu'un système CMTS choisit l'un de ces deux modes pour tous les réseaux L2VPN. Il n'y a cependant aucune prescription qui empêcherait un vendeur d'implémenter différents modes de réexpédition dans différents ensembles de réseaux L2VPN.

7 Fonctionnement d'un réseau L2VPN

7.1 Exigences relatives au modèle de pontage par système CMTS

Le système CMTS DOIT réexpédier de façon transparente, vers des ports d'interface NSI configurés de façon à encapsuler des paquets dans un réseau L2VPN particulier, les unités L2PDU-DOCSIS reçues à partir d'un flux de service en voie montante configuré de façon à recevoir des paquets pour ce réseau L2VPN. Le système CMTS DOIT réexpédier de façon transparente, vers une unité L2PDU DOCSIS en voie descendante chiffrée dans un identificateur SAID unique pour le réseau L2VPN et pour le câblo-modem auxquels les paquets sont réexpédiés, les paquets reçus avec une encapsulation de flux à l'interface NSI configurée dans un réseau L2VPN particulier.

Un système CMTS DEVRAIT implémenter une fonction de pontage à capacité de réseau VLAN comme spécifié par l'IEEE 802.1S. Aux fins de la conformité à la spécification 802.1S, chaque port de pont implémenté à une interface RFI DEVRAIT être considéré comme étant une interface 802.1Q entièrement balisée pour laquelle l'identificateur entrant de réseau VLAN est déterminé par l'identificateur SID en voie montante, et pour laquelle l'identificateur sortant de réseau VLAN est balisé avec un identificateur SAID d'interface BPI. Un système CMTS compatible avec un réseau L2VPN NE DOIT PAS insérer de balise 802.Q dans les paquets descendant vers une interface RFI.

Le système CMTS PEUT restreindre la configuration d'une valeur de multiplexage du service d'encapsulation à l'interface NSI (p. ex. l'identificateur de réseau VLAN-IEEE 802.1Q) à un unique flux de service. Dans ce mode de réexpédition point à point, le système CMTS PEUT omettre l'acquisition intelligente d'adresses MAC d'équipement CPE à insérer dans une base de données de réexpédition. Un système CMTS point à point DOIT prendre en charge de multiples codages L2VPN par flux de service individuel avec le même sous-type d'encapsulation de flux à l'interface NSI tant qu'ils sont sur le même câblo-modem.

Si le système CMTS permet que plus d'un seul flux de service soit configuré de façon à ponter vers la même valeur de multiplexage du service d'encapsulation à l'interface NSI, ce système est réputé implémenter le mode de réexpédition multipoint. Dans le mode de réexpédition multipoint, le système CMTS DOIT associer les adresses MAC d'origine des équipements CPE au câblo-modem particulier à partir duquel elles ont été acquises.

Un système CMTS DOIT prendre en charge à la fois la réexpédition par réseaux L2VPN et la réexpédition par réseaux non L2VPN dans le même domaine d'adresses MAC à l'interface RFI. Un système CMTS DOIT ponter en transparence le trafic d'équipement CPE à partir des câblo-modems configurés avec des codages L2VPN conformes à la présente Recommandation. Un système CMTS DOIT réexpédier le trafic d'équipement CPE issu des câblo-modems sans aucun codage par réseau L2VPN, avec ses algorithmes de réexpédition normaux de réexpédition de paquets non L2VPN, sauf spécification contraire dans la présente Recommandation.

Un système CMTS DOIT prendre en charge la réexpédition du trafic en voie montante par réseaux aussi bien L2VPN que non L2VPN à partir de différents flux de service quand seuls des codages L2VPN par flux de service individuel sont signalés.

7.2 Configuration de la réexpédition L2VPN

Un ensemble d'un ou de plusieurs réglages de configuration de codage L2VPN, contenu dans un fichier de configuration de câblo-modem, détermine si nécessaire la façon dont le système CMTS exécute la réexpédition en voie montante ou descendante des paquets d'équipement CPE par réseau L2VPN.

Le paramètre de codage L2VPN est codé sous la forme d'un paramètre d'informations générales d'extension (informations GEI, *general extension information*), c'est-à-dire qu'il est codé comme un sous-type du paramètre d'informations propres au vendeur de type 43, au moyen de l'identificateur de vendeur 0xFFFFFF (voir § C.1.1.17 de [UIT-T J.122]). Le codage L2VPN sous forme de

paramètre d'informations GEI permet de l'inclure dans le fichier de configuration de tout câblo-modem conforme à la spécification DOCSIS, y compris les câblo-modems DOCSIS 1.0.

Le paramètre de codage L2VPN peut apparaître aux emplacements suivants:

- au niveau supérieur d'un fichier de configuration de câblo-modem, auquel cas il est appelé *codage L2VPN par câblo-modem individuel*;
- en tant que sous-type d'un paramètre d'informations GEI intégré dans un codage de flux de service en voie montante (type 24), auquel cas il est appelé *codage L2VPN dans chaque flux de service ou réexpédition*;
- en tant que sous-type d'un paramètre d'informations GEI intégré dans un réglage de configuration de classificateur de paquet en voie descendante (type 23), auquel cas il est appelé *codage L2VPN par classificateur en voie descendante*;
- en tant que sous-type d'un paramètre d'informations GEI intégré dans un réglage de configuration de classification de paquet en voie montante (type 22), auquel cas il est appelé *codage L2VPN par classificateur en voie montante*.

Le paramètre de codage L2VPN proprement dit est défini comme un paramètre multivalent avec plusieurs paramètres de sous-type intégrés. Le Tableau 7-1 ci-dessous énumère chacun de ces sous-types et indique à quel emplacement chaque sous-type est défini, selon ce qui est nécessaire ou facultatif pour cet emplacement.

Tableau 7-1 – Localisation du sous-type de codage dans le réseau L2VPN (résumé)

Numéro du sous-type	Paramètre de sous-type	Niveau supérieur (par CM)	Flux de service en voie montante	Classificateur en voie descendante	Classificateur en voie montante
43.5.1	Identificateur de réseau VPN	Requis	Requis	Requis	
43.5.2	Encapsulation de flux à l'interface NSI	Facultatif [c)]			
43.5.3	Activation de la surveillance du trafic DHCP par entité eSAFE	Facultatif [a)]			
43.5.4	Masque d'interface avec un câblo-modem	Facultatif		Facultatif [a)]	Facultatif [a)]
43.5.5	Identificateur collectif de rattachement	Facultatif [c)]			
43.5.6	Identificateur individuel de rattachement à l'origine	Facultatif [c)]			
43.5.7	Identificateur individuel de rattachement à la destination	Facultatif [c)]			
43.5.8	Priorité d'insertion de l'utilisateur dans un flux		Facultatif		
43.5.9	Niveaux de priorité d'un utilisateur			Facultatif	

Tableau 7-1 – Localisation du sous-type de codage dans le réseau L2VPN (résumé)

Numéro du sous-type	Paramètre de sous-type	Niveau supérieur (par CM)	Flux de service en voie montante	Classificateur en voie descendante	Classificateur en voie montante
43.5.10	Descripteur d'association de sécurité L2VPN	Requis [b)]			
43.5.43	Propre au vendeur	Facultatif	Facultatif	Facultatif	Facultatif

[a)] Le système CMTS DOIT accepter un paramètre identifié comme *facultatif dans ce tableau* dans un codage de réexpédition par réseau non L2VPN.

[b)] Le système CMTS insère le sous-type de descripteur d'association de sécurité L2VPN dans son premier message à un câblo-modem figurant dans tout message de gestion d'adresse MAC qui contient un codage de réexpédition L2VPN; le sous-type de descripteur d'association de sécurité L2VPN n'est pas configuré dans un fichier de configuration de câblo-modem.

[c)] Il s'agit d'une configuration pour chaque réseau L2VPN au niveau du port d'interface NSI, qui n'est définie qu'en mode de réexpédition point à point dans un codage L2VPN par câblo-modem individuel.

Si un sous-type n'est pas défini comme étant "Requis" ou "Facultatif" à un emplacement, le système CMTS DEVRAIT l'ignorer de façon transparente quand il apparaît à cet emplacement. Si un sous-type n'est pas défini comme étant requis ou facultatif à un emplacement, le câblo-modem DEVRAIT l'ignorer de façon transparente quand il apparaît à cet emplacement. Un système CMTS DOIT ignorer de façon transparente les sous-types non reconnus dans un codage L2VPN. Un câblo-modem DOIT ignorer de façon transparente les sous-types non reconnus dans un codage L2VPN.

Le codage L2VPN de niveau supérieur commande le comportement de CM et de CMTS pour chaque réseau L2VPN particulier. Le codage de flux de service en voie montante L2VPN spécifie quel ou quels flux de service en voie montantes vont transporter le trafic L2VPN. Le fonctionnement correct d'un réseau L2VPN nécessite qu'au moins un seul flux de service en voie montante soit configuré pour la réexpédition L2VPN.

Etant donné que de multiples flux de service en voie montante peuvent être configurés de façon à réexpédier vers le même réseau L2VPN, tous les paramètres de réseau L2VPN particulier qui sont communs à ce même réseau L2VPN sont insérés dans l'unique codage L2VPN de niveau supérieur plutôt que d'exiger ou de permettre qu'ils soient dupliqués dans de multiples codages de flux de service en voie montante.

La réexpédition L2VPN en voie montante est configurée par flux de service individuel. Le câblo-opérateur peut configurer au moins un seul flux de service en voie montante, à l'intérieur d'un fichier de configuration de câblo-modem contenant un codage L2VPN qui définit l'identificateur de réseau VPN vers lequel le système CMTS réexpédie en voie montante le trafic issu de ce flux de service. Le codage par câblo-modem individuel ou par niveau supérieur de réseau L2VPN n'est requis dans un fichier de configuration de câblo-modem qu'en mode de réexpédition point à point, afin de définir le format d'encapsulation de flux à l'interface NSI pour ce réseau L2VPN de façon que le système CMTS puisse déterminer à quel câblo-modem il convient de réexpédier le trafic L2VPN en voie descendante. Avec le mode de réexpédition multipoint dans un réseau L2VPN, de multiples câblo-modems peuvent réexpédier vers de multiples encapsulations de flux à l'interface NSI, de sorte qu'une configuration d'encapsulation de flux à l'interface NSI n'est pas définie individuellement pour chaque câblo-modem.

Le plus simple fichier de configuration de câblo-modem pour le fonctionnement en réseau L2VPN contient les éléments suivants:

- en mode multipoint, un unique codage L2VPN par flux de service individuel dans la définition du flux de service primaire en voie montante;
- en mode point à point, un unique codage L2VPN par flux de service individuel dans la définition du flux de service primaire en voie montante, ainsi qu'un unique codage L2VPN par câblo-modem individuel avec un sous-type d'encapsulation de flux à l'interface NSI pour ce réseau L2VPN.

Dans un message de réponse d'inscription, le système CMTS contient toujours un codage L2VPN (ajouté si nécessaire) dans chaque câblo-modem. Ce codage fournit au moins un seul descripteur d'association de sécurité L2VPN pour chiffrer et baliser les paquets en voie descendante comme constituant le trafic L2VPN pour le câblo-modem. Le système CMTS PEUT attribuer plus d'un seul identificateur SAID au même réseau L2VPN, auquel cas de multiples sous-types de descripteur d'association de sécurité L2VPN peuvent apparaître dans un codage L2VPN de niveau supérieur.

Sauf configuration contraire, le système CMTS livre le trafic L2VPN en voie descendante à un unique câblo-modem par le flux de service primaire en voie descendante de ce câblo-modem. L'opérateur peut spécifier dans le fichier de configuration du câblo-modem une qualité de service renforcée (QS) pour le trafic L2VPN en voie descendante avec un flux de service en voie descendante distinct pour la réexpédition L2VPN. Ce trafic L2VPN en voie descendante peut être classifié selon ce flux de service descendant particulier en définissant un classificateur contenant un codage L2VPN de classificateur en voie descendante faisant référence à ce flux de service.

Le système CMTS DOIT rejeter l'inscription d'un câblo-modem possédant un codage non valide de réseau L2VPN. Une configuration valide de câblo-modem contient un nombre quelconque de codages L2VPN par flux de service individuel, de codages L2VPN de classificateur en voie descendante et de codages L2VPN de classificateur en voie montante. Le système CMTS DOIT accepter un demande d'inscription de câblo-modem qui contient de multiples codages L2VPN par flux de service individuel qui réexpédient vers le même identificateur de réseau privé virtuel (VPN).

Un codage valide L2VPN par flux de service individuel apparaît comme un sous-type dans le codage de flux de service en voie montante (type 24) d'un message de fichier de configuration de câblo-modem DOCSIS 1.1, REG-REQ, DSA-REQ, ou DSC-REQ. Le codage L2VPN de réexpédition par flux de service individuel configure le système CMTS de façon à exécuter la réexpédition par pont L2VPN de tous les paquets d'équipement CPE reçus dans le flux de service décrit. Un codage valide de réexpédition L2VPN par flux de service individuel contient un seul sous-type d'identificateur de réseau L2VPN. Le système CMTS contient un codage L2VPN par câblo-modem individuel dans son message REG-RSP. Après inscription, un câblo-modem PEUT inclure des codages L2VPN par câblo-modem individuel dans le niveau supérieur des messages de gestion dynamique des adresses MAC de service qui par ailleurs ajoutent, modifient, ou suppriment des codages L2VPN de réexpédition par flux de service individuel.

Afin de configurer des adresses MAC particulières d'équipement CPE pour la réexpédition L2VPN, le câblo-modem peut être configuré avec des codages de classification de paquet en voie montante qui concordent avec l'adresse MAC d'équipement CPE d'origine recherchée. Le câblo-modem classifie le paquet de façon à aller vers un flux de service en voie montante qui est configuré de façon à réexpédier ce paquet vers un réseau L2VPN particulier. Le codage de classification de paquet en voie montante faisant référence à un codage L2VPN de réexpédition par flux de service en voie montante ne contient pas de sous-type d'identificateur VPNID proprement dit.

Le système CMTS DOIT considérer qu'un flux de service en voie montante doit être configuré pour réexpédition L2VPN par flux de service individuel quand un message REG-REQ, DSA-REQ ou DSC-REQ contient exactement un seul codage valide de réexpédition L2VPN par flux de service individuel dans un codage de flux de service en voie montante. Un codage valide de réexpédition

L2VPN par flux de service individuel contient un seul sous-type d'identificateur VPNID. Le système CMTS DOIT rejeter une transaction par flux de service qui contient plus d'un seul codage L2VPN par flux de service individuel.

Le système CMTS DOIT accepter un message valide DSC-REQ contenant un codage valide L2VPN par flux de service individuel et modifier en conséquence le traitement de réexpédition en voie montante des paquets reçus à partir de ce flux de service. Cela implique, p. ex., l'adjonction, la modification ou la suppression de tout sous-type autorisé de codage L2VPN par flux de service individuel, y compris le sous-type d'identificateur de réseau VPN.

Le système CMTS DOIT supprimer la réexpédition L2VPN par un flux de service individuel quand celui-ci est supprimé par une transaction valide de suppression de service dynamique (DSD, *dynamic service delete*) ou par l'exécution d'une transaction de modification de service dynamique (DSC, *dynamic service change*) qui omet un codage L2VPN par flux de service individuel déjà signalé.

Le système CMTS DOIT prendre en charge de multiples codages L2VPN par flux de service individuel, chacun sur un flux de service distinct, avec la même valeur de sous-type d'identificateur VPNID.

Un système CMTS de réexpédition multipoint PEUT accepter les sous-types par réseau VPN individuel définis seulement pour le mode point à point, mais le fonctionnement d'un système CMTS avec différentes valeurs de sous-type sur différents câblo-modems n'est pas défini.

7.2.1 Sous-type d'identificateur VPNID

Le sous-type d'identificateur VPNID est une séquence d'octets opaque qui identifie un réseau L2VPN logique. Tous les serveurs locaux rattachés au même réseau L2VPN logique communiquent les uns avec les autres comme s'ils étaient rattachés au même réseau local privé. Un réseau L2VPN réexpédie des paquets sur la seule base des informations de couche 2 comme les adresses MAC d'un réseau Ethernet et toutes balises identificatrices de réseau VLAN encapsulant ces paquets. Le terme *identificateur de réseau VLAN* ne devrait être utilisé qu'afin de décrire les 12 bits du champ d'identificateur de réseau VLAN codé dans une balise IEEE 802.1Q ou dans une paire de balises IEEE 802.1ad d'un paquet L2VPN réexpédié par un port d'interface NSI.

Un câblo-opérateur est censé configurer un unique VPNID pour chaque entreprise commerciale à laquelle il offre un service transparent de réseau local (TLS). Le câblo-opérateur peut choisir tout format recherché pour l'identificateur VPNID, mais ce format devrait être unique à l'échelle mondiale. Une approche suggérée est [b-IETF RFC 2685], qui définit un mécanisme permettant d'attribuer des identificateurs de réseau VPN uniques à l'échelle mondiale, codés sur 7 octets par combinaison d'un identificateur unique désignant l'organisation qui attribue l'identificateur (p. ex. Le câblo-opérateur proprement dit) avec les 4 octets d'un identificateur de réseau privé virtuel (VPN) attribué par cette organisation. Un autre approche suggérée est [b-IETF RFC 2547], qui décrit un sélecteur de route sur 8 octets qui peut être utilisé comme identificateur VPNID unique à l'échelle mondiale.

Le système CMTS DOIT ignorer un codage L2VPN par flux de service individuel qui omet un sous-type d'identificateur VPNID ou qui contient plus d'un seul sous-type d'identificateur VPNID. Le système CMTS DOIT prendre en charge au moins quatre (4) valeurs différentes d'identificateur VPNID selon chaque câblo-modem, signalées dans au moins quatre codages L2VPN par flux de service individuel.

Dans une application de service IETF de LAN privé virtuel (VPLS), l'identificateur VPNID est destiné à être l'identificateur collectif de rattachement (AGI, *attachment group ID*) signalé entre le système CMTS et d'autres éléments de réseau du service VPLS.

7.2.2 Codage L2VPN de classificateur en voie descendante

Un codage L2VPN de classificateur en voie descendante apparaît dans un codage de classification de paquet en voie descendante (voir § C.2.1.2 de [UIT-T J.122]). La présence d'un codage L2VPN dans un codage de classification de paquet en voie descendante restreint l'application du classificateur aux seuls paquets renvoyés par le réexpéditeur L2VPN. Par ailleurs, seuls les classificateurs qui contiennent un codage L2VPN s'appliquent aux paquets renvoyés par le réexpéditeur L2VPN. En d'autres termes, les classificateurs en voie descendante s'appliquent soit au trafic L2VPN ou au trafic non L2VPN, mais jamais aux deux.

Un codage L2VPN de classificateur en voie descendante peut contenir zéro ou un seul sous-type d'identificateur de réseau VPN et/ou zéro ou un seul sous-type d'étendue de priorités d'utilisateur. Il peut ne contenir aucun sous-type que ce soit (c'est-à-dire un paramètre 43.5 de longueur nulle), auquel cas le classificateur s'applique à tous les paquets L2VPN réexpédiés en voie descendante vers le CM, quel que soit l'identificateur de réseau privé virtuel (VPN) ou le niveau de priorité d'utilisateur.

La présence d'un sous-type d'identificateur VPNID dans un codage L2VPN de classificateur en voie descendante donne instruction au système CMTS d'appliquer le classificateur au seul trafic réexpédié en voie descendante par le réseau L2VPN indiqué. Etant donné que le réseau L2VPN du trafic réexpédié par réseau L2VPN est toujours *impliqué* à l'interface RFI-DOCSIS et n'est pas explicitement présent dans le paquet contenu, il s'agit de la seule façon de classifier le trafic réexpédié en voie descendante d'un réseau L2VPN vers un flux de service particulier, sur la base de l'identificateur VPNID proprement dit.

Si le codage L2VPN de classificateur en voie descendante contient un sous-type d'étendue des priorités d'utilisateur, le classificateur ne s'applique qu'aux paquets L2VPN réexpédiés en voie descendante avec une priorité d'utilisateur à l'extraction de flux conforme à l'étendue indiquée (limites incluses). Cela permet de classifier le trafic L2VPN à priorité élevée comme étant un flux de service avec qualité de service renforcée.

Une valeur de priorité d'utilisateur en sortie de flux, appariée à un sous-type d'étendue des priorités d'utilisateur, est la priorité qui est transmise logiquement par le réexpéditeur L2VPN en voie descendante jusqu'à l'interface avec la couche de commande MAC-DOCSIS. Cela signifie qu'il s'agit de la valeur *après* toute régénération éventuelle de la valeur de priorité d'utilisateur par le réexpéditeur L2VPN. Un vendeur de système CMTS PEUT implémenter des mécanismes propres au vendeur afin de déterminer et de régénérer la priorité d'utilisateur des paquets L2VPN réexpédiés en voie descendante.

Un système CMTS DOIT rejeter l'inscription d'un câblo-modem possédant un codage de classificateur de paquet en voie descendante qui contient plus d'un seul codage L2VPN.

7.2.3 Sous-type de descripteur d'association de sécurité L2VPN

Le sous-type de descripteur d'association de sécurité L2VPN est un codage à parties multiples qui est défini dans la confidentialité de base [UIT-T J.125] et qui fournit:

- l'identificateur d'association de sécurité (SAID) à l'interface avec la confidentialité de base (BPI, *baseline privacy*), que le système CMTS utilise afin de chiffrer le trafic L2VPN en voie descendante pour le réseau L2VPN identifié dans le codage L2VPN;
- une suite chiffrante qui identifie l'algorithme de chiffrement;
- un type d'association de sécurité (type SA).

Un système CMTS DOIT coder le descripteur d'association de sécurité L2VPN comme un type d'association de sécurité dynamique(2). Un câblo-modem DOIT ignorer le type d'association de sécurité et le considérer comme étant de type dynamique(2).

En voie montante, le trafic L2VPN est toujours chiffré dans l'identificateur SAID primaire du câblo-modem qui émet le trafic en voie montante.

Le sous-type de descripteur d'association de sécurité L2VPN n'est pas signalé dans un fichier de configuration de câblo-modem. Au contraire, le système CMTS ajoute un ou plusieurs sous-types de descripteur d'association de sécurité L2VPN à des codages L2VPN de niveau supérieur par câblo-modem individuel, contenus dans son message REG-RSP envoyé au câblo-modem, en ajoutant si nécessaire le codage L2VPN par câblo-modem individuel au message REG-RSP. Après avoir effectué l'authentification par interface BPI, le câblo-modem lance une transaction de clé de chiffrement de trafic (TEK, *traffic encrypting key*) avec le système CMTS pour chaque descripteur d'association de sécurité L2VPN d'un message REG-RSP.

Le système CMTS insère un identificateur SAID-L2VPN dans un codage de sous-type de descripteur d'association de sécurité L2VPN au niveau supérieur d'un message DSA-REQ ou DSC-REQ lancé par le système CMTS qui par ailleurs définit un flux de service de réexpédition en voie montante L2VPN. De même, le système CMTS insère un sous-type de descripteur d'association de sécurité dans un codage L2VPN de niveau supérieur, transporté dans ses réponses DSA-RSP ou DSC-RSP à une transaction de service dynamique lancée par un câblo-modem, en définissant un flux de service de réexpédition en voie montante L2VPN. Un identificateur SAID signalé dans un codage de sous-type de descripteur d'association de sécurité L2VPN est désigné par le terme d'*identificateur SAID-L2VPN*. Un identificateur SAID qui n'est connu par le câblo-modem qu'à partir de messages autres qu'un sous-type de descripteur d'association de sécurité L2VPN est appelé *identificateur SAID de réseau non L2VPN*. Le paragraphe 7.5 ci-dessous décrit la façon dont le chiffrement par interface BPI isole les trafics L2VPN et non L2VPN sur le réseau radioélectrique.

Après l'exécution de toute transaction par message de gestion de commande MAC d'un service dynamique qui présente un nouvel identificateur SAID au câblo-modem, le câblo-modem lance une transaction de clé TEK avec le système CMTS afin d'obtenir le matériel de calcul de clé pour le nouvel identificateur SAID.

Dans le mode de réexpédition point à point par réseau L2VPN, le système CMTS attribue à chaque câblo-modem un identificateur SAID-L2VPN individuel. Si le câblo-modem relaie plus d'un seul réseau L2VPN, le système CMTS attribue à chaque réseau L2VPN un identificateur différent de réseau L2VPN individuel. Dans le mode de réexpédition multipoint L2VPN, le système CMTS attribue un identificateur SAID collectif de réseau L2VPN que tous les câblo-modems relayant ce réseau L2VPN se partageront.

