Groupe de travail Réseau
Request for Comments : 4762
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

M. Lasserre, éd., Alcatel-Lucent
V. Kompella, éd., Alcatel-Lucent
janvier 2007

Service de LAN privé virtuel (VPLS) utilisant la signalisation du protocole de distribution d'étiquettes (LDP)

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Note de l'IESG
Le groupe de travail L2VPN a produit deux documents séparés, la RFC 4761 et le présent document, qui effectuent en fin de compte des fonctions similaires de manières différentes. Il faut savoir que chaque méthode est couramment appelée "VPLS" bien qu'elles soient distinctes et incompatibles entre elles.

Résumé
Le présent document décrit une solution de service de LAN privé virtuel (VPLS, *Virtual Private LAN Service*) utilisant des pseudo-filaires, un service précédemment mis en œuvre sur des technologies de tunnelage et connu sous le nom de services de LAN transparents (TLS, *Transparent LAN Services*). Un VPLS crée un segment émulé de LAN pour un ensemble donné d'utilisateurs ; c'est-à-dire, il crée un domaine de diffusion de couche 2 qui est pleinement capable d'apprendre et de transmettre sur des adresses MAC Ethernet et qui est fermé pour un certain ensemble d'utilisateurs. Plusieurs services de VPLS peuvent être pris en charge à partir d'un seul nœud de côté fournisseur (PE, *Provider Edge*).

Le présent document décrit les fonctions de plan de contrôle d'étiquettes de pseudo filaire de signalisation en utilisant le protocole de distribution d'étiquettes (LDP, *Label Distribution Protocol*) étendant la RFC 4447. Il est neutre à l'égard des protocoles de découverte. Les fonctions de plan des données de transmission sont aussi décrites, en se concentrant en particulier sur l'acquisition des adresses MAC. L'encapsulation des paquets de VPLS est décrite dans la RFC 4448.

Table des matières

1. Introduction....2
2. Terminologie....2
2.1 Conventions....3
3. Acronymes....3
4. Modèle topologique pour VPLS....3
4.1 Arrosage et transmission....4
4.2 Acquisition d'adresse....4
4.3 Topologie de tunnel....4
4.4 VPLS sans boucle....4
5. Découverte....5
6. Plan de contrôle....5
6.1 Signalisation des démultiplexeurs fondée sur LDP....5
6.2 Retrait d'adresse MAC....5
7. Transmission des données sur un PW Ethernet....7
7.1 Actions d'encapsulation de VPLS....7
7.2 Actions d'acquisition de VPLS....7
8. Transmission de données sur un PW de VLAN Ethernet....8
8.1 Actions d'encapsulation de VPLS....8
9. Fonctionnement d'un VPLS....8

9.1 Vieillissement d'adresse MAC....9
10. Modèle VPLS hiérarchique....9
10.1 Connexité hiérarchique....10
10.1.2 Avantages de la connexité de rayons....11
10.2 Connexions de rayons redondantes....12
10.3 Service VPLS multi-domaines....13
11. Modèle VPLS hiérarchique utilisant un réseau d'accès Ethernet....14
11.1 Adaptabilité....15
11.2 Double rattachement et récupération de défaillance....15
12. Contributeurs....15
13. Remerciements....15
14. Considérations sur la sécurité....15
15. Considérations relatives à l'IANA....16
16. Références....16
16.1 Références normatives....16
16.2 Références pour information....16
Appendice A. Signalisation de VPLS en utilisant l'élément de FEC PWid....17
Adresse des auteurs....17
Déclaration complète de droits de reproduction....17

1. Introduction

Ethernet est devenu la technologie prédominante pour la connexité des réseaux de zone locale (LAN, *Local Area Network*) et a été accepté comme technologie d'accès, en particulier dans les réseaux de zone métropolitaine (MAN, *Metropolitan Area Network*) et réseaux de large zone (WAN, *Wide Area Network*). La principale motivation des services de LAN privé virtuel (VPLS, *Virtual Private LAN Service*) est de fournir la connexité entre des sites de consommateur géographiquement dispersés à travers des MAN et WAN, comme si ils étaient connectés en utilisant un LAN. L'application prévue pour l'utilisateur final peut être divisée en les deux catégories suivantes :

- Connexité entre routeurs de consommateur : application d'acheminement de LAN
- Connexité entre commutateurs Ethernet de consommateurs : application de commutation de LAN.

Les services de diffusion et diffusion groupée sont disponibles sur les LAN traditionnels. Les sites qui appartiennent au même domaine de diffusion et qui sont connectés via un réseau MPLS s'attendent à ce que le trafic de diffusion, diffusion groupée, et en envoi individuel soit transmis aux sites appropriés. Cela exige l'apprentissage/vieillissement des adresses MAC sur la base du pseudo-filaire, et la duplication de paquet à travers les pseudo-filaires pour le trafic de diffusion groupée/diffusion et pour l'arrosage du trafic de destination inconnue en envoi individuel.

La [RFC4448] définit comment porter les trames de couche 2 (L2, *Layer 2*) sur les pseudo-filaires (PW) en point à point. Le présent document décrit des extensions à la [RFC4447] pour transporter le trafic Ethernet/802.3 et de VLAN [802.1Q] à travers plusieurs sites qui appartiennent au même domaine de diffusion L2 ou VPLS. Noter que le même modèle peut être appliqué aux autres technologies 802.1. Il décrit une façon simple et adaptable pour offrir des services de LAN virtuel, incluant l'arrosage approprié de trafic de destination de diffusion, diffusion groupée, et d'envoi individuel de destination inconnue sur MPLS, sans avoir besoin de serveurs de résolution d'adresse ou autres serveurs externes, comme exposé dans la [RFC4665].

La discussion qui suit s'applique aux appareils qui sont à capacité VPLS et ont un moyen de tunneler les paquets étiquetés entre chaque autre. L'ensemble résultant d'appareils interconnectés forme un VPN privé MPLS.

2. Terminologie

Q dans Q : extensions de pont de fournisseur 802.1ad aussi appelé un VLAN empilable ou Q dans Q.

Apprentissage qualifié : mode d'apprentissage dans lequel chaque consommateur VLAN est transposé en sa propre instance de VPLS.

Délimiteur de service : informations utilisées pour identifier une instance spécifique de service de consommateur. C'est normalement codé dans l'en-tête d'encapsulation des trames de consommateur (par exemple, identifiant de VLAN).

Trame étiquetée : trame avec un identifiant de VLAN 802.1Q.

Apprentissage non qualifié : mode d'apprentissage où tous les VLAN d'un seul consommateur sont transposés en un seul VPLS.

Trame non étiquetée : trame sans identifiant de VLAN 802.1Q.

2.1 Conventions

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Acronymes

AC *(Attachment Circuit)* : circuit de rattachement
BPDU *(Bridge Protocol Data Unit)* : Unité de données de protocole de pont
CE *(Customer Edge device)* : appareil côté utilisateur
FEC *(Forwarding Equivalence Class)* : classe d'équivalence de transmission
FIB *(Forwarding Information Base)* : base de données d'informations de transmission
GRE *(Generic Routing Encapsulation)* : encapsulation d'acheminement générique
IPsec *(IP security)* : sécurité du protocole IP
L2TP *(Layer Two Tunneling Protocol)* : protocole de tunnelage de couche deux
LAN *(Local Area Network)* : réseau de zone locale
LDP *(Label Distribution Protocol)* : protocole de distribution d'étiquettes
MTU-s *(Multi-Tenant Unit switch)* : commutateur d'unités multi occupants
PE *(Provider Edge device)* : appareil côté fournisseur
PW *(Pseudowire)* : pseudo filaire
STP *(Spanning Tree Protocol)* : protocole d'arborescence d'expansion
VLAN *(Virtual LAN)* : réseau virtuel de zone locale

4. Modèle topologique pour VPLS

Une interface qui participe à un VPLS doit être capable d'arroser, transmettre, et filtrer les trames Ethernet. La Figure 1, ci-dessous, montre le modèle topologique d'un VPLS. L'ensemble d'appareils PE interconnectés via des PW apparaît comme un seul LAN émulé au consommateur X. Chaque PE va former une association d'adresses MAC distantes au PW et associer directement les adresses MAC rattachées aux accès face au consommateur local. Ceci est modélisé sur l'apprentissage standard d'adresse MAC IEEE 802.1.

