Groupe de travail Réseau
Request for Comments : 5251
Catégorie : Sur la voie de la normalisation
juillet 2008
Traduction Claude Brière de L'Isle

D. Fedyk, éditeur, Nortel
Y. Rekhter, éd., Juniper Networks
D. Papadimitriou, Alcatel-Lucent
R. Rabbat, Google
L. Berger, LabN

Mode de base de VPN de couche 1

Résumé
Le présent document décrit le mode de base des VPN de couche 1 (L1VPN, *Layer 1 VPN*). Le mode de base de VPN de couche 1 (L1VPN BM, *L1VPN Basic Mode*) est un VPN fondé sur l'accès. Dans le mode de base de VPN de couche 1, l'unité de base de service est un chemin de commutation d'étiquettes (LSP, *Label Switched Path*) entre une paire d'accès d'abonnés au sein d'une certaine topologie d'accès de VPN. Le présent document définit le modèle de fonctionnement en utilisant le mécanisme de provisionnement ou d'auto-découverte de VPN, et les extensions de signalisation pour le L1VPN BM.

Table des Matières

1. Introduction

Le présent document décrit le mode de base des VPN de couche 1 (L1VPN BM) qui est présenté dans la [RFC4847]. L'applicabilité des VPN de couche 1 est traitée dans la [RFC5253]. Dans le présent document, on considère un réseau de fournisseur de services de couche 1 consistant en appareils qui prennent en charge GMPLS (par exemple, des appareils capables de commutation Lambda (LSC, *Lambda Switch Capable*) des brasseurs optiques, des interconnexions de réseau optique synchrone/hiérarchie numérique synchrone (SONET/SDH) etc.). On divise ces appareils en P (fournisseur) et PE (côté fournisseur). Dans le contexte de ce document, on se réfère aux premiers juste par "P", et aux autres appareils juste par "PE". Les P sont connectés seulement aux appareils au sein du réseau du fournisseur. Les PE sont connectés aux autres appareils au sein du réseau (P ou PE) ainsi qu'aux appareils en dehors du réseau du fournisseur de services. On se réfère à ces autres appareils comme étant côté consommateur (CE, *Customer Edge*). Un exemple de CE serait un appareil à capacité GMPLS qui serait un routeur, une interconnexion SDH, ou un commutateur Ethernet.

La [RFC4208] définit la signalisation du CE au PE. Dans la [RFC4208], le terme de nœud cœur (CN, *Core Node*) correspond aux nœuds P et PE, et le terme de nœud bordure (EN, *Edge Node*) correspond aux nœuds CE. On définit de plus un "nœud cœur de bordure" qui correspond à un PE.

La Figure 1 illustre les composants dans un réseau L1VPN.

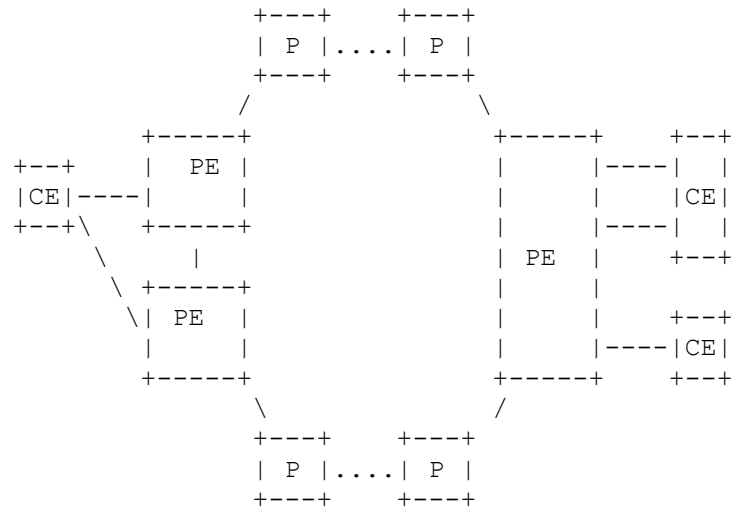


Figure 1 : Modèle de référence de VPN de couche 1 généralisé

Le présent document spécifie comment le service du modèle de base de L1VPN peut être réalisé en utilisant des mécanismes de provisionnement hors ligne ou d'auto-découverte de VPN, de signalisation de la commutation d'étiquettes multi protocoles généralisée (GMPLS, *Generalized Multi-Protocol Label Switching*) [RFC3471], [RFC3473], d'acheminement [RFC4202], et du protocole de gestion de liaisons (LMP, *Link Management Protocol*) [RFC4204].

L'auto-découverte de L1VPN a des exigences similaires à celle de la [RFC4847] pour l'auto-découverte de L3VPN. Comme avec les L3VPN, il y a des choix de protocole à faire avec l'auto-découverte. Le paragraphe 4.1.1 traite des informations qui ont besoin d'être découvertes.

L'acheminement et la signalisation GMPLS sont utilisées sans extension au sein du réseau du fournisseur de services pour établir et maintenir les connexions de LSC ou SONET/SDH (en multiplexage à répartition dans le temps (TDM, *Time Division Multiplexing*)) entre les nœuds du fournisseur de services. Cela suit le modèle de la [RFC4208].

Dans le mode de base de L1VPN, l'utilisation de LMP facilite le remplissage des tableaux d'informations d'accès du fournisseur de services. Bien sûr, LMP PEUT être utilisé comme option pour automatiser la découverte de liaison locale de CE à PE. LMP PEUT aussi renforcer l'acheminement (en mode amélioré) ainsi que les capacités de traitement de défaillances.

La prise en compte des L1VPN inter AS et inter fournisseurs exige des analyses complémentaires qui sortent du domaine d'application du présent document.

1.1 Conventions utilisées dans le présent document

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

Le présent document suppose le lecteur familiarisé avec la terminologie définie et utilisée dans les [RFC3471], [RFC3473], [RFC3477], [RFC3945], [RFC4201], [RFC4202], [RFC4204], [RFC4208], et les documents auxquels il est fait référence ici.

2. Service de VPN de couche 1

Les services de VPN de couche 1 sur les interfaces d'accès de consommateur et de fournisseur de services PEUVENT être toute interface de couche 1 prise en charge par GMPLS. Comme les mécanismes spécifiés dans ce document utilisent GMPLS comme mécanisme de signalisation, et comme GMPLS s'applique aux interfaces de SONET/SDH (TDM) et de LSC, il s'ensuit que les services de L1VPN incluent (mais n'y sont pas restreints) les équipements fondés sur LSC ou TDM. Noter que le présent document décrit les L1VPN de mode de base et à ce titre exigent que :

(1) GMPLS RSVP-TE soit utilisé pour la signalisation à la fois chez le fournisseur de services (entre les PE) et entre le consommateur et le fournisseur de services (entre CE et PE) ;

(2) l'acheminement GMPLS sur la liaison CE à PE sorte de la portée du mode de base de fonctionnement de L1VPN ; voir la [RFC4847].