7.2.4 Codage L2VPN propre au vendeur

Le sous-type de codage L2VPN propre au vendeur est accepté à tout emplacement du codage L2VPN et fournit des informations spécifiques au vendeur de CMTS ou de CM. Il peut par exemple indiquer à un vendeur de système CMTS une sous-interface particulière de port NSI vers laquelle le réseau L2VPN réexpédiera le trafic en mode point à point. Le codage L2VPN propre au vendeur peut être en éléments binaires ou en caractères ASCII; sa définition est laissée aux soins au vendeur de système CMTS.

Une implémentation de système CMTS PEUT permettre qu'un codage L2VPN propre au vendeur *remplace* un sous-type d'identificateur VPNID ou d'encapsulation de flux à l'interface NSI, mais les codages L2VPN propres au vendeur NE DOIVENT PAS être requis par un système CMTS pour les essais de certification de réseau L2VPN.

7.2.5 Exigences relatives aux erreurs de configuration

Un système CMTS de réexpédition multipoint DOIT rejeter – par un code de confirmation de rejet d'interface NSI multipoint – une transaction d'inscription ou de service dynamique qui essaye de configurer de multiples codages L2VPN de réexpédition en voie montante avec le même

identificateur de réseau L2VPN mais avec des valeurs différentes des sous-types d'encapsulation de flux aux interfaces NSI, AGI, TAII ou SAII.

Un système CMTS de réexpédition point à point DOIT rejeter – par un code de confirmation de rejet d'identificateur de réseau VLAN en usage – une transaction d'inscription ou de flux de service ayant un sous-type d'encapsulation de flux L2VPN à l'interface NSI qui exige une réexpédition sur le port L2VPN sélectionné avec un identificateur de réseau VLAN déjà assigné à un réseau non L2VPN. Un système CMTS de réexpédition point à point DOIT rejeter toute tentative de configurer un port L2VPN sélectionné avec un identificateur de réseau VLAN déjà assigné par un codage de sous-type d'encapsulation de flux L2VPN à l'interface NSI.

Un système CMTS de réexpédition point à point DOIT rejeter – avec un code de confirmation de rejet de réseau L2VPN multipoint – une transaction d'inscription ou de flux de service qui essaye de configurer plus d'un seul circuit de rattachement câblé (c'est-à-dire plus d'un seul câblo-modem) avec la même valeur de multiplexage du service d'encapsulation à l'interface NSI du réseau L2VPN.

7.2.6 Encapsulation à l'interface entre réseau et système de terminaison (NSI, *network system interface*)

Les commutateurs et routeurs de réseau local modernes implémentent un riche ensemble d'éléments de service de pontage dans la couche 2. L'exploitation interurbaine de réseaux L2VPN sur des réseaux infrastructurels tunnellisés MPLS et IP est un secteur actif d'innovation industrielle et d'efforts de normalisation. La présente Recommandation ne spécifie *pas* entièrement la réexpédition en couche 2 de paquets Ethernet entre systèmes CMTS, mais elle essaie de spécifier la configuration de réexpédition L2VPN à l'intérieur d'un même système CMTS, en particulier dans un circuit de rattachement entre interfaces RFI et NSI d'un câblo-modem. Les vendeurs de système CMTS sont invités à prendre en charge les protocoles et éléments de service de pontage existants et futurs dans la couche 2 des réseaux infrastructurels lors de la réexpédition du trafic de couche 2 à destination et en provenance d'une interface RFI de commande MAC-DOCSIS.

7.2.6.1 Sous-type d'encapsulation de flux à l'interface NSI

Bien que la présente Recommandation spécifie essentiellement le fonctionnement d'un réseau L2VPN à l'interface RFI-DOCSIS, elle spécifie également un degré limité de fonctionnement à une interface NSI pour les raisons suivantes:

- afin de normaliser la configuration d'un réseau L2VPN pour les essais de certification;
- afin de normaliser, entre vendeurs de systèmes CMTS, un utile sous-ensemble de capacités de réseau L2VPN.

La présente Recommandation définit un sous-type d'encapsulation de flux à l'interface NSI dans un codage L2VPN (voir § B.3.2) afin de décrire facultativement comment des paquets de réseau L2VPN sont encapsulés à un seul port d'interface NSI sélectionné. L'implémentation par le vendeur de système CMTS peut permettre que ce port NSI sélectionné soit modifié en cas de défaillance de port ou d'autres événements. Un vendeur de système CMTS PEUT utiliser le sous-type d'encapsulation de flux à l'interface NSI pour des scénarios additionnels et PEUT utiliser des sous-types propres au vendeur dans l'encapsulation de flux à l'interface NSI, de façon à prendre en charge – de façon propre au vendeur – un mappage des circuits de rattachement avec des pseudo-circuits de réseau infrastructurel ou avec des instances internes de commutation virtuelle.

La présente Recommandation prescrit que les systèmes CMTS n'implémentent qu'un seul format d'encapsulation de flux L2VPN à l'interface NSI: le balisage IEEE 802.1Q avec une valeur, configurée statiquement sur 12 bits, d'identificateur de réseau VLAN en tant que valeur de multiplexage de service. Si le système CMTS implémente d'autres formats d'encapsulation L2VPN par un port d'interface NSI, ce système devrait utiliser le codage de sous-type d'encapsulation de flux à l'interface NSI si le code de format particulier est défini pour ce sous-type.

Quand un identificateur de réseau VLAN en format d'encapsulation de flux à l'interface NSI est configuré statiquement, cet identificateur est censé ne s'appliquer qu'au port Ethernet sélectionné. La sélection d'une interface NSI particulière afin de relayer un réseau L2VPN particulier, ou un circuit de rattachement particulier, relève des compétences du vendeur. Le sous-type L2VPN propre au vendeur peut servir à cette fin.

Un système CMTS de réexpédition point à point DOIT rejeter une transaction d'inscription de câblo-modem ou de flux de service ayant un codage L2VPN qui omet le sous-type d'encapsulation de flux à l'interface NSI ou qui omet un sous-type, propre au vendeur, identifiant une valeur de multiplexage de service à l'interface NSI. Le système CMTS de réexpédition multipoint ne nécessite pas de sous-type d'encapsulation de flux à l'interface NSI dans un codage L2VPN, mais DOIT accepter et implémenter le sous-type si celui-ci est spécifié. Un système CMTS en mode de réexpédition point à point ou multipoint DOIT rejeter une transaction d'inscription de câblo-modem ou de flux de service ayant un codage L2VPN qui contient un sous-type d'encapsulation de flux à l'interface NSI applicable à un identificateur de réseau VPN qui diffère du sous-type d'encapsulation de flux à l'interface NSI pour cet identificateur VPNID à l'intérieur de tout autre codage L2VPN accepté.

Dans l'encapsulation à l'interface NSI selon la spécification IEEE 802.1Q, les valeurs d'identificateur de réseau VLAN 0, 1 et 4095 ne sont pas autorisées comme identificateur configuré de réseau VLAN. La valeur 0 d'identificateur de réseau VLAN est réservée aux balises de priorité absolue dans la spécification IEEE 802.1Q. La valeur 1 d'identificateur de réseau VLAN est réservée à l'identificateur par défaut d'un port de réseau VLAN dans la spécification IEEE 802.1Q. Le fait d'autoriser des réseaux L2VPN d'abonné à configurer la valeur 1 d'identificateur de réseau VLAN risque de se traduire par une réexpédition inopportune, dans la couche 2, d'un trafic de gestion hors bande sur ce réseau L2VPN d'abonné. La valeur 4095 d'identificateur de réseau VLAN (série de chiffres 1) est réservée par l'institut IEEE.

La question de savoir si le système CMTS accepte du trafic non L2VPN par un port d'interface NSI avec balise IEEE 802.1Q de priorité absolue (c'est-à-dire avec une valeur 0 d'identificateur de réseau VLAN) relève d'une implémentation propre au vendeur.

7.2.6.2 Réexpédition L2VPN selon la spécification IEEE 802.1ad

La spécification [b-IEEE 802.1ad] décrit une approche de double balisage pour la réexpédition L2VPN dans un réseau infrastructurel. Un paquet possède une balise externe d'identificateur de réseau VLAN sur 12 bits et une balise interne d'identificateur de réseau VLAN sur 12 bits. Le sous-type d'encapsulation de flux à l'interface NSI permet de configurer la paire de balises d'identificateur de réseau VLAN sur 12 bits pour chaque câblo-modem ou flux de service exécutant une réexpédition L2VPN. La configuration des doubles balises dépend du mode de réexpédition L2VPN du système CMTS et des éléments de mise en réseau IEEE 802.1ad contenus dans le réseau infrastructurel.

7.2.6.2.1 Réexpédition point à point par système CMTS selon la spécification 802.1ad

Dans ce scénario, les éléments IEEE 802.1ad de mise en réseau infrastructurel réexpédient simplement en mode point à point, sans acquisition intelligente des adresses MAC. La balise 802.1ad externe identifie un élément de réseau destinataire qui exécute les fonctions de pontage L2VPN d'acquisition intelligente d'adresses MAC sur un port de pont et les fonctions de réexpédition/élargissement entre ces ports de pont. La balise 802.1ad interne identifie un port de pont particulier sur cet élément externe de pont L2VPN.

Dans ce cas, le système CMTS n'est pas autrement configuré avec l'adresse IP ou l'identité du nœud destinataire. Il est configuré avec seulement les deux balises identificatrices de réseau VLAN à utiliser pour l'encapsulation au port d'interface NSI.

Quand des trames à doubles balises 802.1ad sont réexpédiées dans le réseau infrastructurel, les nœuds intermédiaires utilisent seulement la balise externe d'identificateur de réseau VLAN afin de prendre des décisions de réexpédition. La spécification 802.1ad prend par exemple en charge la fourniture de trames de réexpédition sur la base de la valeur de la balise externe, sans recherche d'adresse MAC.

Le pont L2VPN visé par la balise externe d'identificateur de réseau VLAN est configuré séparément afin d'indiquer à quel client logique L2VPN chaque port de pont à balise interne est connecté.

7.2.6.2.2 Réexpédition point à point par système CMTS avec élément de réseau de pont L2VPN

La spécification [b-IEEE 802.1ad] peut être déployée de façon à construire un élément de réseau infrastructurel remplissant la fonction de commutation L2VPN permettant d'effectuer la réexpédition/l'élargissement dans la couche de commande MAC entre circuits de rattachement appartenant au même réseau L2VPN.

Dans ce scénario, la balise interne d'identificateur de réseau VLAN représente le réseau L2VPN logique et la balise externe d'identificateur de réseau VLAN représente un circuit individuel de rattachement à ce réseau L2VPN logique. Le commutateur de réseau L2VPN-IEEE 802.1ad considère que la balise externe d'identificateur de réseau VLAN représente une interface interurbaine de nature virtuelle et distincte, tandis que la balise interne représente un commutateur logique. Le commutateur L2VPN-IEEE 802.1ad construit une base de données de réexpédition dans la couche 2 au moyen des adresses MAC qu'il acquiert à partir de chaque interface interurbaine virtuelle, puis réexpédie/élargit les paquets entre ces interfaces interurbaines virtuelles. De cette façon, ce commutateur L2VPN assure la réexpédition entre tous les circuits de rattachement d'un réseau L2VPN. Au moyen de cette technique, plus de 4000 instances de service L2VPN peuvent être prises en charge entre un seul système CMTS et le commutateur de réseau L2VPN-IEEE 802.1ad, chacun de ces éléments pouvant avoir plus de 4000 associations entre câblo-modems et flux de service dans le système CMTS.

7.2.7 Service de LAN privé virtuel (VPLS) et service de ligne privée virtuelle

7.2.7.1 Encapsulation de flux à l'interface NSI en formats MPLS et L2TPv3

Les formats MPLS et L2TPv3 du sous-type d'encapsulation de flux à l'interface NSI sont destinés à prendre en charge l'interfonctionnement de la réexpédition L2VPN-DOCSIS avec les prochaines normes de service de ligne privée virtuelle (VPWS, *virtual private wire service*) et de service de LAN privé virtuel (VPLS, *virtual private LAN service*), issues du groupe IETF. Le modèle IETF est fondé sur des circuits de rattachement aux entités de réexpédition L2VPN. Chaque câblo-modem possédant au moins un flux de service de réexpédition en voie montante dans un réseau L2VPN correspond à un circuit de rattachement au réseau L2VPN. Etant donné que la capacité L2VPN-DOCSIS permet de multiples flux de service pour le même réseau L2VPN et n'associe pas de flux de service particuliers en voie descendante à des flux de service en voie montante, un circuit de rattachement câblé à un réseau L2VPN est considéré comme étant le câblo-modem et non pas un flux de service individuel sur ce câblo-modem.

Les paquets de couche 2 sont destinés à être réexpédiés sur les pseudo-circuits par l'intermédiaire d'un port d'interface NSI, chaque pseudo-circuit étant un chemin à commutation MPLS ou une session de tunnel L2TPv3. Un pseudo-circuit particulier s'assimile à une entrée de flux à une extrémité avec une pile d'une ou de plusieurs étiquettes MPLS ou avec un identificateur de session L2TPv3. Les protocoles L2VPN du groupe IETF visent à prendre en charge la sélection dynamique de ces valeurs d'encapsulation dans un tunnel, par négociation de la création de pseudo-circuits entre extrémités qui implémentent le même réseau L2VPN logique. Il s'agit de la principale raison pour laquelle un sous-type d'identificateur VPNID unique à l'échelle mondiale est configuré dans chaque codage L2VPN de réexpédition par flux de service individuel. Dans le cas des extrémités

implémentant des protocoles compatibles de création dynamique de tunnel, seuls les champs d'identificateur VPNID et de protocole d'encapsulation de flux à l'interface NSI ont besoin d'être configurés dans un câblo-modem ou flux de service conforme à la spécification DOCSIS.

Si des valeurs d'encapsulation de pseudo-circuit (c'est-à-dire des valeurs d'étiquette MPLS ou d'identificateur de session L2TPv3) ne peuvent pas être dynamiquement négociées, on peut les configurer avec des paramètres de sous-type propres au vendeur de réseau L2VPN ou avec une autre configuration propre au vendeur du système CMTS.

7.2.7.2 Configuration des services VPLS/VPWS

La signalisation dans le plan de commande concernant le service VPLS utilise trois champs configurables afin d'identifier les réseaux L2VPN et leurs circuits de rattachement:

- identificateur collectif de rattachement;
- identificateur individuel de rattachement à l'origine (SAII);
- identificateur individuel de rattachement à la destination (TAII).

Afin de normaliser la configuration DOCSIS des champs contenus dans un fichier de configuration de câblo-modem, la présente Recommandation définit un sous-type de codage L2VPN pour chaque champ.

Le sous-type d'identificateur collectif de rattachement (AGI, *attachment group ID*) contenu dans un codage L2VPN n'est actuellement défini que dans un des codages L2VPN de réexpédition par flux de service individuel. Il fournit la valeur du champ d'identificateur AGI lors de l'installation d'une ligne privée en protocole MPLS ou L2TPv3 à l'interface NSI entre un réseau infrastructurel et un circuit de rattachement câblé. Il n'est applicable qu'à une réexpédition en mode point à point entre le circuit de rattachement et la ligne privée. Voir dans la référence [b-IETF RFC 3985] une description de l'architecture d'émulation de pseudo-circuit.

Le sous-type d'identificateur individuel de rattachement à l'origine (SAII, *source attachment individual ID*) n'est défini que dans un codage L2VPN de réexpédition par flux de service individuel. Il indique la valeur dynamiquement signalée par le réexpéditeur L2VPN en tant que champ d'identificateur SAII lors de l'annonce d'une valeur de multiplexage du service d'encapsulation à l'interface NSI telle qu'une étiquette MPLS ou un identificateur de session L2TPv3. Ce champ n'est utilisé que dans les applications L2VPN du groupe IETF telles que le service de LAN privé virtuel (VPLS) ou le service de ligne privée virtuelle (VPWS), quand le système CMTS fonctionne en mode de réexpédition point à point entre lignes privées à l'interface NSI et circuits de rattachement à un câblo-modem/flux de service. L'identificateur SAII configuré est destiné à concorder avec l'identificateur individuel de rattachement à la destination (TAII, *target attachment individual ID*) d'une requête entrante d'établissement dynamique de ligne privée.

Le sous-type d'identificateur individuel de rattachement à la destination (TAII) n'est défini que dans un codage L2VPN de réexpédition par flux de service individuel. Il fournit la valeur dynamiquement signalée par le réexpéditeur L2VPN comme étant le champ d'identificateur TAII lors du lancement de l'établissement d'une ligne Privée L2VPN selon le groupe IETF à une interface NSI. Ce champ n'est utilisé que pour les applications L2VPN du groupe IETF telles que les services VPLS ou VPWS quand le système CMTS doit ouvrir une ligne privée vers un élément de réseau distant qui va implémenter une réexpédition en mode point à point. L'identificateur TAII est destiné à concorder avec l'identificateur SAII d'un des circuits de rattachement de l'élément de réseau distant.

Un système CMTS DEVRAIT utiliser tout sous-type configuré d'identificateur collectif de rattachement (AGI), tout sous-type configuré d'identificateur individuel de rattachement à l'origine (SAII) ou tous sous-types d'identificateur individuel de rattachement à la destination (TAII) configurés, dans un codage de réexpédition L2VPN pour les valeurs des champs correspondants,

avec des protocoles spécifiés par l'IETF qui tentent de commuter une ligne privée vers un circuit de rattachement à l'interface NSI.

7.3 Réexpédition L2VPN en voie montante

Le système CMTS NE DOIT PAS interpréter une balise 802.1Q apparaissant déjà dans un paquet en voie montante comme fournissant la priorité ou l'identificateur de réseau L2VPN dans un pontage de réexpédition L2VPN. Cela implique une balise à priorité absolue. Le système CMTS DOIT réexpédier de façon transparente toute balise 802.1Q fournie par un abonné. Si le paquet balisé par un abonné est réexpédié par un port Ethernet de terminaison 802.1Q à l'interface NSI, le système CMTS DOIT préfixer une balise externe 802.1Q avant la balise interne fournie par l'abonné.

Le système CMTS DOIT être en mesure d'envoyer et de recevoir, pour réexpédition L2VPN à toutes les interfaces, un paquet de 1522 octets qui contient une seule balise d'abonné empilée, plus toutes éventuelles informations L2VPN délimitatrices de service à l'interface. Par exemple, à une interface NSI avec un réseau Ethernet acceptant des balises 802.1Q pour l'encapsulation de flux L2VPN à l'interface NSI, le système CMTS accepte et réexpédie un paquet Ethernet de 1526 octets. Un tel paquet est réexpédié au domaine de commande MAC, en voie descendante vers l'interface RFI, sous forme d'un paquet de 1522 octets composé d'un paquet Ethernet d'une longueur nominale maximale de 1518 octets, avec une seule balise d'abonné non délimitatrice de service sur 4 octets.

Le système CMTS NE DOIT PAS compter les adresses MAC d'équipement CPE de réseau L2VPN qui sont acquises à partir de paquets dirigés en voie montante vers un quelconque réglage docsSubMgtCpeControlMaxCPEIp exécuté pour le câblo-modem, § C.1.1.18.1 de [UIT-T J.122]. Ce réglage ne s'applique qu'aux adresses IP d'abonné qui ont été acquises et réexpédiées par un réseau non L2VPN. Les systèmes CMTS en mode multipoint ont une exigence particulière, visant à limiter le nombre d'adresses MAC d'origine acquises sur chaque réseau L2VPN.

Le système CMTS NE DOIT PAS appliquer le filtrage de gestion d'abonné, § C.1.1.18 de [UIT-T J.122] aux paquets L2VPN réexpédiés en voie montante.

Le système CMTS NE DOIT PAS appliquer la fonction de surécriture du champ de type de service (ToS), § C.2.2.6.10 de [UIT-T J.122] aux paquets réexpédiés en voie montante L2VPN.

Un réexpéditeur L2VPN tient à jour hors bande un champ de 3 bits de priorité d'utilisateur associé à chaque paquet réexpédié. Le système CMTS DOIT utiliser les 3 éléments binaires du champ de priorité d'utilisateur contenu dans les balises IEEE 802.1Q comme étant sa priorité d'utilisateur lors de l'acceptation de paquets L2VPN réexpédiés avec une encapsulation à l'interface NSI conforme à la spécification IEEE 802.1Q. Le système CMTS DOIT utiliser cette priorité d'utilisateur lorsqu'il classifie les paquets en voie descendante. Le système CMTS DOIT coder la valeur de sortie de priorité d'utilisateur comme spécifié pour le format d'encapsulation de flux à l'interface NSI (p. ex. dans les bits de priorité d'utilisateur d'une balise IEEE 802.1Q). Le système CMTS DEVRAIT offrir le mappage de priorité d'utilisateur à la sortie de flux en fonction de la classe de trafic de transmission par port d'interface NSI conformément à la spécification [b-IEEE 802.1S]. Le nombre de classes de trafic de transmission par port d'interface NSI relève des compétences du vendeur. Si un codage de flux de service en voie montante L2VPN omet le sous-type de priorité d'utilisateur selon la norme IEEE 802.1, le système CMTS DOIT par défaut réexpédier de tels paquets vers un port d'interface NSI avec encapsulation à l'interface NSI selon l'IEEE 802.1Q et avec une priorité d'utilisateur égale à zéro. Dans une configuration propre au vendeur, le système CMTS PEUT réexpédier avec des valeurs par défaut de priorité d'utilisateur différentes de zéro.

Le système CMTS DOIT prendre en charge la réexpédition, aussi bien par réseaux L2VPN que par réseaux non L2VPN, du trafic en voie montante issu d'un flux de service L2VPN de réexpédition sur la base de la vérification de l'adresse MAC d'origine par rapport à un masque d'interface avec un câblo-modem configuré pour ce flux de service. Le système CMTS DOIT aiguiller vers le

réexpéditeur L2VPN les paquets issus des adresses MAC d'origine indiquées avec un chiffre '1' dans le masque d'interface avec un câblo-modem. Le système CMTS NE DOIT PAS aiguiller vers le réexpéditeur L2VPN les paquets issus du câblo-modem intégré et d'au moins une seule autre adresse MAC d'origine d'entité eSAFE, même si ces paquets sont reçus par un flux de service de réexpédition en voie montante L2VPN, quand les interfaces correspondant à ces adresses MAC d'origine sont indiquées avec un '0' dans le masque d'interface avec un câblo-modem.

Un système CMTS PEUT reconnaître le moment où les masques d'interface avec un câblo-modem, contenus dans l'ensemble des codages L2VPN de classificateur de paquets en voie montante d'un câblo-modem conforme, lui permettent d'éviter la vérification des adresses MAC en voie montante depuis l'origine et lui permettent au contraire de réexpédier les paquets en voie montante vers le réexpéditeur par réseau soit L2VPN soit non L2VPN, uniquement sur la base du flux de service en voie montante.

Le système CMTS DOIT reconnaître un critère de masque d'interface avec un câblo-modem dans un codage de classificateur de paquet en voie descendante L2VPN, que ce codage classifie un trafic L2VPN ou non L2VPN. Le système CMTS DOIT ranger l'adresse MAC de destination d'un paquet en voie descendante dans une seule des trois classes suivantes:

1) une adresse MAC de câblo-modem;

2) une adresse MAC d'équipement CPE;

3) une adresse MAC d'entité eSAFE d'un type particulier de serveur local d'entité eSAFE.

Le système CMTS DOIT considérer le critère comme ayant été trouvé en correspondance quand l'adresse MAC de destination du paquet en voie descendante dans la couche 2 est une adresse MAC de câblo-modem ou une adresse MAC d'entité eSAFE qui correspond à un type de serveur local ayant un chiffre '1' dans le masque d'interface avec un câblo-modem. Le système CMTS DOIT considérer le critère comme ayant été trouvé en correspondance quand l'adresse MAC de destination est une adresse MAC d'équipement CPE et quand le masque d'interface avec un câblo-modem active le bit de *tout* type de serveur local d'équipement CPE, c'est-à-dire quand l'un quelconque des bits 1 ou 5 à 15 est activé. Le système CMTS DOIT considérer le critère comme n'étant pas trouvé en correspondance quand l'adresse MAC de destination est un câblo-modem ou une adresse MAC d'entité eSAFE et quand l'unique bit de masque d'interface avec un câblo-modem correspondant à ce type de serveur local a la valeur '0'. Le système CMTS DOIT considérer le critère comme n'étant pas trouvé en correspondance quand l'adresse MAC de destination est une adresse MAC d'équipement CPE et quand le masque d'interface avec un câblo-modem possède un bit zéro dans toutes les positions binaires du type de serveur local d'équipement CPE, c'est-à-dire quand le masque possède un bit zéro dans les positions 1 et 5 à 15.

Le système CMTS DOIT rejeter toute tentative (c'est-à-dire inscription ou transaction DSx) visant à configurer de multiples codages L2VPN de classificateur en voie montante de façon qu'ils classifient dans le même flux de service en voie montante, mais avec différents sous-types d'identificateur VPNID. Le système CMTS utilise le flux de service en voie montante afin de déterminer un unique identificateur VPNID pour la réexpédition L2VPN.

