

Groupe de travail Réseau
Request for Comments : 4026
 Catégorie : Information
 Traduction Claude Brière de L'Isle

L. Andersson
 T. Madsen
 Acreo AB
 mars 2005

Terminologie des réseaux privés virtuels (VPN) approvisionnés par le fournisseur

Statut de ce mémoire

Le présent mémoire apporte des informations à la communauté de l'Internet. Il ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright

Copyright (C) The Internet Society (2005).

Résumé

L'intérêt largement répandu qui est porté aux solutions de réseau privé virtuel (VPN, *Virtual Private Network*) approvisionné par le fournisseur amène des articles qui proposent des solutions différentes et qui se recouvrent. Les groupes de travail de l'IETF (VPN approvisionnés par le fournisseur, VPN de couche 2, et VPN de couche 3) ont discuté ces propositions et les spécifications qui s'y réfèrent. Ceci a conduit au développement d'un ensemble partiellement nouveau de concepts utilisés pour décrire l'ensemble des services de VPN.

Dans une certaine mesure, plus d'un terme recouvre le même concept, et parfois le même terme recouvre plus d'un concept. Le présent document cherche à rendre plus claire et plus intuitive la terminologie dans ce domaine.

Table des Matières

1. Introduction.....	2
2. Terminologie des PPVPN.....	2
3. Services de réseau privé virtuel approvisionné par le fournisseur.....	2
3.1 VPN de couche 3 (L3VPN).....	3
3.2 VPN de couche 2 (L2VPN).....	3
3.3 Service de LAN privé virtuel (VPLS).....	3
3.4 Service de liaison privée virtuelle (VPWS).....	3
3.5 Service IP seul de type LAN (IPLS).....	3
3.6 Pseudo circuit (PW).....	3
3.7 Service de LAN transparent (TLS).....	4
3.8 LAN virtuel (VLAN).....	4
3.9 Service de liaison louée virtuelle (VLLS).....	4
3.10 Réseau privé virtuel (VPN).....	4
3.11 Réseau privé virtuel commuté (VPSN).....	4
4. Classification des VPN.....	4
5. Blocs de construction.....	5
5.1 Appareils d'extrémité client (CE).....	5
5.2 Extrémité fournisseur (PE).....	6
5.3 Cœur.....	7
5.4 Désignation dans des projets Internet spécifiques.....	7
6. Fonctions.....	8
6.1 Circuit de rattachement.....	8
6.2 Liaisons de service.....	8
6.3 Découverte de points d'extrémité.....	8
6.4 Arrosage.....	8
6.5 Apprentissage d'adresse MAC.....	8
6.6 Signalisation.....	9
7. "Boîtes".....	9
7.1 Boîtes d'agrégation.....	9
7.2 Équipement des locaux d'utilisateur (CPE).....	9
7.3 Unité multi utilisateurs (MTU).....	9
8. Réseau à commutation de paquets.....	9
8.1 Différenciateur de chemin.....	10
8.2 Réflecteur de chemin.....	10

8.3 Chemin cible (RT).....	10
8.4 Tunnel.....	10
8.5 Multiplexeur de tunnel.....	10
8.6 Canal virtuel (VC).....	10
8.7 Étiquette de VC.....	10
8.8 Étiquette interne.....	10
8.9 Tableau d'acheminement et transmission de VPN (VRF).....	11
8.10 Instance de VPN de transmission (VFI).....	11
8.11 Instance de commutateur virtuel (VSI).....	11
8.12 Routeur virtuel (VR).....	11
9. Considérations pour la sécurité.....	11
10. Remerciements.....	11
11. Références pour information.....	11
Adresse des auteurs.....	12
Déclaration des droits de reproduction.....	12

1. Introduction

Un nombre relativement important d'articles ont été soumis à l'ancien groupe de travail PPVPN, et aux groupes de travail L2VPN, L3VPN, et PWE3, qui traitent tous du même espace de problèmes, le réseautage de réseau privé virtuel assuré par le fournisseur aux utilisateurs finaux. Les mémoires traitent d'une large gamme de services, mais il y a aussi un grand nombre de points communs entre les solutions proposées.

Cela a conduit au développement d'un ensemble partiel de nouveaux concepts utilisés pour décrire cet ensemble de services de VPN. Dans une certaine mesure, plus d'un terme couvre le même concept, et parfois le même terme couvre plus d'un concept.

Le présent document propose une base pour une terminologie unifiée pour les groupes de travail L2VPN et L3VPN. Dans certains cas, les concepts parallèles au sein du groupe de travail PWE3 sont utilisés comme références.

2. Terminologie des PPVPN

Les concepts et termes de cette liste sont collectés à partir des projets Internet envoyés aux listes de diffusion de L2VPN et L3VPN (antérieurement, la liste de diffusion PPVPN) et des RFC relevant des groupes de travail L2VPN et L3VPN. L'accent est mis sur la terminologie et les concepts qui sont spécifiques du domaine PPVPN, mais cela n'est pas mis strictement en application ; par exemple, certains concepts et termes au sein des domaines PWE3 et MPLS (généralisé) sont en relation étroite. Nous avons essayé de trouver les utilisations les plus récentes des termes et concepts.