Un CE est connecté à un PE via une ou plusieurs liaisons. Dans le contexte de ce document, une liaison est une construction de liaison d'ingénierie du trafic (TE, *Traffic Engineering*) GMPLS, comme définie dans la [RFC4202]. Dans le contexte de ce document, une liaison TE est une construction logique qui est membre d'un VPN, donc introduisant la notion de membre d'un ensemble de CE formant le VPN. Les interfaces à la fin de chaque liaison sont limitées à TDM ou LSC comme pris en charge par GMPLS. Plus précisément, une liaison <CE, PE> DOIT être du type <X, LSC> ou <Y, TDM> où X = PSC (Packet Switch Capable, *à capacité de commutation de paquets*), L2SC (Layer 2 Switch Capable, *à capacité de commutation de couche 2*) ou TDM et Y = PSC ou L2SC. Dans le cas où le LSP n'est pas terminé par le CE, X PEUT aussi être = LSC et Y = TDM. Une des applications d'une connexion L1VPN est de fournir un "lambda virtuel privé" ou similaire. Dans ce cas, le CE est vraiment le point d'extrémité en termes de GMPLS, et sa capacité de commutation sur la liaison TE n'est pas pertinente (bien que son identifiant de protocole généralisé (GPID, *Generalized Protocol Identifier*) DOIVE être signalé et identique aux deux CE, c'est-à-dire, CE d'extrémité de tête et de queue).

De même, les PEs pourraient être tout appareil de couche 1 qui est pris en charge par GMPLS (par exemple, des brasseurs optiques, ou SDH) alors que les CE PEUVENT être des appareils aux couches 1, 2, et 3, comme, respectivement, un brasseur SDH, un commutateur Ethernet, et un routeur).

Chaque liaison TE PEUT consister en un ou plusieurs canaux ou sous-canaux (par exemple, respectivement en longueur d'onde ou longueur d'onde et intervalle de temps,). Pour les besoins de cet exposé, tous les canaux dans une liaison donnée DOIVENT partager des caractéristiques similaires (par exemple, capacité de commutation, codage, type, etc.) et PEUVENT être choisis indépendamment du point de vue du CE. Les canaux sur des liaisons différentes d'un CE n'ont pas besoin d'avoir les mêmes caractéristiques.

Il PEUT y avoir plus d'une liaison TE entre une certaine paire de CE-PE. Un CE PEUT être connecté à plus d'un PE (avec au moins un accès par PE). Et à l'inverse, un PE PEUT avoir plus d'un CE provenant de différents VPN qui lui sont connectés.

Si un CE est connecté à un PE via plusieurs liaisons TE et si toutes les liaisons appartiennent au même VPN, ces liaisons (appelées des liaisons composantes) PEUVENT être traitées comme une seule liaison TE en utilisant la construction de faisceau de liaisons [RFC4201].

Afin de satisfaire aux exigences du mode de base L1VPN, il est EXIGÉ que pour une paire de CE-PE donnée au moins une des liaisons entre eux ait au moins un canal porteur de données, et au moins un canal porteur de contrôle, ou qu'il y ait l'accessibilité IP entre le CE et le PE qui pourrait être utilisée pour échanger les informations de contrôle.

Une liaison point à point a deux points d'extrémité : un sur le CE et un sur le PE. Le présent document se réfère au premier comme "l'accès CE", et au dernier comme "l'accès PE". De cela, il résulte qu'un CE est connecté à un PE via un ou plusieurs accès, où chaque accès PEUT consister en un ou plusieurs canaux ou sous-canaux (par exemple, respectivement de longueur d'onde ou de longueur d'onde et d'intervalle de temps) et tous les canaux dans un accès donné partagent des caractéristiques similaires et peuvent être interchangés du point de vue du CE. Comme pour la définition d'une liaison TE, dans le contexte de ce document, les accès sont des constructions logiques qui sont utilisées pour représenter un groupement de ressources physiques utilisées pour connecter un CE à un PE par L1VPN.

À tout moment, un certain accès sur un PE est associé à au plus un L1VPN, ou, pour être plus précis, à au plus un tableau d'informations d'accès tenu par le PE (bien que différents accès sur un PE donné pourraient être associés à différents L1VPN, ou, pour être plus précis, avec différents tableaux d'informations d'accès). L'association d'un accès à un VPN

PEUT être définie par provisionnement de la relation sur les appareils du fournisseur de services. En d'autres termes, le contexte d'une appartenance à un VPN en mode de base est appliqué sous le contrôle du fournisseur de services.

Il est EXIGÉ que l'interface (qui est entre le CE et le PE et qui est utilisée pour les besoins de la signalisation) soit capable d'initier/traiter les messages de protocole GMPLS [RFC3473] et de suivre les procédures décrites dans la [RFC4208].

Un important but de service de L1VPN est la capacité de prendre en charge ce qui est appelé un "provisionnement à une seule extrémité", où l'ajout d'un nouvel accès à un certain L1VPN n'implique de changement de configuration que sur le PE qui a cet accès. L'extension de ce modèle au CE sort du domaine d'application de L1VPN BM.

Un autre important but de service de L1VPN est la capacité d'établir/terminer un LSP entre une paire d'accès (existants) au sein d'in L1VPN à partir des appareils CE sans impliquer de changement de configuration dans un des appareils du fournisseur de services. En d'autres termes, la topologie de VPN est sous le contrôle de l'appareil CE (en supposant que la connexité PE à PE sous-jacente est fournie et permise par le réseau).

Les mécanismes expliqués dans le présent document visent à réaliser les buts ci-dessus. Précisément, au titre de l'offre du service de L1VPN, ces mécanismes (1) permettent au fournisseur de services de restreindre l'ensemble d'accès auxquels un accès donné pourrait être connecté et (2) permettent à un CE d'établir le LSP réel à un sous ensemble d'accès. Finalement, les mécanismes permettent que des topologies arbitraires de L1VPN soient prises en charge, incluant des topologies allant du réseau en étoile à des connexions point à point à maillage complet. Seules les liaisons en point à point sont prises en charge.

L'échange des informations d'acheminement de CE ou de topologie au fournisseur de services sort du domaine d'application du mode L1VPN BM.

3. Adressage, accès, liaisons, et canaux de contrôle

Les conventions établies par GMPLS pour l'adressage et la numérotation des liaisons sont discutées dans la [RFC3945]. Cette section s'appuie sur ces définitions pour le cas du L1VPN où on a maintenant des adresses de consommateur et de fournisseur de services dans le contexte d'une couche 1.

3.1 Domaine de fournisseur de service

Il est EXIGÉ qu'un fournisseur de services, ou un groupe de fournisseurs de service qui offrent collectivement un service de L1VPN, ait un seul domaine d'adressage qui s'étende sur tous les appareils PE impliqués dans la fourniture du service de L1VPN. Cela est nécessaire pour permettre aux mécanismes GMPLS d'établir et maintenir le chemin. On se réfère à ce domaine comme au domaine d'adressage du fournisseur de services. Il est de plus EXIGÉ que chaque consommateur de L1VPN ait son propre domaine d'adressage avec une complète liberté d'utiliser des adresses privées ou publiques. On se réfère à ces domaines comme à des domaines d'adressage de consommateur. Les domaines d'adressage de consommateur PEUVENT se chevaucher (c'est-à-dire, avec des adresses non uniques) les uns les autres, et PEUVENT aussi avoir des adresses qui se chevauchent avec le domaine du fournisseur de services.