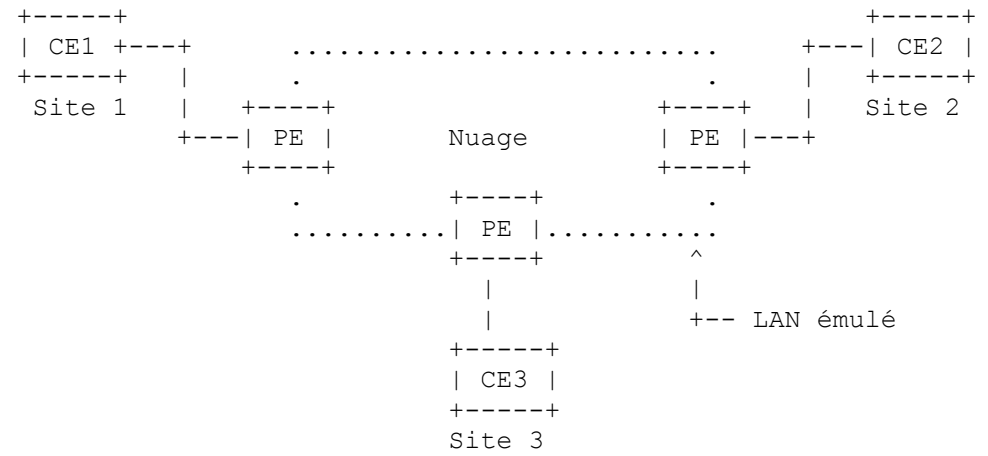


Figure 1 : Modèle topologique d'un VPLS pour le consommateur X avec trois sites

On note encore ici qu'alors que le présent document montre des exemples spécifiques qui utilisent des tunnels de transport MPLS, d'autres tunnels qui peuvent être utilisés par les PW (comme mentionné dans la [RFC4447]) -- par exemple, GRE, L2TP, IPsec -- peuvent aussi être utilisés, pour autant que le PE d'origine puisse être identifié, car c'est utilisé dans le processus d'apprentissage MAC.

La portée du VPLS se limite aux PE dans le réseau du fournisseur de services, en soulignant le fait que à part la délimitation du service de consommateur, la forme d'accès au site d'un consommateur n'est pas pertinente pour le VPLS [RFC4665]. En d'autres termes, le circuit de rattachement (AC, *attachment circuit*) connecté au consommateur pourrait être un accès physique Ethernet, un accès logique (étiqueté) Ethernet, un PVC ATM portant des trames Ethernet, etc., ou même un PW Ethernet.

Le PE est normalement un routeur de bordure capable de faire fonctionner le protocole de signalisation LDP et/ou des protocoles d'acheminement aux PW établis. De plus, il est capable d'établir des tunnels de transport vers les autres PE et de livrer le trafic sur les PW.

4.1 Arrosage et transmission

Un des attributs d'un service Ethernet est que les trames envoyées aux adresses de diffusion et aux adresses MAC de destination inconnue sont arrosées à tous les accès. Pour réaliser l'arrosage au sein du réseau de fournisseur de services, toutes les trames en envoi individuel, en diffusion et en diffusion groupée inconnues sont arrosées sur les PW correspondants à tous les nœuds PE qui participent au VPLS, ainsi qu'à tous les AC.

Noter que les trames en diffusion groupée sont un cas particulier et n'ont pas nécessairement à être envoyées à tous les membres du VPN. Pour simplifier, l'approche par défaut de la diffusion des trames de diffusion groupée est utilisée.

Pour transmettre une trame, un PE DOIT être capable d'associer une adresse MAC de destination à un PW. Il n'est pas raisonnable et peut-être impossible d'exiger que les PE configurent statiquement une association de toutes les adresses MAC de destination possibles à un PW. Donc, les PE à capacité VPLS DEVRAIENT avoir la capacité d'apprendre de façon dynamique les adresses MAC sur les AC et les PW et de transmettre et dupliquer les paquets à travers les AC et les PW.

4.2 Acquisition d'adresse

À la différence des VPN BGP [RFC4364], les informations d'accessibilité ne sont pas annoncées et distribuées via un plan de contrôle. L'accessibilité est obtenue par les fonctions standard de pont d'apprentissage dans le plan des données.

Quand un paquet arrive sur un PW, si l'adresse MAC de source est inconnue, il doit être associé au PW, afin que les paquets sortants pour cette adresse MAC puissent être livrés sur le PW associé. De même, quand un paquet arrive sur un AC, si l'adresse MAC de source est inconnue, il doit être associé à l'AC, afin que les paquets sortants pour cette adresse MAC puissent être livrés sur l'AC associé.

Les actions standard d'apprentissage, de filtrage, et de transmission, comme définies dans [802.1D-ORIG], [802.1D-REV], et [802.1Q], sont exigées quand l'état d'un PW ou AC change.

4.3 Topologie de tunnel

Les routeurs PE sont supposés avoir la capacité d'établir des tunnels de transport. Les tunnels sont établis entre les PE pour agréger le trafic. Les PW sont signalés pour démultiplexer les trames Ethernet encapsulées provenant de multiples instances de VPLS qui traversent les tunnels de transport.

Dans un L2VPN Ethernet, il devient de la responsabilité du fournisseur de services de créer la topologie sans boucle. Pour simplifier, on définit que la topologie d'un VPLS est un maillage complet des PW.

4.4 VPLS sans boucle

Si la topologie du VPLS n'est pas restreinte à un maillage complet, il se peut alors que deux PE ne soient pas directement connectés via des PW ; ils devraient alors utiliser un PE intermédiaire pour relayer les paquets. Cette topologie exigerait

l'utilisation d'un protocole de rupture de boucles, comme un protocole d'arborescence d'expansion.

Au lieu de cela, un maillage complet des PW est établi entre les PE. Comme chaque PE est maintenant directement connecté à chaque autre PE dans le VPLS via un PW, il n'y a plus besoin de relayer les paquets, et on peut instancier une plus simple règle pour casser les boucles : la règle de "l'horizon partagé", par laquelle un PE NE DOIT PAS transmettre de trafic provenant d'un PW à un autre dans le même maillage VPLS.

Noter qu'il est permis aux consommateurs d'utiliser un protocole d'arborescence d'expansion (STP, *Spanning Tree Protocol*) (par exemple, comme défini dans [802.1D-REV]) comme quand un consommateur a des liaisons "de secours" utilisées pour assurer une redondance dans le cas d'une défaillance au sein du VPLS. Dans ce cas, les PDU de pont STP (BPDU, *STP Bridge PDU*) sont simplement tunnelées à travers le nuage du fournisseur.

5. Découverte

La capacité de configurer manuellement les adresses des PE distants est EXIGÉE. Cependant, l'utilisation d'une configuration manuelle n'est pas nécessaire si une procédure d'auto découverte est utilisée. Un certain nombre de procédures d'auto découverte sont compatibles avec le présent document ([RADIUS-DISC], [RFC5195]).

6. Plan de contrôle

Le présent document décrit les fonctions de plan de contrôle de signalisation des étiquettes de PW. Des travaux fondamentaux sont en cours dans le domaine de la prise en charge du multi rattachements. Les extensions pour la fourniture de la prise en charge du multi rattachements devraient fonctionner indépendamment du fonctionnement de base de VPLS, et elles ne sont pas décrites ici.

6.1 Signalisation des démultiplexeurs fondée sur LDP

Un maillage complet des sessions LDP est utilisé pour établir le maillage des PW. L'exigence d'un maillage complet des PW peut résulter en un grand nombre de session LDP ciblées. La Section 10 discute l'option d'établir des topologies hiérarchiques afin de minimiser la taille du maillage VPLS complet.

Une fois qu'une session LDP a été formée entre deux PE, tous les PW entre ces deux PE sont signalé sur cette session.

Dans la [RFC4447], deux types de FEC sont décrits : l'élément de FEC PWid (type de FEC 128) et l'élément de FEC PWid généralisé (type de FEC 129). L'élément de FEC original utilisé pour VPLS était compatible avec l'élément de FEC PWid. Le texte pour la signalisation en utilisant l'élément de FEC PWid a été déplacé à l'Appendice A. Ce qu'on décrit ci-dessous remplace cela par un descripteur L2VPN plus généralisé, l'élément de FEC PWid généralisé.

6.1.1 Utilisation de l'élément de FEC PWid généralisé

La [RFC4447] décrit une structure de FEC généralisée qui est à utiliser pour la signalisation VPLS de la manière suivante. On décrit l'allocation des champs de l'élément de FEC PWid généralisé dans le contexte de la signalisation VPLS.

Bit de contrôle (C) : ce bit est utilisé pour signaler l'utilisation du mot de contrôle comme spécifié dans la [RFC4447].

Type de PW : les types de PW permis sont Ethernet (0x0005) et le mode Ethernet étiqueté (0x004), comme spécifié dans la [RFC4446].

Longueur d'informations de PW : comme spécifié dans la [RFC4447].

Identifiant de groupe de rattachement (AGI, *Attachment Group Identifier*), Longueur, Valeur : le nom unique de ce VPLS. AGI identifie un type de nom, et Longueur note la longueur de Valeur, qui est le nom du VPLS. On utilise le terme AGI de façon interchangeable avec identifiant de VPLS.