Le présent document est destiné à couvrir pleinement les concepts au sein des documents centraux des groupes de travail L2VPN et L3VPN ; c'est-à-dire, les [RFC3809], [RFC4031], [RFC4110], [RFC4664], et [RFC4665]. L'intention est de créer un ensemble complet et unifié de concepts pour ces documents et, par extension, pour le domaine PPVPN tout entier. Pour ce faire, il est aussi nécessaire de donner certains des développements par lesquels sont passés les concepts du domaine.

Le document est structuré en quatre sections majeures. La Section 4 fait la liste des différents services qui ont été ou seront spécifiés. La Section 5 fait la liste des blocs de construction qui sont utilisés pour spécifier ces services. La Section 6 fait la liste des fonctions nécessaires dans ces services. La Section 7 énumère certains appareils typiques utilisés dans les réseaux chez les utilisateurs et le fournisseur.

3. Services de réseau privé virtuel approvisionné par le fournisseur

Dans cette section, on définit la terminologie qui se rapporte à l'ensemble des services pour des solutions spécifiées par les groupes de travail L2VPN et L3VPN. Le concept de "pseudo circuit", qui relève du groupe de travail PWE3, est inclus pour des besoins de référence. Pour les exigences sur les VPN provisionnés par les fournisseurs, voir la [RFC4031].

Tous les termes et abréviations sont mentionnés ensemble avec une brève description du service. La liste est structurée de façon à donner d'abord les informations générales et ensuite les plus spécifiques. Les noms des services pour lesquels

L'IETF travaille à des solutions ont été placés au sommet de la liste. La terminologie plus ancienne et plus datée a été refoulée à la fin de la liste.

3.1 VPN de couche 3 (L3VPN)

Un L3VPN interconnecte des ensembles d'hôtes et routeurs sur la base des adresses de couche 3; voir la [RFC4110].

3.2 VPN de couche 2 (L2VPN)

Trois types de L2VPN sont décrits dans le présent document : le service de liaison privée virtuelle (VPWS, *Virtual Private Wire Service*) (paragraphe 3.4) le service de LAN privé virtuel (VPLS, *Virtual Private LAN Service*) (paragraphe 3.3) et le service IP seul de type LAN (IPLS, *IP-only LAN-like Service*) (paragraphe 3.5).

3.3 Service de LAN privé virtuel (VPLS)

Un VPLS est un service de fournisseur qui émule toutes les fonctionnalités d'un réseau de zone locale (LAN, *Local Area Network*) traditionnel. Un VPLS rend possible l'interconnexion de plusieurs segments de LAN sur un réseau à commutation de paquets (PSN, *packet switched network*) et fait que les segments distants de LAN se comportent comme un seul LAN. Pour les premiers travaux sur la définition d'une solution et d'un protocole pour un VPLS, voir les [RFC4665] et [RFC4762].

Dans un VPLS, le réseau fournisseur émule un pont d'acquisition, et les décisions de transmission sont prises sur la base des adresses MAC ou des adresses MAC et des étiquettes de VLAN.

3.4 Service de liaison privée virtuelle (VPWS)

Un service de liaison privée virtuelle (VPWS, *Virtual Private Wire Service*) est un circuit en point à point (liaison) qui connecte deux appareils d'extrémité client (CE, *Customer Edge*). La liaison est établie logiquement à travers un réseau à commutation de paquets. La CE dans le réseau client est connectée à une extrémité fournisseur (PE, *Provider Edge*) dans le réseau fournisseur via un circuit de rattachement (voir le paragraphe 6.1) ; le circuit de rattachement est soit un circuit physique, soit un circuit logique.

Les PE dans le cœur de réseau sont connectés via un pseudo circuit (PW, *Pseudo Wire*).

Les appareils de CE peuvent être des routeurs, des ponts, des commutateurs, ou des hôtes. Dans certaines mises en œuvre, un ensemble de VPWS est utilisé pour créer un réseau L2VPN multi sites. Un exemple de solution de VPWS est décrit dans [PPVPN-L2VPN].

Un VPWS diffère d'un VPLS (paragraphe 3.3) en ce que le VPLS est en point à multipoint, tandis que le VPWS est en point à point. Voir la [RFC4664].

3.5 Service IP seul de type LAN (IPLS)

Un IPLS est très semblable à un VPLS (voir le paragraphe 3.3), sauf que

- o on suppose que les appareils de CE (voir au paragraphe 5.1) sont des hôtes ou des routeurs, pas des commutateurs,
- o on suppose que le service aura seulement à porter des paquets IP, et à prendre en charge des paquets comme ICMP et ARP (autrement les paquets de couche 2 qui ne contiennent pas IP ne sont pas acceptés) et
- o l'hypothèse que seuls des paquets IP sont portés par le service s'applique également aux paquets IPv4 et IPv6.

Bien que ce service soit un sous ensemble fonctionnel du service de VPLS, il est considéré séparément parce que on peut le produire en utilisant des mécanismes différents, qui peuvent lui permettre de fonctionner sur certaines plateformes de matériel qui ne peuvent pas prendre en charge la pleine fonctionnalité de VPLS [RFC4664].