3.2 Accès et indices de couche 1

Dans un L1VPN donné, chaque accès sur un CE qui connecte le CE à un PE a un identifiant qui est unique au sein de ce L1VPN (mais n'a pas besoin d'être unique sur plusieurs L1VPN). Une façon de construire un tel identifiant est d'allouer à chaque accès une adresse unique au sein d'un certain L1VPN, et d'utiliser cette adresse comme identifiant d'accès. Une autre façon de construire un tel identifiant est d'allouer à chaque accès d'un CE un indice unique au sein de ce CE, d'allouer à chaque CE une adresse unique au sein d'un L1VPN donné, et ensuite d'utiliser un couple <indice d'accès, adresse de CE> comme identifiant d'accès. Noter que l'accès et l'adresse de CE PEUVENT tous deux être une adresse de plusieurs formats. Cela inclut, mais n'est pas limité à, IPv4 et IPv6. Cet identifiant fait partie du domaine d'adressage de consommateur et est utilisé par l'appareil de CE pour identifier l'accès de CE et l'accès distant de CE pour la signalisation. Les CE ne connaissent pas ni ne comprennent les adresses du domaine de fournisseur de services.

Dans un réseau de fournisseur de services, chaque accès sur un PE qui connecte ce PE à un CE a un identifiant qui est unique dans ce réseau. Une façon de construire un tel identifiant est d'allouer à chaque accès d'un PE un indice unique au sein de ce PE, d'allouer à chaque PE une adresse IP unique dans le domaine d'adressage du fournisseur de services, et ensuite d'utiliser un couple <indice d'accès, adresse IPv4 de PE> ou <indice d'accès, adresse IPv6 de PE> comme

identifiant d'accès au sein du réseau de fournisseur de services. Une autre façon de construire un tel identifiant est d'allouer une adresse IPv4 ou IPv6 unique au sein du domaine d'adressage du fournisseur de services à chacun de ces accès. De toutes façons, cette adresse IPv4 ou IPv6 est interne au réseau de fournisseur de services et est utilisée pour la signalisation GMPLS au sein du réseau de fournisseur de services.

Par suite, chaque liaison qui connecte le CE au PE est associée à un accès de CE qui a un identifiant unique dans un certain L1VPN, et à un accès de PE qui a un identifiant unique au sein du réseau de fournisseur de services. On appelle le premier un identifiant d'accès de consommateur (CPI, *Customer Port Identifier*) et le dernier un identifiant d'accès de fournisseur (PPI, *Provider Port Identifier*).

3.3 Transposition d'accès et d'indice

Le présent document exige que chaque accès de PE qui a un PPI ait aussi un identifiant unique dans le domaine d'adressage de consommateur L1VPN du L1VPN associé à cet accès. Une façon de construire un tel identifiant est d'allouer à chaque accès une adresse unique au sein d'un certain domaine d'adressage de consommateur L1VPN, et d'utiliser cette adresse comme identifiant d'accès. Une autre façon de construire un tel identifiant est d'allouer à chaque accès un indice unique au sein d'un PE donné, d'allouer à chaque PE une adresse IP unique au sein d'un domaine d'adressage de consommateur L1VPN donné (mais qui n'a pas besoin d'être unique au sein du réseau de fournisseur de services) et ensuite d'utiliser un couple <indice d'accès, adresse IP de PE> qui agit comme un identifiant d'accès. On appelle un tel identifiant d'accès le VPN-PPI. Voir la Figure 2.

Pour les L1VPN, il est exigé que les opérations de fournisseur de services soient indépendantes du domaine d'adressage du consommateur de VPN et que le domaine d'adressage du fournisseur de services soit caché au consommateur. Pour réaliser cela, on définit deux identifiants au PE, un face au consommateur et l'autre face au fournisseur de services. L'adresse IP de PE utilisée pour le VPN-PPI est indépendante de l'adresse IP de PE utilisée pour le PPI (car les deux sont tirées de domaines d'adressage différents, le premier du domaine d'adressage du consommateur, et le second du domaine d'adressage d'un fournisseur de services de VPN). Si pour un accès donné sur un PE, les identifiants d'accès de PPI et le VPN-PPI ne sont pas numérotés, ils pourraient alors utiliser tous deux exactement le même indice d'accès. Ceci est une simple hypothèse parce que PPI et VPN_PPI peuvent être dans toute combinaison de formats valides.

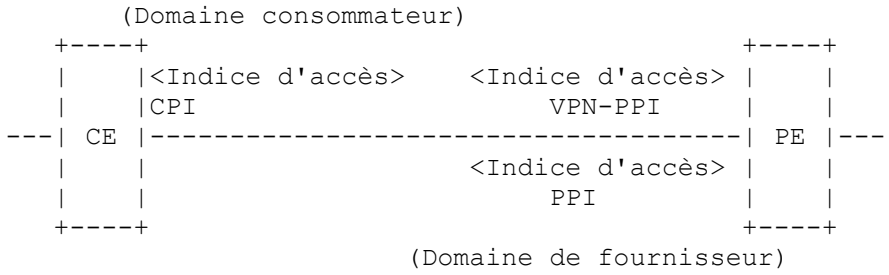


Figure 2 : Transposition d'accès/indice de consommateur/fournisseur

Noter, comme mentionné précédemment, que les adresses IP utilisée pour les CPI, PPI, et VPN-PPI pourraient être des adresses de format IPv4 ou IPv6.

Pour une liaison connectant un CE à un PE :

- Si le CPI est une adresse IPv4, alors le VPN-PPI DOIT être aussi une adresse IPv4 car les VPN-PPI sont créés à partir de l'espace d'adresse de consommateur. Si le CPI est un couple <indice d'accès, adresse IPv4 de CPI>, alors le VPN-PPI DOIT être un couple <indice d'accès, adresse IPv4 de PE> pour la même raison.

- Si le CPI est une adresse IPv6, alors le VPN-PPI DOIT aussi être une adresse IPv6 car les VPN-PPI sont créés à partir de l'espace d'adresse de consommateur. Si le CPI est un couple <indice d'accès, adresse IPv6 de CPI>, alors le VPN-PPI DOIT être un couple <indice d'accès, adresse IPv6 de PE> pour la même raison.

Note : pour un accès donné sur le PE, que le VPN-PPI de cet accès soit une adresse IP ou un <indice d'accès, adresse IP de PE> est indépendant du format du PPI de cet accès.