Identifiant individuel de rattachement cible (TAII, *Target Attachment Individual Identifier*), Identifiant individuel de rattachement source (SAII, *Source Attachment Individual Identifier*) : ils sont nuls parce que le maillage des PW dans un

VPLS se termine sur les tableaux d'apprentissage de MAC, plutôt que sur des circuits individuels de rattachement. L'utilisation de TAII et SAII non nuls est réservée pour de futures améliorations.

Paramètres d'interface : les paramètres d'interface pertinents sont :
- MTU : la MTU (unité maximum de transmission) du VPLS DOIT être la même sur tous les PW du maillage.
- Chaîne de description facultative : la même que dans la [RFC4447].
- Identifiant de VLAN demandé : si le type de PW est le mode Ethernet étiqueté, ce paramètre peut être utilisé pour signaler l'insertion de l'identifiant de VLAN approprié, comme défini dans la [RFC4448].

6.2 Retrait d'adresse MAC

Il PEUT être souhaitable de supprimer ou désapprendre les adresses MAC qui ont été apprises dynamiquement pour une convergence plus rapide. Ceci est accompli par l'envoi d'un message Retrait d'adresse LDP avec la liste des adresses MAC à supprimer à tous les autres PE sur les sessions LDP correspondantes.

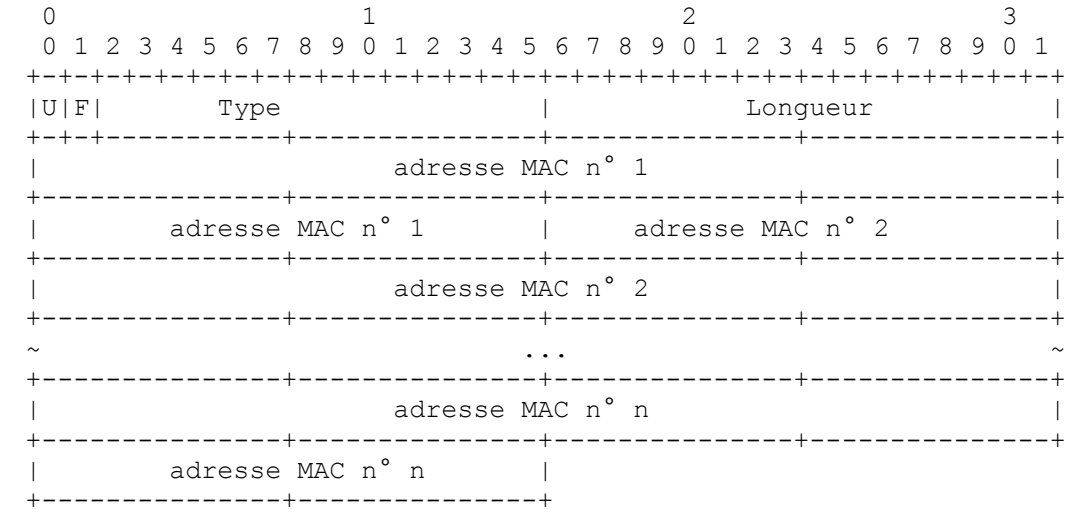
On introduit un TLV facultatif Liste MAC dans LDP pour spécifier une liste d'adresses MAC qui peuvent être supprimées ou désapprises en utilisant le message Retrait d'adresse LDP.

Le message Retrait d'adresse LDP avec les TLV Liste MAC PEUT être pris en charge afin de réaliser la suppression des adresses MAC par suite d'un changement de topologie (par exemple, défaillance de la liaison principale pour un commutateur à double rattachements à capacité VPLS).

Afin de minimiser l'impact sur le temps de convergence de LDP, quand le TLV Liste MAC contient un grand nombre d'adresses MAC, il peut être préférable d'envoyer un message Retrait d'adresse MAC avec une liste vide.

6.2.1 TLV Liste MAC

Les adresses MAC à désapprendre peuvent être signalées en utilisant un message Retrait d'adresse LDP qui contient un nouveau TLV : Liste MAC. Son format est décrit ci-dessous. Le codage d'une adresse de TLV Liste MAC est celui de l'adresse MAC de six octets spécifié dans les documents [802.1D-ORIG] et [802.1D-REV].



Bit U : bit inconnu. Ce bit DOIT être réglé à 1. Si le format d'adresse MAC n'est pas compris, le TLV n'est alors pas compris et DOIT être ignoré.

Bit F : bit transmettre. Ce bit DOIT être réglé à 0. Comme le mécanisme LDP utilisé ici est ciblé, le TLV NE DOIT PAS être transmis.

Type : ce champ DOIT être réglé à 0x0404. Cela identifie le type de TLV comme Liste MAC.

Longueur : ce champ spécifie la longueur totale en octets des adresses MAC dans le TLV. La longueur DOIT être un multiple de 6.

Adresse MAC : la ou les adresses MAC à supprimer.

Le message Suppression d'adresse MAC contient un TLV FEC (pour identifier le VPLS affecté) un TLV Adresse MAC, et des paramètres facultatifs. Aucun paramètre facultatif n'a été défini pour la signalisation de suppression d'adresse MAC. Noter que si un PE reçoit un message Suppression d'adresse MAC et qu'il ne le comprend pas, il DOIT ignorer le message. Dans ce cas, au lieu de purger son tableau d'adresses MAC, il va continuer d'utiliser des informations périmées, sauf si :
- il reçoit un paquet avec une association d'adresse MAC connue, mais provenant d'un PW différent, auquel cas il remplace la vieille association ; ou
- il périme la vieille association.

Le message Suppression d'adresse MAC aide seulement à accélérer la convergence, de sorte que les PE qui ne comprennent pas le message peuvent continuer de participer au VPLS.

6.2.2 Message de retrait d'adresse contenant le TLV Liste MAC

Le traitement du TLV Liste MAC reçu dans un message Retrait d'adresse est :

Pour chaque adresse MAC dans le TLV :
- supprimer l'association entre l'adresse MAC et le AC ou PW sur lequel ce message est reçu.

Pour un message Suppression d'adresse MAC avec une liste vide :
- supprimer toutes les adresses MAC associées à l'instance de VPLS (spécifiée par le TLV FEC) sauf les adresses MAC apprises sur le PW associé à la session de signalisation sur laquelle le message a été reçu.

La portée d'un TLV Liste MAC est le VPLS spécifié dans le TLV FEC dans le message Suppression d'adresse MAC. Le nombre d'adresses MAC peut être déduit du champ Longueur dans le TLV.

7. Transmission des données sur un PW Ethernet

Cette Section décrit le comportement du plan des données sur un PW Ethernet utilisé dans un VPLS. Bien que l'encapsulation soit similaire à celle décrite dans la [RFC4448], on décrit les fonctions de suppression de l'étiquette de délimitation de service et l'utilisation d'une trame Ethernet "normalisée".

7.1 Actions d'encapsulation de VPLS

Dans un VPLS, une trame de consommateur Ethernet sans préambule est encapsulée avec un en-tête comme défini dans la [RFC4448]. Une trame de consommateur Ethernet est définie comme suit :

- Si la trame, comme elle arrive au PE, a une encapsulation qui est utilisée par le PE local comme délimiteur de service, c'est-à-dire, pour identifier le consommateur et/ou le service particulier de ce consommateur, alors cette encapsulation peut être supprimée avant l'envoi de la trame dans le VPLS. Lorsque la trame sort du VPLS, on peut lui insérer une encapsulation de délimitation de service.

- Si la trame, lorsque elle arrive au PE, a une encapsulation qui n'est pas une délimitation de service, c'est une trame de consommateur dont l'encapsulation ne devrait pas être modifiée par le VPLS. Cela couvre, par exemple, une trame qui porte des étiquettes de VLAN spécifiques du consommateur que le fournisseur de services ne connaît pas et ne veut pas modifier.

En application de ces règles, une trame de consommateur peut arriver à l'accès qui fait face au consommateur avec une étiquette de VLAN qui identifie l'instance de VPLS du consommateur. Cette étiquette va être supprimée avant d'être encapsulée dans le VPLS. À la sortie, la trame peut être étiquetée à nouveau, si une étiquette de délimitation de service est utilisée, ou elle peut être non étiquetée si aucune n'est utilisée.

De même, si une trame de consommateur arrive à l'accès face au consommateur sur un VC ATM ou de relais de trame qui identifie l'instance de VPLS du consommateur, l'encapsulation ATM ou FR est alors supprimée avant que la trame soit passée dans le VPLS.

Au contraire, si une trame de consommateur arrive à l'accès face au consommateur avec une étiquette de VLAN qui

identifie un domaine de VLAN dans le réseau de couche 2 du consommateur, l'étiquette n'est alors pas modifiée ou supprimée, car elle appartient au reste de la trame de consommateur.