3.6 Pseudo circuit (PW)

Le groupe de travail PWE3 au sein de l'IETF spécifie la technologie de pseudo circuit. Un pseudo circuit est une émulation de connexion point à point sur un réseau à connexion de paquets qui permet l'interconnexion de deux nœuds avec toute technologie de couche 2. Le PW partage certains des blocs de construction et des constructions architecturales des solutions de point à multipoint ; pour un exemple de PE (voir au paragraphe 5.2) et de CE (voir au paragraphe 5.1). Une première

solution pour les PW est décrite dans la [RFC4906]. Le format d'encapsulation déjà utilisé dans les VPWS, les VPLS, et les PW est décrit dans la [RFC4905]. Les exigences pour les PW se trouvent dans la [RFC3916], et la [RFC3985] présente un cadre architectural pour les PW.

3.7 Service de LAN transparent (TLS)

TLS a été le premier nom utilisé pour décrire le service VPLS. TLS a été remplacé par VPLS, qui est le terme actuel.

3.8 LAN virtuel (VLAN)

Le terme de VLAN a été spécifié par la norme IEEE 802.1Q ; il définit une méthode de différenciation du trafic sur un LAN en étiquetant les trames Ethernet. Par extension, VLAN est utilisé pour désigner le trafic séparé par étiquetage de la trame Ethernet ou des mécanismes similaires.

3.9 Service de liaison louée virtuelle (VLLS)

Le terme VLLS a été remplacé par celui de VPWS. VLLS était utilisé dans un document maintenant périmé destiné à créer des métriques par lesquelles il aurait été possible de comparer différentes solutions de L2VPN. Ce document est maintenant arrivé à expiration, et il a été mis fin à ce travail.

3.10 Réseau privé virtuel (VPN)

VPN est un terme générique qui couvre l'utilisation de réseaux publics ou privés pour créer des groupes d'utilisateurs qui sont séparés des autres utilisateurs du réseau et qui peuvent communiquer entre eux comme si ils étaient sur un réseau privé. Il est possible d'améliorer le niveau de séparation (par exemple, par le chiffrement de bout en bout) mais ceci sort du domaine du mandat du groupe de travail VPN de l'IETF. Cette définition de VPN est tirée de la [RFC2764].

Dans la [RFC4110], le terme VPN est utilisé pour se référer à un ensemble spécifique de sites comme un intranet ou un extranet qui ont été configurés de façon à permettre la communication. Noter qu'un site est un membre d'au moins un VPN et peut être membre de plusieurs.

Dans le présent document, "VPN" est aussi utilisé comme nom générique pour tous les services mentionnés à la Section 3.

3.11 Réseau privé virtuel commuté (VPSN)

Le terme de VPSN a été remplacé par celui de VPLS. Les exigences ont été fusionnées dans celles de L3VPN [RFC4031] et de L2VPN [RFC4665].

4. Classification des VPN

La terminologie utilisée dans la [RFC3809] est définie sur la base de la figure ci-dessous.

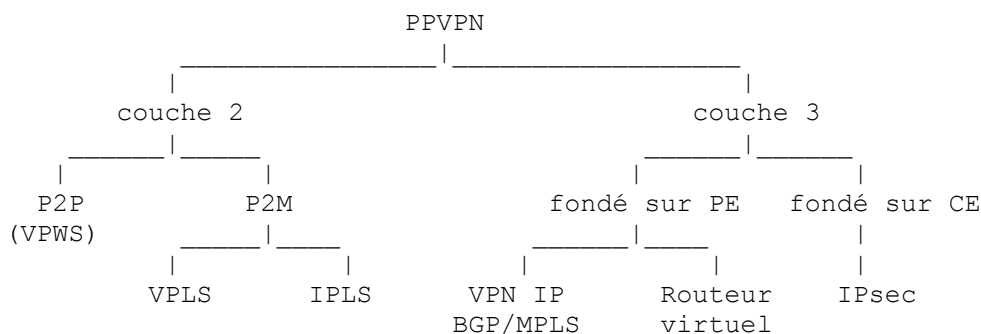


Figure 1

La figure ci-dessus présente une taxonomie des technologies de PPVPN. Certaines des définitions sont données ci-dessous:

VPN fondés sur CE : approche de VPN dans laquelle le réseau du fournisseur de service partagé n'a aucune connaissance du VPN client. Ces informations sont limitées à l'équipement de CE. Toutes les procédures spécifiques de VPN sont effectuées dans les appareils de CE, et les appareils de PE ne sont en aucune façon informés que le trafic qu'ils traitent est du trafic de VPN (voir aussi la [RFC4110]).