Le présent document suppose que l'allocation des PPI est contrôlée seulement par le fournisseur de services (sans aucune coordination avec les consommateurs du L1VPN) tandis que l'allocation des adresses utilisées par les CPI et les VPN-PPI

est contrôlée seulement par les administrateurs de L1VPN. Cela donne une souplesse maximale. L'administrateur de L1VPN est l'entité qui contrôle les spécificités du service de L1VPN pour les consommateurs du L1VPN. Cette fonction peut appartenir au fournisseur de services mais peut aussi être effectuée par un tiers qui a un accord avec le fournisseur de services. Et, bien sûr, chaque consommateur de L1VPN pourrait allouer de lui-même de telles adresses, sans aucune coordination avec d'autres L1VPN.

Le présent document exige aussi la connexité IP entre le CE et le PE, comme spécifié précédemment, qui est utilisée pour le canal de contrôle entre CE et PE. Cette connexité pourrait être soit un seul bond IP, qui pourrait être réalisé par une liaison dédiée ou par un VPN de couche 2, ou par un réseau privé IP, comme un L3VPN. La seule exigence pour cette connexité est une façon non ambiguë de corréler un canal de contrôle CE à PE particulier avec un L1VPN particulier. Quand un tel canal est réalisé par une liaison dédiée, une telle liaison devrait être associée à un L1VPN particulier. Quand un tel canal est réalisé par un L2VPN, un L2VPN distinct devrait être associé à un L1VPN. Quand un tel canal est réalisé par un L3VPN, un L3VPN distinct devrait être associé à un L1VPN.

On appelle l'adresse du CE de ce canal l'adresse de canal de contrôle de CE (CE-CC-Addr, *CE Control Channel Address*) et l'adresse du PE de ce canal l'adresse de canal de contrôle de PE (PE-CC-Addr, *PE Control Channel Address*). Il est EXIGÉ que CE-CC-Addr et PE-CC-Addr soient toutes deux uniques au sein du L1VPN auquel elles appartiennent, mais il n'est pas EXIGÉ qu'elles soient uniques sur plusieurs L1VPN. Les adresses de canal de contrôle ne sont pas partagées entre plusieurs VPN. L'allocation de CE-CC-Addr et PE-CC-Addr est contrôlée par les administrateurs du L1VPN.

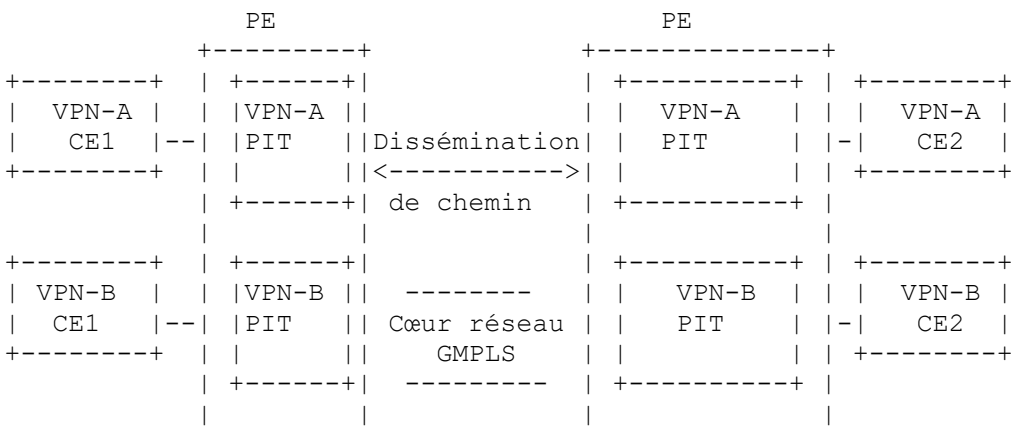
Plusieurs accès sur un CE pourraient partager le même canal de contrôle pour autant que tous ces accès appartiennent au même L1VPN. De même, plusieurs accès sur un PE pourraient partager le même canal de contrôle pour autant que ces accès appartiennent au même L1VPN.

4. Mode de base de VPN de couche 1 fondé sur l'accès

Un L1VPN est un service de VPN fondé sur l'accès où une paire de CE pourrait être connectée à travers le réseau de fournisseur de services via un LSP fondé sur GMPLS au sein d'une certaine topologie d'accès de VPN. C'est précisément ce LSP qui forme l'unité de base du service de L1VPN qu'offre le réseau de fournisseur de services. Si un accès par lequel un CE est connecté à un PE consiste en plusieurs canaux (par exemple, plusieurs longueurs d'onde) le CE pourrait établir des LSP avec plusieurs autres CE dans le même VPN sur ce seul accès.

Dans le L1VPN, le fournisseur de services n'initie pas la création d'un LSP entre une paire d'accès de CE. L'établissement du LSP est initié par le CE. Cependant, le LSP, en utilisant les mécanismes/outils mentionnés dans le présent document, restreint l'ensemble des autres accès de CE, qui peuvent être les points d'extrémité distants des LSP qui ont cet accès comme point d'extrémité local. Sous réserve de ces restrictions, la connexité CE à CE est sous le contrôle des CE eux-mêmes. En d'autres termes, le SP permet au L1VPN d'avoir un certain ensemble de topologies (exprimées comme une matrice de connexité d'accès à accès). La signalisation initiée par les CE est utilisée pour choisir une topologie particulière dans cet ensemble.

Pour chaque L1VPN qui a au moins un accès sur un certain PE, le PE tient un tableau des informations d'accès (PIT, *Port Information Table*) associé à ce L1VPN. Ce tableau contient une liste des couples <CPI, PPI> pour tous les accès au sein de son L1VPN. De plus, pour les accès de PE locaux d'un certain L1VPN, les couples incluent aussi les VPN-PPI de ces accès.



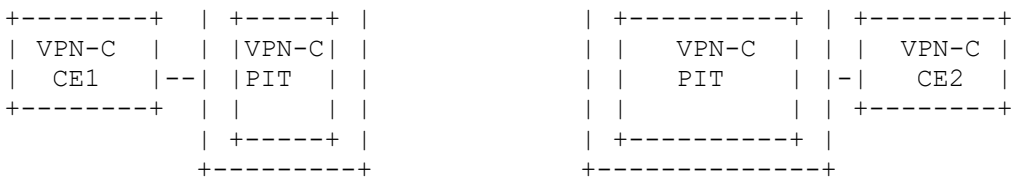


Figure 3 : Mode de base de service L1VPN

4.1 Tabeaux d'information d'accès de L1VPN

La Figure 3 illustre trois VPN, VPN-A, VPN-B, et VPN-C, avec leurs PIT associés. Un PIT consiste en informations locales ainsi qu'en informations distantes. Il s'ensuit qu'un PIT sur un certain PE est rempli à partir de deux sources d'informations :
1. les informations relatives aux accès du CE qui sont rattachés aux accès locaux de ce PE,
2. les informations sur les CE connectés aux PE distants.

Un PIT PEUT être rempli par provisionnement ou par les procédures d'auto-découverte. Quand le provisionnement est utilisé, le tableau entier PEUT être rempli par des commandes de provisionnement à une console ou par un système de gestion qui peut avoir une certaine capacité d'automatisation. Avec la croissance du réseau , une certaine forme d'automatisation est désirable.