7.4 Réexpédition L2VPN en voie descendante

Le système CMTS DOIT rejeter toute requête REG-REQ contenant un codage L2VPN si l'interface BPI n'est pas également activée dans cette requête REG-REQ. Le système CMTS DOIT rejeter toute requête DSA-REQ ou DSC-REQ contenant un codage L2VPN si l'interface BPI n'est pas également activée pour le câblo-modem.

Le système CMTS NE DOIT PAS appliquer de filtres de gestion d'abonné (voir le § C.1.1.18 de [UIT-T J.122]) au trafic réexpédié en voie descendante d'un réseau L2VPN.

Le système CMTS DOIT accepter un unique codage L2VPN de classificateur en voie descendante dans un codage de classification de paquet en voie descendante d'un message REG-REQ, DSA-REQ, ou DSC-REQ. Un système CMTS ne DOIT appliquer qu'aux paquets réexpédiés par le réexpéditeur L2VPN les règles de classificateur qui contiennent un codage L2VPN. Par ailleurs, seuls les classificateurs contenant un codage L2VPN peuvent être appliqués au trafic réexpédié en voie descendante d'un réseau L2VPN.

- Le système CMTS DOIT rejeter l'inscription des câblo-modems ayant des codages non valides de classification de paquet en voie descendante.
- Un codage L2VPN valide de classification en voie descendante contient zéro ou un seul sous-type d'identificateur VPNID, zéro ou un seul sous-type d'étendue de priorités d'utilisateur et un nombre quelconque de sous-types de paramètre L2VPN propre au vendeur. Le système CMTS DOIT ignorer de façon transparente tous les sous-types invalides de codages L2VPN.
- Le système CMTS DOIT accepter comme valide et ignorer de façon transparente tout sous-type non reconnu de codages L2VPN.
- Le système CMTS DOIT accepter les multiples réglages de configuration de la classification en voie descendante qui contiennent un codage L2VPN de classificateur en voie descendante classifiant différents identificateurs L2VPN dans le même flux de service de référence.
- Le système CMTS DOIT prendre en charge les mêmes options de critère de classificateur dans les codages L2VPN de classificateur en voie descendante des réseaux L2VPN et non L2VPN.
- Le système CMTS DOIT interpréter un codage de classificateur de paquet en voie descendante, ne contenant aucun autre critère qu'un codage L2VPN de classificateur, comme étant en concordance avec *tous* les paquets réexpédiés en voie descendante sur le réseau L2VPN désigné par l'identificateur VPNID du codage L2VPN de classificateur, et DOIT classifier tous les paquets de ce type dans le flux de service de référence.
- Le système CMTS PEUT accepter de multiples codages L2VPN de classificateur en voie descendante contenant un même identificateur VPNID classifiant les paquets dans différents flux de service. L'opération n'est pas définie quand plus d'un seul classificateur en voie descendante concorde avec un paquet particulier en voie descendante.
- Le système CMTS DOIT rejeter une demande de transaction par flux de service contenant un codage non valide L2VPN de classificateur en voie descendante.
- Si le codage L2VPN contient un sous-type d'étendue des priorités d'utilisateur, le système CMTS ne DOIT mettre le classificateur en correspondance qu'avec les paquets L2VPN réexpédiés avec une priorité d'utilisateur de sortie de flux contenue dans l'étendue indiquée. Sinon, le classificateur s'applique à toutes les priorités d'utilisateur à l'extraction de flux.

Après acceptation d'un codage L2VPN valide de classificateur en voie descendante, le réexpéditeur L2VPN du système CMTS DOIT réexpédier, dans le flux de service de référence du classificateur, tout le trafic de câblo-modem unique destiné, en voie descendante, aux équipements CPE rattachés à ce câblo-modem. Dans le mode point à point, cela implique tout le trafic en voie descendante sur le réseau L2VPN; dans le mode multipoint, cela implique le trafic unidiffusé à destination d'adresses MAC d'équipement CPE acquises à partir du trafic en voie montante issu du câblo-modem. Si le trafic réexpédié en voie descendante d'un réseau L2VPN n'est pas classifié dans un flux de service particulier en voie descendante, le système CMTS DOIT réexpédier le trafic de câblo-modem unique sur le flux de service primaire en voie descendante de ce câblo-modem.

Le système CMTS DOIT classifier les paquets de couche 2 comme ils apparaissent à l'interface RFI, c'est-à-dire SANS y inclure d'éventuelles balises délimitatrices de service 802.1Q qui apparaissaient au port de l'interface NSI avec le système CMTS. C'est-à-dire que les codages

802.1Q de classification de paquet selon le § C.2.1.7 de [UIT-T J.122] s'appliquent seulement à la balise d'abonné privé ou à la balise interne 802.1Q et non pas à l'identificateur de réseau VLAN du paquet réexpédié par réseau L2VPN.

Un système CMTS NE DOIT PAS appliquer de filtres de gestion d'abonné (voir le § C.1.1.18 de [UIT-T J.122]) au trafic L2VPN en voie descendante.

Un système CMTS DOIT réexpédier les paquets en voie descendante de réseaux L2VPN différents sur des flux de service en voie descendante différents, ce qui garantit le découplage de la qualité du service de réseau L2VPN.

Sauf configuration contraire de façon à combiner la base de données de réexpédition de différents réseaux L2VPN, le réexpéditeur L2VPN du CMTS DOIT conserver le découplage des voies montante et descendante du trafic réexpédié dans la couche 2 entre les circuits de rattachement configurés avec différents identificateurs VPNID. Le nombre de câblo-modems ou flux de service pris en charge pour la réexpédition L2VPN relève des compétences du vendeur du système CMTS. Le nombre d'identificateurs VPNID uniques pris en charge par un système CMTS relève des compétences du vendeur.

7.4.1 Réexpédition multipoint en voie descendante

Le système CMTS DOIT rejeter (avec un code de confirmation de rejet permanent) une transaction d'inscription ou de flux de service qui nécessiterait la définition d'identificateurs SAID-L2VPN excédant la capacité du câblo-modem en terme d'identificateurs SAID en voie descendante (voir le § C.1.3.1.7 de [UIT-T J.122]).

Un système CMTS en mode de réexpédition multipoint DOIT acquérir les adresses MAC d'origine du trafic montant d'équipement CPE et les associer à un câblo-modem particulier sur ce réseau L2VPN.

Un système CMTS de réexpédition multipoint DOIT limiter le nombre d'adresses MAC, autorisées à être acquises sur tout réseau L2VPN unique, à une valeur configurable qui s'applique à tous les réseaux L2VPN. Le système CMTS DEVRAIT permettre la configuration individuelle du nombre maximal d'adresses MAC dans chaque réseau L2VPN.

Un système CMTS de réexpédition multipoint DOIT réexpédier sur différents flux de service les paquets en voie descendante chiffrés dans différents identificateurs SAID-L2VPN.

7.5 Découplage et confidentialité d'un réseau L2VPN

Un objectif fondamental de la présente Recommandation consiste à *découpler* le trafic descendant entre abonnés de réseaux L2VPN et de réseaux non L2VPN, ainsi qu'entre différents abonnés L2VPN. Les abonnés non L2VPN (c'est-à-dire résidentiels) ne devraient pas être en mesure de voir le trafic réexpédié aux abonnés d'un réseau L2VPN lesquels, par ailleurs, ne devraient pas voir le trafic destiné à des abonnés résidentiels non L2VPN.

7.5.1 Protection du trafic L2VPN

La présente Recommandation utilise le chiffrement par interface BPI afin de découpler le trafic L2VPN du trafic non L2VPN en voie descendante. Cela implique qu'un câblo-opérateur configure les câblo-modems fournissant le service de réseau L2VPN de façon à permettre le fonctionnement de l'interface avec la confidentialité de base (BPI, *baseline privacy interface*). Le câblo-opérateur est censé configurer tous les câblo-modems, avec et sans réexpédition L2VPN, de façon à activer l'interface BPI de telle sorte que tous ces câblo-modems puissent recevoir un trafic IP multidiffusé et chiffré.

Le système CMTS DOIT rejeter toute tentative (c'est-à-dire inscription ou transaction DSx) visant à configurer un codage de réexpédition L2VPN si le câblo-modem n'est pas également configuré de façon à prendre en charge le fonctionnement de l'interface BPI.

Un système CMTS DOIT attribuer au moins un seul identificateur SAID-L2VPN pour la réexpédition en voie descendante vers chaque réseau L2VPN distinct qui est réexpédié par le système CMTS sur une voie descendante. Un identificateur SAID unique de réseau L2VPN, assigné à tous les câblo-modems du même réseau L2VPN, est appelé *identificateur SAID collectif de réseau L2VPN*. Le système CMTS PEUT attribuer des valeurs d'identificateur SAID-L2VPN différentes au même réseau L2VPN sur différentes voies descendantes. Un système CMTS PEUT attribuer de multiples identificateurs SAID-L2VPN au même réseau L2VPN sur la même voie descendante, p. ex. afin d'attribuer un identificateur SAID-L2VPN individuel à chaque câblo-modem en mode de réexpédition point à point. Le système CMTS DOIT attribuer un identificateur collectif ou individuel de réseau L2VPN qui diffère de tout autre identificateur SAID primaire assigné à cette voie. Un système CMTS PEUT attribuer de multiples identificateurs SAID au même réseau L2VPN sur le même câblo-modem.

Un système CMTS DOIT ajouter, au codage de réexpédition L2VPN de ses messages REG-RSP et de service dynamique envoyés à un câblo-modem L2VPN conforme, un ou plusieurs sous-types de descripteur d'association de sécurité L2VPN contenus dans son ou ses identificateurs SAID-L2VPN assignés en vue de la réexpédition en voie descendante vers ce réseau L2VPN, sur la voie descendante de ce câblo-modem. Le système CMTS DOIT coder des séquences L2VPN distinctes de niveau supérieur pour chaque identificateur distinct de réseau L2VPN. Un système CMTS PEUT ajouter des sous-types de descripteur d'association de sécurité L2VPN dans des messages envoyés à des câblo-modems non conformes, mais ces sous-types seront ignorés par ces câblo-modems. Le système CMTS DOIT décrire l'identificateur SAID-L2VPN avec un type d'association de sécurité de valeur égale à *dynamic* dans un codage de descripteur d'association de sécurité L2VPN.

Un système CMTS n'insère PAS de descripteurs d'association de sécurité dans tous les identificateurs SAID-L2VPN qu'il a assignés en vue d'une inscription de modem dans sa réponse d'autorisation initiale d'interface BPI, envoyée à ce câblo-modem après son inscription.

Un système CMTS DOIT chiffrer tout le trafic réexpédié en voie descendante d'un réseau L2VPN, dans un identificateur SAID-L2VPN assigné au réseau L2VPN.

Le système CMTS NE DOIT PAS réexpédier le trafic L2VPN en voie descendante à un câblo-modem tant que celui-ci n'a pas terminé l'autorisation de l'interface BPI et la négociation de clé TEK pour l'identificateur SAID du réseau L2VPN dans lequel le trafic doit être chiffré.

Un système CMTS de réexpédition point à point DEVRAIT attribuer le même identificateur SAID collectif de réseau L2VPN à différents câblo-modems du même domaine de commande MAC se rattachant au même identificateur de réseau L2VPN, mais ce système PEUT décider d'attribuer au câblo-modem un unique identificateur de réseau L2VPN individuel.

Un système CMTS de réexpédition multipoint DOIT attribuer au moins un seul identificateur SAID-L2VPN diffusé à tous les câblo-modems du même domaine de commande MAC, se rattachant au même identificateur de réseau L2VPN. Le système CMTS de réexpédition multipoint DOIT réexpédier les paquets diffusés en voie descendante du réseau L2VPN chiffré avec un tel identificateur SAID-L2VPN diffusé.

Un système CMTS PEUT prendre en charge une configuration propre au vendeur afin de lancer ou arrêter dynamiquement une réexpédition L2VPN au moyen d'un câblo-modem enregistré. Un système CMTS qui interrompt la réexpédition L2VPN au moyen d'un câblo-modem DOIT supprimer dynamiquement tous les flux de service en voie montante qui réexpédient vers ce réseau L2VPN et DOIT signaler un codage L2VPN de niveau supérieur au câblo-modem qui omet tous les descripteurs d'association de sécurité pour ce réseau L2VPN. Cette opération signale au câblo-modem qu'il doit interrompre le déchiffrement en voie descendante pour les identificateurs SAID-L2VPN associés au réseau L2VPN.

7.5.2 Prévention de la fuite de trafic non L2VPN

Un problème posé par le fonctionnement d'un réseau L2VPN est le trafic non L2VPN en voie descendante dans la couche 2 vers une adresse MAC collective (GMAC), c'est-à-dire une diffusion ou multidiffusion en couche 2. Le trafic non L2VPN diffusé en voie descendante contient des protocoles de réponse ARP allant du système CMTS à des équipements CPE non L2VPN, ainsi que des annonces de routeur CMTS pour le protocole RIP ou OSPF. Par défaut, *tous* les câblo-modems – L2VPN et non L2VPN – réexpédieront, vers leur interface avec l'équipement CPE, le trafic diffusé en voie descendante qui n'est *pas* chiffré. Par ailleurs, le trafic non L2VPN d'adresses GMAC non chiffrées, envoyé à la même adresse de destination Ethernet multidiffusée que celle qui est utilisée par un réseau privé L2VPN, sera également réexpédié par un câblo-modem L2VPN vers son interface avec l'équipement CPE. Sans précautions particulières, le trafic non L2VPN d'adresses GMAC en voie descendante va fuir dans le réseau d'équipement CPE – censé être privé – de l'abonné au réseau L2VPN.

La présente Recommandation traite le problème des fuites d'adresses GMAC dans le trafic non L2VPN par les mécanismes ci-après:

- filtrage du trafic descendant non chiffré (DUT);
- chiffrement multidiffusé en voie IP descendante (DIME, *downstream IP multicast encryption*).

7.5.2.1 Filtrage du trafic descendant non chiffré (DUT)

Un câblo-opérateur peut empêcher la fuite de trafic non chiffré non L2VPN au travers de câblo-modems conformes au modèle L2VPN, par activation du codage de filtrage du trafic descendant non chiffré (DUT). Quand le filtrage du trafic DUT est activé, un masque d'interface entre le trafic DUT et le câblo-modem (masque CMIM du trafic DUT) est défini afin de limiter le trafic de réexpédition en voie descendante non chiffré aux seules interfaces ayant un bit '1' pour cette interface dans le masque CMIM. Le masque CMIM du trafic DUT ne contient par défaut des bits '1' que pour les interfaces, internes au serveur local, avec le câblo-modem intégré et avec l'entité eSAFE, nécessitant que le câblo-modem empêche la réexpédition d'un tel trafic vers l'interface ou les interfaces CMCI du câblo-modem. Le filtrage du trafic DUT empêche à lui seul que des adresses GMAC de réseau non L2VPN dérivent dans un réseau d'équipement CPE d'abonné L2VPN.

7.5.2.2 Chiffrement multidiffusé en voie IP descendante (DIME)

Par défaut, les câblo-modems doivent permettre une réexpédition en mode espion d'adresses GMAC pour le fonctionnement en réseau L2VPN. Dans la plupart des câblo-modems DOCSIS 2.0 et antérieurs, ce mode provoque l'acheminement de tout le trafic non chiffré d'adresses GMAC jusqu'au logiciel du câblo-modem. Bien que le filtrage du trafic DUT par le logiciel du câblo-modem empêche pratiquement ce trafic de fuir dans l'interface avec l'équipement CPE, ce trafic peut, s'il est de volume notable, affecter la performance en terme de réexpédition du trafic L2VPN utile passant par le câblo-modem. Il est souhaitable de permettre que les câblo-modems L2VPN utilisent leurs filtres matériels d'identification SAID de façon à rejeter le volume important du trafic GMAC non L2VPN.

Dans la plupart des déploiements de systèmes CMTS, l'on s'attend que le trafic de session IP multidiffusé sera la plus notable source d'un gros volume de trafic GMAC en voie descendante. Il est souhaitable de chiffrer ce trafic dans un identificateur SAID qui soit inconnu des câblo-modems L2VPN, de telle sorte que leurs circuits matériels filtrent les paquets avant de les livrer au logiciel du réseau L2VPN.

Un système CMTS DOIT implémenter une option configurable de façon à activer ou désactiver le chiffrement multidiffusé en voie IP descendante (DIME). Avec le chiffrement DIME activé, le système CMTS DOIT chiffrer tout le trafic IP multidiffusé en voie descendant d'un réseau non

L2VPN qui est rejoint statiquement au moyen de la base MIB d'interface BPI+ ou qui est rejoint dynamiquement au moyen de requêtes SA-MAP en voie montante à partir d'un câblo-modem. Le chiffrement DIME ne nécessite pas que le système CMTS chiffre les multidiffusions IP en voie descendante d'un réseau non L2VPN *non rejoint*, (p. ex. multidiffusions en protocole RIPv2 ou OSPF).

En chiffrant, dans un identificateur SAID de réseau non L2VPN, le trafic IP multidiffusé sur un réseau non L2VPN rejoint, l'éventuel volume élevé du trafic multidiffusé en voie descendante d'un réseau non L2VPN est appelé à être filtré par les câblo-modems DOCSIS 2.0 implémentant la présente Recommandation.

Etant donné que le trafic GMAC non L2VPN est chiffré dans un identificateur SAID inconnu du câblo-modem L2VPN, celui-ci filtre le trafic en voie descendante et l'empêche de fuir dans le réseau d'équipement CPE privé.

7.5.2.3 Combinaison de réexpédition par réseaux L2VPN et par réseaux non L2VPN sur le même câblo-modem

La capacité de réseau L2VPN prend en charge la combinaison de réexpédition par réseaux L2VPN et par réseaux non L2VPN dans différents serveurs locaux d'équipement CPE connectés au même câblo-modem. Dans ce cas, les trafics L2VPN et non L2VPN ne sont évidemment pas découplés du ou des réseaux à l'interface CMCI avec le câblo-modem, aussi bien en voie montante qu'en voie descendante. De façon à prendre en charge les réseaux mixtes L2VPN et non L2VPN, le câblo-opérateur peut configurer des classificateurs L2VPN en voie montante, contenus dans le câblo-modem, avec une règle qui identifie le type particulier de trafic qui sera réexpédié sur le réseau L2VPN (p. ex. le trafic avec l'adresse MAC d'origine d'un équipement CPE particulier).

La présente Recommandation ne nécessite pas que le câblo-modem restreigne la réexpédition entre serveurs locaux L2VPN et non L2VPN d'équipement CPE quand ces serveurs sont connectés à différent ports d'interface CMCI d'un câblo-modem. Le modèle de réseau VLAN intégré (eVLAN) de réexpédition par câblo-modem, s'il est implémenté sur le câblo-modem, peut offrir ce découplage (voir Appendice III).

Le filtrage du trafic DUT ne devrait pas être activé en cas de combinaison de serveurs locaux L2VPN et non L2VPN d'équipement CPE sur le même câblo-modem, parce qu'il est nécessaire que les équipements CPE non L2VPN continuent à recevoir en voie descendante les messages ARP et DHCP diffusés. Avec un filtrage du trafic DUT désactivé, tout le trafic GMAC non chiffré en voie descendante va toutefois passer dans le réseau mixte d'équipement CPE. Afin d'empêcher ce passage, le chiffrement multidiffusé en voie IP descendante (DIME) peut être activé afin d'empêcher la réexpédition du trafic multidiffusé non rejoint, vers le réseau local en mode mixte de l'équipement CPE.

7.6 Exclusion du câblo-modem et de l'entité eSAFE

La présente Recommandation utilise le terme *inclus* afin de qualifier le trafic réexpédié au moyen du réexpéditeur L2VPN et le terme *exclu* afin de désigner tous les autres trafics non L2VPN.

Le service de réseau local transparent à l'abonné nécessite que le trafic des équipements CPE soit inclus dans la réexpédition L2VPN, alors que le trafic issu de câblo-modems intégrés et de tout autre serveur local intégré dans le câblo-modem sera exclu de la réexpédition L2VPN.

La capacité de réseau L2VPN peut toutefois être configurée de telle sorte que le trafic du câblo-modem intégré et de l'entité eSAFE intégrée puisse être réexpédié sur des réseaux L2VPN distincts, le cas échéant.

7.6.1 Modèle de réexpédition à partir du serveur local d'entité eSAFE et du câblo-modem

La Figure 7-1 décrit le modèle global de réexpédition L2VPN par le système CMTS et par le câblo-modem dans les serveurs locaux d'entité SAFE et de câblo-modem.

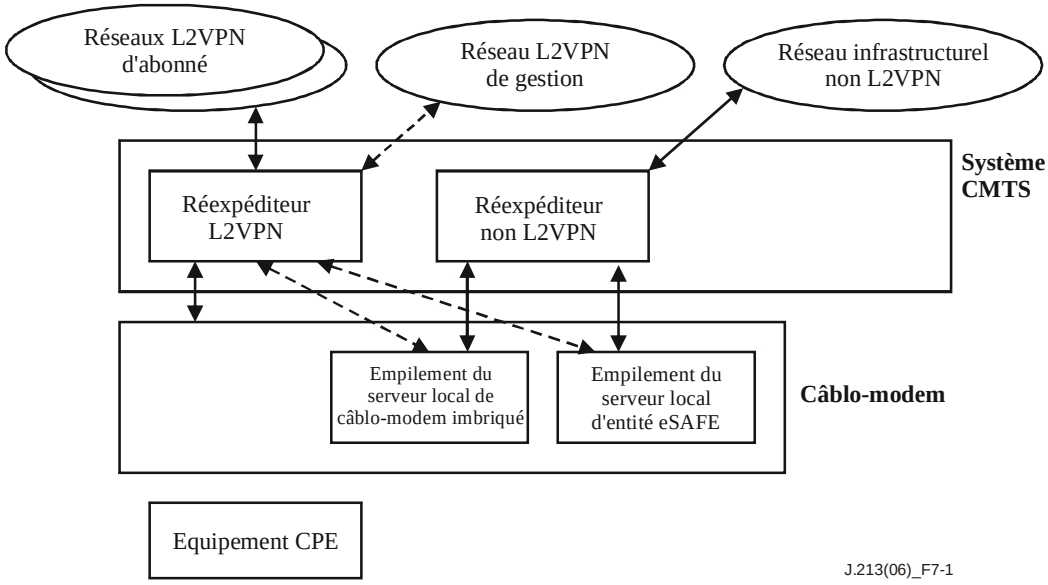

Figure 7-1 – Réexpédition par câblo-modem, adaptateur eMTA et équipement CPE

Dans le service TLS, le trafic à destination et en provenance de l'empilement IP du serveur local de câblo-modem intégré et d'entité eSAFE est exclu de la réexpédition L2VPN et est réexpédié par le réexpéditeur normal de flux non L2VPN du système CMTS, comme décrit par un trait plein dans la Figure 7-1.

Avec la capacité de gestion L2VPN, le trafic de post-inscription de câblo-modem intégré est classifié dans un flux de service de réexpédition L2VPN et inclus pour réexpédition L2VPN (trait interrompu). Aucun trafic de préinscription de câblo-modem intégré ne peut utiliser la capacité de réseau L2VPN parce que le chiffrement dans un identificateur SAID-L2VPN n'est pas possible avant l'inscription.

Le trafic de gestion à destination et en provenance d'un serveur local d'entité eSAFE peut utiliser le même réseau L2VPN gestionnaire que le câblo-modem intégré, ou son propre réseau L2VPN gestionnaire particulier, selon ce qui convient.

7.6.2 Masques d'interface avec le pont de commande MAC du câblo-modem

Conformément au modèle de pontage par adresses de commande MAC décrit dans la référence [b-UIT-T J.126], un câblo-modem appliquant la présente Recommandation est considéré comme implémentant un ensemble d'interfaces avec des ponts de commande MAC, comme résumé ci-dessous.

Tableau 7-2 – Interfaces avec le pont de commande MAC du câblo-modem

ifIndex	Description
(0)	(eCM: interface avec le serveur local, intégrée dans le câblo-modem)
1	Interface primaire avec l'équipement CPE, de même qu'avec les services de portail intégrés J.192 (ePS)
2	Interface RF
16	eMTA: interface avec le serveur local de l'agent de transport multimédia IPCablecom intégré
17	eSTB-IP: interface avec le serveur local IP du terminal adaptateur OpenCable intégré
18	Décodeur eSTB de passerelle DSG: interface avec la passerelle terminale DOCSIS du terminal adaptateur OpenCable intégré

La présente Recommandation introduit la convention que la valeur 0 de l'indice ifIndex est considérée comme devant s'appliquer à l'interface interne du serveur local avec l'empilement IP de gestion du câblo-modem, ou à son interface intégrée.