VPN fondés sur PE : approche de VPN de couche 3 dans laquelle un réseau de fournisseur de service est utilisé pour interconnecter les sites clients en utilisant des ressources partagées. Précisément, l'appareil de PE conserve l'état de VPN, en isolant les utilisateurs d'un VPN des utilisateurs des autres. Comme l'appareil de PE conserve tous les états de VPN requis, l'appareil de CE peut se comporter comme si il était connecté à un réseau privé. Précisément, le CE dans un VPN fondé sur PE ne doit pas exiger de changement ou d'ajout de fonctionnalités pour être connecté à un PPVPN qu'exigé pour un réseau privé. Les appareils de PE savent que certain trafic est du trafic de VPN. Ils transmettent le trafic (à travers des tunnels) sur la base de l'adresse IP de destination du paquet, et facultativement sur la base d'autres informations dans l'en-tête IP du paquet. Les appareils de PE sont eux-mêmes les points d'extrémité du tunnel. Les tunnels peuvent utiliser diverses encapsulations pour envoyer du trafic sur le réseau SP (comme, mais sans s'y restreindre, des tunnels GRE, IP dans IP, IPsec, ou MPLS) [RFC4110].

Style routeur virtuel (VR, *Virtual Router*) : approche de VPN fondé sur PE dans laquelle le routeur PE conserve un routeur logique complet pour chaque VPN qu'il prend en charge. Chaque routeur logique conserve un tableau de transmission unique et exécute une instance unique des protocoles d'acheminement. Ces VPN sont décrits dans [L3VPN-VR].

VPN IP BGP/MPLS : approche de VPN fondé sur PE dans laquelle le routeur PE conserve un environnement de transmission séparé et un tableau de transmission séparé pour chaque VPN. Afin de conserver plusieurs instances de tableau de transmission tout en ne faisant fonctionner qu'une seule instance de BGP, les VPN IP BGP/MPLS marquent les annonces de chemin avec des attributs qui identifient leur contexte de VPN. Ces VPN se fondent sur l'approche décrite dans la [RFC4364].

Style RFC 2547 : le terme a été utilisé par L3VPN pour décrire les extensions des VPN définies dans la [RFC2547] pour information. Ce terme a été maintenant remplacé par le terme de VPN IP BGP/MPLS.

5. Blocs de construction

En commençant par les spécifications des L3VPN (par exemple, les spécifications des [RFC2547] et [RFC4364] et des routeurs virtuels [L3VPN-VR]), il a été développé une façon de décrire les blocs de construction et l'allocation des fonctions dans les solutions de VPN. Les blocs de construction sont souvent utilisés dans les conversations de tous les jours somme si ils étaient des boîtes physiques, communes pour tous les services.

Cependant, pour diverses raisons, ceci est un peu trop simpliste. Chacun des blocs de construction pourrait être mis en œuvre sur plus d'une boîte physique. Le caractère courant de l'utilisation de telles mises en œuvre sort du domaine d'application du présent document.

5.1 Appareils d'extrémité client (CE)

Un appareil d'extrémité client (CE, *client edge*) est le nom de l'appareil qui a les fonctionnalités nécessaires dans les locaux du client pour accéder aux services spécifiés par l'ancien groupe de travail PPVPN en relation avec les travaux effectués sur les L3VPN [RFC4110]. Le concept a été modifié ; par exemple, lorsque les L2VPN et les VPN fondés sur le CE ont été définis. Ceci est traité plus en détails dans les paragraphes de cette section.

Deux aspects différents ont été pris en considération pour nommer les appareils de CE. On pourrait commencer par le type d'appareil qui est utilisé pour mettre en œuvre le CE (voir au paragraphe 5.1.1). Il est aussi possible d'utiliser le service que fournit le CE par lequel le résultat sera un ensemble de "CE préfixés", (voir au paragraphe 5.1.2).

Il est de pratique courante d'utiliser "CE" pour indiquer une de ces boîtes, car c'est très souvent sans ambiguïté dans le contexte spécifique.

5.1.1 Dénomination de CE fondée sur l'appareil

5.1.1.1 Routeur d'extrémité client (CE-R, *Customer Edge Router*)

Un CE-R est un routeur dans le réseau du client qui fait l'interface du réseau du fournisseur. Il y a de nombreuses raisons d'utiliser un routeur dans le réseau du client ; par exemple, dans un L3VPN qui utilise un adressage IP privé, c'est le routeur

qui est capable de faire la transmission sur la base des adresses privées. Une autre raison d'exiger l'utilisation d'un CE-R sur le côté client est qu'on veut limiter le nombre d'adresses MAC à apprendre dans le réseau du fournisseur.

Un CE-R pourrait être utilisé pour accéder aux services de couche L2 et L3.

5.1.1.2 Commutateur d'extrémité client (CE-S, *Customer Edge Switch*)

Un CE-S est un commutateur à capacité de service de couche L2 dans le réseau du client qui assure l'interface avec le réseau du fournisseur. Dans un VPWS ou un VPLS, il n'est pas strictement nécessaire d'utiliser un routeur dans le réseau client ; un commutateur de couche 2 peut très bien faire le travail.

5.1.2 Dénomination de CE fondée sur le service

La liste ci-dessous contient des exemples de la façon dont différentes fonctionnalités ont été utilisées pour désigner les CE. Il y a de nombreux exemples de ce type de désignation, et on traitera seulement les noms fonctionnels les plus fréquemment utilisés. Comme ce sont des noms fonctionnels, il est tout à fait possible que sur un même équipement il y ait des plateformes pour plus d'un type de fonction. Par exemple, un routeur peut au même moment être à la fois un L2VPN-CE et un L3VPN-CE. Il se peut aussi que les fonctions nécessaires pour un L2VPN-CE ou un L3VPN-CE soient réparties sur plus d'une plateforme.