Pour les informations locales entre un CE et un PE, un PE PEUT renforcer le LMP pour remplir les informations de liaison <CPI, VPN-PPI>. Ces informations locales doivent aussi être propagées aux autres PE qui partagent le même VPN. Les mécanismes pour cela sortent du domaine d'application du présent document, mais les informations doivent être échangées comme décrit au paragraphe 4.1.1.

Le PIT est par nature spécifique du VPN. Il est EXIGÉ d'un PE qu'il tienne un PIT pour chaque L1VPN pour lequel il a des CE membres rattachés localement. Un PE n'a pas besoin de tenir des PIT pour d'autres L1VPN. Cependant, l'ensemble complet des PIT avec toutes les entrées L1VPN pour plusieurs VPN PEUT aussi être disponible à tous les PE.

Les informations distantes dans le contexte d'un identifiant de VPN (c'est-à-dire, les CE distants de ce VPN) PEUVENT aussi être envoyées au CE local appartenant au même VPN. L'échange de ces informations sort du domaine d'application de ce document.

4.1.1 Informations d'auto-découverte locale

Les informations qui doivent être découvertes sur un accès PE local sont le CPI local et le VPN-PPI.

Ces informations PEUVENT être configurées ; ou, si LMP est utilisé entre CE et PE, LMP PEUT être utilisé pour échanger ces informations.

Une fois qu'un CPI a été découvert, le VPN-PPI correspondant transpose un contexte local en un identifiant de VPN et un PPI correspondant. Une façon d'appliquer un contexte de VPN contrôlé par le fournisseur est de pré-provisionner les VPN-PPI avec un identifiant de VPN. Les autres mécanismes de politique pour réaliser cela sortent du domaine d'application de ce document. De cette manière, une relation d'un CPI à un VPN et accès PPI peut être établie quand l'accès est provisionné comme appartenant au VPN.

4.1.2 Informations d'auto-découverte de PE distant

Ce paragraphe donne les informations qui sont portées par tout mécanisme d'auto-découverte, et sont utilisées pour remplir dynamiquement un PIT. Les informations donnent une seule transposition <CPI, PPI>. Chaque mécanisme d'auto-découverte va définir la ou les méthodes par lesquelles plusieurs transpositions <CPI, PPI> sont communiquées, ainsi que invalidées.

Ces informations devraient être cohérentes sans considération du mécanisme utilisé pour distribuer les informations [RFC5195], [RFC5252].

Le format du codage d'un seul couple <PPI, CPI> est :

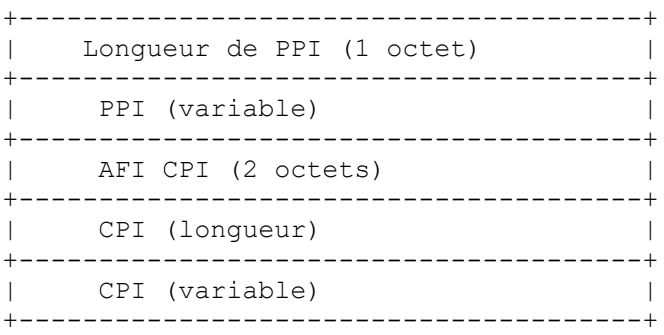


Figure 4 : Informations d'auto découverte

L'utilisation et la signification de ces champs sont comme suit :

Longueur de PPI : champ d'un octet dont la valeur indique la longueur du champ PPI.

PPI : champ de longueur variable qui contient la valeur du PPI (soit une adresse soit un couple <indice d'accès, adresse>). Noter que le PPI est toujours codé de façon cohérente au sein d'un domaine de fournisseur de sorte que le format du champ PPI est implicite au sein d'un réseau de fournisseur donné.

AFI CPI : champ de deux octets dont la valeur indique la famille d'adresses du CPI. Cette valeur est tirée de la [RFC1700].

Longueur de CPI : champ d'un octet dont la valeur indique la longueur du champ de CPI.

CPI : champ de longueur variable qui contient la valeur du CPI (soit une adresse, soit un couple <indice d'accès, adresse>).

Les couples de <PPI, CPI> DOIVENT aussi être associés à un ou plusieurs identifiants uniques au monde associés à un VPN particulier. Un identifiant unique au monde peut coder un VPN-ID, une cible de chemin, ou tout autre identifiant unique au monde. Les identifiants uniques au monde sont sous le contrôle des fournisseurs de réseau. L'unicité au sein d'un domaine administratif de fournisseur de services est suffisante pour le fonctionnement en mode de base. Dans le cas de plusieurs fournisseurs de réseau (ce qui sort du domaine d'application de ce document) l'identifiant unique au monde doit seulement être unique et cohérent entre ces fournisseurs. Dans le présent document, on spécifie un format de codage générique pour l'identifiant unique au monde commun à tous les mécanismes d'auto-découverte. Cependant, chaque mécanisme d'auto-découverte va définir la ou les méthodes spécifiques par lesquelles le codage est distribué et l'association avec un couple <PPI, CPI> est faite. Le codage de l'identifiant unique au monde associé au VPN est :

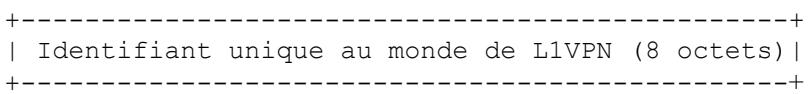


Figure 5 : Format d'identifiant d'auto découverte unique au monde

4.2 Établissement de LSP de CE à CE

Pour établir un LSP, un CE doit identifier tous les autres CE dans le L1VPN du CE auquel il veut se connecter. Un CE peut déjà avoir obtenu cette information par provisionnement ou par d'autres schémas (ces schémas sortent du domaine d'application de ce document).

Les accès associés à une certaine liaison de CE à PE PEUVENT aussi avoir d'autres informations, en plus des CPI et PPI qui leur sont associés qui décrivent les caractéristiques et contraintes des canaux au sein de ces accès, comme le codage pris en charge par les canaux, la bande passante d'un canal, la bande passante totale non réservée sur l'accès, etc. Ces informations pourraient être encore augmentées avec des informations sur certaines capacités du réseau de fournisseur de services (par exemple, la prise en charge du sur-débit de section de régénération (RSOH, *regeneration section overhead*), la transparence du canal de communications de données (DCC, *Data Communications Channel*) l'enchaînement arbitraire, etc.). Ces informations sont utilisées pour assurer que les accès à chaque extrémité d'un LSP ont des caractéristiques compatibles, et qu'il y a des ressources non allouées suffisantes pour établir un LSP entre ces accès.

Il peut arriver que pour une certaine paire d'accès au sein d'un L1VPN, chacun des CE connectés à ces accès essaye concurremment d'établir un LSP avec l'autre CE. Si avoir une paire de LSP entre une paire d'accès est vu comme indésirable, la façon de résoudre cela est d'exiger que le CE avec la plus faible valeur de CPI termine le LSP généré par le CE. Cette option pourrait être contrôlée par configuration sur les appareils de CE.