La réexpédition par câblo-modem dans la couche 2 d'un réseau L2VPN est considérée comme ne se produisant qu'en fonction d'une liste explicite des interfaces précédentes avec des ponts de commande MAC. Par exemple, le service transparent de réseau local implique qu'un routage n'a lieu qu'entre l'interface RF avec les commandes MAC (ifIndex 2) et l'interface primaire avec l'équipement CPE (ifIndex 1). Le service TLS n'est pas autorisé à accéder à l'interface intégrée dans le câblo-modem intégré ni à une quelconque autre interface avec le serveur local d'une entité eSAFE.

Pour chaque réseau L2VPN qui est réexpédié à l'intérieur d'un câblo-modem, un paramètre de masque d'interface avec un câblo-modem (CMIM) est configuré avec l'ensemble des interfaces avec des ponts de commande MAC qui sont autorisés à réexpédier des paquets à destination et en provenance de ce réseau L2VPN. Chaque interface avec un pont de commande MAC reçoit l'assignation d'une position binaire dans le masque CMIM correspondant à sa valeur d'indice ifIndex. L'interface avec le serveur local du câblo-modem intégré reçoit l'assignation de la position binaire 0 dans le masque CMIM.

Le paramètre de masque CMIM d'un réseau L2VPN est codé avec le même codage L2VPN par flux de service individuel que celui qui définit l'identificateur VPNID-L2VPN. Si le sous-type du masque CMIM est omis d'un codage de réexpédition L2VPN, sa valeur par défaut est celle qui est appropriée au service TLS (c'est-à-dire avec seulement les bits d'interface RFI (ifIndex 2) et d'interface primaire avec l'équipement CPE (ifIndex 1) activés). Le paramètre de masque CMIM est codé de la même façon que par les règles de codage de base d'un type d'objet "BITS" du protocole SNMP. Dans un nuplet TLV de sous-type de masque CMIM, le masque binaire est codé comme une chaîne d'octets de longueur variable, où la position binaire 0 est le premier bit de poids fort du premier octet; la position 1 est le second bit de poids fort; la position 7 est le bit de poids faible du premier octet. La position binaire 8 est le bit de poids fort du second octet. Par exemple, la valeur par défaut du masque CMIM, avec les positions binaires 1 et 2 activées, peut être codée comme un unique octet avec la valeur 0x60.

7.6.3 Exclusion du serveur local intégré

Quand un masque CMIM a la valeur zéro dans une position binaire d'interface avec un pont de commande MAC, tout le trafic de cette interface est configuré de façon à être exclu de la réexpédition L2VPN. En particulier, l'interface avec le serveur local intégrée dans le câblo-modem intégré (position binaire 0 d'interface dans le masque CMIM) est exclue des réseaux L2VPN du service TLS. Quand l'interface avec le serveur local intégrée dans le câblo-modem intégré est exclue d'un sous-type du masque CMIM dans un flux de service de réexpédition en voie montante L2VPN, le système CMTS DOIT exclure, de la réexpédition L2VPN en voie montante, tout le trafic

qui contient une adresse MAC d'origine qui concorde avec l'adresse MAC du serveur local par câblo-modem.

Etant donné que les câblo-modems non conformes sont incapables de classifier le trafic L2VPN du trafic non-L2VN en voie montante, un système CMTS DOIT prendre en charge le trafic de réexpédition en voie montante par réseaux aussi bien L2VPN que non L2VPN, issu d'un flux de service L2VPN de réexpédition d'un câblo-modem non conforme, sur la base de la vérification de l'adresse MAC d'origine par rapport à un masque d'interface avec un câblo-modem configuré pour ce flux de service. Le système CMTS DOIT aiguiller vers le réexpéditeur L2VPN les paquets issus des types de serveur local inclus. Le système CMTS NE DOIT PAS acheminer vers le réexpéditeur L2VPN le trafic issu des types de serveur local exclu.

Un système CMTS DOIT prendre en charge l'exclusion de l'adresse MAC de câblo-modem et au moins d'une seule autre adresse MAC d'entité eSAFE dans tous les flux de service de réexpédition L2VPN issus de câblo-modems aussi bien non conformes que conformes. Les câblo-modems non conformes peuvent avoir, au plus, une seule adresse MAC d'entité eSAFE vérifiée de cette façon. La présente Recommandation ne prend pas en charge la réexpédition L2VPN à partir d'un câblo-modem non conforme ayant plus d'un seul serveur local d'entité eSAFE. La présente Recommandation ne prend en charge la réexpédition L2VPN, à partir de câblo-modems conformes ayant plus d'un seul serveur local d'entité eSAFE, que par configuration de codages de classification de paquet en voie montante qui classifient explicitement le trafic d'entité eSAFE de réexpédition par réseau non L2VPN vers des flux de service de réexpédition en voie montante de réseau non L2VPN.

7.6.4 Acquisition intelligente, par le système CMTS, de l'adresse MAC du serveur intégré

Un système CMTS DOIT acquérir l'adresse MAC d'un câblo-modem intégré à partir de l'adresse MAC d'origine du message de demande de télémétrie initiale du câblo-modem et doit l'inclure dans la base docsDevCmCmtsStatusTable.

Le système CMTS utilise deux techniques afin d'acquérir l'adresse MAC des serveurs locaux d'entité eSAFE:

- dans les câblo-modems L2VPN conformes, le système CMTS DOIT acquérir les adresses MAC d'entité eSAFE à partir des codages de capacité de serveur local d'entité eSAFE (§ B.1.2) quand le câblo-modem s'inscrit;
- dans les câblo-modems non L2VPN conformes, le système CMTS DOIT surveiller les paquets DHCP en voie montante afin de déterminer les adresses MAC d'entité eSAFE.

7.6.4.1 Activation du sous-type de surveillance du trafic DHCP par entité eSAFE

Le système CMTS DOIT permettre la surveillance du trafic DHCP afin de déterminer les adresses MAC d'entité eSAFE issues d'un câblo-modem non conforme quand un sous-type d'activation de surveillance du trafic DHCP par entité eSAFE est présent dans un codage L2VPN par flux de service individuel (voir § B.3.3). La valeur du codage est un masque binaire qui permet de surveiller des serveurs locaux particuliers d'entité eSAFE. Le système CMTS NE DOIT PAS permettre la surveillance du trafic DHCP quand le sous-type d'activation de la surveillance du trafic DHCP par entité eSAFE est absent de tous les codages L2VPN par flux de service individuel ou ne possède pas de bit '1' pour le type particulier de serveur local d'entité eSAFE quand il est présent. Cette règle vise à empêcher la simulation d'entité eSAFE par des équipements CPE non intégrés et non autorisés.

Quand la surveillance du trafic DHCP par entité eSAFE est activée, le système CMTS DOIT prendre en charge la détection du type de serveur local d'entité eSAFE d'une adresse MAC, à partir de la sous-chaîne initiale de l'option 60 du paquet DISCOVER diffusé par protocole DHCP et à partir du serveur local d'entité eSAFE qui est relayé par le système CMTS, quand l'option 60 est présente. Quand la surveillance du trafic DHCP par entité eSAFE est activée, le système CMTS

DOIT prendre en charge la détection du type de serveur local d'entité eSAFE contenu dans une adresse MAC à partir du sous-type 2 de l'option 43 d'un paquet DISCOVER du protocole DHCP, issu du serveur local d'entité eSAFE relayé par le système CMTS, quand le sous-type 2 de l'option 43 est présent. Le Tableau 7-3 ci-dessous fournit les valeurs de ces options du protocole DHCP pour chaque type de serveur local d'entité eSAFE actuellement défini.

Tableau 7-3 – Sous-chaînes de surveillance du trafic DHCP par entité eSAFE

Type de serveur local d'entité eSAFE	Sous-chaîne de l'option 60 du protocole DHCP	Sous-chaîne de la sous-option 2 de l'option 43 du protocole DHCP
Adaptateur de terminal multimédia intégré [b-UIT-T J.167]	pktc	EMTA
Services de portail intégrés [b-UIT-T J.192]	CableHome	EPS

Le système CMTS DOIT acquérir l'adresse MAC de l'entité eSAFE à partir du champ d'identificateur de circuits matériels clients du paquet DISCOVER surveillé dans le protocole DHCP.

Dès que le système CMTS acquiert les adresses MAC des serveurs locaux d'entité eSAFE, le système CMTS exclut, de la réexpédition L2VPN, tout le trafic en voie montante issu de cette adresse MAC du serveur local DOCSIS.

7.6.5 Classification fondée sur l'interface

Le domaine de commande MAC à l'interface RF implémente les classificateurs DOCSIS de paquet en voie montante qui classifient, dans un flux de service en voie montante, une unité L2PDU pontée vers l'interface avec le domaine de commande MAC.

Dans un codage de classification de paquet en voie montante, le sous-type du masque CMIM représente une règle qui concorde avec le port du pont d'insertion de l'unité L2PDU. Cela permet aux classificateurs de classifier génériquement le trafic de l'équipement CPE, du câblo-modem intégré et de l'entité eSAFE, par type de serveur local, au lieu d'exiger que les classificateurs statiques soient fondés sur l'adresse MAC réelle ou sur l'adresse IP assignée du serveur local.

La capacité de classification au serveur local est très utile lors de l'implémentation de réseaux L2VPN de gestion afin de découpler le trafic de gestion CM et eSAFE du trafic de charge utile dans la couche 2 d'un réseau infrastructurel. Elle permet aux classificateurs du câblo-modem de classifier le trafic en voie montante d'un câblo-modem intégré et/ou d'une entité eSAFE afin de l'insérer dans un autre flux de service de réexpédition en voie montante L2VPN pour le réseau L2VPN gestionnaire.

7.7 Qualité de service d'un réseau L2VPN

7.7.1 Découplage des flux de service

Un important aspect de l'offre de service L2VPN par un opérateur est le découplage, non seulement de la réexpédition du trafic, mais également de la qualité de service. Il ne devrait pas être possible qu'un seul flux de trafic L2VPN (ou même qu'un flux de trafic non L2VPN) de volume excessif puisse affecter notablement la qualité de service reçue par tout autre flux de réseau L2VPN. En conséquence, la présente Recommandation impose que les trafics en voie descendante de réseaux L2VPN soit découplés les uns des autres ainsi que du trafic non L2VPN par insertion de chaque trafic dans un flux de service distinct (SF, *service flow*). Dans le cas d'une réexpédition en mode point à point, ce découplage se produit automatiquement parce que chaque câblo-modem possède

déjà un flux de service primaire en voie descendante. Dans le cas d'une réexpédition multipoint, la présente Recommandation impose que chaque réseau L2VPN possède un flux de service distinct pour son trafic en voie descendante d'adresses MAC collectives élargies et d'adresses MAC individuelles à destination inconnue.

7.7.2 Priorité d'utilisateur IEEE 802.1

Le modèle de pontage dans la couche 2 selon l'IEEE 802.1 utilise le concept de priorité d'utilisateur avec huit valeurs possibles afin d'indiquer la qualité de service à fournir lors de la réexpédition d'une unité L2PDU [IEEE 802.1Q]. Ce champ sert à offrir une qualité de service différenciée à différents flux de trafic *dans le même* réseau L2VPN.

Quand une unité L2PDU est réexpédiée avec une balise IEEE 802.1 par une interface NSI entre un réseau Ethernet et un réseau interurbain, la priorité d'utilisateur du paquet est codée dans les trois positions binaires supérieures d'une valeur de commande de balise 802.1Q. L'Appendice II fournit des détails sur l'encapsulation IEEE 802.1Q.

Un système CMTS DOIT accepter les bits de priorité d'une balise délimitatrice de service 802.1Q à un port d'entrée dans l'interface NSI en tant qu'attribut, contenu dans le paquet, de priorité d'insertion de l'utilisateur dans un flux L2VPN. Le système CMTS DOIT conserver la priorité d'utilisateur du paquet dans le réexpéditeur L2VPN (éventuellement en le régénérant au moyen d'une configuration propre au vendeur) et DOIT utiliser la valeur d'extraction de priorité d'utilisateur afin de vérifier sa concordance avec le sous-type d'étendue des priorités d'utilisateur contenu dans les codages L2VPN de classificateur en voie descendante.

En voie montante, la présente Recommandation prescrit que la priorité d'utilisateur du trafic L2VPN en voie montante soit explicitement configurée comme étant le sous-type de priorité d'insertion de l'utilisateur, contenu dans un codage de réexpédition L2VPN. Elle prescrit que le réexpéditeur L2VPN conserve cette priorité d'utilisateur (éventuellement régénérée) lors du codage de la balise IEEE 802.1Q en vue de l'extraction du flux d'un port d'interface NSI. Si le sous-type de priorité d'insertion de l'utilisateur dans un flux est omis, le système CMTS part du principe que la priorité d'insertion de l'utilisateur dans un flux est égale à zéro. La prescription que la priorité d'utilisateur soit explicitement configurée dans le codage de réexpédition L2VPN empêche l'équipement CPE de soumettre des paquets L2VPN ayant une valeur arbitraire de priorité d'utilisateur dans le réseau infrastructurel L2VPN du câblo-opérateur.

7.7.3 Classification des niveaux de priorité d'insertion de l'utilisateur en voie descendante

La présente Recommandation définit un sous-type d'étendue des priorités d'utilisateur contenu dans un codage L2VPN qui apparaît comme un nouveau critère de concordance avec une règle dans un codage de classificateur de paquet en flux de service descendant. Le sous-type d'étendue des priorités d'utilisateur est décrit dans le § B.3.9. Quand un sous-type d'étendue des priorités d'utilisateur est présent dans un codage de classificateur de paquet en flux de service descendant, le système CMTS ne DOIT faire correspondre ce classificateur qu'aux paquets L2VPN réexpédiés avec une priorité d'utilisateur incluse dans l'étendue indiquée.

7.7.4 Priorité d'entrée de l'utilisateur en voie montante

La présente Recommandation demande que le système CMTS associe une priorité configurée d'utilisateur à un flux de service de réexpédition L2VPN en voie montante sur la base d'un sous-type configuré de priorité d'entrée de l'utilisateur contenu dans le codage L2VPN par flux de service individuel qui a défini ce flux de service. Le sous-type de priorité d'entrée de l'utilisateur dans un flux est décrit dans le § B.3.8.

Un système CMTS PEUT implémenter une configuration propre au vendeur afin de sélectionner la priorité d'entrée de l'utilisateur dans un flux de paquets L2VPN en voie montante. Le modèle particulier de pontage implémenté par le système CMTS (p. ex. [IEEE 802.1s] ou [IEEE 802.1ad])

PEUT assurer la régénération d'une priorité d'entrée de l'utilisateur en voie montante en fonction d'une autre valeur interne de priorité d'utilisateur pour le paquet dans le système CMTS.

Le système CMTS NE DOIT PAS utiliser de balise de priorité absolue, appliquée par l'équipement CPE afin de déterminer la priorité d'entrée de l'utilisateur dans un flux de paquets en voie montante. Si nécessaire, le câblo-modem peut être configuré de façon à classifier le paquet balisé par l'équipement CPE comme étant à priorité absolue en voie montante, de façon à l'insérer dans un flux de service configuré avec un sous-type explicite de priorité d'entrée de l'utilisateur. Si le système CMTS implémente un réexpéditeur par pont IEEE 802.1ad, ce système CMTS PEUT appliquer la balise interne de priorité d'utilisateur client à la balise externe de priorité d'utilisateur de service.

Noter que le paramètre de priorité d'utilisateur d'un paquet L2VPN définit seulement la priorité de la réexpédition du paquet par l'intermédiaire des ponts du réseau infrastructurel de couche 2; il n'affecte pas la réexpédition du paquet en voie montante ou en voie descendante à l'interface RF-DOCSIS. Seul l'ensemble paramétrique de qualité de service du flux de service dans lequel le paquet est classifié définit la priorité de réexpédition de ce paquet à une interface RF-DOCSIS.

7.7.5 Qualité de service du réseau infrastructurel de couche 2

Dans le réseau ponté du réseau infrastructurel de couche 2, la priorité de pontage d'un paquet L2VPN peut être indiquée de diverses façons:

- dans les bits de priorité d'utilisateur d'une balise IEEE 802.1 externe;
- dans les bits expérimentaux EXP d'une étiquette de ligne privée à commutation MPLS;
- dans les bits de séquence DSCP d'une encapsulation de ligne privée L2TPv3.

Le système CMTS DOIT transmettre un paquet en voie montante L2VPN par un port d'interface NSI avec la priorité d'utilisateur de sortie de flux codée en fonction de son encapsulation de flux à l'interface NSI. Le mappage de priorité d'utilisateur de sortie de flux sur des bits EXP de commutation MPLS ou sur des valeurs de séquence DSCP est hors du domaine d'application de la présente Recommandation.

Concernant l'encapsulation IETF d'une ligne privée à l'interface NSI avec le trafic d'un réseau L2VPN, la détermination de la priorité d'entrée de l'utilisateur en voie descendante et le codage de la priorité d'utilisateur de sortie de flux montant sur la base de bits EXP de commutation MPLS ou de valeurs L2TPv3 de séquence DSCP sont hors du domaine d'application de la présente Recommandation.

7.8 Fonctionnement à balises 802.1Q empilées ou intégrées

La sélection du réseau L2VPN particulier pour le trafic routé en voie montante est toujours indiquée par le sous-type d'identificateur VPNID du codage L2VPN. La présente Recommandation ne vise pas l'interprétation des balises 802.1Q appliquées par l'équipement CPE et reçues par le port Ethernet d'un câblo-modem afin de réexpédier en voie montante. De telles balises sont considérées comme non délimitatrices de service et sont toujours ignorées aux fins de la sélection de réseau L2VPN par le système CMTS-DOCSIS. Ces balises non délimitatrices de service sont réexpédiées dans le cadre de la charge utile de l'équipement CPE. Les systèmes CMTS-DOCSIS et les câblo-modems conformes à la présente Recommandation prennent en charge la réexpédition de paquets Ethernet de longueur maximale avec une seule balise 802.1Q non délimitatrice de service d'abonné. C'est-à-dire qu'un câblo-modem prenant en charge la présente Recommandation est en mesure de réexpédier des paquets de 1522 octets entre ses interfaces RF et CPE, tandis qu'un système CMTS est en mesure de réexpédier des paquets de 1526 octets sur son port d'interface NSI avec un réseau Ethernet à balisage 802.1Q.

Quand un paquet muni par l'équipement CPE d'une balise interne non délimitatrice de service est réexpédié par un port d'interface NSI qui est également en train d'utiliser l'encapsulation IEEE 802.1Q, le système CMTS ajoute une balise externe délimitatrice de service contenant

l'identificateur de réseau VLAN configuré en format d'encapsulation de flux à l'interface NSI. Il s'agit de ce qui est appelé *balisage 802.1Q empilé ou intégré*. Les critères IEEE 802.1P/Q de codage de classification de paquet, indiqués dans le § C.2.1.7 de [UIT-T J.122], s'appliquent seulement à une éventuelle balise 802.1Q non délimitatrice de service fournie par l'équipement CPE lorsque le paquet apparaît à l'interface RFI. Ces critères ne s'appliquent pas à la valeur de balise externe délimitatrice de service fournie lorsque le paquet apparaît par un port d'interface NSI. Par exemple, le câblo-modem peut classifier les paquets en voie montante d'équipement CPE vers un flux de service particulier, sur la base des bits de priorité de la balise appliquée par l'équipement CPE.

Afin d'empêcher l'équipement CPE de faire un usage erroné des priorités d'utilisateur dans la couche 2 du réseau infrastructurel, le système CMTS NE DOIT PAS interpréter une balise à priorité absolue, appliquée par l'équipement CPE, comme définissant la priorité d'entrée de l'utilisateur en voie montante d'un paquet L2VPN. La priorité d'utilisateur d'un paquet en voie montante n'est définie que par le sous-type configuré de priorité d'utilisateur selon la norme IEEE 802.1, contenu dans le codage L2VPN de réexpédition par flux de service individuel qui s'applique à ce paquet. Une balise à priorité absolue appliquée par l'équipement CPE est traitée comme une balise non délimitatrice de service et est empilée comme une balise interne quand elle est réexpédiée par le système CMTS. Si une balise de priorité appliquée par l'équipement CPE est recherchée afin de sélectionner la priorité d'entrée de l'utilisateur en voie montante, le câblo-modem devrait être configuré de façon à classifier le paquet vers un flux de service ayant un sous-type explicite de priorité d'entrée de l'utilisateur. Cela permet au câblo-opérateur de commander la priorité des paquets réexpédiés dans la couche 2 du réseau infrastructurel.

En voie descendante, les critères IEEE 802.1P/Q du codage de classification de paquet selon le § C.2.1.7 de [UIT-T J.122] ne s'appliquent qu'à une balise interne, non délimitatrice de service, contenue dans le paquet tel qu'il apparaît à l'interface RFI. Noter que les systèmes CMTS ne sont pas tenus d'implémenter ces critères de couche 2 en voie descendante. Ce qui est habituellement recherché consiste toutefois à classifier le trafic en voie descendante conformément à la priorité ou à l'identificateur de réseau VLAN figurant dans la balise délimitatrice de service externe lorsque le paquet est apparu à l'*interface NSI*. La présente Recommandation définit les codages L2VPN de classificateur en voie descendante de façon à permettre une classification sur la base de l'identificateur VPNID et de la priorité d'utilisateur du paquet comme signalé dans son encapsulation à l'interface NSI.

7.9 Interconnexion arborescente par chemin critique et détection des boucles logiques

La [UIT-T J.122] décrit le protocole DOCSIS d'interconnexion arborescente par chemin critique (DSTP, *DOCSIS spanning tree protocol*). Malheureusement, peu de câblo-modems – s'il en existe – implémentent le protocole DSTP, de sorte que l'on ne peut compter sur celui-ci afin d'éviter les boucles de pontage L2VPN. Un opérateur est censé configurer les réseaux d'abonné L2VPN de façon exempte de boucles ou est censé dépendre de l'équipement d'abonné proprement dit afin d'implémenter le protocole d'interconnexion arborescente de l'IEEE et de supprimer tout pontage en boucle sur un réseau L2VPN d'abonné. Le présent paragraphe décrit les exigences d'un système CMTS afin d'empêcher un refus de service L2VPN quand un abonné configure un pontage en boucle, accidentellement ou intentionnellement.

Le système CMTS DOIT réexpédier de façon transparente le protocole d'interconnexion arborescente (STP, *spanning tree protocol*) de l'IEEE dans le réseau L2VPN de l'abonné.

Un système CMTS PEUT implémenter le protocole d'interconnexion arborescente DOCSIS et transmettre des unités BPDU du protocole DSTP à toutes les interfaces NSI et RF configurées pour le fonctionnement en réseau L2VPN. Le système CMTS DOIT transmettre les paquets du protocole DOCSIS d'interconnexion arborescente par chemin critique en format non balisé par une interface NSI avec un flux IEEE 802.1Q, ces paquets étant chiffrés dans un identificateur SAID fourni aux câblo-modems L2VPN à une interface RF avec le domaine de commande MAC du système CMTS.

Un système CMTS PEUT implémenter un identificateur SAID d'interconnexion arborescente DOCSIS (DST) afin de réexpédier spécifiquement par interconnexion DST vers les ports d'équipement CPE de tous les câblo-modems L2VPN.

Un système CMTS DOIT empêcher un pontage en boucle dans un réseau L2VPN donné, qui refuserait toute réexpédition ou élargissement de trafic dans un autre réseau L2VPN non ponté en boucle. Afin de répondre à cette exigence, un système CMTS PEUT nécessiter une configuration des débits maximaux de réexpédition par flux de service, aussi bien en voie descendante qu'en voie montante, à condition que de telles limites ne soient pas inférieures à 10% de la capacité de liaison.

8 Exigences relatives au câblo-modem

Un câblo-modem DOIT accepter un ou plusieurs sous-types de descripteur d'association de sécurité L2VPN, ajoutés par un système CMTS à tout codage de réexpédition L2VPN dans un message REG-RSP ou DSx-RSP adressé à ce câblo-modem. Celui-ci associe, au réseau L2VPN unique identifié dans le codage L2VPN, les identificateurs SAID des descripteurs d'association de sécurité contenus dans le codage L2VPN. Le câblo-modem DOIT être capable d'associer à un réseau L2VPN un nombre quelconque de ses identificateurs SAID disponibles. Le câblo-modem DOIT être capable d'associer plus d'un seul identificateur SAID à un même réseau L2VPN. Un câblo-modem recevant un codage L2VPN avec un sous-type de descripteur d'association de sécurité L2VPN concernant un identificateur SAID qui n'est pas encore établi sur ce câblo-modem DOIT lancer une transaction de gestion BPKM de clé TEK afin d'établir le nouvel identificateur SAID-L2VPN [UIT-T J.125]. Un câblo-modem recevant un sous-type de descripteur d'association de sécurité L2VPN dans un message REG-RSP DOIT attendre l'exécution de l'autorisation d'interface BPI avant de lancer la gestion BPKM de clé TEK. Le câblo-modem détermine qu'un paquet en voie descendante doit être réexpédié sur un réseau L2VPN quand ce paquet est chiffré avec un identificateur SAID-L2VPN. Un câblo-modem DOIT remplacer l'ensemble des identificateurs SAID d'un réseau L2VPN quand il reçoit un codage L2VPN de niveau supérieur dans un message de gestion d'adresse MAC qui identifie ce réseau L2VPN. Le câblo-modem DOIT interrompre le déchiffrement en voie descendante d'un identificateur SAID-L2VPN quand il reçoit, dans un message de flux de service dynamique, un codage L2VPN de niveau supérieur dans un identificateur de réseau L2VPN qui omet le sous-type de descripteur d'association de sécurité avec cet identificateur SAID.