5.1.2.1 L3VPN-CE

Un L3VPN-CE est l'appareil ou ensemble d'appareils dans les locaux d'utilisateur qui se rattache au L3VPN fourni par l'opérateur, une mise en œuvre 2547bis.

5.1.2.2 VPLS-CE

Un VPLS-CE est l'appareil ou ensemble d'appareils dans les locaux d'utilisateur qui se rattachent à un VPLS fourni par l'opérateur.

5.1.2.3 VPWS-CE

Un VPWS-CE est l'appareil ou ensemble d'appareils dans les locaux d'utilisateur qui se rattachent au VPWS fourni par l'opérateur.

5.2 Extrémité fournisseur (PE)

PE (*Provider Edge*) est le nom de l'appareil ou ensemble d'appareils à la bordure du réseau du fournisseur qui a la fonctionnalité nécessaire pour assurer l'interface avec le consommateur. Sans autre qualification, PE est très souvent utilisé pour désigner les appareils car cela est sans ambiguïté dans le contexte.

Trois aspects doivent être pris en considération pour la désignation des PE : le service pris en charge, si la fonctionnalité nécessaire pour le service est répartie entre plusieurs appareils, et le type d'appareil qui l'incorpore.

5.2.1 Dénomination de PE fondée sur l'appareil

Les routeurs et les commutateurs peuvent être utilisés pour mettre en œuvre les PE ; cependant, les propriétés d'adaptabilité seront différentes selon le type d'équipement choisi.

5.2.1.1 Routeur d'extrémité fournisseur (PE-Rr)

Un PE-R (*Provider Edge Route*) est un appareil de couche L3 qui participe à l'acheminement sur le réseau à commutation par paquets (PSN, voir la Section 8) et transmet les paquets sur la base des informations d'acheminement.

5.2.1.2 Commutateur d'extrémité fournisseur (PE-S)

Un PE-S (*Provider Edge Switch*) est un appareil de couche L2 qui participe par exemple à un Ethernet commuté en prenant des décisions de transmission de paquets sur la base des informations d'adresse de couche L2.

5.2.2 Dénomination de PE fondée sur le service

5.2.2.1 L3VPN-PE

Un L3VPN-PE est un appareil ou ensemble d'appareils à la bordure du réseau du fournisseur qui fait l'interface avec le réseau du client, avec les fonctionnalités nécessaires pour un L3VPN.

5.2.2.2 VPWS-PE

Un VPWS-PE est un appareil ou ensemble d'appareils à la bordure du réseau du fournisseur qui fait l'interface avec le réseau du client, avec les fonctionnalités nécessaires pour un VPWS.

5.2.2.3 VPLS-PE

Un VPLS-PE est un appareil ou ensemble d'appareils à la bordure du réseau du fournisseur qui fait l'interface avec le réseau du client, avec les fonctionnalités nécessaires pour un VPLS.

5.2.3 Dénomination de PE fondée sur la répartition

Pour des raisons d'adaptabilité, dans les cas de VPLS/VPWS il est parfois désiré de répartir les fonctions dans le VPLS/VPWS-PE à travers plus d'un appareil. Par exemple, il est faisable d'allouer l'apprentissage d'adresse MAC sur un appareils relativement petit et peu coûteux proche du site du client, tout en participant à la signalisation du PSN et l'établissement des tunnels de PE à PE est fait par des routeurs plus proches du cœur de réseau.

Lors de la distribution des fonctionnalités entre les appareils, un protocole est nécessaire pour échanger les informations entre le PE face au réseau (N-PE, *Network facing PE*) (voir au paragraphe 5.2.3.1) et le PE face à l'utilisateur (U-PE, *User facing PE*) (voir au paragraphe 5.2.3.2).

5.2.3.1 PE face au réseau (N-PEE)

Le N-PE est l'appareil auquel les fonctions de signalisation et de contrôle sont allouées lorsque un VPLS-PE est distribué à travers plus d'une boîte.

5.2.3.2 PE face à l'utilisateur (U-PE)

L'U-PE est l'appareil auquel les fonctions nécessaires pour prendre les décisions de transmission ou de commutation à l'entrée du réseau fournisseur.

5.3 Cœur

5.3.1 Routeur fournisseur (P, *Provider Router*)

Le P est défini comme un routeur dans le réseau cœur qui n'a pas d'interface directe avec un client. Donc un routeur P n'a pas besoin de conserver l'état de VPN et n'est pas au courant du VPN.

5.4 Désignation dans des projets Internet spécifiques

5.4.1 PE de couche 2 (L2PE)

L2PE est le nom conjoint des appareils dans le réseau fournisseur qui mettent en œuvre les fonctions de couche L2 nécessaires pour un VPLS ou un VPWS.