En suivant les règles ci-dessus, la trame Ethernet qui traverse un VPLS est toujours une trame Ethernet de consommateur. Noter que les deux actions, à l'entrée et à la sortie, de traiter avec des délimiteurs de service sont des actions locales qu'aucun des PE n'a à signaler à l'autre. Cela permet, par exemple, un mélange de services de VLAN étiquetés et non étiquetés à l'une ou l'autre extrémité, et de ne pas transporter à travers un VPLS une étiquette de VLAN qui n'a de signification que locale. Le délimiteur de service peut aussi être une étiquette MPLS, par laquelle un PW Ethernet donné par la [RFC4448] peut servir de connexion côté accès dans un PE. Une encapsulation de PVC ponté de la RFC1483 pourrait aussi servir de délimiteur de service. En limitant la portée des encapsulations à signification locale à la bordure, les modèles de VPLS hiérarchiques peuvent être développés pour fournir la capacité de déploiements de VPLS adaptables par les ingénieurs réseau, comme décrit ci-dessous.

7.2 Actions d'acquisition de VPLS

L'apprentissage est fait sur la base de la trame Ethernet du consommateur, comme défini ci-dessus. La base de données d'informations de transmission (FIB, *Forwarding Information Base*) garde la trace de la transposition de l'adressage de la trame Ethernet de consommateur et du PW approprié à utiliser. On définit deux modes d'apprentissage : l'apprentissage qualifié et l'apprentissage non qualifié. L'apprentissage qualifié est le mode par défaut et DOIT être pris en charge. La prise en charge de l'apprentissage non qualifié est FACULTATIVE.

Dans l'apprentissage non qualifié, tous les VLAN d'un seul consommateur sont traités par un seul VPLS, ce qui signifie qu'ils partagent tous un seul domaine de diffusion et un seul espace d'adresses MAC. Cela signifie que les adresses MAC doivent être uniques et non chevauchantes parmi les VLAN de consommateur, ou autrement qu'elles ne peuvent pas être différenciées au sein de l'instance de VPLS, et il peut en résulter une perte de trames de consommateur. Une application d'apprentissage non qualifié est un service VPLS fondé sur l'accès pour un consommateur donné (par exemple, un consommateur avec un AC non multiplexé où tout le trafic est sur un support physique, qui peut inclure plusieurs VLAN de consommateur, est transposé en une seule instance de VPLS).

Dans l'apprentissage qualifié, chaque VLAN de consommateur est alloué à sa propre instance de VPLS, ce qui signifie que chaque VLAN de consommateur a son propre domaine de diffusion et espace d'adresses MAC. Donc, dans l'apprentissage qualifié, les adresses MAC parmi les VLAN de consommateur peuvent se chevaucher les unes les autres, mais elles vont être traitées correctement car chaque VLAN de consommateur a sa propre FIB ; c'est-à-dire, chaque VLAN de consommateur a son propre espace d'adresses MAC. Comme VPLS diffuse les trames de diffusion par défaut, l'apprentissage qualifié offre l'avantage de limiter la portée de diffusion à un certain VLAN de consommateur. L'apprentissage qualifié peut résulter en grandes tailles de tableaux de FIB, parce que l'adresse MAC logique est maintenant une étiquette de VLAN + l'adresse MAC.

Pour que STP fonctionne en mode d'apprentissage qualifié, un PE VPLS doit être capable de transmettre les BPDU STP sur l'instance de VPLS appropriée. Dans le cas d'un VPLS hiérarchique (voir les détails à la Section 10) les étiquettes de délimitation de service (Q dans Q ou de la [RFC4448]) peuvent être ajoutées de façon que les PE puissent identifier sans ambiguïté tout le trafic de consommateur, incluant les BPDU STP. Dans le cas de VPLS de base, les commutateurs en amont doivent insérer de telles étiquettes de délimitation de service. Quand un accès est partagé par plusieurs consommateurs, un VLAN réservé par domaine de consommateur doit être utilisé pour porter le trafic STP. Les trames STP sont encapsulées avec une unique étiquette de fournisseur par consommateur (comme le trafic régulier de consommateur) et les PE cherchent l'étiquette de fournisseur pour envoyer ces trames à travers l'instance de VPLS appropriée.

8. Transmission de données sur un PW de VLAN Ethernet

Cette Section décrit le comportement du plan de données sur un PW de VLAN Ethernet dans un VPLS. Bien que l'encapsulation soit similaire à celle décrite dans la [RFC4448], on décrit les fonctions d'imposition des étiquettes et d'utilisation d'une trame Ethernet "normalisée". Le comportement d'apprentissage est le même que pour les PW Ethernet.

8.1 Actions d'encapsulation de VPLS

Dans un VPLS, une trame Ethernet de consommateur sans préambule est encapsulée avec un en-tête comme défini dans la [RFC4448]. Une trame Ethernet de consommateur est définie comme suit :

- Si la trame, quand elle arrive au PE, a une encapsulation qui fait partie de la trame de consommateur et est aussi utilisée par le PE local comme délimiteur de service, c'est-à-dire, pour identifier le consommateur et/ou le service particulier de ce consommateur, alors cette encapsulation est préservée lorsque la trame est envoyée dans le VPLS, sauf si le paramètre facultatif Identifiant de VLAN demandé a été signalé. Dans ce cas, l'étiquette de VLAN est réécrite avant l'envoi de la trame sur le PW.

- Si la trame, quand elle arrive au PE, a une encapsulation qui n'a pas l'étiquette de VLAN requise, une étiquette nulle est apposée si le paramètre facultatif Identifiant de VLAN demandé n'était pas signalé.

En application de ces règles, une trame de consommateur peut arriver à l'accès face au consommateur avec une étiquette de VLAN qui identifie l'instance de VPLS du consommateur et aussi identifie un VLAN de consommateur. Cette étiquette va être préservée car elle est encapsulée dans le VPLS.

Le PW de VLAN Ethernet fournit un moyen simple de préserver les bits 802.1p du consommateur.

Un VPLS PEUT avoir des PW à la fois Ethernet et de VLAN Ethernet. Cependant, si un PE n'est pas capable de prendre en charge les deux PW simultanément, il DEVRAIT envoyer un message Libération d'étiquette sur les messages du PW qu'il ne peut pas prendre en charge avec un code d'état "FEC inconnue" comme indiqué dans la [RFC3036].

9. Fonctionnement d'un VPLS

On montre dans la Figure 2 ci-dessous, un exemple de la façon dont fonctionne un VPLS. La discussion qui suit utilise la figure ci-dessous, où un VPLS a été établi entre PE1, PE2, et PE3. Le VPLS connecte un consommateur avec 4 sites marqués A1, A2, A3, et A4 à travers respectivement, CE1, CE2, CE3, et CE4.

Initialement, le VPLS est établi afin que PE1, PE2, et PE3 aient un maillage complet de PW Ethernet. L'instance de VPLS est munie d'un identifiant (AGI). Pour l'exemple ci-dessous, disons que PE1 signale l'étiquette de PW 102 à PE2 et 103 à PE3, et que PE2 signale l'étiquette de PW 201 à PE1 et 203 à PE3.

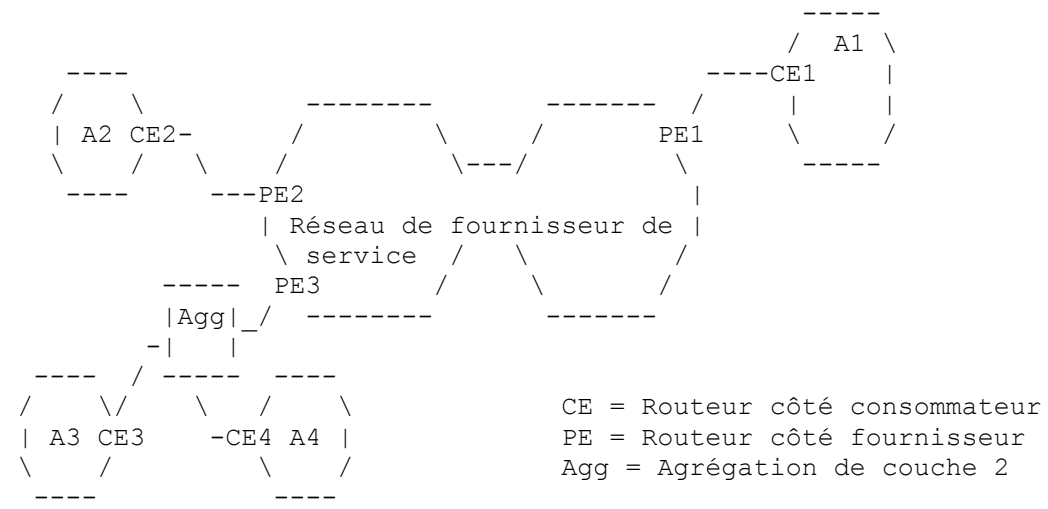


Figure 2 : Exemple de VPLS

Supposons qu'un paquet provenant de A1 soit destiné à A2. Quand il quitte CE1, disons qu'il a une adresse MAC de source de M1 et une destination MAC de M2. Si PE1 ne sait pas où est M2, il va arroser le paquet; c'est-à-dire, l'envoyer à PE2 et PE3. Quand PE2 reçoit le paquet, il va avoir une étiquette de PW de 201. PE2 peut en conclure que l'adresse MAC de source M1 est derrière PE1, car il a distribué l'étiquette 201 à PE1. Il peut donc associer l'adresse MAC M1 à l'étiquette de PW 102.