Un câblo-modem DOIT réexpédier en mode espion tout le trafic destiné en voie descendante à des adresses MAC collectives (GMAC), qui est chiffré dans un identificateur SAID-L2VPN signalé au câblo-modem, quelle que soit la destination des adresses GMAC du paquet.

Le câblo-modem NE DOIT PAS appliquer les règles de filtrage ou de réexpédition multipoint selon le § 5.3.1.3.1 [UIT-T J.122] à un trafic GMAC chiffré en voie descendante dans un identificateur SAID-L2VPN. Un câblo-modem DOIT continuer à implémenter les règles DOCSIS 2.0 de réexpédition d'adresses GMAC en voie descendante pour tous les paquets non chiffrés et pour les paquets chiffrés dans un identificateur SAID de réseau non L2VPN.

Un câblo-modem NE DOIT PAS appliquer les règles de réexpédition multidiffusée par protocole IGMP du § 5.3.1.3.1 [UIT-T J.122] à d'éventuels paquets en voie montante (p. ex. comptes rendus d'appartenance au protocole IGMP) classifiés dans un flux de service L2VPN de réexpédition. Le câblomodem DOIT continuer à mettre en œuvre les règles DOCSIS de réexpédition multidiffusée par protocole IGMP pour les comptes rendus d'appartenance au protocole IGMP non classifiés en voie montante dans un flux de service L2VPN de réexpédition.

Un câblo-modem conforme DOIT restreindre la réexpédition par pont, des paquets en voie descendante chiffrés dans un identificateur SAID-L2VPN, aux seules interfaces de pont signalées par un bit '1' dans le masque d'interface avec câblo-modem (CMIM) configuré pour ce réseau L2VPN. Par exemple, le câblo-modem n'achemine pas le trafic L2VPN en voie descendante

jusqu'au câblo-modem intégré ou jusqu'à un serveur local interne d'entité eSAFE si le masque CMIM omet cette interface avec le serveur local (c'est-à-dire contient un bit '0' pour cette interface), même si le paquet est envoyé à l'adresse MAC de destination individuelle de ce serveur local. De même, le câblo-modem n'achemine pas, jusqu'à des serveurs locaux internes, le trafic destiné à des adresses collectives (GMAC) étiquetées dans un réseau L2VPN, quand le masque CMIM de ce réseau L2VPN omet l'interface interne avec le serveur local.

Un câblo-modem DOIT prendre en charge un critère de règle de classification signalé par un masque d'interface avec un câblo-modem (CMIM) dans le codage L2VPN d'un paquet de classificateur en voie montante, que ce codage classifie ou non vers un flux de service L2VPN de réexpédition. Le câblo-modem DOIT considérer le critère comme ayant été trouvé en correspondance quand l'adresse MAC d'origine d'un paquet en voie montante concerne un type de serveur local avec un bit '1' dans le masque d'interface avec un câblo-modem. Le câblo-modem DOIT considérer le critère comme n'étant pas trouvé en correspondance et DOIT réexpédier ou rejeter un paquet en conséquence, quand l'adresse MAC d'origine concerne un type de serveur local avec un bit '0' dans le masque d'interface avec un câblo-modem.

Un câblo-modem DOIT prendre en charge l'élément de service de filtrage du trafic descendant non chiffré (DUT) comme décrit dans le § B.2 et annoncer cela dans un codage de capacité de filtrage du trafic DUT (voir le § B.1.3). Quand le filtrage du trafic DUT est activé, un câblo-modem DOIT restreindre la réexpédition par pont du trafic descendant non chiffré aux seules interfaces indiquées dans le masque d'interface entre le trafic DUT et le câblo-modem (masque CMIM du trafic DUT) impliqué ou configuré par le codage de filtrage du trafic DUT.

Etant donné que la position binaire 1 du masque CMIM (correspondant à l'interface ifIndex 1 avec le pont du câblo-modem) représente l'*ensemble* de *toutes* les interfaces avec l'équipement CPE dans les codages de réexpédition L2VPN, de filtrage du trafic DUT et de classificateur en voie montante, un câblo-modem conforme qui implémente plus d'une seule interface avec l'équipement CPE PEUT attribuer une position binaire de masque CMIM comprise entre 5 et 15 afin de représenter son unique interface primaire avec l'équipement CPE. Il en va de telle sorte que les valeurs de masque CMIM (et des autres filtres DOCSIS propres à chaque interface) peuvent représenter l'interface primaire avec l'équipement CPE proprement dite, indépendamment de l'ensemble de toutes les autres interfaces avec l'équipement CPE. Le câblo-modem DOIT continuer à signaler seulement l'indice ifIndex 1 comme désignant son interface primaire avec l'équipement CPE.

Un câblo-modem DOIT réexpédier en voie montante ou descendante des paquets de longueur pouvant atteindre 1522 octets, ce qui autorise une unique balise 802.1Q d'abonné sur un paquet Ethernet de longueur maximale.

Un câblo-modem DOIT annoncer le sous-type de capacité L2VPN dans le codage des capacités du modem (voir § B.1.1) de sa demande d'inscription.

Un câblo-modem avec serveurs locaux d'entités intégrées eSAFE DOIT les annoncer au système CMTS dans un message de demande d'inscription avec un codage de capacité de serveur local d'entité eSAFE (voir § B.1.2) pour chaque serveur local d'entité eSAFE.

Un câblo-modem DOIT ignorer de façon transparente un codage L2VPN contenu dans tout contexte de nuplet TLV non mentionné dans la présente Recommandation. Un câblo-modem DOIT ignorer de façon transparente tout sous-type non reconnu de codage L2VPN et DOIT traiter normalement tous les codages L2VPN reconnus.

Annexe A

Exigences relatives à la base DOCS-L2VPN-MIB du système CMTS

Un système CMTS DOIT implémenter la base DOCS-L2VPN-MIB. Un câblo-modem n'implémente pas la base DOCS-L2VPN-MIB.

A.1 Conformité de la base DOCS-L2VPN-MIB

Légende

M	Obligatoire
NA	Non applicable
RO	Lecture seulement
RC	Lecture-Création

Base DOCS-L2VPN-MIB				
DocsL2vpnIdToIndexTable (modes point à point et multipoint)				
Objet	CM	Accès	CMTS	Accès
docsL2vpnIdToIndexIdx	NA	NA	M	RO
docsL2vpnIndexToIdTable (modes point à point et multipoint)				
Objet	CM	Accès	CMTS	Accès
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				
Objet	CM	Accès	CMTS	Accès

Base DOCS-L2VPN-MIB				
docsL2vpnVpnCmDhcpSnooping	NA	NA	M	RO
docsL2vpnVpnCmCMIM	NA	NA	M	RO
docsL2vpnVpnCmVendorSpecific	NA	NA	M	RO
docsL2vpnVpnCmStatsTable (modes point à point et multipoint)				
Objet	CM	Accès	CMTS	Accès
docsL2vpnVpnCmStatsUpstreamPkts	NA	NA	M	RO
docsL2vpnVpnCmStatsUpstreamDiscards	NA	NA	M	RO
docsL2vpnVpnCmStatsDownstreamPkts	NA	NA	M	RO
docsL2vpnVpnCmStatsDownstreamDiscards	NA	NA	M	RO
docsL2vpnPortStatusTable (modes point à point et multipoint)				
Objet	CM	Accès	CMTS	Accès
docsL2vpnPortStatusSAID	NA	NA	M	RO
docsL2vpnSfStatusTable (modes point à point et multipoint)				
Objet	CM	Accès	CMTS	Accès
docsL2vpnSfStatusL2vpnId	NA	NA	M	RO
docsL2vpnSfStatusIngressUserPriority	NA	NA	M	RO
docsL2vpnSfStatusVendorSpecific	NA	NA	M	RO
docsL2vpnPktClassTable (modes point à point et multipoint)				
Objet	CM	Accès	CMTS	Accès

Base DOCS-L2VPN-MIB				
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 (mode point à point seulement)				
Objet	CM	Accès	CMTS	Accès
docsL2vpnCmNsiEncapSubtype	NA	NA	M	RO
docsL2vpnCmNsiEncapValue	NA	NA	M	RO
docsL2vpnCmNsiAGI	NA	NA	M	RO
docsL2vpnCmNsiSAII	NA	NA	M	RO
docsL2vpnCmVpnCpeTable (Multipoint seulement)				
Objet	CM	Accès	CMTS	Accès
docsL2vpnCmVpnCpeMacAddress	NA	NA	M	RO
docsL2vpnVpnCmCpeTable (Multipoint seulement)				
Objets	CM	Accès	CMTS	Accès
docsL2vpnVpnCmCpeMacAddress	NA	NA	M	RO
docsL2vpnDot1qTpFdbExtTable (Multipoint seulement)				
Objets	CM	Accès	CMTS	Accès
docsL2vpnDot1qTpFdbExtTransmitPkts	NA	NA	M	RO

Base DOCS-L2VPN-MIB				
docsL2vpnDot1qTpFdbExtReceivePkts	NA	NA	M	RO
docsL2vpnDot1qTpGroupExtTable (Multipoint seulement)				
Objets	CM	Accès	CMTS	Accès
docsL2vpnDot1qTpGroupExtTransmitPkts	NA	NA	M	RO
docsL2vpnDot1qTpGroupExtReceivePkts	NA	NA	M	RO

A.2 Définitions de la base 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
        "This is the management MIB for devices complying to the
```

```
        DOCSIS L2VPN Feature."
    REVISION "200603280000Z"
    DESCRIPTION
        "Initial version."
    ::= { clabProjDocsis 8 }

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

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

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

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

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

    SYNTAX      OCTET STRING

-- Cable Modem Interface List

DocsL2vpnIfList ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
            "An object of this type indicates a set of CM
```

```
            MAC bridge interfaces, encoded as a BITS syntax with a ?1?
            Bit for each interface included in the set.

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

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

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

            ifIndex value 2 corresponds to the docsCableMacLayer
            RF MAC interface.

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

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

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

            ifIndex value 17 is assigned to the IP management host
            interface of an embedded Set Top Box (eSTB). ifIndex value
            18 is reserved for the DOCSIS Set-top Gateway (DSG) traffic
            delivered to an eSTB.

            ifIndex values 19 through 31 are
            reserved for future defined embedded Service Application."
    SYNTAX      BITS {
        eCm(0),
        cmci(1),
        docsCableMacLayer(2),
        docsCableDownstream(3),
        docsCableUpstream(4),
        -- 5..15 reserved for other CPE interfaces
        eMta(16),
        eStbIp(17),
        eStbDsg(18)
        -- 19..31 reserved for other eSAFE interfaces
    }

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

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

--  None defined
```

```
--
-- L2VPN MIB Objects
--

docsL2vpnMIBObjects OBJECT IDENTIFIER ::= { docsL2vpnMIB 1 }

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

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

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

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

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

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

-------------------------------------------------------------
--
-- L2VPN Index to L2VPN Identifier mapping tables
--
docsL2vpnIndexToIdTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnIndexToIdEntry
```

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

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

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

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

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

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

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

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

```
    ::= { docsL2vpnCmTable 1 }

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

            If the CMTS does not allocate an individual SAID for
            multipoint forwarding (as is recommended),it MUST
```

```
            report this object as zero."
    ::= { docsL2vpnVpnCmEntry 2 }

docsL2vpnVpnCmVendorSpecific OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object encodes the concatenation of all Vendor
            Specific Subtype encodings that appeared in any
            registration per-CM L2VPN Encoding associated with this
            entry."
    ::= { docsL2vpnVpnCmEntry 3 }

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

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

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

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

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

docsL2vpnVpnCmStatsUpstreamDiscards OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
            "The number of L2-forwarded packets
            discarded from this instance's
            Cable Modem on this instance's VPN."
    ::= { docsL2vpnVpnCmStatsEntry 3 }

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

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

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

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

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

DocsL2vpnPortStatusEntry ::= SEQUENCE {
        docsL2vpnPortStatusGroupSAId   Integer32
    }

docsL2vpnPortStatusGroupSAId OBJECT-TYPE
    SYNTAX      Integer32 (0..16383)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
            "The Group SAID associated with this VPN on a
            particular CMTS MAC domain. This SAID is used to encrypt
            all downstream flooded bridge traffic sent to CMs on
            this VPN and CMTS MAC domain bridge port.

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

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

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

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

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

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

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

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

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

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

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

docsL2vpnPktClassTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnPktClassEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table provides the L2VPN-specific objects for
            packet classifiers that apply to only L2VPN traffic.
            The indices of this table are a subset of the
            indices of classifiers in docsQosPktClassTable."
    ::= { docsL2vpnMIBObjects 8 }

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

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

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

docsL2vpnPktClassUserPriRangeLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The lower priority of the user Priority Range subtype
```

```
            of a Downstream Classifier L2VPN Encoding. If the subtype
            was omitted, this object has value 0."
    ::= { docsL2vpnPktClassEntry 2 }

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

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

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

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

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

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

docsL2vpnCmNsiEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnCmNsiEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry indexed by VPN ID and Cable Modem Index that
```

```
            describes the point-to-point forwarding between a single
            NSI encapsulation and a single CM. This table is
            implemented only for a CM forwarding an L2VPN on a
            point-to-point basis. It is associated with a single
            per-CM L2VPN encoding."
    INDEX { docsL2vpnIdx, docsIfCmtsCmStatusIndex }
    ::= { docsL2vpnCmNsiTable 1 }

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

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

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

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

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

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

--------------------------------------------------------------------
--
-- Point-to-Multipoint Only
```

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

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

docsL2vpnCmVpnCpeEntry OBJECT-TYPE
    SYNTAX      DocsL2vpnCmVpnCpeEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table is a list of CPEs, indexed by the VPNs on a
            Cable Modem."
    INDEX { docsIfCmtsCmStatusIndex,
        docsL2vpnIdx,
        docsL2vpnCmVpnCpeMacAddress }
    ::= { docsL2vpnCmVpnCpeTable 1 }

DocsL2vpnCmVpnCpeEntry ::= SEQUENCE {
        docsL2vpnCmVpnCpeMacAddress   MacAddress
    }

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

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

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

```
DocsL2vpnVpnCmCpeEntry ::= SEQUENCE {
        docsL2vpnVpnCmCpeMacAddress   MacAddress
    }