5.4.2 PE logique (LPE)

Le terme de PE logique (*LPE Logical PE*) a son origine dans un projet Internet périmé, "VPN L2 VPLS/LPE : Services de LAN virtuel privé utilisant l'architecture de PE logique", et a été utilisé pour décrire un ensemble d'appareils servant dans un réseau fournisseur à mettre en œuvre un VPLS. Dans un LPE, les fonctions de VPLS sont distribuées entre de petits appareils (PE d'extrémités/U-PE) et des appareils rattachés à un cœur de réseau (PE-Cœur/N-PE). Dans une solution LPE, le PE d'extrémité et le PE-Cœur peuvent être interconnectés par un réseau de transport Ethernet commuté ou des liaisons montantes. Le LPE va apparaître au réseau cœur comme un seul PE. Dans le présent document, les appareils qui constituent

le LPE sont appelés N-PE et U-PE.

5.4.3 PE-CLE

Un autre nom pour le U-PE suggéré dans le projet Internet périmé, "Architectures VPLS".

5.4.4 PE-Cœur

Voir les origines et l'utilisation de ce concept au paragraphe 5.4.2.

5.4.5 PE d'extrémité

Voir les origines et l'utilisation de ce concept au paragraphe 5.4.2.

5.4.6 PE-POP

Un autre nom pour le U-PE suggéré dans le projet Internet périmé, "Architectures VPLS".

5.4.7 VPLS d'extrémité (VE)

Le terme VE (*VPLS Edge*) a son origine dans un projet Internet périmé sur un service de LAN transparent réparti et a été utilisé pour décrire l'appareil utilisé par un réseau fournisseur pour relayer un VPLS à un client. Dans le présent document, le VE est appelé un VPLS-PE. Ce nom est périmé.

6. Fonctions

Dans cette section, on a groupé un certain nombre de concepts et termes qui ont à être effectués pour faire fonctionner les services de VPN.

6.1 Circuit de rattachement

Dans un VPN de couche 2, le CE est rattaché au PE via un circuit de rattachement (AC, *Attachment Circuit*). Le AC peut être une liaison physique ou logique.

6.2 Liaisons de service

Les liaisons de service (*Backdoor Links*) sont des liaisons entre des appareils de CE qui sont fournies par le consommateur d'extrémité plutôt que par le fournisseur de service ; elles peuvent être utilisées pour interconnecter les appareils de CE dans des arrangements de multi rattachements [RFC4110].

6.3 Découverte de points d'extrémité

La découverte des point d'extrémité est le processus par lequel les appareils qui sont capables d'un service de VPN spécifique vont trouver tous les clients qui font face à des accès qui appartiennent au même service.

Les exigences sur la découverte des points d'extrémité et la signalisation sont discutées dans la [RFC4031]. Cela a aussi été le sujet d'un projet Internet maintenant périmé rapportant l'activité d'une équipe de conception sur la découverte de VPN.

6.4 Arrosage

L'arrosage est une fonction qui se rapporte aux services de couche 2 ; lorsque un PE reçoit une trame avec une adresse MAC de destination inconnue, cette trame est envoyée (arrosée) à toutes les autres interface.

6.5 Apprentissage d'adresse MAC

L'apprentissage d'adresse MAC est une fonction qui se rapporte aux services de couche 2; lorsque un PE reçoit une trame avec une adresse MAC de source inconnue, les relations entre cette adresse MAC et l'interface est apprise pour les besoins

futurs de transmission. Dans une solution de VPN de couche 2 du groupe de travail L2VPN, cette fonction est allouée au VPLS-PE.

6.5.1 Apprentissage qualifié

Dans l'apprentissage qualifié, les décisions d'apprentissage au U-PE se fondent sur l'adresse MAC de la trame du client Ethernet et de l'étiquette de VLAN, si une étiquette de VLAN existe. Si il n'y en a pas, le VLAN par défaut est supposé.

6.5.2 Apprentissage non qualifié

Dans l'apprentissage non qualifié, l'apprentissage se fonde seulement sur l'adresse MAC de la trame du client Ethernet.

6.6 Signalisation

La signalisation est le processus par lequel les PE qui ont des VPN derrière eux échangent des informations pour établir des PW, des tunnels PSN, et des multiplexeurs de tunnel. Ce processus peut être automatisé par un protocole ou fait par configuration manuelle. Différents protocoles peuvent être utilisés pour établir les tunnels PSN et échanger les multiplexeurs de tunnels.

7. "Boîtes"

On énumère un ensemble de boîtes qui vont normalement être utilisées dans un environnement qui prend en charge différentes sortes de services de VPN. On a choisi d'inclure certains noms de boîtes dont l'origine est extérieure aux organisations qui spécifient le protocole.

7.1 Boîtes d'agrégation

La boîte d'agrégation est normalement un commutateur de couche L2 qui ignore le service et est seulement utilisé pour agréger le trafic sur des points plus riches en fonctions dans le réseau.