9.1 Vieillissement d'adresse MAC

Les PE qui apprennent des adresses MAC distantes DEVRAIENT avoir un mécanisme de vieillissement pour supprimer les entrées non utilisées associées à une étiquette de PW. C'est important à la fois pour la conservation de la mémoire et pour

les besoins d'administration. Par exemple, si un site de consommateur A est fermé, éventuellement les autres PE devraient désapprendre l'adresse MAC de A.

Le temporisateur de vieillissement pour l'adresse MAC M DEVRAIT être réinitialisé quand un paquet avec l'adresse MAC de source M est reçu.

10. Modèle VPLS hiérarchique

La solution décrite ci-dessus exige un maillage complet des tunnels LSP entre tous les routeurs PE qui participent au service VPLS. Pour chaque service VPLS, n*(n-1)/2 PW doivent être établis entre les routeurs PE. Bien que cela crée une surcharge de signalisation, le réel inconvénient d'un déploiement à grande échelle est l'exigence de duplication des paquets pour chaque PW provisionné sur un routeur PE. La connexité hiérarchique, décrite dans le présent document, réduit la surcharge de signalisation et de duplication pour permettre un déploiement à grande échelle.

Dans de nombreux cas, les fournisseurs de service placent de plus petits appareils de bordure dans des constructions multi-locataires et les agrègent dans un PE dans des facilités d'un grand office central (CO, *Central Office*). Dans certaines instances, les techniques standard d'étiquetage IEEE 802.1q (Dot 1Q) peuvent être utilisées pour faciliter la transposition des interfaces de CE aux circuits d'accès VPLS à un PE.

Il est souvent avantageux d'étendre les techniques de tunnelage du service VPLS dans le domaine de la commutation d'accès. Cela peut être accompli en traitant l'appareil d'accès comme un PE et en provisionnant les PW entre lui et chaque autre bord, comme un VPLS de base. Une autre solution est d'utiliser les PW de la [RFC4448] ou les interfaces logiques Q dans Q entre l'appareil d'accès et les routeurs PE choisis à capacité VPLS. L'encapsulation Q dans Q est une autre forme de technique de tunnelage de couche 2, qui peut être utilisée en conjonction avec la signalisation MPLS, comme on va le décrire plus loin. Les deux paragraphes qui suivent se concentrent sur cette autre approche. Les PW du cœur de VPLS (pivot) sont augmentés de PW d'accès (rayons) pour former un VPLS hiérarchique (H-VPLS) à deux niveaux.

Les PW rayons peuvent être mis en œuvre en utilisant tout mécanisme de tunnelage de couche 2, et en étendant la portée du premier niveau pour inclure les routeurs PE non pontants du VPLS. Le routeur PE non pontant va étendre un PW rayon à partir d'un commutateur de couche 2 qui le connecte, à travers le réseau de cœur du service, à un routeur PE pontant du VPLS qui prend en charge les PW pivots. On décrit aussi comment les nœuds du VPLS en cause et les CE de l'extrémité basse sans capacité MPLS peuvent participer à un VPLS hiérarchique.

Pour la suite de cette discussion, on se réfère à un appareil d'accès capable de pontage comme un MTU-s et à un PE sans capacité de pontage comme un PE-r. On appelle un appareil capable d'acheminement et de pontage un PE-rs.

10.1 Connexité hiérarchique

Ce paragraphe décrit le modèle de connexité de pivot et rayons et décrit les exigences des appareils capable de pontage et les MTU-s non pontants pour la prise en charge de la connexion des rayons.

10.1.1 Connexité de rayons pour appareils capable de pontage

Dans la Figure 3, ci-dessous, trois sites de consommateur sont connectés à un MTU-s à travers CE-1, CE-2, et CE-3. Le MTU-s a une seule connexion (PW-1) à PE1-rs. Les appareils PE-rs sont connectés dans un maillage complet de VPLS de base. Pour chaque service VPLS, un seul PW rayon est établi entre le MTU-s et le PE-rs sur la base de la [RFC4447]. À la différence des PW traditionnels qui se terminent sur un accès physique (ou un accès logique de VLAN étiqueté) un PW rayon se termine sur une instance de commutateur virtuel (VSI, *virtual switch instance*) (voir la [RFC4664]) sur les appareils MTU-s et PE-rs.

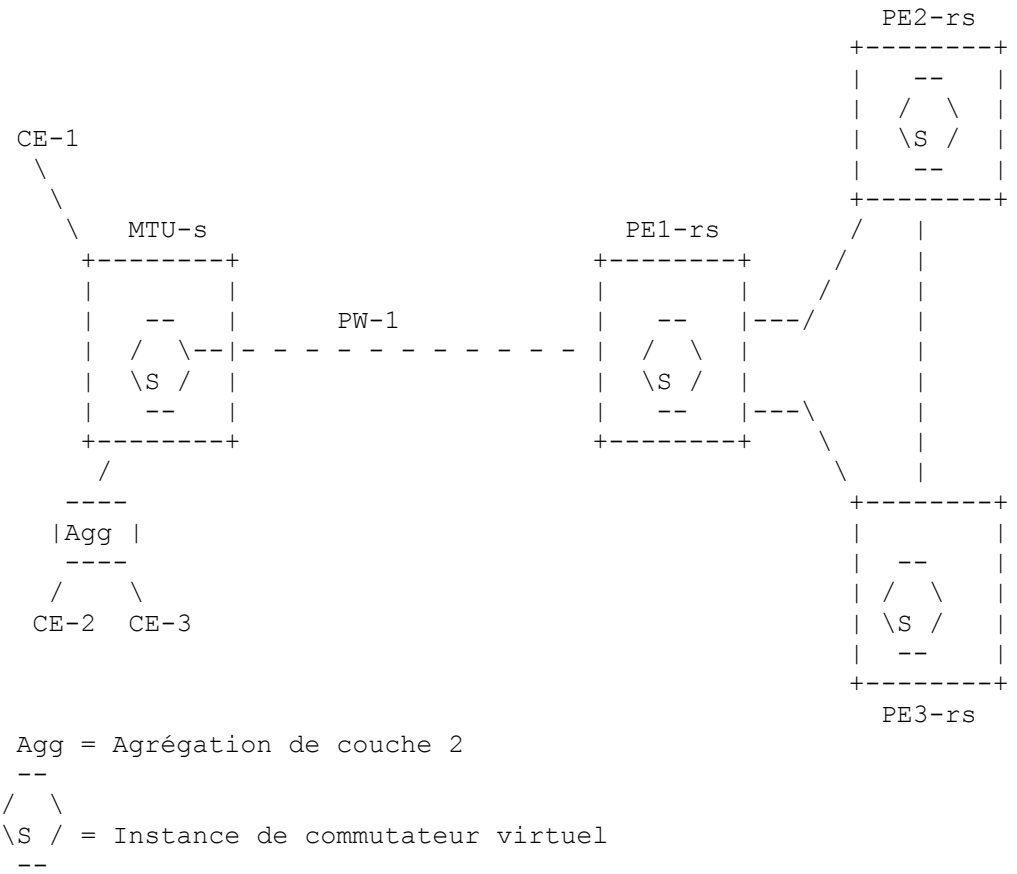


Figure 3 : Exemple de modèle de VPLS hiérarchique

Le MTU-s et le PE-rs traitent chaque connexion rayon comme un AC du service VPLS. L'étiquette de PW est utilisée pour associer le trafic provenant du rayon à une instance de VPLS.

10.1.1.1 Fonctionnement de MTU-s

Un MTU-s est défini comme un appareil qui prend en charge la fonction de commutation de couche 2 et assure les fonctions normales de pontage d'apprentissage et de duplication sur tous ses accès, incluant le rayon, qui est traité comme un accès virtuel. Les paquets pour des destinations inconnues sont dupliqués à tous les accès dans le service incluant le rayon. Une fois que l'adresse MAC est apprise, le trafic entre CE1 et CE2 va être commuté localement par le MTU-s, économisant la capacité du rayon au PE-rs. De façon similaire le trafic entre CE1 ou CE2 et toute destination distante est commuté directement sur le rayon et envoyé au PE-rs sur le PW en point à point.