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

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

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

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

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

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

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

```
-- dot1qTpGroupTable Extension
--  (Point-to-multipoint only)
--
docsL2vpnDot1qTpGroupExtTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF DocsL2vpnDot1qTpGroupExtEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains packet counters for
            Multicast MAC Addresses within a VPN."
    ::= { docsL2vpnMIBObjects 13 }

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

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

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

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

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

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

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

    MODULE    -- docsL2vpn
      -- conditionally mandatory groups
    GROUP docsL2vpnBaseGroup
```

```
    DESCRIPTION
            "Mandatory in all CMTSs."

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

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

    ::= { docsL2vpnCompliances 1 }

docsL2vpnBaseGroup OBJECT-GROUP
    OBJECTS {
        docsL2vpnIdToIndexIdx,
        docsL2vpnIndexToIdId,

        docsL2vpnCmCompliantCapability,
        docsL2vpnCmDutFilteringCapability,
        docsL2vpnCmDutCMIM,
        docsL2vpnCmDhcpSnooping,

        docsL2vpnVpnCmCMIM,
        docsL2vpnVpnCmVendorSpecific,
        docsL2vpnVpnCmIndividualSAId,

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

        docsL2vpnPortStatusGroupSAId,

        docsL2vpnSfStatusL2vpnId,
        docsL2vpnSfStatusIngressUserPriority,
        docsL2vpnSfStatusVendorSpecific,

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

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

docsL2vpnMultipointGroup OBJECT-GROUP
    OBJECTS {
```

```
        docsL2vpnCmVpnCpeMacAddress,

        docsL2vpnVpnCmCpeMacAddress,

        docsL2vpnDot1qTpFdbExtTransmitPkts,
        docsL2vpnDot1qTpFdbExtReceivePkts,

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

Annexe B

Codage des paramètres

B.1 Capacités

B.1.1 Capacité de réseau L2VPN

Cette capacité indique si le câblo-modem est conforme aux exigences L2VPN qui sont spécifiées dans le § 8. Le fonctionnement d'un réseau L2VPN peut cependant être assuré par des câblo-modems qui n'implémentent pas ces exigences, mais avec possibilité de limitations.

Type	Longueur	Valeur
5.17	1	0 CM non conforme à L2VPN-DOCSIS, § 8 (par défaut) 1 CM conforme à L2VPN-DOCSIS, § 8

B.1.2 Capacité de serveur local d'entité fonctionnelle intégrée de service ou d'application (eSAFE)

Ce codage de capacité informe le système CMTS du type et de l'adresse MAC d'un serveur local d'entité eSAFE intégrée dans le câblo-modem. Cette opération est nécessaire afin que le système CMTS garantisse une réexpédition appropriée selon les versions IPv4 et IPv6 (à venir) du trafic en voie montante issu du serveur local d'entité eSAFE. Un codage distinct de capacité du serveur local d'entité eSAFE est requis pour chaque serveur local d'entité eSAFE intégrée dans le câblo-modem.

Type	Longueur	Valeur
5.18	7	indice ifIndex d'entité eSAFE (1 octet), adresse MAC d'entité eSAFE (6 octets) indice ifIndex d'entité eSAFE: 1 ePS 15 Adaptateur eMTA 17 Décodeur eSTB-IP 18 Décodeur eSTB de passerelle DSG

B.1.3 Filtrage du trafic descendant non chiffré (DUT)

Cette capacité indique si le câblo-modem prend en charge l'élément de service de filtrage du trafic DUT comme décrit dans le § 7.5.2.1.

Type	Longueur	Valeur
5.19	1	0 Filtrage du trafic DUT non pris en charge (par défaut) 1 Filtrage du trafic DUT pris en charge

B.2 Codage de filtrage du trafic descendant non chiffré (DUT)

Le paramètre de filtrage du trafic DUT est destiné aux câblo-modems implémentant des réseaux privés virtuels de couche 2 ou 3. Dans de tels réseaux, le trafic en voie descendante destiné au réseau privé est toujours chiffré avec interface BPI. Etant donné que le flux radioélectrique en voie descendante est diffusé à tous les câblo-modems, le trafic non chiffré d'adresses MAC collectives destiné à d'autres câblo-modems va toutefois fuir dans les ports d'interface CMCI entre le réseau VPN et le câblo-modem à moins qu'il ne soit filtré dans cette interface. Ce paramètre permet à l'interface entre les câblo-modems et le réseau VPN de filtrer tout le trafic descendant non chiffré, allant vers des destinations MAC aussi bien individuelles que collectives.

Codage TLV de haut niveau pour filtrage du trafic DUT

Type	Longueur	Valeur
45	1..N	Octet 1 (commande de trafic DUT) Bit 0 = 0: désactivation du filtrage du trafic DUT (par défaut) Bit 0 = 1: activation du filtrage du trafic DUT. Bits 1..7: positions binaires réservées. Octets 2..N (masque CMIM du trafic DUT, facultatif) Masque d'interface avec un câblo-modem (CMIM) limitant les interfaces à la sortie du trafic DUT. Si le masque CMIM du trafic DUT est omis, sa valeur contient par défaut les interfaces avec le câblo-modem intégré et toutes les entités eSAFE, mais non les interfaces avec un équipement CPE quelconque.

Si le codage de filtrage du trafic DUT est omis, ou si la valeur de l'octet de commande du codage de filtrage du trafic DUT est égale à zéro, alors le câblo-modem ponte le trafic descendant non chiffré, reçu de son interface RF (ifIndex 2) conformément aux spécifications DOCSIS applicables, à savoir en réexpédiant le trafic de commande MAC unidiffusé vers le port de pont interne (eCM/eSAFE) ou externe (CPE) à partir duquel une adresse MAC d'origine a été acquise ou configurée, et en réexpédiant le trafic d'adresses MAC collectives (GMAC), acquises par protocole IGMP ou configurées, vers tous les autres ports de pont, internes et externes.

Si le codage de filtrage du trafic DUT est présent et si le bit d'activation du filtrage du trafic DUT est activé, le câblo-modem DOIT restreindre le trafic de réexpédition en voie descendante non chiffré (vers des destinations MAC aussi bien individuelles que collectives) au seul ensemble d'interfaces indiqué dans un masque d'interface entre le trafic DUT et le câblo-modem (masque CMIM du trafic DUT) configuré ou impliqué par le codage. Un masque explicite CMIM du trafic DUT suit l'octet de commande de trafic DUT et a le format défini dans le § B.3.4. Noter que les positions binaires d'un masque CMIM sont, comme une chaîne de variables de type BITS, numérotées de gauche (bit de poids fort) à droite (bit de poids faible), dans la séquence d'octets qui représente la chaîne de type BITS.

Si aucun octet ne suit l'octet de commande de trafic DUT (c'est-à-dire si le codage de filtrage du trafic DUT possède une longueur de 1 octet seulement), le masque CMIM impliqué du trafic DUT contient le câblo-modem intégré (position binaire CMIM 0) et contient toutes les interfaces avec une entité eSAFE implémentées sur le câblo-modem (positions binaires CMIM 16 et au-dessus), mais exclut toutes les interfaces avec l'équipement CPE. Ce masque CMIM impliqué du trafic DUT permet à un câblo-opérateur de configurer un codage de filtrage du trafic DUT commun à tous les types de dispositif offrant un service transparent de réseau local par câblo-modem.

B.3 Codage L2VPN

Le paramètre de codage L2VPN est un codage à parties multiples qui configure la façon dont le système CMTS exécute le routage de réseau privé virtuel dans la couche 2 pour les paquets d'équipement CPE. Le fonctionnement d'un réseau L2VPN est spécifié dans le § 7.

Un codage L2VPN est désigné soit comme étant un *codage L2VPN par flux de service individuel* quand il apparaît comme un sous-type du codage de flux de service en voie montante (type 24). Il est un *codage L2VPN de classificateur en voie descendante* quand il apparaît dans un réglage de configuration de classification de paquet en voie descendante (type 23). Il est désigné comme étant un *codage L2VPN par classificateur en voie montante* quand il apparaît dans un réglage de configuration de classification de paquet en voie montante (type 22).

Un codage de réexpédition L2VPN est tel qu'il contient un sous-type L2VPN d'identificateur VPNID qui configure la réexpédition de paquets sur un réseau L2VPN particulier.

Le codage L2VPN est codé sous la forme d'informations générales d'extension (GEI) (voir § C.1.1.17 du [UIT-T J.122]) en tant que codage propre au vendeur avec l'identificateur de vendeur 0xFFFFFF. Le sous-type 5 d'informations GEI est assigné aux codages L2VPN.

Codage L2VPN encapsulé dans les informations GEI

Type	Longueur	Valeur
43.5	n	Nuplets de sous-type/longueur/valeur L2VPN

Le codage L2VPN proprement dit contient un ou plusieurs codages de sous-type L2VPN.

B.3.1 Identificateur de réseau VPN

Le codage de sous-type d'identificateur de réseau VPN (VPNID) est un identificateur en chaîne d'octets opaque qui associe un circuit de rattachement (c'est-à-dire un câblo-modem ou un seul flux de service d'un câblo-modem) ou un classificateur en voie descendante, à un réseau privé virtuel de couche 2 particulier. Les valeurs d'identificateur de réseau privé virtuel (VPN) sont avantageusement configurées sous la forme de chaînes de caractères ASCII imprimables. Les valeurs d'identificateur VPNID sont uniques à l'intérieur d'un même système CMTS. Les valeurs d'identificateur VPNID sont avantageusement configurées sous une forme unique dans *tous* les systèmes CMTS inclus dans le domaine administratif du câblo-opérateur exploitant le système CMTS. Les valeurs d'identificateur VPNID peuvent être configurées de façon à être uniques *à l'échelle mondiale* afin de faciliter la réexpédition interdomaniale par réseau L2VPN.

Aux fins de la modularité, un câblo-opérateur peut configurer des chaînes d'identificateur VPNID de façon à s'appliquer algorithmiquement à des chaînes d'octets binaires uniques à l'échelle mondiale. Des exemples de chaînes d'octets binaires uniques à l'échelle mondiale pour réseaux VPN sont le format de 7 octets de l'identificateur de réseau privé virtuel (VPNID) décrit dans la référence [b-IETF RFC 2685] et le sélecteur de route de 8 octets qui est décrit dans la référence [b-IETF RFC 2547]. Un seul sous-type d'identificateur VPNID est présent dans les codages valides de réexpédition L2VPN.

En général, de multiples circuits de rattachement (c'est-à-dire CM/flux de service) peuvent se connecter au même réseau L2VPN: ils seront donc configurés avec la même valeur de sous-type d'identificateur VPNID. Si le système CMTS exécute seulement une réexpédition point à point par le réseau L2VPN indiqué à un port d'interface NSI, il fait en sorte que le codage L2VPN contienne également un sous-type d'encapsulation de flux à l'interface NSI.

Un système CMTS exécutant une réexpédition multipoint L2VPN DOIT à cette fin assurer une acquisition transparente dans la couche 2 entre ports de pont 802.1Q, câblo-modems et flux de service configurés avec le même identificateur VPNID.

Dans les codages L2VPN par flux de service individuel, l'identificateur VPNID désigne le réseau L2VPN sur lequel le trafic en voie montante doit être réexpédié. Dans les codages L2VPN de classificateur en voie descendante contenus dans le réglage de classification de paquet en voie descendante, l'identificateur VPNID configure l'application du classificateur au seul trafic réexpédié en voie descendante sur le réseau L2VPN identifié par l'identificateur VPNID.

Un système CMTS DEVRAIT utiliser la valeur de l'identificateur VPNID avec tout protocole de signalisation qui détermine dynamiquement les valeurs du champ de multiplexage de services dans les paquets L2VPN encapsulés à un port d'interface NSI. L'identificateur VPNID est destiné à devenir l'identificateur collectif de rattachement (AGI) dans les protocoles de signalisation collective L2VPN selon l'IETF (ou à s'appliquer à cet identificateur).

Le système CMTS DOIT prendre en charge la configuration de valeurs d'identificateur VPNID d'au moins 16 octets et d'au plus 255 octets. Le nombre de valeurs d'identificateur VPNID unique pris en charge par le système CMTS relève des compétences du vendeur.

Sous-type	Longueur	Valeur
43.5.1	1..N	Chaîne d'octets opaque qui identifie un réseau privé virtuel dans la couche 2. La variable N est propre au vendeur, mais doit être dans l'étendue de 16..255.

B.3.2 Sous-type d'encapsulation de flux à l'interface NSI

Au minimum, ce sous-type n'est requis qu'afin de spécifier la façon dont le système CMTS encapsule les paquets réexpédiés en mode point à point par réseau L2VPN sur un unique port sélectionné d'interface NSI avec un réseau Ethernet, essentiellement pour essais de certification de capacité de réseau L2VPN. Ce sous-type est toutefois destiné à normaliser également la configuration, par le câblo-opérateur, de l'émulation IETF de pseudo-circuit [b-IETF RFC 3985] par chaque circuit de rattachement câblé (câblo-modem ou flux de service) utilisant le réseau infrastructurel raccordé à l'interface NSI.

Dans le mode Ethernet sélectionné, le système CMTS est configuré de façon à réexpédier, à un moment quelconque, tout le trafic L2VPN au moyen d'un unique port d'interface NSI avec un réseau Ethernet. Quand un port Ethernet sélectionné est identifié, le système CMTS DOIT accepter le code de format d'encapsulation à l'interface NSI selon la spécification IEEE 802.1Q, contenu dans les codages de réexpédition L2VPN, et PEUT accepter les autres codes.

Bien que le sous-type d'encapsulation de flux à l'interface NSI soit destiné essentiellement aux modes de réexpédition point à point, le système CMTS PEUT l'accepter en mode multipoint (y compris dans le mode Ethernet sélectionné). Dans ce cas, le système CMTS DOIT appliquer la règle que les codages L2VPN, ayant le même sous-type d'identificateur de réseau VPN contenant un sous-type d'encapsulation de flux à l'interface NSI, DOIVENT tous avoir la même valeur de codage de sous-type d'encapsulation de flux à l'interface NSI.

La valeur du sous-type d'encapsulation de flux à l'interface NSI est un unique nuplet de Code de format-Longueur-Valeur qui identifie un code de format d'encapsulation de flux à l'interface NSI et éventuellement une valeur de multiplexage du service d'encapsulation à l'interface NSI.

Sous-type	Longueur	Valeur
43.5.2	n	Nuplet unique: code de format d'encapsulation de flux à l'interface NSI/longueur/valeur

Si le sous-type d'encapsulation de flux à l'interface NSI ou un sous-type L2VPN propre au vendeur ne configure pas statiquement une valeur de multiplexage de service, le système CMTS DOIT dynamiquement sélectionner et acquérir la valeur de multiplexage de service dans un codage de réexpédition L2VPN, à partir des homologues L2VPN du système CMTS et par l'intermédiaire de l'interface NSI. La valeur acquise dynamiquement de multiplexage de services peut être différente sur différents ports d'interface NSI.

Code de format d'encapsulation de flux à l'interface NSI	Longueur	Valeur de multiplexage de service
43.5.2.1	0	*Autre format*: le format d'encapsulation de flux L2VPN à l'interface NSI est différent de ceux qui sont spécifiés ci-dessous. Dans ce cas, les codages L2VPN de sous-type propre au vendeur (sous-type d'informations GEI 5.43) DOIVENT offrir le format d'encapsulation de flux à l'interface NSI et l'une quelconque des valeurs statiques de multiplexage de service recherchées.

Code de format d'encapsulation de flux à l'interface NSI	Longueur	Valeur de multiplexage de service
43.5.2.2	2	*IEEE 802.1Q*. La valeur est la balise de 16 bits selon l'IEEE 802.1Q (octet de plus fort poids en premier) qui contient, dans ses 12 positions binaires de poids faible, un identificateur de réseau VLAN servant à reconnaître les paquets L2VPN au port sélectionné d'interface NSI avec un réseau Ethernet. Les 4 bits de poids fort de la valeur de balise de 16 octets sont réservés. Le système CMTS DEVRAIT ignorer les 4 bits de plus fort poids des 16 octets de la valeur de balise IEEE 802.1Q d'encapsulation de flux à l'interface NSI. Le nombre maximal de valeurs uniques d'identificateur de réseau VLAN acceptées par un système CMTS dépend du vendeur. Un système CMTS DOIT accepter l'étendue complète des 12 positions binaires des valeurs d'identificateur de réseau VLAN pour les valeurs uniques qu'il peut accepter.
43.5.2.3	4	*IEEE 802.1ad*. La valeur est une paire de valeurs de 16 bits (octet de plus fort poids en premier) dont le premier champ de 16 bits contient un identificateur de réseau VLAN de fournisseur de service dans ses 12 positions binaires de poids faible, le second champ de 16 bits contenant l'identificateur de réseau VLAN du client dans ses 12 positions binaires de poids faible. Les 4 bits de plus fort poids de chaque valeur de 16 bits sont réservés. Le nombre maximal de valeurs d'identificateur de réseau VLAN de fournisseur de service et de client que le système CMTS accepte dépend du vendeur, mais le système CMTS DOIT accepter l'étendue complète des 12 positions binaires des valeurs d'identificateur de réseau VLAN.
43.5.2.4	5 ou 17	*Homologue en commutation MPLS*. La valeur est un code InetAddressTypeCode (ipv4(1) ou ipv6(2)) sur un seul octet, suivi par une adresse IPv4 ou IPv6 de type InetAddress. Le trafic L2VPN du circuit de rattachement est destiné à réexpédier les flux vers l'homologue par un chemin à commutation d'étiquettes MPLS. Le système CMTS DEVRAIT sélectionner dynamiquement les empilements d'étiquettes entrantes et acquérir dynamiquement les empilements d'étiquettes sortantes. Le système CMTS PEUT utiliser des sous-types de réseau L2VPN propres à un vendeur afin de configurer statiquement les empilements d'étiquettes d'entrée et de sortie de flux. Le système CMTS PEUT limiter les valeurs d'étiquette MPLS configurées statiquement à une étendue propre au vendeur.
43.5.2.5	5 ou 17	*Homologue L2TPv3*. La valeur est un seul octet de code InetAddressTypeCode (ipv4(1) ou ipv6(2)) suivi par une adresse IPv4 ou IPv6 de type InetAddress. Le trafic L2VPN du circuit de rattachement est destiné à réexpédier dans un tunnel L2TPv3 vers l'homologue destinataire. Le système CMTS DEVRAIT sélectionner et acquérir dynamiquement les identificateurs de session locaux et distants pour chaque tunnel. Le système CMTS PEUT utiliser des sous-types L2VPN propres à un vendeur afin de configurer statiquement les identificateurs de session, les adresses de réseau homologue L2TPv3 et d'autres informations selon les besoins du vendeur. Le système CMTS PEUT limiter à une étendue propre au vendeur les valeurs configurées statiquement d'identificateur de session ou d'autres valeurs de multiplexage de service.

B.3.3 Surveillance du trafic DHCP par entité eSAFE

Ce paramètre n'est défini que par codage L2VPN de réexpédition par flux de service individuel. C'est un masque binaire dont les positions binaires sont définies pour chaque type possible de serveur local d'entité eSAFE. Une valeur '1' dans la position binaire de type de serveur local d'entité eSAFE permet au système CMTS de détecter automatiquement l'adresse MAC de ce serveur local d'entité eSAFE, par surveillance du trafic DHCP réexpédié entre le câblo-modem et un serveur distant de protocole DHCP. Les positions binaires contenues dans le paramètre de surveillance du trafic DHCP par entité eSAFE s'apparient avec celles du masque d'interface avec un câblo-modem (CMIM) désignant l'interface associée au type de serveur local d'entité eSAFE.

Sous-type	Longueur	Valeur
43.5.3	1..N	Masque binaire des serveurs locaux d'entité eSAFE activé pour la surveillance du trafic DHCP Bit 1 (0x40 00 00): services de portail intégrés (ePS) Bit 16 (0x00 00 80): adaptateur EMTA-IPCablecom Bit 17 (0x00 00 40): décodeur eSTB de flux IP Bit 18 (0x00 00 20): décodeur eSTB de passerelle DSG Bits 19..31 (0x00 00 1F FF): autres interfaces avec entité eSAFE

B.3.4 Sous-type de masque d'interface avec un câblo-modem (CMIM)

Ce paramètre est un masque binaire qui décrit un ensemble d'indices d'interface avec un câblo-modem intégré [b-UIT-T J.126], contenu dans un codage de réexpédition L2VPN. Le sous-type de masque d'interface avec un câblo-modem décrit l'ensemble des interfaces avec un port de pont sur lesquelles le câblo-modem réexpédie des paquets L2VPN.

Chaque bit du masque CMIM correspond à une interface avec un port logique de pont d'adresses MAC de couche 2, implémenté dans un câblo-modem intégré. Ce paramètre est codé comme la chaîne d'octets du codage selon les règles de codage de base d'une chaîne binaire de variables de type BITS du protocole SNMP. La position binaire K dans le codage de type BITS correspond à l'interface eDOCSIS K avec un pont de commande MAC. Par convention, la position binaire 0 correspond à l'interface avec le serveur local automatique du câblo-modem intégré. L'adresse MAC du serveur local automatique eCM est signalée comme si elle utilisait un indice ifIndex égal à zéro (0) désignant une interface avec un port de pont, bien qu'aucune interface de cette sorte n'existe réellement.

Sous-type	Longueur	Valeur
43.5.4	N	Variable de type BITS du protocole SNMP – le bit codé correspond à la position binaire K représentant la valeur d'indice K de l'interface logique avec le câblo-modem intégré. La position binaire 0 représente le serveur local automatique du câblo-modem intégré proprement dit. La position binaire 0 est le bit de plus fort poids du premier octet. Voir [b-UIT-T J.126] pour les plus récentes affectations d'indice d'interface logique. Bit 0 (0x80): interface avec le serveur local automatique du câblo-modem intégré. Bit 1 (0x40): interface primaire avec l'équipement CPE (ainsi qu'avec un portail ePS) Bit 2 (0x20): interface RF Bits 3,4: positions réservées

Sous-type	Longueur	Valeur
		Bits 5..15 (0x07 FF): autres équipements CPE interfaces Bits 16-31: interfaces logiques intégrées. Les interfaces actuellement définies sont les suivantes: Bit 16 (0x00 00 80): adaptateur EMTA-IPCablecom Bit 17 (0x00 00 40): décodeur eSTB de flux IP Bit 18 (0x00 00 20): décodeur eSTB de passerelle DSG Bits 19..31 (0x00 00 1F FF): autres interfaces avec entité eSAFE

Si le sous-type de masque d'interface avec un câblo-modem n'est pas présent dans un codage de réexpédition L2VPN, sa valeur par défaut ne concerne que l'interface primaire avec l'équipement CPE (indice 1) et l'interface RF avec le réseau câblé (indice 2), c'est-à-dire la valeur de masque CMIM 0x60. Un câblo-modem DOIT ignorer de façon transparente les positions binaires de masque CMIM concernant des interfaces non implémentées. Un système CMTS PEUT signaler qu'une valeur de masque CMIM – c'est-à-dire 0x47 FF – représente toutes les interfaces possibles avec l'équipement CPE ayant une valeur de masque CMIM aux positions 1 et 5-15.

B.3.5 Identificateur collectif de rattachement

Le système CMTS DEVRAIT utiliser, si elle est présente, cette valeur de sous-type comme élément de signalisation d'identificateur collectif de rattachement, associée à un identificateur de réseau VPN, lors de l'établissement dynamique d'une ligne privée à l'interface NSI pour la réexpédition en mode point à point du circuit de rattachement. Cette valeur n'est applicable que dans le cadre de l'encapsulation de flux à l'interface NSI par protocole MPLS ou L2TPv3 et de la réexpédition en mode point à point entre le circuit de rattachement et la ligne privée.

Sous-type	Longueur	Valeur
43.5.5	0..16	Chaîne d'octets opaque qui identifie le câblo-modem ou flux de service comme étant un circuit de rattachement pour le protocole de signalisation L2VPN-IETF.

B.3.6 Identificateur individuel de rattachement à l'origine

Le système CMTS DEVRAIT utiliser, si elle est présente, cette valeur de sous-type comme élément de signalisation d'identificateur individuel de rattachement à l'origine (SAII), associée au rattachement local de ligne privée lors de l'établissement d'une ligne privée dans le réseau infrastructurel, à l'interface NSI avec ce circuit de rattachement câblé. Cette valeur n'est applicable que dans le cadre d'un sous-type MPLS ou L2TPv3 d'encapsulation de flux à l'interface NSI et de réexpédition en mode point à point entre le circuit de rattachement câblé et la ligne privée.

Sous-type	Longueur	Valeur
43.5.6	0..16	Chaîne d'octets opaque signalée comme circuit d'identificateur SAII en protocole de signalisation L2VPN-IETF.

B.3.7 Identificateur individuel de rattachement à la destination