7.2 Équipement des locaux d'utilisateur (CPE)

L'équipement de CPE (*Customer Premises Equipment*) est la boîte qu'un fournisseur place chez le consommateur. Il sert deux objectifs : donner au consommateur les accès où se brancher et permettre au fournisseur de surveiller la connectivité du site consommateur. Le CPE est normalement une boîte de faible coût qui a des fonctions limitées et, dans la plupart des cas, ignore les services de VPN offerts par le fournisseur de réseau. Le CPE n'est pas nécessairement l'équipement auquel les fonctions de CE sont allouées, mais fait partie du réseau du fournisseur et est utilisé à des fins de surveillance.

Le nom de CPE est principalement utilisé dans le fonctionnement du réseau et les contextes de développement et ne devrait pas être utilisé dans les spécifications de protocole.

7.3 Unité multi utilisateurs (MTU)

Une MTU (*Multi-Tenant Unit*) est normalement un commutateur de couche L2 placé par un fournisseur de service dans un bâtiment où sont situés plusieurs consommateurs de ce fournisseur de service. Le terme a été introduit dans un projet Internet qui spécifie une solution VPLS avec une fonction distribuée entre la MTU et l'extrémité fournisseur (PE, *Provider Edge*) dans le contexte de la [RFC4762].

Le nom d'appareil MTU est principalement utilisé dans le fonctionnement du réseau et les contextes de déploiement et ne devrait pas être utilisé dans les spécifications de protocole, car c'est aussi l'abréviation de unité maximum de transmission (MTU, *Maximum Transmission Unit*).

8. Réseau à commutation de paquets

Un réseau à commutation de paquets (PSN, *Packet Switched Network*) est le réseau au travers duquel sont établis les tunnels qui supportent les services de VPN.

8.1 Différenciateur de chemin

Un différenciateur de chemin (RD, *Route Distinguisher*) [RFC4364] est une valeur de 8 octets qui, en conjonction avec une adresse IPv4 de quatre octets identifie une famille d'adresse de VPN-IPv4. Si deux VPN utilisent le même préfixe d'adresse IPv4, les PE les traduisent en préfixes uniques d'adresses VPN-IPv4. Cela assure que si la même adresse est utilisée dans deux VPN différents, il est possible d'installer deux chemins complètement différents pour cette adresse, une pour chaque VPN.

8.2 Réflecteur de chemin

Un réflecteur de chemin est un élément de réseau appartenant à un fournisseur de service, qui est utilisé pour distribuer les chemins BGP aux routeurs à capacité BGP du fournisseur de service [RFC4110].

8.3 Chemin cible (RT)

Un attribut chemin cible (RT, *Route Target*) [RFC4364] peut être vu comme identifiant un ensemble de sites ou, plus précisément, un ensemble de tableaux d'acheminement et transmission de VPN (voir au paragraphe 8.9).

Associer un chemin cible particulier à un chemin permet que ce chemin soit placé dans tous les tableaux d'acheminement et transmission de VPN (VRF, *VPN routing and forwarding*) utilisés pour acheminer le trafic reçu des sites correspondants.

Un attribut Chemin cible est aussi un terme de la communauté BGP étendue utilisé dans les [RFC2547] et [RFC4761]. Une communauté Chemin cible est utilisée pour restreindre la distribution des informations de VPN à l'ensemble des VRF. Un chemin cible peut être perçu comme identifiant un ensemble de sites ou, plus précisément, un ensemble de VRF.

8.4 Tunnel

Un tunnel est la connexité à travers un PSN qui est utilisée pour envoyer du trafic à travers le réseau d'un PE à un autre. Le tunnel donne un moyen pour transporter les paquets d'un PE à l'autre. La séparation du trafic d'un consommateur de celui d'un autre est faite sur la base des multiplexeurs de tunnels (voir au paragraphe 8.5). Comment le tunnel est établi dépend des mécanismes de tunnelage fournis par le PSN ; par exemple, le tunnel peut se fonder sur l'en-tête IP, sur une étiquette MPLS, sur l'identifiant de session L2TP, ou sur le champ Key GRE.

8.5 Multiplexeur de tunnel

Un multiplexeur de tunnel est une entité qui est envoyée avec les paquets qui traversent le tunnel et rendent possible de décider à quelle instance d'un service appartient un paquet et de quel envoyeur il a été reçu. Dans [PPVPN-L2VPN], le multiplexeur de tunnel est formaté comme une étiquette MPLS.

8.6 Canal virtuel (VC)

Un canal virtuel (VC, *virtual channel*) est transporté dans un tunnel et identifié par son multiplexeur de tunnel. Un canal virtuel est identifié par un identifiant de canal virtuel (VCI, *Virtual Channel Identifier*). Dans le contexte PPVPN, un VCI est une étiquette de VC ou un multiplexeur de tunnel, et dans le cas Martini, il est égal au VCID.

8.7 Étiquette de VC

Dans un réseau IP à capacité MPLS, une étiquette de VC est une étiquette MPLS utilisée pour identifier le trafic au sein d'un tunnel qui appartient à un VPN particulier ; c'est-à-dire que l'étiquette de VC est le multiplexeur de tunnel dans les réseaux qui utilisent des étiquettes MPLS.

8.8 Étiquette interne

C'est un autre nom pour l'étiquette de VC (voir au paragraphe 8.6).