4.3 Signalisation

Dans L1VPN BM, un CE doit être configuré avec les CPI des autres accès. Une fois qu'un CE est configuré avec les CPI des autres accès au sein du même L1VPN, qu'on va appeler les "accès cibles", le CE utilise un sous ensemble de la signalisation GMPLS pour demander au réseau fournisseur d'établir un LSP à un accès cible.

Pour la connexité inter CE, le CE génère une demande qui contient le CPI d'un de ses accès qu'il veut utiliser pour le LSP, et le CPI de l'accès cible. Quand le PE rattaché au CE qui a généré la demande reçoit la demande, le PE identifie le PIT approprié, et utilise ensuite les informations de ce PIT pour trouver le PPI associé au CPI de l'accès cible porté dans la demande. Le PPI devrait être suffisant pour que le PE établisse un LSP. Finalement, la demande arrive au CE associé au CPI cible (noter que la demande porte encore le CPI du CE qui a généré la demande). Si le CE associé au CPI cible accepte la demande, le LSP est établi.

Noter qu'un CE n'a pas besoin d'établir un LSP pour chaque accès cible dont le CE a connaissance, c'est-à-dire, c'est une affaire de politique locale de CE de choisir un sous ensemble des accès cibles auxquels ce CE va essayer d'établir des LSP.

La procédure pour établir une connexion individuelle entre deux CE correspondants est la même que celle spécifiée pour le recouvrement GMPLS [RFC4208].

4.3.1 Procédures de signalisation

Quand un CE d'entrée envoie un message Path RSVP à un PE d'entrée, l'adresse IP de source dans le paquet IP qui porte le message est réglée à la CE-CC-Addr appropriée, et l'adresse de destination IP dans le paquet est réglée à la PE-CC-Addr appropriée. Quand le PE d'entrée renvoie au CE d'entrée le messages Resv correspondant, l'adresse IP de source dans le paquet IP qui porte le message est réglée à la PE-CC-Addr, et l'adresse IP de destination est réglée à la CE-CC-Addr.

De même, quand un PE de sortie envoie un message Path RSVP à un CE de sortie, l'adresse IP de source dans le paquet IP qui porte le message est réglée à la PE-CC-Addr appropriée, et l'adresse de destination IP dans le paquet est réglée à la CE-CC-Addr appropriée. Quand le CE de sortie renvoie au PE de sortie le message Resv correspondant, l'adresse de source IP dans le paquet IP qui porte le message est réglée à CE-CC-Addr, et l'adresse de destination IP est réglée à PE-CC-Addr.

En plus d'être utilisées pour les adresses IP dans le paquet qui porte les messages RSVP entre CE et PE, CE-CC-Addr et PE-CC-Addr sont aussi utilisées dans le champ Adresse de prochain/précédent bond de l'objet IF_ID RSVP_Hop qui est porté entre les CE et les PE.

Dans le cas où une liaison entre CE et PE est une liaison numérotée non en faisceau, le CPI et le VPN-PPI de cette liaison sont utilisés pour les TLV de type 1 ou 2 de l'objet IF_ID RSVP_Hop qui est porté entre le CE et le PE. Dans le cas où une liaison entre CE et PE est une liaison non numérotée non en faisceau, le CPI et le VPN-PPI de cette liaison sont utilisés pour le champ Adresse IP de la TLV de type 3. Dans le cas où une liaison entre CE et PE est une liaison en faisceau, le CPI et le VPN-PPI de cette liaison sont utilisés pour le champ Adresse IP des TLV de type 3.

Un traitement supplémentaire relatif aux liaisons non numérotées est décrit à la Section 3 ("Traitement de l'objet IF_ID RSVP_HOP") et au paragraphe 4.1 ("Adjacences de transmission non numérotées") de la [RFC3477].

Quand un CE d'entrée génère un message Path pour établir un LSP d'un accès particulier sur ce CE à un accès de cible particulier, le CE utilise le CPI de son accès dans l'objet "Sender Template". Si le CPI de l'accès ce cible est une adresse IP, alors le CE l'utilise dans l'objet Session. Et si le CPI de l'accès de cible est un couple <indice d'accès, adresse IP>, alors le CE utilise la partie adresse IP du couple dans l'objet Session, et le couple entier comme sous objet Identifiant d'interface non numérotée dans l'objet Chemin explicite (ERO, *Explicit Route Object*).

Il y a deux options pour les sessions RSVP-TE. Une option est d'avoir une seule session RSVP-TE de bout en bout où les adresses du consommateur et du fournisseur sont échangées au PE ; ceci est appelé un brassage *(shuffling)*. L'autre option est quand un brochage *(stitching)* ou une hiérarchie est utilisée pour créer deux sessions de LSP, une entre le ou les PE de fournisseur et une autre session de bout en bout entre les CE.

4.3.1.1 Sessions brassées

Les sessions brassées sont utilisées quand on désire avoir un seul LSP qui a pour origine le CE et se termine au CE d'extrémité distante. Les adresses de consommateur sont brassées avec les adresses de fournisseur au PE d'entrée, et rebrassées aux adresses de consommateur au PE de sortie en utilisant la transposition fournie par le PIT.

Quand le message Path arrive au PE d'entrée, le PE choisit le PIT associé au L1VPN, et utilise ensuite ce PIT pour transposer les CPI portés dans les objets Session et Sender Template en les PPI appropriés. Une fois la transposition faite, le PE d'entrée remplace les CPI par ces PPI. Par suite, les objets Session et Sender Template qui sont portés dans la signalisation GMPLS au sein du réseau de fournisseur de services portent les PPI, et non les CPI.

Au PE de sortie, l'opération de transposition inverse est effectuée. Le PE extrait les valeurs de PPI d'entrée/sortie portées dans respectivement les objets Sender Template et Session. Le PE de sortie identifie le PIT approprié pour trouver le CPI approprié associé au PPI du CE de sortie. Une fois la transposition effectuée, le PE de sortie remplace les valeurs de PPI d'entrée/sortie par les valeurs correspondantes de CPI. Par suite, les objets Session et Sender Template (inclus dans le message Path GMPLS RSVP-TE envoyé du PE de sortie au CE de sortie) portent les CPI, et non les PPI.

Là aussi, pour les messages Path GMPLS RSVP-TE envoyés du PE de sortie au CE, l'adresse IP de source (du paquet IP qui porte ce message) est réglée à la PE-CC-Addr appropriée, et l'adresse de destination IP (du paquet IP qui porte ce message) est réglée à la CE-CC-Addr appropriée.

À ce point, la vue du CE est un seul LSP qui est en point à point entre les deux CE avec une liaison virtuelle entre les nœuds PE : CE-PE(-)PE-CE. Les nœuds PE du L1VPN ont une vue du segment de LSP de PE à PE dans tous ses détails. Les PE PEUVENT filtrer la signalisation RSVP-TE, c'est-à-dire, supprimer les informations sur la topologie du fournisseur et la remplacer par une vue d'une liaison virtuelle.

Cette traduction des adresses et des identifiants de session est appelée un brassage et est pilotée par les tableaux d'information d'accès de L1VPN (voir la Section 4). Ceci DOIT être effectué pour tous les messages RSVP-TE aux PE de bordure. Dans ce cas, il y a une session de CE à CE.