Le système CMTS DEVRAIT utiliser cette valeur de sous-type, si elle est présente, comme élément de signalisation d'identificateur individuel de rattachement à la destination (TAII) associé au rattachement distant de ligne privée lors de l'établissement d'une ligne privée à l'interface NSI avec le circuit de rattachement. Elle n'est applicable que dans le cadre d'un sous-type MPLS ou L2TPv3 d'encapsulation de flux à l'interface NSI et de réexpédition en mode point à point entre le circuit de rattachement câblé et la ligne privée.

Sous-type	Longueur	Valeur
43.5.7	0..16	Chaîne d'octets opaque qui identifie le câblo-modem ou le flux de service comme étant un circuit de rattachement en protocole de signalisation L2VPN-IETF.

B.3.8 Priorité d'entrée de l'utilisateur dans un flux

Les protocoles de routage IEEE 802.1 nécessitent la détection ou la production, la régénération facultative et la signalisation d'un attribut de priorité d'utilisateur de tous les paquets routés. Le sous-type de priorité d'entrée de l'utilisateur dans un flux sert à configurer la priorité d'utilisateur IEEE 802.1 des paquets L2VPN entrant en voie montante. Elle est définie seulement dans les codages L2VPN de réexpédition en voie montante par flux de service individuel.

Sauf configuration contraire du réexpéditeur L2VPN, le CMTS DOIT transmettre la priorité d'entrée signalée avec ce sous-type sous la forme des bits de priorité d'utilisateur d'une balise IEEE 802.1Q, quand ce CMTS réexpédie ce paquet vers un port d'interface NSI avec encapsulation IEEE 802.1Q. Si ce sous-type est omis d'un codage de réexpédition L2VPN, le système CMTS considère que la priorité d'utilisateur entrante est égale à zéro (0). Ce sous-type n'apparaît pas plus d'une seule fois dans un codage valide de réexpédition L2VPN.

Sous-type	Longueur	Valeur
43.5.8	1	Valeur de priorité d'insertion de l'utilisateur dans un flux IEEE 802.1, comprise dans l'étendue de 0..7 et codée dans les trois positions binaires de poids faible. Des valeurs supérieures indiquent une priorité supérieure.

B.3.9 Niveaux de priorité d'un utilisateur

Dans un codage de classification de paquet en voie descendante, la présence d'un codage L2VPN avec ce sous-type restreint le classificateur aux seuls paquets réexpédiés en voie descendante avec l'étendue indiquée des valeurs de priorité d'utilisateur (et entre ces limites). La priorité d'utilisateur classifiée est celle qui est transmise à l'interface avec la couche de commande MAC-DOCSIS et qui est donc considérée comme venant *après* toute sélection de valeur par défaut de priorité d'utilisateur à l'entrée de flux ou toute régénération de priorité d'utilisateur effectuée par le réexpéditeur L2VPN. Ce sous-type ne peut apparaître que dans un codage L2VPN de classificateur en voie descendante et une seule fois au plus dans un même codage L2VPN. Si ce sous-type est omis, le classificateur s'applique à toutes les valeurs de priorité d'utilisateur à la sortie de flux.

Sous-type	Longueur	Valeur
43.5.9	2	Priorité basse, priorité élevée. La valeur inférieure de priorité d'utilisateur dans l'étendue des priorités d'utilisateur est codée dans les 3 positions binaires de plus faible poids du premier octet et la valeur supérieure de l'étendue est codée dans les 3 positions binaires de plus faible poids du second octet.

B.3.10 Sous-type de descripteur d'association de sécurité L2VPN

Le système CMTS ajoute ce sous-type dans les messages en voie descendante de réponse d'inscription et de service dynamique qui contiennent des codages de réexpédition L2VPN afin d'informer un câblo-modem L2VPN conforme de la ou des valeurs d'identificateur SAID que le système CMTS utilisera afin de chiffrer le trafic réexpédié en voie descendante à ce réseau L2VPN au moyen du câblo-modem. Un codage valide de réseau L2VPN peut avoir de multiples sous-types de descripteur d'association de sécurité L2VPN.

Sous-type	Longueur	Valeur
43.5.10	N	Codage de descripteur d'association de sécurité tel que spécifié dans la référence [UIT-T J.125] qui fournit la valeur d'identificateur SAID que le système CMTS utilisera afin de chiffrer le trafic réexpédié en voie descendante dans un réseau L2VPN. Le type d'association de sécurité du descripteur d'association de sécurité doit être "dynamique".

B.3.11 Sous-type de réseau L2VPN propre à un vendeur

Ce sous-type est interprété par le système CMTS de façon propre au vendeur. Un exemple de données relatives à l'utilisation consiste à configurer la sous-interface NSI ou le circuit virtuel auquel les paquets issus en voie montante du câblo-modem ou du flux de service sont pontés en mode point à point. Le contenu du sous-type propre au vendeur peut être des données à codage binaire ou ASCII.

Type de GEI	Longueur	Valeur
43.5.43	N	08, 3, identificateur de vendeur selon le nuplet: type propre au vendeur/longueur/valeur.

B.4 Codes de confirmation

Le présent paragraphe définit de nouveaux codes de confirmation pour le fonctionnement en réseau L2VPN. Il étend la liste de codes de confirmation figurant dans le § C.4 de [UIT-T J.122].

Les codes additionnels de confirmation définis pour la capacité L2VPN-DOCSIS sont les suivants.

- reject-VLAN-ID-in-use(26): indique qu'un identificateur de réseau VLAN de type IEEE 802.1q ou IEEE 802.1ad, demandé pour l'encapsulation de flux à l'interface NSI du trafic L2VPN, est déjà assigné pour utilisation par le trafic non L2VPN. Voir § 7.2.5.
- reject-multipoint-L2VPN(27): indique que le mode de réexpédition multipoint L2VPN n'est pas pris en charge et qu'un câblo-modem est en train d'essayer de configurer plus d'un seul circuit de rattachement L2VPN au même réseau L2VPN. Voir § 7.2.5.
- reject-multipoint-NSI(28): indique qu'un réseau L2VPN de réexpédition multipoint contenait de multiples codages L2VPN avec différentes valeurs d'encapsulation du trafic à l'interface NSI.

B.5 Codage d'erreur L2VPN

Ce codage fournit des informations complémentaires à partir du câblo-modem quand celui-ci rejette un codage L2VPN signalé par le système CMTS. Le câblo-modem doit inclure un codage d'erreur L2VPN dans sa réponse de gestion de commande MAC quand il rejette un codage L2VPN contenu dans un message REG-RSP, DSA-REQ, DSA-RSP, DSC-REQ ou DSC-RSP.

Type de GEI	Longueur	Valeur
43.5.254	N	Codage d'erreur L2VPN composé d'exactement un seul codage de paramètre L2VPN erroné, d'exactement un seul codage de code d'erreur L2VPN, et de zéro ou un seul codage de message d'erreur L2VPN.

B.5.1 Paramètre L2VPN erroné

Ce paramètre fournit une séquence de types et de sous-types qui identifient l'emplacement et le sous-type du codage L2VPN qui est rejeté. Un codage valide d'erreur L2VPN contient exactement une seule chaîne de type Paramètre L2VPN erroné.

Type de GEI	Longueur	Valeur
43.5.254.1	N	Séquence de types et de sous-types

La séquence de type/sous-type commence au niveau supérieur des codages de nuplet TLV contenus dans le message de gestion d'adresse MAC qui incluait le codage L2VPN. Cette séquence dépend de l'emplacement du codage L2VPN, comme décrit dans le § 7.2. En particulier:

- une chaîne paramétrique d'erreur L2VPN dans un codage L2VPN de niveau supérieur commence par deux octets pour le code de type d'informations GEI du codage L2VPN, ou (43.5);
- une chaîne paramétrique d'erreur L2VPN dans un codage de flux de service en voie montante commence par le code de type de ce codage (24) suivi par le type d'informations GEI du codage L2VPN, ou (24.43.5);
- une chaîne paramétrique d'erreur L2VPN dans un réglage de configuration de classification de paquet en voie descendante commence par le type de ce codage (23) suivi par le type d'informations GEI du codage L2VPN, ou (23.43.5);
- une chaîne paramétrique d'erreur L2VPN dans un réglage de configuration de classification de paquet en voie montante commence par le type de ce codage (22) suivi par le type d'informations GEI du codage L2VPN, ou (22.43.5).

Si la totalité du codage L2VPN est rejetée, le câblo-modem PEUT n'inclure, dans la chaîne de type de paramètre d'erreur L2VPN, que les deux ou trois octets qui identifient l'emplacement d'un codage L2VPN complet. Si la raison du rejet est due à un sous-type particulier du codage L2VPN, le câblo-modem DEVRAIT inclure des octets additionnels dans la chaîne de type de paramètre d'erreur L2VPN afin d'identifier le sous-type particulier du codage L2VPN qu'il a rejeté. Une raison de rejeter un codage L2VPN complet est que le nombre maximal des réseaux L2VPN pris en charge par le câblo-modem a été dépassé. Une raison de rejeter un sous-type particulier, p. ex. le codage de sous-type de descripteur d'association de sécurité L2VPN, est que le nombre d'identificateurs SAID pris en charge par le câblo-modem a été dépassé.

B.5.2 Code d'erreur L2VPN

Ce paramètre fournit un code de confirmation comme défini dans le § C.4 de [UIT-T J.122] afin d'identifier la raison pour laquelle un codage ou sous-type L2VPN a été rejeté. Un codage valide d'erreur L2VPN contient exactement un seul code de confirmation L2VPN.

Type de GEI	Longueur	Valeur
43.5.254.2	1	Code de confirmation

B.5.3 Message d'erreur L2VPN

Ce paramètre, si présent, inscrit un message d'affichage dans le journal de console du système CMTS concernant la raison du rejet. Un câblo-modem DEVRAIT inclure ce paramètre dans un codage d'erreur L2VPN. Un codage valide d'erreur L2VPN contient zéro ou un seul sous-type de message d'erreur L2VPN.

Type de GEI	Longueur	Valeur
43.5.254.3	N	Chaîne de caractères ASCII terminée par zéro

B.6 Critères de classification des masques d'interface avec un câblo-modem

La présente Recommandation définit un mécanisme générique afin de classifier les trafics en voie montante ou descendante sur la base des ports d'interface logique d'entrée ou de sortie de flux prévue dans le câblo-modem.

Dans un codage de classificateur de paquet en voie montante (type 22), le sous-type de masque d'interface avec un câblo-modem définit un critère réglementaire afin de vérifier sa concordance avec l'interface d'insertion d'une unité L2PDU.

Dans un codage de classificateur de paquet en voie descendante (type 23), le sous-type de masque d'interface avec un câblo-modem définit un critère réglementaire afin de vérifier sa concordance avec une adresse MAC de destination unidiffusée en voie descendante. Dans un cas comme dans l'autre, le codage de sous-type de masque CMIM, contenu dans un codage de classificateur de paquet, s'applique aux deux trafics, L2VPN et non L2VPN.

Chaque bit du masque CMIM correspond à une interface avec un port logique de pont d'adresses MAC dans la couche 2 implémenté dans la partie intégrée d'un câblo-modem. Le paramètre est codé comme la chaîne d'octets du codage selon les règles de codage de base d'une chaîne binaire de variables de type BITS du protocole SNMP. La position binaire K dans le codage de type BITS correspond à l'interface K avec un pont de commande MAC selon eDOCSIS. Par convention, la position binaire 0 correspond à l'interface avec le serveur local automatique du câblo-modem intégré (c'est-à-dire à l'empilement IP du câblo-modem). L'adresse MAC du serveur local automatique eCM est signalée comme si elle était désignée par un indice ifIndex d'interface avec un port de pont égal à zéro (0), bien qu'aucune interface de cette sorte n'existe réellement.

Sous-type	Longueur	Valeur
[22/23].13	N	Variable de type BITS du protocole SNMP – le bit codé correspond à la position binaire K représentant la valeur d'indice K de l'interface logique avec le câblo-modem intégré. La position binaire 0 représente le serveur local automatique du câblo-modem intégré proprement dit. La position binaire 0 est le bit de plus fort poids du premier octet. La spécification DOCSIS intégrée (eDOCSIS) [b-UIT-T J.126] définit les affectations de l'indice d'interface. A titre d'information, les affectations actuelles sont les suivantes. Bit 0 (0x80): interface avec le serveur local intégré dans le câblo-modem intégré Bit 1 (0x40): interface primaire avec l'équipement CPE (de même qu'avec un portail ePS) Bit 2 (0x20): interface RF Bits 3,4: positions réservées Bits 5..15 (0x07 FF): interfaces avec d'autres équipements CPE Bits 16-31: interfaces logiques avec équipement CPE pour serveurs locaux d'entité eSAFE. Les affectations actuelles sont les suivantes. Bit 16 (0x00 00 80): adaptateur EMTA-IpCablecom Bit 17 (0x00 00 40): décodeur eSTB de flux IP Bit 18 (0x00 00 20): décodeur eSTB de passerelle DSG Bits 19..31 (0x00 00 1F FF): autres interfaces avec entité eSAFE

Dans un codage de classificateur en voie montante, un câblo-modem DOIT ignorer de façon transparente les positions binaires désignant des interfaces non implémentées. Par exemple, un critère de classificateur de masque CMIM en voie montante, destiné à ne correspondre qu'à des interfaces externes avec l'équipement CPE d'un câblo-modem, possède une valeur de masque CMIM activant les bits 1 et 5-15, c'est-à-dire un codage égal à 0x47 FF.

Dans un codage de classificateur en voie descendante qui contient un critère de masque CMIM, le système CMTS vérifie l'adresse MAC de destination afin de déterminer si elle est l'adresse MAC du serveur local automatique du câblo-modem ou une adresse MAC reconnue de serveur local d'entité eSAFE. Toute autre adresse MAC unidiffusée est considérée comme étant une adresse MAC d'équipement CPE. Le système CMTS n'est pas informé de l'interface particulière avec l'équipement CPE par laquelle le câblo-modem a acquis une adresse MAC d'équipement CPE. Le système CMTS considère seulement que le bit 1 du masque CMIM concorde avec une adresse MAC d'équipement CPE contenue dans un codage de classificateur de paquet en voie descendante. Le nombre maximal d'adresses MAC d'entité eSAFE destinataires, reconnu par un système CMTS, dépend du vendeur.

Appendice I

Exemple de codages L2VPN

Le codage L2VPN est toujours encapsulé au moyen d'un codage d'informations générales d'extension (GEI, *general extension information*) qui utilise le code de type 43 avec l'identificateur réservé de vendeur 0xFFFFFF.

I.1 Exemple de liaison point à point

Le présent paragraphe décrit des codages L2VPN pour trois câblo-modems exécutant une réexpédition point à point par réseau L2VPN de tout le trafic se trouvant sur leur flux de service par défaut en voie montante. Deux des câblo-modems sont pontés de l'extérieur vers la même entreprise (identificateur de réseau L2VPN 0234560001); un des câblo-modems est ponté vers une entreprise distincte (identificateur de réseau L2VPN 0234560002). Cet exemple est décrit dans la Figure I.1:

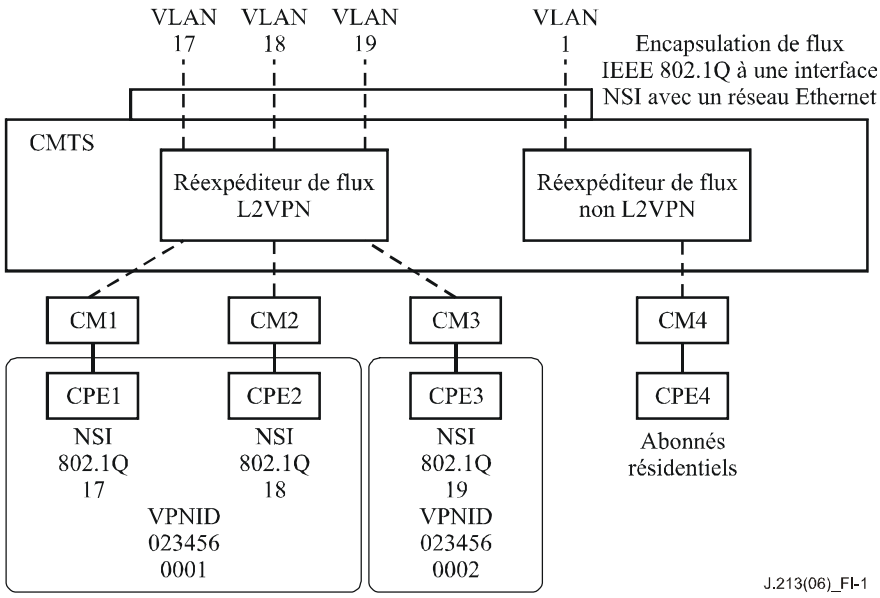

Figure I.1 – Exemple de réexpédition point à point d'un trafic L2VPN

Tableau I.1 – Codage L2VPN d'une liaison point à point par CM1

Fichier de configuration de liaison point à point par CM1				
43				Codage L2VPN par câblo-modem individuel
20				Longueur globale
	08 03 FFFFFF			Identificateur de vendeur: 0xFFFFFF pour GEI
	05			GEI 43.5 pour codage L2VPN
	13			Longueur de sous-type GEI.5
		01 05 x0234560001		Sous-type d'identificateur VPNID
		02		Sous-type d'encapsulation de flux à l'interface NSI
		04		Longueur de sous-type GEI.5.2
			02	Sous-type de format IEEE 802.1Q
			02	Longueur de sous-type GEI.5.2.2
			0x0011	Identificateur de réseau VLAN 17
24				Codage de flux de service en voie montante
19				Longueur
	6			Sous-type du type d'ensemble paramétrique de QoS
	1			
		0x07		
	43			Sous-type propre au vendeur:
	14			Longueur globale
		08 03 FFFFFF		Identificateur de vendeur pour GEI
		05		GEI 43.5 pour codage L2VPN
		7		Longueur de sous-type GEI.5
			01 05 x0234560001	Sous-type d'identificateur VPNID
45				Filtrage du trafic DUT:
01				Longueur globale
	01			Filtrage du trafic DUT activé

Tableau I.2 – Codage L2VPN d'une liaison point à point par CM2

Fichier de configuration de liaison point à point par CM2				
43				Codage L2VPN par câblo-modem individuel
20				Longueur globale
	08 03 FFFFFF			Identificateur de vendeur: 0xFFFFFF pour GEI
	05			GEI 43.5 pour codage L2VPN
	13			Longueur de sous-type GEI.5
		01 05 x0234560001		Sous-type d'identificateur VPNID
		02		Sous-type d'encapsulation de flux à l'interface NSI
		04		Longueur de sous-type GEI.5.2
			02	Sous-type de format IEEE 802.1Q
			02	Longueur de sous-type GEI.5.2.2
			0x0012	Identificateur de réseau VLAN 18
24				Codage de flux de service en voie montante
19				Longueur
	6			Sous-type du type d'ensemble paramétrique de QoS
	1			
		0x07		
	43			Sous-type propre au vendeur:
	14			Longueur globale
		08 03 FFFFFF		Identificateur de vendeur pour GEI
		05		GEI 43.5 pour codage L2VPN
		7		Longueur de sous-type GEI.5
			01 05 x0234560001	Sous-type d'identificateur VPNID
45				Filtrage du trafic DUT:
01				Longueur globale
	01			Filtrage du trafic DUT activé

L'équipement CPE2 est ponté de l'extérieur vers le même réseau L2VPN que l'équipement CPE1 (VPNID x0234560001), mais toute la réexpédition L2VPN pour l'équipement CPE2 se produit sur l'identificateur 18 de réseau VLAN à l'interface NSI avec un flux IEEE 802.1Q.

Tableau I.3 – Codage L2VPN d'une liaison point à point par CM3

Fichier de configuration de liaison point à point par CM3				
43				Codage L2VPN par câblo-modem individuel
20				Longueur globale
	08 03 FFFFFF			Identificateur de vendeur: 0xFFFFFF pour GEI
	05			GEI 43.5 pour codage L2VPN
	13			Longueur de sous-type GEI.5
		01 05 x0234560002		Sous-type d'identificateur VPNID
		02		Sous-type d'encapsulation de flux à l'interface NSI
		04		Longueur de sous-type GEI.5.2
			02	Sous-type de format IEEE 802.1Q
			02	Longueur de sous-type GEI.5.2.2
			0x0013	Identificateur de réseau VLAN 19
24				Codage de flux de service en voie montante
19				Longueur
	6			Sous-type du type d'ensemble paramétrique de QoS
	1			
		0x07		
	43			Sous-type propre au vendeur:
	14			Longueur globale
		08 03 FFFFFF		Identificateur de vendeur pour GEI
		05		GEI 43.5 pour codage L2VPN
		7		Longueur de sous-type GEI.5
			01 05 x0234560002	Sous-type d'identificateur VPNID
45				Filtrage du trafic DUT:
01				Longueur globale
	01			Filtrage du trafic DUT activé

I.2 Exemple de liaison multipoint

Le présent paragraphe donne un exemple de codages L2VPN pour la réexpédition multipoint, comme décrit ci-dessous. Pour la réexpédition multipoint, l'encapsulation de flux à l'interface NSI avec un réseau L2VPN peut être configurée de l'une des deux façons suivantes:

- par configuration propre au vendeur du système CMTS;
- par le fichier de configuration d'un ou de plusieurs des câblo-modems inclus dans le réseau L2VPN.

Dans l'exemple donné par la Figure I.2, l'encapsulation de flux à l'interface NSI pour chaque réseau L2VPN apparaît dans le fichier de configuration du câblo-modem pour tous les câblo-modems.

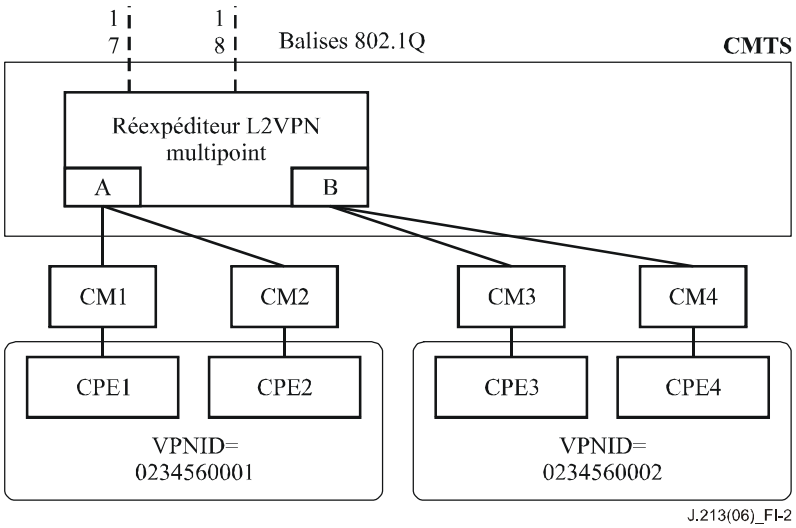

Figure I.2 – Exemple de réexpédition multipoint de trafic L2VPN

Tableau I.4 – Codage L2VPN d'une liaison multipoint par CM1

Fichier de configuration de liaison multipoint par CM1				
43				Codage L2VPN par câblo-modem individuel
20				Longueur globale
	08 03 FFFFFF			Identificateur de vendeur: 0xFFFFFF pour GEI
	05			GEI 43.5 pour codage L2VPN
	13			Longueur de sous-type GEI.5
		01 05 x0234560001		Sous-type d'identificateur VPNID
		02		Sous-type d'encapsulation de flux à l'interface NSI
		04		Longueur de sous-type GEI.5.2
			02	Sous-type de format IEEE 802.1Q
			02	Longueur de sous-type GEI.5.2.2
			0x0011	Identificateur de réseau VLAN 17
24				Codage de flux de service en voie montante
19				Longueur
	6			Sous-type du type d'ensemble paramétrique de QoS
	1			
		0x07		
	43			Sous-type propre au vendeur:
	14			Longueur globale
		08 03 FFFFFF		Identificateur de vendeur pour GEI
		05		GEI 43.5 pour codage L2VPN
		7		Longueur de sous-type GEI.5
			01 05 x0234560001	Sous-type d'identificateur VPNID
45				Filtrage du trafic DUT:
01				Longueur globale
	01			Filtrage du trafic DUT activé

Tableau I.5 – Codage L2VPN d'une liaison multipoint par CM2

Fichier de configuration de liaison multipoint par CM2				
43				Codage L2VPN par câblo-modem individuel
20				Longueur globale
	08 03 FFFFFF			Identificateur de vendeur: 0xFFFFFF pour GEI
	05			GEI 43.5 pour codage L2VPN
	13			Longueur de sous-type GEI.5
		01 05 x0234560001		Sous-type d'identificateur VPNID
		02		Sous-type d'encapsulation de flux à l'interface NSI
		04		Longueur de sous-type GEI.5.2
			02	Sous-type de format IEEE 802.1Q
			02	Longueur de sous-type GEI.5.2.2
			0x0011	Identificateur de réseau VLAN 17
24				Codage de flux de service en voie montante
19				Longueur
	6			Sous-type du type d'ensemble paramétrique de QoS
	1			
		0x07		
	43			Sous-type propre au vendeur:
	14			Longueur globale
		08 03 FFFFFF		Identificateur de vendeur pour GEI
		05		GEI 43.5 pour codage L2VPN
		7		Longueur de sous-type GEI.5
			01 05 x0234560001	Sous-type d'identificateur VPNID
45				Filtrage du trafic DUT:
01				Longueur globale
	01			Filtrage du trafic DUT activé
NOTE – Les codages L2VPN pour liaison multipoint par CM2 sont exactement les mêmes que par CM1.				

Tableau I.6 – Codage L2VPN d'une liaison multipoint par CM3

Fichier de configuration de liaison multipoint par CM3				
43				Codage L2VPN par câblo-modem individuel
20				Longueur globale
	08 03 FFFFFF			Identificateur de vendeur: 0xFFFFFF pour GEI
	05			GEI 43.5 pour codage L2VPN
	13			Longueur de sous-type GEI.5
		01 05 x0234560002		Sous-type d'identificateur VPNID
		02		Sous-type d'encapsulation de flux à l'interface NSI
		04		Longueur de sous-type GEI.5.2
			02	Sous-type de format IEEE 802.1Q
			02	Longueur de sous-type GEI.5.2.2
			0x0012	Identificateur de réseau VLAN 18
24				Codage de flux de service en voie montante
19				Longueur
	6			Sous-type du type d'ensemble paramétrique de QoS
	1			
		0x07		
	43			Sous-type propre au vendeur:
	14			Longueur globale
		08 03 FFFFFF		Identificateur de vendeur pour GEI
		05		GEI 43.5 pour codage L2VPN
		7		Longueur de sous-type GEI.5
			01 05 x0234560002	Sous-type d'identificateur VPNID
45				Filtrage du trafic DUT:
01				Longueur globale
	01			Filtrage du trafic DUT activé

Tableau I.7 – Codage L2VPN d'une liaison multipoint par CM4

Fichier de configuration de liaison multipoint par CM4				
43				Codage L2VPN par câblo-modem individuel
20				Longueur globale
	08 03 FFFFFF			Identificateur de vendeur: 0xFFFFFF pour GEI
	05			GEI 43.5 pour codage L2VPN
	13			Longueur de sous-type GEI.5
		01 05 x0234560002		Sous-type d'identificateur VPNID
		02		Sous-type d'encapsulation de flux à l'interface NSI
		04		Longueur de sous-type GEI.5.2
			02	Sous-type de format IEEE 802.1Q
			02	Longueur de sous-type GEI.5.2.2
			0x0012	Identificateur de réseau VLAN 18
24				Codage de flux de service en voie montante
19				Longueur
	6			Sous-type du type d'ensemble paramétrique de QoS
	1			
		0x07		
	43			Sous-type propre au vendeur:
	14			Longueur globale
		08 03 FFFFFF		Identificateur de vendeur pour GEI
		05		GEI 43.5 pour codage L2VPN
		7		Longueur de sous-type GEI.5
			01 05 x0234560002	Sous-type d'identificateur VPNID
45				Filtrage du trafic DUT:
01				Longueur globale
	01			Filtrage du trafic DUT activé
NOTE – Le codage L2VPN pour liaison multipoint par CM4 est le même que par CM3.				

I.3 Exemple de classificateur en voie montante L2VPN

Cet exemple montre la classification d'un trafic en voie montante à partir d'un certain équipement CPE1 vers un flux de service L2VPN en voie montante, où tous les autres équipements CPE rattachés au câblo-modem réexpédient vers le réexpéditeur de flux non L2VPN, comme décrit dans le Tableau I.8.

Tableau I.8 – Codage d'un classificateur en voie montante L2VPN

Fichier de configuration de câblo-modem à classificateur en voie montante L2VPN				
43				Codage L2VPN par câblo-modem individuel
20				Longueur globale
	08 03 FFFFFF			Identificateur de vendeur: 0xFFFFFF pour GEI
	05			GEI 43.5 pour codage L2VPN
	13			Longueur de sous-type GEI.5
		01 05 x0234560003		Sous-type d'identificateur VPNID
		02		Sous-type d'encapsulation de flux à l'interface NSI
		04		Longueur de sous-type GEI.5.2
			02	Sous-type de format IEEE 802.1Q
			02	Longueur de sous-type GEI.5.2.2
			0x0019	identificateur de réseau VLAN 25
24				Codage par défaut de flux de service en voie montante
07				Longueur
	01 02 0001			Référence de flux de service 0001
	06 01 07			Sous-type du type d'ensemble paramétrique de QoS
24				Codage L2VPN de flux de service en voie montante
19				Longueur
	06 01 07			Sous-type du type d'ensemble paramétrique de QoS
	43			Sous-type propre au vendeur:
	14			Longueur globale
		08 03 FFFFFF		Identificateur de vendeur pour GEI
		05		GEI 43.5 pour codage L2VPN
		7		Longueur de sous-type GEI.5
			01 05 x0234560003	Sous-type d'identificateur VPNID
22				Codage de classificateur en voie montante
14				Longueur

Tableau I.8 – Codage d'un classificateur en voie montante L2VPN

Fichier de configuration de câblo-modem à classificateur en voie montante L2VPN				
	03 02 0001			Référence de flux de service: 0001
	10			Classification de paquet Ethernet/LLC
	8			
		02		Adresse MAC d'origine
		6		Longueur
			x0001020000AA	Adresse MAC des équipements CPE1
45				Filtrage du trafic DUT:
01				Longueur globale
	01			Filtrage du trafic DUT activé

Appendice II

Encapsulation IEEE 802.1Q