Comme le MTU-s est capable de pontage, un seul PW est nécessaire par instance de VPLS pour tout nombre de connexions d'accès dans le même service VPLS. Cela réduit encore la charge de signalisation entre le MTU-s et le PE-rs.

Si le MTU-s est directement connecté au PE-rs, les autres techniques d'encapsulation, comme Q dans Q, peuvent être utilisées pour le rayon.

10.1.1.2 Fonctionnement des PE-rs

Un PE-rs est un appareil qui prend en charge toutes les fonctions de pontage pour le service VPLS et prend en charge l'acheminement et l'encapsulation MPLS ; c'est-à-dire, il prend en charge toutes les fonctions décrites pour un VPLS de base, comme décrit ci-dessus.

Le fonctionnement du PE-rs est indépendant du type de l'appareil à l'autre extrémité du rayon. Donc, le rayon provenant du MTU-s est traité comme un accès virtuel, et le PE-rs va commuter le trafic entre le PW rayon, les PW pivots, et les AC une fois qu'il a appris les adresses MAC.

10.1.2 Avantages de la connexité de rayons

La connexité des rayons offre plusieurs avantages d'adaptabilité et de fonctionnement pour créer des mises en œuvre de VPLS à grande échelle, tout en conservant la capacité d'offrir toutes les fonctionnalités du service VPLS :

- Elle élimine le besoin d'un maillage complet des tunnels et des PW par service entre tous les appareils qui participent au service VPLS.
- Elle minimise les frais généraux de signalisation, car moins de PW sont exigés pour le service VPLS.
- La découverte des nœuds de segments VPLS. Le MTU-s doit connaître seulement le nœud PE-rs, bien qu'il participe au service VPLS qui s'étend sur plusieurs appareils. Par ailleurs, chaque PE-rs VPLS doit connaître tous les autres PE-rs VPLS et tous ses appareils MTU-s et PE-r connectés localement.
- L'ajout d'autres sites exige la configuration du nouveau MTU-s mais n'exige pas de provisionnement des appareils MTU-s existants sur ce service.
- Des connexions hiérarchiques peuvent être utilisées pour créer un service VPLS qui s'étend sur plusieurs domaines de fournisseurs de services. Ceci est expliqué dans un paragraphe suivant.

Noter que lorsque plus d'appareils participent au VPLS, il y a plus d'appareils qui exigent la capacité d'apprentissage et de duplication.

10.1.3 Connexité de rayons pour appareils non pontants

Dans certains cas, un PE-rs pontant ne peut pas être déployé, ou un PE-r peut avoir déjà été déployé. Dans ce paragraphe, on explique comment un PE-r qui ne prend pas en charge la fonction de pontage de VPLS peut participer au service VPLS.

Dans la Figure 4, trois sites de consommateur sont connectés à travers CE-1, CE-2, et CE-3 au VPLS par PE-r. Pour chaque circuit de rattachement qui participe au service VPLS, PE-r crée un PW point à point qui se termine sur le VSI de PE1-rs.

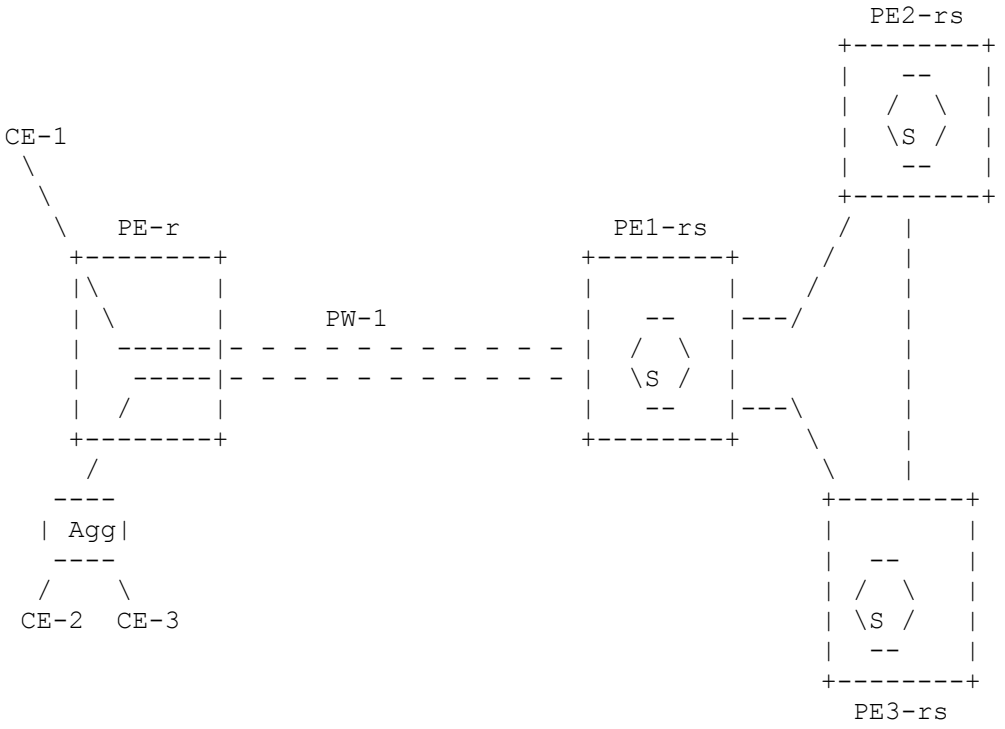


Figure 4 : Exemple de VPLS hiérarchique avec rayons non pontants

Le PE-r est défini comme un appareil qui prend en charge l'acheminement mais ne prend pas en charge de fonction de pontage. Cependant, il est capable d'établir des PW entre lui-même et le PE-rs. Pour chaque accès pris en charge dans le service VPLS, un PW est établi du PE-r au PE-rs. Une fois les PW établis, il n'y a plus de fonction d'apprentissage ou de duplication exigée de la part du PE-r. Tout le trafic reçu sur un des AC est transmis sur le PW. De même, tout le trafic reçu sur un PW est transmis à l'AC où le PW se termine. Donc, le trafic provenant de CE1 destiné à CE2 est commuté à PE1-rs et non à PE-r.

Noter que dans le cas où les appareils PE-r utilisent les VLAN de fournisseur (P-VLAN, *Provider VLAN*) comme des

démultiplexeurs au lieu des PW, PE1-rs peut les traiter comme tels et transposer ces "circuits" dans un domaine VPLS pour fournir une prise en charge du pontage entre eux.

Cette approche ajoute plus de frais généraux que celle des rayons capables de pontage (MTU-s) car un PW est nécessaire pour chaque AC qui participe au service contre un seul PW requis par service (sans considération des AC) quand un MTU-s est utilisé. Cependant, cette approche offre l'avantage de la fourniture d'un service VPLS en conjonction avec un service Internet acheminé sans exiger l'ajout d'un nouvel MTU-s.

10.2 Connexions de rayons redondantes

Une faiblesse évidente de l'approche du pivot et des rayons décrite jusqu'ici est que le MTU-s a une seule connexion au PE-rs. En cas de défaillance de la connexion ou du PE-rs, le MTU-s subit une perte totale de connexité.

Dans ce paragraphe, on décrit comment des connexions redondantes peuvent être fournies pour éviter une perte totale de connexité de la part du MTU-s. Le mécanisme décrit est identique pour les deux appareils, MTU-s et PE-r.

10.2.1 MTU-s à double rattachement

Pour protéger contre la défaillance de connexion du PW ou de la défaillance du PE-rs, le MTU-s ou le PE-r est à double rattachements dans deux appareils PE-rs. Les appareils PE-rs doivent faire partie de la même instance de service VPLS.

Dans la Figure 5, deux sites de consommateur sont connectés à travers CE-1 et CE-2 à un MTU-s. Le MTU-s établit deux PW (un pour chaque PE1-rs et PE3-rs) pour chaque instance de VPLS. Un des deux PW est désigné comme principal et est celui qui est activement utilisé dans les conditions normales, tandis que le second PW est désigné comme secondaire et reste en attente. Le MTU-s négocie les étiquettes de PW pour les deux PW principal et secondaire, mais n'utilise le PW secondaire qu'en cas de défaillance du PW principal. Comment un rayon est désigné comme principal ou secondaire sort du domaine d'application du présent document. Par exemple, une instance d'arborescence d'expansion fonctionnant seulement entre le MTU-s et les deux nœuds PE-rs est une méthode possible. Une autre méthode pourrait être la configuration.