4.3.1.2 Sessions brochées ou incorporées

Les options de brochage ou d'incorporation dépendent des types de commutation de LSP. Si les LSP de CE à CE et de PE à PE sont identiques en type et capacité de commutation, le LSP PEUT être broché ensemble et les procédures de la [RFC5150] s'appliquent. Si les LSP de CE à CE et de PE à PE ne sont pas du même type de commutation, ou sont de capacités différentes mais compatibles, les LSP PEUVENT être incorporés et les procédures de la [RFC4206] s'appliquent. Comme les deux procédures de signalisation de LSP brochées et incorporées impliquent un établissement de session de PE à PE compatible avec les paramètres de session de CE, elles sont décrites ensemble.

Quand le message Path arrive au PE d'entrée, celui-ci choisit le PIT associé au L1VPN, et utilise ensuite ce PIT pour transposer les CPI portés dans les objets Session et Sender Template en les PPI appropriés. Une fois la transposition faite, une nouvelle session de PE à PE est établie avec les paramètres compatibles pour la session de CE. La session de PE à PE étant bien établie, la demande de signalisation de PE est envoyée au PE de sortie.

Au PE d'entrée, quand le brochage et l'incorporation sont utilisées, une session de PE à PE est établie. Cela pourrait être réalisé de plusieurs façons :
- Associer un LSP de PE à PE déjà établi ou un LSP d'adjacence de transmission (FA-LSP, *Forwarding Adjacency LSP*) à la destination qui satisfasse les paramètres demandés.
- Établir un segment de LSP de PE à PE conforme.

À ce point, la vue du CE est un seul LSP qui est en point à point entre les deux CE avec a un nœud virtuel entre les nœuds PE :
CE-PE(-)PE-CE. Les nœuds PE de L1VPN ont une vue du segment de LSP de PE à PE dans tous ses détails. Les PE n'ont pas à filtrer la signalisation RSVP-TE en supprimant les informations sur la topologie du fournisseur parce que la signalisation de PE à PE n'est pas visible aux nœuds CE.

4.3.1.3 Autre signalisation

Un PE d'entrée peut recevoir et potentiellement rejeter un message Path qui contient un objet Chemin explicite et donc causer l'échec de l'établissement de la connexion commutée. Cependant, le PE d'entrée peut accepter les ERO, qui incluent une séquence de {<PE d'entrée (strict), CPI de sortie (lâche)>}.

Message Path sans ERO : quand un PE d'entrée reçoit un message Path d'un CE d'entrée qui ne contient pas d'ERO, il DOIT calculer un chemin vers la destination pour le LSP de PE à PE et inclure ce chemin dans un ERO, avant de transmettre le message Path. Une exception serait si le nœud de cœur de sortie était aussi adjacent à ce nœud cœur.

Message Path avec ERO : quand un PE d'entrée reçoit un message Path d'un CE d'entrée qui contient un ERO (de la forme précisée ci-dessus) il calcule un chemin pour joindre le PE de sortie. Il insère ensuite ce chemin au titre de l'ERO avant de transmettre le message Path.

Dans le cas de brassage, les règles de recouvrement pour la notification et le traitement de RRO sont identiques à celles de du modèle d'interface usager-réseau (UNI, *User-Network Interface*) ou de recouvrement [RFC4208], qui déclarent que un PE de bordure PEUT supprimer/éditer des notifications de fournisseur et des RRO quand il passe les messages aux CE.

4.4 Procédures de récupération

Signalisation : un CE demande un LSP à réseau protégé (c'est-à-dire, un LSP qui est protégé de PE à PE) en utilisant la technique décrite dans la [RFC4873]. L'identification dynamique des nœuds de fusion est prise en charge via les fanions de récupération de segment de LSP portés dans l'objet Protection (voir le paragraphe 6.2 de la [RFC4873]).

Notification : un objet Notify Request PEUT être inséré dans des messages Path ou Resv pour indiquer l'adresse d'un CE à qui devrait être notifiée la défaillance d'un LSP. Des notifications PEUVENT être demandées dans les deux directions amont et aval :
- la notification amont est indiquée via l'inclusion d'un objet Notify Request dans le message Path correspondant.
- la notification aval est indiquée via l'inclusion d'un objet Notify Request dans le message Resv correspondant.

Un PE qui reçoit un message contenant un objet Notify Request DEVRAIT mémoriser l'adresse du nœud notifié dans le bloc d'état RSVP correspondant. Le PE DEVRAIT aussi inclure un objet Notify Request dans le message Path ou Resv sortant. L'adresse du nœud notifié sortant PEUT être mise à jour sur la base de la politique locale. Cela signifie qu'un PE, à réception de cet objet provenant du CE, PEUT mettre à jour la valeur de l'adresse du nœud notifié.

Si le CE d'entrée inclut un objet Notify Request dans le message Path, le PE d'entrée PEUT remplacer l'adresse du nœud notifié reçue par sa propre "adresse de nœud notifié" choisie, et en particulier l'identifiant de routeur TE local. L'objet Notify Request PEUT être porté dans les messages Path ou Resv (Section 7 de la [RFC3473]). Le format de l'objet Notify Request est défini dans la [RFC3473]. Selon le paragraphe 4.2.1 de la [RFC3473], les adresses de nœud notifié DEVRONT être réglées à IPv4 ou IPv6.

L'inclusion d'un objet Notify Request est utilisée pour demander la génération de notifications lors de la survenance d'une défaillance mais ne garantit pas qu'un message Notify va être généré.

5. Considérations pour la sécurité

La sécurité des L1VPN est traitée dans les [RFC4847] et [RFC5253]. Le présent document, discute des aspects de sécurité qui relèvent du plan de contrôle.

L'association d'un accès particulier à un L1VPN particulier (ou pour être plus précis, avec un PIT particulier) est une opération de configuration, généralement faite manuellement par le fournisseur de services au titre du processus de provisionnement du service. Donc, elle ne peut pas être altérée via la signalisation entre CE et PE. Cela signifie que la signalisation ne peut pas être utilisée pour livrer le trafic de L1VPN à un mauvais consommateur. L'opérateur devrait appliquer les mécanismes de sécurité appropriés à la gestion et au processus de configuration, et devrait envisager les techniques de vérification du plan des données pour protéger contre une mauvaise configuration accidentelle. Le consommateur peut aussi appliquer des essais de bout en bout (c'est-à-dire, de CE à CE) de connexité du plan des données sur la connexion de L1VPN pour détecter une mauvaise connexion. L'essai de connexité du plan des données peut être effectué en utilisant le protocole de gestion de liaison (LMP, *Link Management Protocol*) [RFC4204].