8.9 Tableau d'acheminement et transmission de VPN (VRF)

Dans les réseaux qui font fonctionner des VPN de la [RFC2547], les routeurs PE tiennent des tableaux d'acheminement et de transmission de VPN (VRF, *VPN routing and forwarding*). Un VRF est un tableau de transmission par site. Chaque site auquel est rattaché le routeur PE est associé à un de ces tableaux. Une adresse IP de destination du paquet particulier n'est recherchée dans un VRF particulier que si ce paquet est arrivé directement d'un site qui est associé à ce tableau.

8.10 Instance de VPN de transmission (VFI)

Une instance de VPN de transmission (VFI, *VPN Forwarding Instance*) est une entité logique qui réside dans un PE qui inclut la base d'informations des routeurs et la base des informations de transmission pour une instance de VPN [RFC4110].

8.11 Instance de commutateur virtuel (VSI)

Dans un contexte de couche 2, un VSI est une instance de commutation virtuelle qui dessert un seul VPLS [RFC4664]. Un VSI effectue des fonctions de pontage de LAN standard (c'est-à-dire, Ethernet). La transmission faite par un VSI se fonde sur les adresses MAC et les étiquettes de VLAN, et éventuellement sur d'autres informations pertinentes VPLS par VPLS. La VSI est allouée au VPLS-PE ou, dans le cas réparti, à l'U-PE.

8.12 Routeur virtuel (VR)

Un routeur virtuel (VR, *Virtual Router*) est une émulation d'un routeur physique fondée sur du logiciel et du matériel. Les routeurs virtuels ont des tableaux indépendants d'acheminement et transmission IP, et ils sont isolés les uns des autres ; voir [L3VPN-VR].

9. Considérations pour la sécurité

Ceci est un document de terminologie qui n'a pas en tant que tel d'implication directe sur la sécurité . Les considérations pour la sécurité seront spécifiques des documents de solutions, cadres et spécifications dont la terminologie est collectée et exposée dans le présent document.

10. Remerciements

Une grande partie du contenu du présent document se fonde sur les discussions au sein des équipes de conception de PPVPN pour "l'auto découverte" et "l2vpn".

Dave McDysan, Adrian Farrel et Thomas Narten ont révisé attentivement le présent document et fourni de nombreuses suggestions utiles.

Thomas Narten a converti une version presque finalisée du présent document en XML, après l'extraction trop pénible d'une version acceptable à partir de Word. Avri Doria a été d'un grand secours pour l'utilisation de XML.

11. Références pour information

[L3VPN-VR] Knight, P., Ould-Brahim, H. et B. Gleeson, "Network based IP VPN Architecture using Virtual Routers", Travail en cours, avril 2004.

[PPVPN-L2VPN] Kompella, K., "Layer 2 VPNs Over Tunnels", Travail en cours, juin 2002.

[RFC2547] E. Rosen, Y. Rekhter, "VPN BGP/MPLS", mars 1999. (*Obsolète, voir RFC4364*) (*Information*)

[RFC2764] B. Gleeson et autres, "Cadre pour les réseaux privés virtuels fondés sur IP", février 2000. (*Information*)

[RFC3809] A. Nagarajan, éd., "Exigences génériques pour les réseaux privés virtuels approvisionnés par le fournisseur (PPVPN)", juin 2004. (*Information*)

- [RFC3916] X. Xiao, D. McPherson et P. Pate, éd., "Exigences pour l'émulation bord à bord pseudo filaire (PWE3)", septembre 2004. (*Information*)
- [RFC3985] S. Bryant et autres, "Architecture d'émulation bord à bord pseudo-filaire (PWE3)", mars 2005. (*Information*)
- [RFC4031] M. Carugi et autres, "Exigences de service de couche 3 des réseaux privés virtuels approvisionnés par le fournisseur (PPVPN)", avril 2005. (*Information*)
- [RFC4110] R. Callon, M. Suzuki, "Cadre pour les réseaux privés virtuels approvisionnés par le fournisseur (PPVPN) de couche 3", 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. (*Information*)
- [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*)
- [RFC4761] K. Kompella et Y. Rekhter, éditeurs "Service de LAN privé virtuel (VPLS) utilisant BGP pour l'auto découverte et la signalisation", janvier 2007.
- [RFC4762] M. Lasserre et V. Kompella, éditeurs, "Service de LAN privé virtuel (VPLS) utilisant la signalisation du protocole de distribution d'étiquette (LDP)", janvier 2007
- [RFC4905] L. Martini et autres, "Méthodes d'encapsulation pour le transport de trames de couche 2 sur des réseaux MPLS", juin 2007. (*Historique*)
- [RFC4906] L. Martini et autres, "Transport de trames de couche 2 sur MPLS", juin 2007. (*Historique*)

Adresse des auteurs

Loa Anderson
Acreo AB
mél : loa@pi.se

Tove Madsen
Acreo AB
mél : tove.madsen@acreo.se

Déclaration des droits de reproduction

Copyright (C) The Internet Society (2005).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à www.rfc-editor.org, et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations qui y sont contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à, toute garantie que l'utilisation des informations ci encloses ne viole aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui

mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr> .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org .

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.