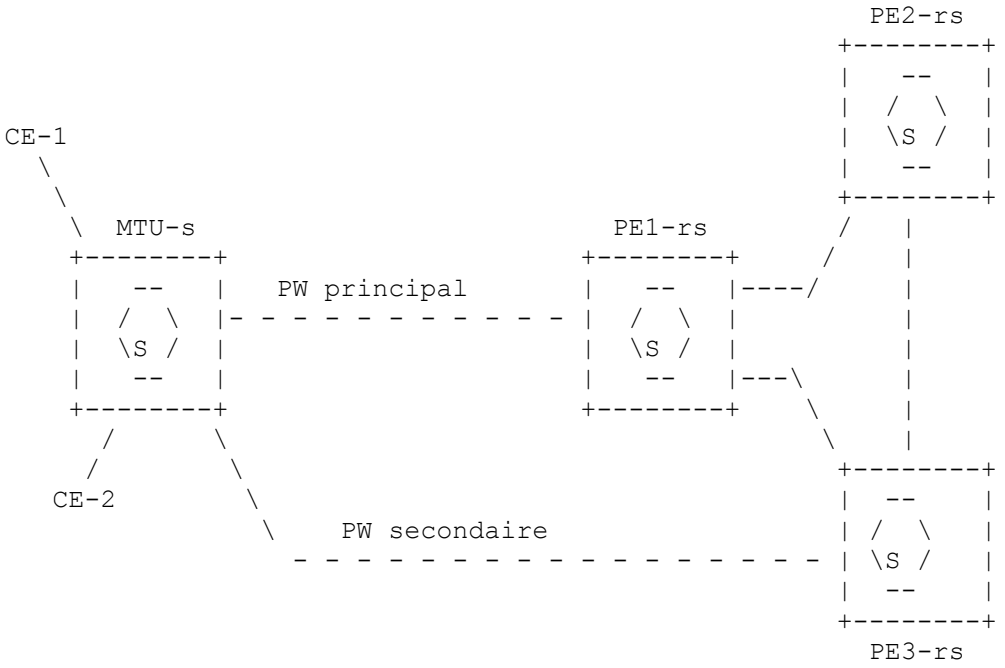


Figure 5 : Exemple d'un MTU-s à double rattachement

10.2.2 Détection de défaillance et récupération

Le MTU-s devrait contrôler l'usage des rayons pour les appareils PE-rs. Si les rayons sont des PW, alors la signalisation LDP est utilisée pour négocier les étiquettes de PW, et les messages hello utilisés pour la session LDP pourraient être utilisés pour détecter la défaillance du PW principal. L'utilisation d'autres mécanismes qui pourraient fournir une détection

plus rapide des défaillances sort du domaine d'application du présent document.

En cas de défaillance du PW principal, le MTU-s commute immédiatement sur le PW secondaire. À ce point, le PE3-rs qui termine le PW secondaire commence à apprendre les adresses MAC sur le PW rayon. Tous les autres nœuds PE-rs dans le réseau pensent que CE-1 et CE-2 sont derrière PE1-rs et peuvent continuer d'envoyer du trafic à PE1-rs jusqu'à ce qu'ils apprennent que les appareils sont maintenant derrière PE3-rs. Le processus de désapprentissage peut prendre longtemps et peut affecter la connexité de protocoles de couche supérieure à partir de CE1 et CE2. Pour permettre une convergence plus rapide, le PE3-rs où le PW secondaire PW a été activé peut envoyer un message de purge (comme expliqué au paragraphe 6.2) en utilisant le TLV Liste MAC, comme défini à la Section 6, à tous les nœuds PE-rs. À réception du message, les nœuds PE-rs purgent les adresses MAC associées à cette instance de VPLS.

10.3 Service VPLS multi-domaines

Une hiérarchie peut aussi être utilisée pour créer un service VPLS à grande échelle au sein d'un seul domaine ou d'un service qui s'étend sur de multiples domaines sans exiger de connexité de maillage complet entre tous les appareils à capacité VPLS. Deux réseaux VPLS à maillage complet sont connectés ensemble en utilisant un seul tunnel LSP entre les appareils VPLS de "bordure". Un seul PW rayon par service VPLS est établi pour interconnecter les deux domaines.

Quand plus de deux domaines doivent être connectés, un maillage complet des rayons inter domaines est créé entre les PE de bordure. Les règles de transmission sur ce maillage sont identiques à celles définies à la Section 4.

Cela crée un modèle hiérarchique à trois niveaux qui consiste en une topologie de pivot et rayons entre les appareils MTU-s et PE-rs, une topologie de maillage complet entre les PE-rs, et un maillage complet des rayons inter domaines entre appareils PE-rs de bordure.

Le présent document ne spécifie pas comment peuvent être pris en charge les PE bordures redondants par domaine et par instance de VPLS.

11. Modèle VPLS hiérarchique utilisant un réseau d'accès Ethernet

Dans cette section, le modèle hiérarchique est étendu pour inclure un réseau d'accès Ethernet. Ce modèle conserve l'architecture hiérarchique exposée précédemment en ce qu'il développe la topologie de maillage complet parmi les appareils PE-rs ; cependant, aucune restriction n'est imposée à la topologie du réseau d'accès Ethernet (par exemple, la topologie entre les appareils MTU-s et PE-rs ne se restreint pas au pivot et aux rayons).

La motivation d'un réseau d'accès Ethernet est que les réseaux fondés sur Ethernet sont actuellement déployés par des fournisseurs de services pour offrir des services de VPLS à leurs consommateurs. Donc, il est important de fournir un mécanisme qui permette à ces réseaux d'intégrer un cœur IP ou MPLS pour fournir des services de VPLS adaptables.

Une approche du tunnelage du trafic Ethernet d'un consommateur via un réseau d'accès Ethernet est d'ajouter une étiquette de VLAN supplémentaire aux données du consommateur (qui peuvent être étiquetées ou non). L'étiquette supplémentaire est appelée VLAN de fournisseur (P-VLAN). À l'intérieur du réseau du fournisseur chaque P-VLAN désigne un consommateur ou plus précisément une instance de VPLS pour ce consommateur. Donc, il y a une correspondance biunivoque entre un P-VLAN et une instance de VPLS. Dans ce modèle, le MTU-s doit avoir la capacité d'ajouter l'étiquette P-VLAN supplémentaire aux AC non multiplexés lorsque les VLAN de consommateur ne sont pas utilisés comme des délimiteurs de service. Cette fonctionnalité est décrite dans [802.1ad].

Si les VLAN de consommateur ont besoin d'être traités comme des délimiteurs de service (par exemple, l'AC est un accès multiplexé) alors le MTU-s doit avoir la capacité supplémentaire de traduire un VLAN de consommateur (C-VLAN) en un P-VLAN, ou de pousser une étiquette de P-VLAN supplémentaire, afin de résoudre les étiquettes de VLAN en chevauchement utilisées par les différents consommateurs. Donc, le MTU-s dans ce modèle peut être considéré comme un pont normal avec cette capacité supplémentaire. Cette fonctionnalité est décrite dans [802.1ad].

Le PE-rs doit être capable d'effectuer la fonction de pontage sur les accès standard Ethernet envers le réseau d'accès, ainsi que sur les PW envers le cœur de réseau. Dans ce modèle, le PE-rs peut avoir besoin de faire fonctionner STP envers le réseau d'accès, en plus de l'horizon partagé sur le cœur MPLS. Le PE-rs doit transposer un P-VLAN en une instance de VPLS et ses PW associés, et vice versa.

Les détails concernant l'opération de pont pour le MTU-s et le PE-rs (par exemple, le format d'encapsulation pour les messages Q dans Q, le traitement du protocole de commande Ethernet du consommateur, etc.) sortent du domaine d'application du présent document et sont couverts par [802.1ad]. Cependant, la partie pertinente est l'interaction entre le module de pont et les PW MPLS/IP dans le PE-rs, qui se comporte juste comme un VPLS régulier.

11.1 Adaptabilité

Comme chaque P-VLAN correspond à une instance de VPLS, le nombre total d'instances de VPLS prises en charge est limité à 4k. Le P-VLAN sert de délimiteur de service local au sein du réseau du fournisseur et il est supprimé lorsque il est transposé en un PW dans une instance de VPLS. Donc, la limite de 4k s'applique seulement au sein d'un réseau d'accès Ethernet (îlot Ethernet) et non au réseau entier. Le réseau SP consiste en un réseau cœur MPLS/IP qui connecte de nombreux îlots Ethernet. Donc, le nombre d'instances de VPLS peut s'adapter en conséquence avec le nombre d'îlots Ethernet (une région métropolitaine peut être représentée par un ou plusieurs îlots).

11.2 Double rattachement et récupération de défaillance

Dans ce modèle, un MTU-s peut être à double rattachements sur différents appareils (agrégateurs et/ou appareils PE-rs). La protection contre la défaillance des nœuds et liaisons de réseau d'accès peut être fournie en utilisant STP dans chaque îlot. Le STP de chaque îlot est indépendant des autres îlots et n'interagit pas avec les autres. Si un îlot a plus d'un PE-rs, un maillage complet dédié de PW est utilisé parmi ces appareils PE-rs pour porter les paquets de BPDU de SP pour cet îlot. Sur la base du P-VLAN, STP va désigner un seul PE-rs à utiliser pour porter le trafic à travers le cœur. La protection contre les boucles à travers le cœur est effectuée en utilisant l'horizon partagé, et la protection contre les défaillances dans le cœur est effectuée par le réacheminement standard IP/MPLS.