Noter qu'il est aussi possible de remplir la partie locale d'un PIT en utilisant l'auto-découverte par LMP. LMP peut être sécurisé comme décrit dans la [RFC4204]. La signalisation entre CE et PE est supposée être sur une liaison privée (par exemple, dans la bande ou sur fibre) ou un réseau privé. L'utilisation d'une liaison privée rend la connexion de CE à PE sûre au même niveau que la liaison de données décrite dans les paragraphes précédents. L'utilisation d'un réseau privé suppose que les entités en dehors du réseau ne peuvent pas usurper l'identité ou modifier les communications de plan de contrôle entre CE et PE. De plus, toutes les entités dans le réseau privé sont supposées être de confiance. Donc, aucun mécanisme de sécurité n'est exigé par les échanges de protocole décrits dans ce document.

Cependant, un opérateur qui est concerné par la sécurité de son réseau privé de plan de contrôle peut utiliser les fonctions d'authentification et d'intégrité disponibles dans RSVP-TE [RFC3473] ou utiliser IPsec ([RFC2411], [RFC4301], [RFC4302], [RFC4306], et [RFC4835]) pour la signalisation point à point entre PE et CE. Voir dans la [RFC5920] une discussion complète des options de sécurité disponibles pour le plan de contrôle GMPLS.

Noter de plus qu'un réseau privé (par exemple, un VPN de couche 2 ou un VPN de couche 3) pourrait être utilisé pour fournir la connexité de plan de contrôle entre un PE et plus d'un CE. Dans ce scénario, il est RECOMMANDÉ que chaque consommateur de L1VPN ait son propre réseau privé. Les mécanismes de sécurité fournis par le réseau privé DEVRAIENT alors être utilisés pour assurer la sécurité de la communication de plan de contrôle entre un consommateur et un fournisseur de services.

6. Références

6.1 Références normatives

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

[RFC3471] L. Berger, éd., "Commutation d'étiquettes multi-protocoles généralisée (GMPLS) : description fonctionnelle de la signalisation", janvier 2003. (*MàJ par* RFC4201, RFC4328, RFC4872, RFC8359) *(P.S.)*

[RFC3473] L. Berger, "Extensions d'ingénierie de protocole - trafic de signalisation de réservation de ressource (RSVP-TE) de commutation d'étiquettes multi-protocoles généralisée (GMPLS)", janvier 2003. *(P.S., MàJ par 4003, 4201, 4420, 4783, 4784, 4873, 4974, 5063, 5151,* 8359)

[RFC3477] K. Kompella, Y. Rekhter, "Signalisation des liaisons non numérotées dans le protocole de réservation de ressource – ingénierie du trafic (RSVP-TE)", janvier 2003. *(P.S.)*

[RFC4202] K. Kompella et autres, "Extensions d'acheminement pour la prise en charge de la commutation généralisée d'étiquettes multi-protocoles (GMPLS)", octobre 2005. *(P.S.)*

[RFC4204] J. Lang, éd., "Protocole de gestion de liaison (LMP)", octobre 2005. *(P.S.)*

[RFC4206] K. Kompella, Y. Rekhter, "Hiérarchie de chemins commutés par étiquettes (LSP) avec l'ingénierie de trafic (TE) de la commutation généralisée d'étiquettes multi-protocoles (GMPLS)", octobre 2005. *(P.S.)*

[RFC4208] G. Swallow et autres, "Interface usager-réseau (UNI) de commutation généralisée d'étiquettes multiprotocoles (GMPLS) : prise en charge du protocole de réservation de ressource - ingénierie du trafic (RSVP-TE) pour le modèle de recouvrement", octobre 2005. *(P.S.)*

[RFC4873] L. Berger et autres, "Récupération de segment GMPLS", mai 2007. *(P.S. ; MàJ* RFC3473, RFC4872 ; *MàJ par* RFC9270*)*

[RFC5150] A. Ayyangar et autres, "Raccordement de chemin à commutation d'étiquette avec la commutation généralisée d'étiquettes multiprotocoles à ingénierie de trafic (GMPLS-TE)", février 2008. *(P.S.)*

6.2 Références pour information

[RFC1700] J. Reynolds et J. Postel, "Numéros alloués", STD 2, octobre 1994. *(Historique, voir www.iana.org))*

[RFC2411] R. Thayer, N. Doraswamy, R. Glenn, "Feuille de route pour la sécurité sur IP", novembre 1998. *(Obs., voir* RFC6071)

[RFC3945] E. Mannie, éd., "Architecture de commutation d'étiquettes multi-protocoles généralisée (GMPLS)", octobre 2004. *(P.S.)*

[RFC4201] K. Kompella et autres, "Faisceaux de liaisons dans l'ingénierie du trafic MPLS", octobre 2005. *(P.S.)*

[RFC4301] S. Kent et K. Seo, "Architecture de sécurité pour le protocole Internet", décembre 2005. *(P.S.) (Remplace la* RFC2401)

[RFC4302] S. Kent, "En-tête d'authentification IP", décembre 2005. *(P.S.)*

[RFC4306] C. Kaufman, "Protocole d'échange de clés sur Internet (IKEv2)", décembre 2005. *(Obsolète, voir la* RFC5996)

[RFC4835] V. Manral, "Exigences pour la mise en œuvre d'algorithme de chiffrement pour l'encapsulation de charge utile de sécurité (ESP) et l'en-tête d'authentification (AH)", avril 2007. (*Remplace* RFC4305) *(P.S.)*

[RFC4847] T. Takeda, éd., "Cadre et exigences pour la couche 1 des réseaux privés virtuels", avril 2007. *(Information)*

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

[RFC5252] I. Bryskin, L. Berger, "Auto découverte de VPN de couche 1 fondée sur OSPF", juillet 2008. *(P.S.)*

[RFC5253] T. Takeda, "Déclaration d'applicabilité du mode de base de réseau privé virtuel de couche 1 (L1VPN)", juillet 2008. *(Information)*

[RFC5920] L. Fang, "Cadre de sécurité pour réseaux MPLS et GMPLS", juillet 2010. *(Information)*

7. Remerciements

Les auteurs tiennent à remercier Adrian Farrel, Hamid Ould-Brahim, et Tomonori Takeda de leurs précieux commentaires.

Sandy Murphy, Charlie Kaufman, Pasi Eronen, Russ Housley, Tim Polk, et Ron Bonica ont fourni des commentaires durant le processus de revue par l'IESG.

Adresse des auteurs

Don Fedyk
Nortel Networks
600 Technology Park
Billerica, MA 01821
téléphone : +1 (978) 288 3041
mél : dwfedyk@nortel.com

Yakov Rekhter
Juniper Networks
1194 N. Mathilda Avenue
Sunnyvale, CA 94089
mél : yakov@juniper.net

Dimitri Papadimitriou
Alcatel-Lucent
Fr. Wellesplein 1,
B-2018 Antwerpen, Belgium
téléphone : +32 3 240-8491
mél : Dimitri.Papadimitriou@alcatel-lucent.être

Richard Rabbat
Google Inc.
1600 Amphitheatre Pky
Mountain View, CA 95054
mél : rabbat@alum.mit.edu

Lou Berger
LabN Consulting, LLC
téléphone : +1 301-468-9228
mél : lberger@labn.net

Déclaration complète de droits de reproduction

Propriété intellectuelle