Le présent appendice fournit des informations de référence sur le format des balises IEEE 802.1Q du côté Ethernet des interfaces NSI. Il s'agit du mécanisme normal pour indiquer le réseau VLAN d'un paquet ponté par une interface avec un réseau Ethernet. Un système CMTS conforme à la présente Recommandation est tenu de prendre en charge la reconnaissance de l'encapsulation de flux IEEE 802.1Q à une interface avec un réseau Ethernet quand il est configuré afin d'effectuer cette tâche.

Etant donné que le système CMTS interprète l'identificateur de réseau VLAN de la balise 802.1Q externe d'un paquet entrant dans une interface NSI, cette balise est dite *balise délimitatrice de service*.

Le réexpéditeur L2VPN *extrait* la balise délimitatrice de service IEEE 802.1Q d'un paquet Ethernet lorsqu'il réexpédie celui-ci en voie descendante et l'*insère* lors de la réexpédition de paquets en voie montante. Le réseau VLAN particulier auquel un paquet L2VPN appartient est explicitement indiqué par une interface avec un réseau Ethernet à flux 802.1Q encapsulé, et est toujours impliqué quand ce réseau est réexpédié par l'interface RF avec les commandes MAC-DOCSIS.

Cette extraction/insertion des balises IEEE 802.1Q est décrite dans la Figure II.1:

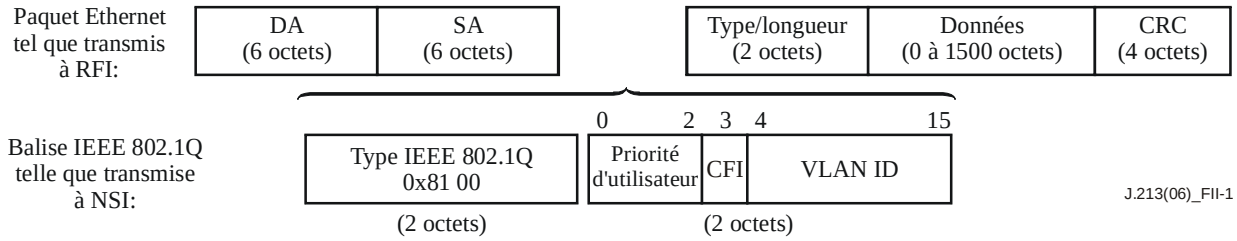

Figure II.1 – Balises 802.1Q dans le protocole Ethernet

Un paquet Ethernet est balisé au format IEEE 802.1Q par insertion de quatre octets entre son adresse d'origine initiale (SA) et son champ initial de longueur/type. Le code de type Ethernet sur deux octets 0x8100 indique qu'une balise IEEE 802.1Q de 16 bits suit. La valeur de balise se compose des 3 bits d'un champ de priorité d'utilisateur dans les 3 positions binaires de plus fort poids, d'un bit indicateur de format canonique (CFI, *canonical format indicator*) et des 12 bits d'un identificateur de réseau VLAN dans les positions binaires de plus faible poids. La valeur du fanion CFI est définie par l'IEEE et est égale à zéro pour les adresses MAC d'un réseau Ethernet. Tous les champs à octets multiples sont transmis avec l'octet de plus fort poids en premier.

Le champ de priorité d'utilisateur indique une priorité de réexpédition du trafic dans l'étendue de 0..7, les valeurs supérieures indiquant une priorité supérieure.

La présente Recommandation permet, mais n'exige pas que le système CMTS utilise l'encapsulation à des ports d'interface NSI autres que IEEE 802.1Q afin de signaler le réseau L2VPN ou le circuit de rattachement pour un paquet réexpédié par réseau L2VPN. L'encapsulation particulière à l'interface NSI, utilisée pour la réexpédition L2VPN, est destinée à être configurée dans le sous-type d'encapsulation de flux à l'interface NSI, contenu dans un codage L2VPN.

Appendice III

Modèle de pontage par câblo-modem d'un réseau VLAN intégré

Le présent appendice propose, à l'attention de la communauté DOCSIS, un modèle de réseau VLAN intégré pour réexpédition par pont de paquets intégré dans un câblo-modem. Ce modèle n'est pas actuellement une exigence pour la certification L2VPN d'un câblo-modem.

La spécification L2VPN utilise le concept de masque d'interface avec un câblo-modem (CMIM) afin de définir l'ensemble des interfaces internes et externes avec un pont, vers lesquelles le câblo-modem peut ponter le trafic en voie descendante. Le masque CMIM définit par exemple le domaine de diffusion de trafic en voie descendante vers des adresses MAC aussi bien individuelles que collectives. Un domaine de diffusion est une certaine interprétation d'un réseau VLAN, de sorte qu'en fait, le masque CMIM doit définir un réseau VLAN interne utilisant les ports internes et externes vers lesquels les trafics DUT et L2VPN sont réexpédiés.

Le modèle de réseau VLAN intégré élargit le pont de commande MAC du modèle eDOCSIS afin qu'il devienne un pont de commande MAC à capacité de réseau VLAN avec des domaines de réexpédition distincts d'adresses MAC dans un réseau VLAN intégré (eVLAN). Au moyen du concept de réseau eVLAN, le câblo-modem est en mesure de découpler le câblo-modem intégré et les serveurs locaux d'entité eSAFE sur la base des domaines de diffusion MAC-L2VPN de clients privés.

La Figure III.1 ci-dessous décrit le modèle de réseau VLAN intégré pour les câblo-modems conformes au modèle L2VPN.

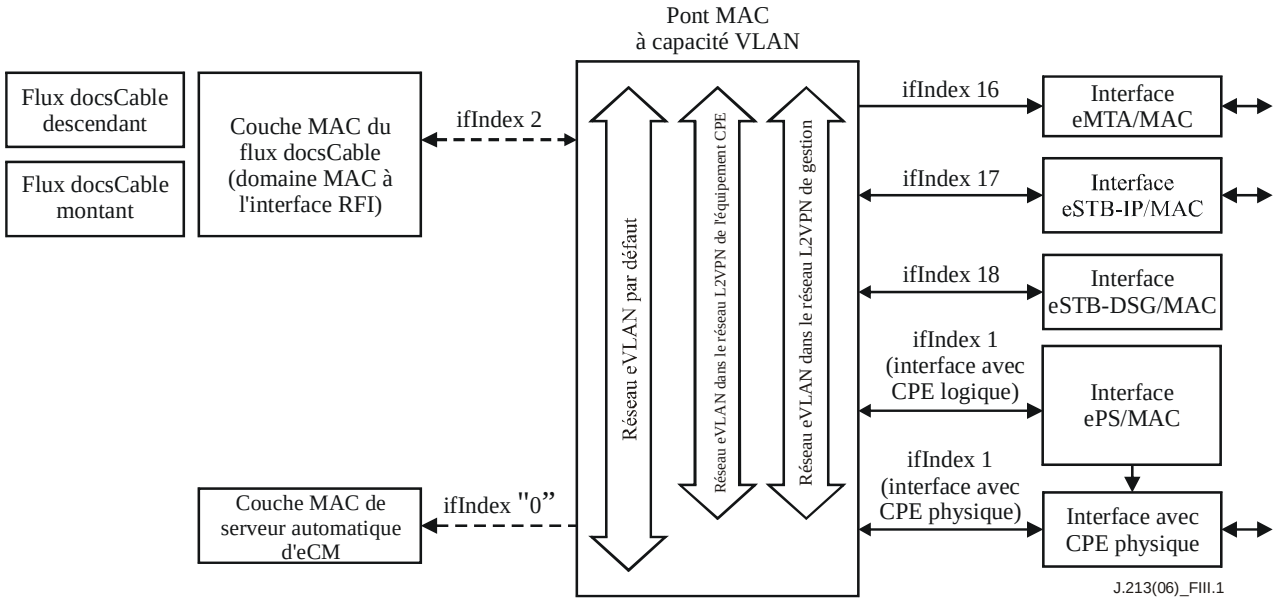

Figure III.1 – Modèle de réseau VLAN intégré (eVLAN) dans un réseau L2VPN

Le pont de commande MAC d'un câblo-modem intégré est considéré comme ayant, à l'indice ifIndex 2, une interface avec un port de pont vers le domaine de commande MAC à l'interface RF; et comme ayant, à l'indice ifIndex 1, une interface primaire avec un port de pont d'équipement CPE. La spécification DOCSIS définit le fonctionnement de la réexpédition d'un flux d'équipement CPE par un câblo-modem résidentiel comme étant une fonction de pontage d'adresses MAC dans la couche 2 entre l'interface RF et l'interface avec l'équipement CPE. Dans la spécification eDOCSIS,

la propre adresse MAC du câblo-modem intégré (celle de son serveur local automatique) est considérée comme étant interne dans le pont de commande MAC et comme étant accessible par toutes les interfaces avec un port de pont.

La spécification eDOCSIS définit une entité fonctionnelle intégrée de service ou d'application (eSAFE) comme étant une entité intégrée dans un câblo-modem intégré (eCM) qui contient ses propres adresses MAC et IP [b-UIT-T J.126]. Les entités eSAFE actuellement définies sont les suivantes:

- serveur local d'adaptateur MTA intégré (eMTA) IPCablecom;
- serveur local de services de portail intégrés (ePS);
- décodeur intégré (eSTB).

Chacun de ces dispositifs eSAFE est considéré comme ayant une interface distincte entre l'équipement CPE logique et le pont de commande MAC. Il reçoit également l'assignation d'un indice d'interface distinct (ifIndex) aux fins de la gestion et de la commande. Dans l'architecture eDOCSIS, le pont MAC du câblo-modem intégré est censé implémenter une unique base de données de réexpédition, associant les adresses MAC à chaque interface avec l'équipement CPE logique et réexpédiant des unités de données de protocole de couche 2 (unités L2PDU) entre tous les ports du pont de commande MAC, conformément à l'adresse MAC de destination (DMAC) de chaque unité L2PDU. Les adresses MAC de l'interface RF, de l'interface ou des interfaces avec l'équipement CPE, du câblo-modem intégré et de toutes les entités eSAFE sont considérées comme étant dans le même domaine de diffusion d'adresses MAC de couche 2 (c'est-à-dire dans un même réseau local).

La spécification L2VPN va élargir cette architecture en introduisant le concept de réseaux VLAN intégrés (réseaux eVLAN) dans le pont de commande MAC du câblo-modem intégré, où ces réseaux eVLAN ont différents ensembles de ports d'équipement CPE logique. Afin de contrôler l'accès à l'adresse MAC automatique du câblo-modem intégré (p. ex. afin de le découpler de l'accès client du réseau L2VPN), l'adresse MAC du câblo-modem intégré est considérée comme résidant dans une interface avec un port de pont automatique.

L'architecture L2VPN présente le concept d'un masque d'interface avec un câblo-modem (CMIM) ayant une position binaire pour chaque port de pont logique contenu dans le pont MAC à capacité VLAN du câblo-modem intégré. Chaque réseau eVLAN passant par le pont de commande MAC contient une valeur de masque CMIM qui représente les ports logiques de pont qui appartiennent à ce réseau eVLAN. Le masque CMIM est représenté comme un codage d'objet SNMP de type BITS, où la position binaire K correspond à l'indice ifIndex de l'interface K avec un port de pont. Dans un masque CMIM, le port logique de pont automatique reçoit l'assignation de la position binaire 0 (c'est-à-dire comme s'il avait la valeur d'indice ifIndex 0). Aucune entrée de table ifStack n'est créée pour l'interface avec le pont automatique, parce que zéro est une valeur invalide d'indice ifIndex.

Dans le pont de commande MAC du câblo-modem intégré, toute réexpédition par réseau non L2VPN est considérée comme étant pontée sur un réseau eVLAN par défaut qui possède un masque CMIM et dont tous les bits d'interface sont réglés à 1. Cela correspond à la réexpédition normale par pont de commande MAC dans un même réseau local, définie précédemment dans la présente Recommandation L2VPN.

Des réseaux eVLAN distincts peuvent cependant être définis avec des *sous-ensembles* des interfaces avec un port de pont de câblo-modem intégré, pour une réexpédition indépendante dans la couche 2. Un service transparent de réseau local (TLS) de clientèle est en particulier implémenté par définition d'un réseau eVLAN pour le réseau L2VPN d'abonné qui contient seulement l'interface RF et l'interface avec l'équipement CPE; un réseau L2VPN à service TLS de clientèle n'est pas autorisé à accéder au câblo-modem intégré ni à d'éventuels serveurs locaux d'entité eSAFE.

Le modèle de réseau eVLAN permet à un câblo-opérateur d'implémenter des réseaux L2VPN de gestion pour le trafic de câblo-modem intégré et d'entité eSAFE, en définissant un réseau L2VPN contenant un masque CMIM qui raccorde seulement l'interface RF, ainsi que les interfaces avec un pont logique de serveur automatique d'eCM et/ou d'entité eSAFE.

III.1 Spécification IEEE 802.1Q et modèle de réseau VLAN intégré

Le fonctionnement et la gestion d'un pont de couche MAC avec de multiples réseaux VLAN sont normalisés par la spécification [IEEE 802.1Q], qui a été d'abord établie en 1998 et qui possède une base MIB de suivi de normalisation [b-IETF RFC 2674]. Le masque CMIM d'un réseau L2VPN peut être considéré comme définissant le masque binaire dot1qVlanCurrentEgressPorts de [b-IETF RFC 2674]. Si le concept de réseau eVLAN est adopté comme modèle de réexpédition dans la couche 2 par câblo-modem DOCSIS, la [b-IETF RFC 2674] définit déjà un riche ensemble d'objets permettant de surveiller et de commander l'exploitation de la couche 2 par un câblo-modem.

La spécification [IEEE 802.1Q] a été notablement enrichie en 2003 par de nombreuses extensions IEEE 802.1 provisoires (y compris [IEEE 802.1p]). Au moment de la parution de la présente Recommandation, la base MIB pour la spécification [IEEE 802.1Q] élargie prend cependant la forme de [b-IETF RFC 4363].

L'adoption du modèle de réexpédition par réseau eVLAN permettra aux futures spécifications DOCSIS d'établir une claire distinction entre le fonctionnement de l'interface RF et le filtrage, la réexpédition et la réplication de flux dans la couche 2 par les diverses interfaces physiques, internes et externes, utilisant des dispositifs DOCSIS à base de câblo-modem.

Le domaine d'application de la spécification [IEEE 802.1Q] est extrêmement général et évolué, de sorte qu'il est aussi extrêmement complexe. Cette spécification compte 327 pages et son projet de base MIB [b-IETF RFC 4363] compte 106 pages. Le fait de n'implémenter que les fonctions minimales spécifiées pour assurer la conformité à la spécification [IEEE 802.1Q], ou les objets minimaux nécessaires pour appliquer la référence [b-IETF RFC 2547], représente beaucoup plus de fonctionnalités et de commandes que cela n'est approprié pour le pont intégré de commande MAC d'un câblo-modem L2VPN conforme.

Et pourtant, les vastes capacités et bases MIB développées par l'IEEE pour le pontage par réseaux VLAN multiples peuvent et devraient servir de modèle pour la future amélioration des spécifications de réexpédition par câblo-modem dans la couche 2. Le concept de réseau eVLAN possède le pouvoir de représenter tous les modèles actuels de réexpédition eDOCSIS et de représenter correctement les modèles de réexpédition dans la couche 2 qui feront l'objet de futures spécifications DOCSIS en vue d'améliorations de la réexpédition iPv6 et de la multidiffusion IP. La spécification [IEEE 802.1Q] définit par exemple des objets de gestion normalisés afin d'exécuter une classification des réseaux VLAN fondée sur le protocole IP et même afin d'exécuter une classification des réseaux VLAN sur la base d'adresses MAC d'origine individuelles.

La présente Recommandation utilise donc les spécifications [IEEE 802.1Q] et [b-IETF RFC 2674] au titre de directives théoriques n'ayant valeur que d'information concernant la fonctionnalité exigée d'un câblo-modem L2VPN conforme (ainsi que d'un système CMTS dans ce domaine). De futures versions de ces spécifications (et d'autres) pourront ajouter de nouvelles fonctions de réexpédition dans la couche 2. Les spécifications [IEEE 802.1Q] et [b-IETF RFC 4363] devraient servir de guide afin de définir ces fonctions.

Par exemple, la spécification L2VPN actuelle ne traite que des paquets non balisés aux interfaces avec un port de pont logique de câblo-modem intégré. A l'interface RF, le réseau L2VPN particulier (ou le réseau VLAN particulier, pour reprendre le terme de [IEEE 802.1Q]) acheminant une unité L2PDU est toujours *impliqué* dans le domaine de commande MAC d'insertion de flux par CMTS ou par CM dans le flux de service en voie montante ou dans les identificateurs SAID en voie

descendante. De futures versions de la présente Recommandation pourront introduire le concept de balise IEEE 802.1Q délimitatrice de services à l'interface RF et/ou à l'interface avec l'équipement CPE du pont de commande MAC contenu dans le câblo-modem intégré. Dans ce cas, la future spécification devrait utiliser les concepts et objets de base MIB déjà normalisés par l'industrie dans les spécifications [IEEE 802.1Q] et IETF.

III.2 Primitives de service dans un domaine de commande MAC de pont intégré

Compte tenu des capacités de flux de service d'un domaine d'interface MAC/RF DOCSIS, un pont MAC de câblo-modem intégré est défini comme offrant le service théorique suivant à ce domaine d'interface RF/MAC:

- en voie descendante (du domaine d'interface MAC/RF jusqu'au pont):
  M_UNITDATA.request (
  L2PDU,
  eVLAN,
  user_priority)
- en voie montante (du pont jusqu'au domaine d'interface MAC/RF):
  M_UNITDATA.indication (
  L2PDU,
  eVLAN,
  user_priority,
  ingress_port)

Où:

- L2PDU est une unité PDU de réseau Ethernet (non balisée) contenant: adresses DMAC, adresses SMAC, champ de type de réseau Ethernet et 0 à 1500 octets de charge utile dans la couche 2;
- eVLAN est un identificateur local dans un réseau eVLAN particulier;
- user_priority est une priorité évaluée à 8 pour la réexpédition dans la couche 2 de l'unité L2PDU, comme défini par la référence [IEEE 802.1Q];
- ingress_port est la valeur d'indice ifIndex de l'interface logique avec le pont duquel l'unité L2PDU a été reçue.

La réexpédition en voie descendante d'un paquet de pont d'eCM s'effectue comme suit:

1) le sous-composant de domaine MAC de CM (CM-MD) reçoit une unité PDU DOCSIS à partir de son interface docsCableDownstream, qui contient une unité L2PDU de gestion d'adresses autres que MAC. L'unité PDU DOCSIS peut contenir un en-tête étendu d'interface BPI ou un en-tête étendu de service en voie descendante;
2) si le paquet a été chiffré avec un identificateur SAID-L2VPN, le sous-composant CM-MD règle le réseau eVLAN du pont demandé à l'identificateur qu'il a créé pour le réseau L2VPN; sinon, le sous-composant CM-MD règle le réseau eVLAN au réseau eVLAN par défaut;
3) si le paquet contenait un identificateur de service en voie descendante (DSID) identifiant le flux de service en voie descendante, le sous-composant CM-MD règle la priorité d'utilisateur demandée (user_priority) au paramètre de priorité de trafic du flux de service descendant; sinon, le sous-composant CM-MD règle à zéro (0) la priorité d'utilisateur demandée;
4) le sous-composant CM-MD demande au pont de commande MAC de réexpédier l'unité L2PDU sur le réseau eVLAN avec la priorité d'utilisateur demandée;

5) le pont de commande MAC réexpédie le paquet à un port d'extraction de pont logique conformément à la liste des ports d'extraction indiqués dans le masque CMIM comme étant autorisés pour le réseau eVLAN. Il peut élargir le paquet vers de multiples ports de pont;

6) si le pont de commande MAC réexpédie l'unité L2PDU vers un port de pont physique à l'interface physique avec l'équipement CPE, ce pont implémente au moins deux classes de trafic IEEE 802.1Q afin d'offrir une réexpédition, à qualité de service rendue prioritaire, des paquets de couche 2. Les câblo-modems peuvent implémenter de deux à huit (8) classes de trafic;

7) si le pont de commande MAC réexpédie l'unité L2PDU vers les services de portail interne J.192 (ePS) avec une priorité d'utilisateur déduite d'un flux de service de priorité de trafic descendant, le service ePS utilise cette valeur comme numéro d'importance de trafic pour son paquet. Cela évite une reclassification en service ePS du paquet, au moyen de sa base MIB cabhQos2PolicyTable.

La réexpédition en voie montante d'un paquet par pont de câblo-modem intégré s'effectue comme suit:

1) l'interface avec l'équipement CPE physique reçoit une unité L2PDU puis demande au pont de commande MAC, contenu dans le câblo-modem intégré, de réexpédier le paquet avec la priorité d'utilisateur 0 et avec le réseau eVLAN par défaut;

2) en variante, une entité eSAFE interne peut demander au pont de commande MAC de réexpédier une unité L2PDU avec une valeur explicite de priorité d'utilisateur et de réseau eVLAN;

3) le pont de commande MAC indique qu'une unité L2PDU doit être transmise au sous-composant de domaine MAC de CM avec indication du réseau eVLAN, de l'interface avec le réseau d'insertion de flux et de la priorité d'utilisateur;

4) le sous-composant CM-MD utilise le réseau eVLAN afin de sélectionner un ensemble de classificateurs de paquet en voie montante; le réseau eVLAN par défaut va sélectionner les classificateurs de réseau non L2VPN, tandis que tout autre réseau eVLAN ne sélectionnera les classificateurs L2VPN de paquet en voie montante que pour le réseau L2VPN correspondant;

5) le sous-composant CM-MD utilise le port d'insertion indiqué afin de faire concorder des règles de classificateur avec un critère de masque CMIM, et utilise la priorité d'utilisateur indiquée afin de faire concorder des règles de classificateur avec un critère d'étendue de priorités d'utilisateur. Ces critères s'appliquent à la réexpédition par réseaux aussi bien L2VPN que non L2VPN;

6) le sous-composant CM-MD classifie l'unité L2PDU vers un flux de service en voie montante et réexpédie le paquet vers l'interface docsCableUpstream.

Actuellement, la Recommandation L2VPN exige que de tels paquets soient considérés comme ayant reçu une priorité d'utilisateur égale à zéro (0). De futures versions de la présente Recommandation pourront implémenter divers mécanismes [IEEE 802.1Q] de signalisation explicite (au moyen de balises de priorité absolue), par configuration (avec valeur par défaut de priorité d'utilisateur à l'entrée) et régénération implicites de la priorité d'utilisateur à l'entrée de flux.

Au lieu de modéliser le flux issu d'un service ePS comme allant directement vers le port physique d'équipement CPE, le modèle devrait être modifié de façon que le service ePS envoie le flux à un réseau eVLAN J.192 distinct, contenant seulement les ports de pont des interfaces avec le service ePS et avec l'équipement CPE. Le numéro d'importance du trafic déterminé par le service ePS devient la priorité d'utilisateur de la demande de service ePS visant à transmettre sur le réseau eVLAN de l'équipement CPE J.192. Ce modèle précise comment un réexpéditeur J.192 (et tout autre futur réexpéditeur par équipement CPE dans la couche 3) peut partager le port physique

d'équipement CPE avec d'autres réexpéditeurs vers le port physique CPE contenu dans le câblo-modem intégré, tout en conservant la priorité de qualité de service demandée.

Appendice IV

Restrictions concernant les câblo-modems non conformes à la spécification L2VPN

Le service de réseau L2VPN est essentiellement implémenté dans le système CMTS. Un opérateur peut déployer le service de réseau L2VPN en utilisant un CMTS conforme et des câblo-modems non conformes. Les restrictions concernant l'utilisation de câblo-modems non conformes sont les suivantes:

- des abonnés L2VPN utilisant des câblo-modems non conformes à la spécification DOCSIS 1.1 et à ses versions ultérieures peuvent ne pas observer une réexpédition transparente des multidiffusions IP, ce qui est particulièrement gênant quand des annonces de protocole OSPF et RIPv2 ne sont pas réexpédiées vers des routeurs d'équipement d'abonné. Les câblo-modems non conformes aux spécifications DOCSIS 1.1 et 2.0 appliqueront cependant des règles de réexpédition multidiffusée en protocole IP et bloqueront donc la réexpédition en voie descendante d'adresses IP collectives de multidiffusion non rejointes. Les câblo-modems DOCSIS 2.0 qui implémentent le paramètre d'adresses MAC multidiffusées statiquement peuvent toutefois être programmés de façon à réexpédier le trafic multidiffusé utile. Les câblo-modems non conformes à la version DOCSIS 1.0 ne rejetteront pas ce trafic multidiffusé. Certains vendeurs de câblo-modem proposent également des configurations privées afin de réexpédier en mode espion toutes les multidiffusions IP en voie descendante;
- les adresses non unidiffusées dans la couche 2 d'un réseau non L2VPN vont fuir dans les réseaux L2VPN privés d'équipement CPE. Voir au § IV.1 une description plus détaillée de ce problème;
- les câblo-modems non conformes peuvent ne pas réexpédier des paquets configurés en longueur maximale avec une balise d'abonné, c'est-à-dire avec une longueur de 1522 octets. Le fonctionnement à balises empilées ou intégrées peut devenir impossible avec de tels câblo-modems;
- les câblo-modems non conformes ne peuvent pas empêcher le trafic L2VPN en voie descendante d'atteindre les piles IP des câblo-modems intégrés et celles des serveurs locaux d'entité eSAFE intégrés dans les câblo-modems L2VPN.

NOTE – Le *trafic en voie montante* issu des câblo-modems intégrés et (habituellement) des serveurs locaux d'entité eSAFE est bloqué, ce qui empêche un accès non autorisé dans les deux sens.

- Les câblo-modems non conformes ne peuvent pas rejoindre dynamiquement les réseaux L2VPN, c'est-à-dire au moyen de messages de flux de service dynamique émis par le système CMTS après inscription. Les câblo-modems non conformes doivent toujours être statiquement configurés de façon à rejoindre tous les réseaux L2VPN requis sur la base des codages L2VPN configurés dans leur fichier de configuration de câblo-modem ou dans le système CMTS.

IV.1 Fuite de trafic au travers de câblo-modems non conformes

La présente Recommandation ne spécifie aucun mécanisme permettant d'empêcher la fuite de trafic non L2VPN non chiffré au moyen de câ*blo-modems non conformes* configurés pour la réexpédition L2VPN. Le Tableau IV.1 résume les conditions dans lesquelles des flux non unidiffusés en voie descendante dans des réseaux non L2VPN peuvent fuir dans un réseau CPE d'abonné quand un câblo-modem non conforme est configuré pour la réexpédition L2VPN.

Tableau IV.1 – Fuite de trafic non L2VPN au travers de câblo-modems non conformes configurés pour le réseau L2VPN

Type de trafic en voie descendante	Chiffrement DIME	
	Activé	Désactivé
Trafic Arp/DHCP diffusé (non chiffré)	Fuit	Fuit
Multidiffusions IP non rejointes, p. ex. RIPv2, OSPF. (non chiffrées)	CM DOCSIS 1.0: fuit CM DOCSIS 1.1: bloqué	CM DOCSIS 1.0: fuit CM DOCSIS 1.1: bloqué
Multidiffusion IP rejointe (chiffré quand DIME est activé)	Bloqué	CM DOCSIS 1.0: fuit CM DOCSIS 1.1: bloqué
Passerelle DSG (jamais chiffrée)	CM DOCSIS 1.0: fuit CM DOCSIS 1.1: bloqué	CM DOCSIS 1.0: fuit CM DOCSIS 1.1: bloqué

NOTE – La fuite du trafic non chiffré et diffusé dans un réseau non L2VPN (en protocoles ARP et DHCP) vers un réseau L2VPN d'abonné ne pose habituellement pas un gros problème à l'abonné, parce qu'un tel trafic est relativement faible. Le trafic IP multidiffusé et rejoint en grand volume est bloqué même par des câblo-modems non conformes quand il est chiffré. Même la fuite de trafic multidiffusé non chiffré au travers des câblo-modems non conformes à la version DOCSIS 1.0 peut être évitée par l'insertion d'un filtre IP approprié dans le fichier de configuration d'un câblo-modem DOCSIS 1.0.

Bibliographie

[b-UIT-T J.126] Recommandation UIT-T J.126 (2004), *Spécification de câblo-modem intégré*.

[b-UIT-T J.167] Recommandation UIT-T J.167 (2005), *Prescriptions d'installation des adaptateurs MTA utilisés pour la fourniture de services en temps réel sur les réseaux de télévision par câble au moyen de câblo-modems*.

[b-UIT-T J.192] Recommandation UIT-T J.192 (2005), *Passerelle résidentielle assurant la remise des services de données par câble*.

[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*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	**Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias**
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2007