12. Contributeurs

Loa Andersson, TLA ; Ron Haberman, Alcatel-Lucent ; Juha Heinanen, indépendant ; Giles Heron, Tellabs ; Sunil Khandekar, Alcatel-Lucent ; Luca Martini, Cisco ; Pascal Menezes, indépendant ; Rob Nath, Alcatel-Lucent ; Eric Puetz, AT&T ; Vasile Radoaca, indépendant ; Ali Sajassi, Cisco ; Yetik Serbest, AT&T ; Nick Slabakov, Juniper ; Andrew Smith, consultant ; Tom Soon, AT&T ; Nick Tingle, Alcatel-Lucent.

13. Remerciements

Nous tenons à remercier Joe Regan, Kireeti Kompella, Anoop Ghanwani, Joel Halpern, Bill Hong, Rick Wilder, Jim Guichard, Steve Phillips, Norm Finn, Matt Squire, Muneyoshi Suzuki, Waldemar Augustyn, Eric Rosen, Yakov Rekhter, Sasha Vainshtein, et Du Wenhua de leurs précieux retours.

Nous remercions aussi Rajiv Papneja (ISOCORE), Winston Liu (Ixia), et Charlie Hundall pour avoir identifié des problèmes dans le projet au cours des essaix d'interopérabilité.

Merci aussi à Ina Minei, Bob Thomas, Eric Gray et Dimitri Papadimitriou de leur relecture technique attentive du document.

14. Considérations sur la sécurité

Une description plus complète des questions de sécurité impliquées dans les L2VPN est couverte par la [RFC4111]. Un service VPLS non protégé est vulnérable à des problèmes de sécurité qui font peser des risques sur le consommateur et les réseaux de fournisseurs. La plupart des problèmes de sécurité peuvent être évités par la mise en œuvre de protections appropriées. Deux d'entre eux peuvent être empêchés par les protocoles existants.

- Aspects du plan des données
- L'isolement du trafic entre domaines de VPLS est garanti par l'utilisation de tableaux de FIB de couche 2 par VPLS et l'utilisation de PW par VPLS.
- Le trafic de consommateur, qui consiste en trames Ethernet, est porté inchangé sur le VPLS. Si la sécurité est requise, le

trafic de consommateur DEVRAIT être chiffré et/ou authentifié avant d'entrer dans le réseau du fournisseur de services.
- Empêcher la diffusion de tempêtes peut être réalisé en utilisant les routeurs comme appareils CPE ou en régulant la quantité de trafic de diffusion que les consommateurs peuvent envoyer.

- Aspects de plan de contrêle
- Les méthodes de sécurité de LDP (authentification) comme décrit dans la [RFC3036] DEVRAIENT être appliquées. Cela va empêcher que des messages non authentifiés perturbent un PE dans un VPLS.

- Attaques de déni de service
- Des moyens pour limiter le nombre d'adresses MAC (par site par VPLS) qu'un PE peut apprendre DEVRAIENT être mis en œuvre.

15. Considérations relatives à l'IANA

Le champ Type dans le TLV Liste MAC est défini comme 0x404 au paragraphe 6.2.1.

16. Références

16.1 Références normatives

[802.1D-ORIG] Original 802.1D - ISO/IEC 10038, ANSI/IEEE Std 802.1D-1993 "MAC Bridges".

[802.1D] Institute of Electrical and Electronics Engineers, "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 3: Media Access Control (MAC) Bridges: Revision. This is a revision of ISO/IEC 10038: 1993, 802.1j- 1992 and 802.6k-1992. It incorporates P802.11c, P802.1p and P802.12e. ISO/IEC 15802-3: 1998.", IEEE Standard 802.1D, juillet 1998.

[802.1Q] 802.1Q - ANSI/IEEE Draft Standard P802.1Q/D11, "IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks", juillet 1998.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC3036] L. Andersson et autres, "Spécification de LDP", janvier 2001. *(Obsolète, voir la* RFC5036)

[RFC4446] L. Martini, "Allocations de l'IANA pour l'émulation de bord à bord pseudo filaire (PWE3)", avril 2006. (BCP0116)

[RFC4447] L. Martini et autres, "Établissement et maintenance de pseudo filaires avec le protocole de distribution d'étiquettes", avril 2006. (*MàJ par la* RFC6723) *(P.S. ; Remplacé par* RFC8077 STD 84)

[RFC4448] L. Martini et autres, "Méthodes d'encapsulation pour le transport d'Ethernet sur des réseaux MPLS", avril 2006. *(P.S. ; MàJ par* RFC8469)

16.2 Références pour information

[802.1ad] "IEEE standard for Provider Bridges", Travail en cours, décembre 2002.

[RADIUS-DISC] Heinanen, J., Weber, G., Ed., Townsley, W., Booth, S., and W. Luo, "Using Radius for PE-Based VPN Discovery", Travail en cours, octobre 2005.

[RFC4111] L. Fang, éd., "Cadre de sécurité pour les réseaux privés virtuels approvisionnés par le fournisseur (PPVPN)", juillet 2005. *(Information)*

[RFC4364] E. Rosen et Y. Rekhter, "Réseaux privés virtuels IP BGP/MPLS", février 2006. (*P.S., MàJ par* RFC4577, RFC4684)

[RFC4664] L. Andersson et E. Rosen, éd., "Cadre pour les réseaux virtuels privés de couche 2 (L2VPN)", septembre 2006. *(Info.)*

[RFC4665] W. Augustyn et Y. Serbest, éditeurs, "Exigences de service pour la couche 2 des réseaux virtuels privés approvisionnés par le fournisseur", septembre 2006. *(Information)*

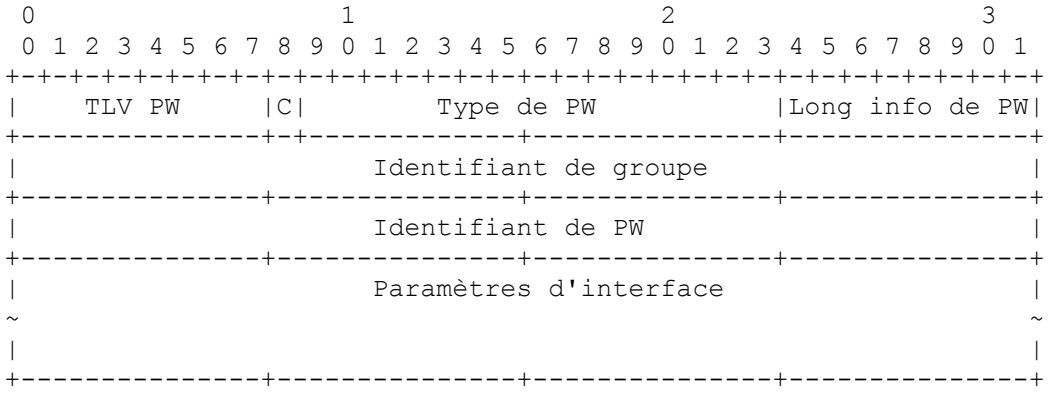
[RFC5195] H. Ould-Brahim et autres, "Auto découverte fondée sur BGP pour VPN de couche 1", juin 2008. *(P.S.)*

Appendice A. Signalisation de VPLS en utilisant l'élément de FEC PWid

Cette section a été conservée parce que des déploiements actifs utilisent cette version de la signalisation pour VPLS.

Les informations de signalisation de VPLS sont portées dans un message Transposition d'étiquette envoyé en mode non sollicité vers l'aval, qui contient le TLV FEC PWid suivant.

Les paramètres PW, C, Longueur d'informations de PW, Identifiant de groupe, et Interface sont définis dans la [RFC4447].



On utilise le type PW Ethernet pour identifier les PW qui portent du trafic Ethernet pour la connexité multipoints.

Dans un VPLS, on utilise un VCID (qui, quand on utilise la FEC PWid, a été remplacé par un identifiant plus général (AGI) pour traiter l'extension de la portée d'un VPLS) pour identifier un segment de LAN émulé. Noter que le VCID spécifié dans la [RFC4447] est un identifiant de service, qui identifie un service émulant un circuit virtuel point à point. Dans un VPLS, le VCID est un seul identifiant de service, de sorte qu'il a une signification globale à travers tous les PE impliqués dans l'instance de VPLS.

Adresse des auteurs

Marc Lasserre
Alcatel-Lucent
mèl : mlasserre@alcatel-lucent.com

Vach Kompella
Alcatel-Lucent
mèl : vach.kompella@alcatel-lucent.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est fourni par l'activité de soutien administratif (IASA) de l'IETF.