Groupe de travail Réseau
Request for Comments : 4847
Catégorie : Information

T. Takeda, éditeur, NTT
avril 2007
Traduction Claude Brière de L'Isle

Cadre et exigences pour les réseaux privés virtuels de couche 1

Résumé
Le présent document fournit un cadre et les exigences de niveau de service pour les réseaux privés viruels de couche 1 (L1VPN, *Layer 1 Virtual Private Network*). Ce cadre est destiné à aider à développer et normaliser les protocoles et mécanismes pour prendre en charge des L1VPN interopérables.

Le document examine les motivations des L1VPN, les exigences de haut niveau (niveau de service) et souligne certains des modèles architecturaux qui pourraient être utilisés pour construire des L1VPN.

Table des Matières

1. Introduction

Le présent document examine les motivations des réseaux privés viruels de couche 1 (L1VPN), donne les exigences de haut niveau (niveau de service) et souligne certains des modèles architecturaux qui pourraient être utilisés pour construire des L1VPN.

L'objectif du document est principalement de présenter les exigences et l'architecture sur la base des travaux entrepris dans la Question 11 du groupe d'études 13 de l'UIT-T.

Les L1VPN fournissent des services sur les réseaux de couche 1. Le présent document donne un cadre pour les L1VPN et la réalisation du cadre par les réseaux contrôlés par les protocoles de commutation multiprotocoles avec étiquetage des flux généralisée (GMPLS, *Generalized Multi-Protocol Label Switching*).

L'utilisation de protocoles GMPLS pour fournir des services de L1VPN présente plusieurs avantages, comme :
- un fonctionnement souple du réseau,
- l'utilisation de protocoles normalisés,
- l'utilisation de protocoles communs de plan de contrôle et de mesures applicables à divers protocoles de couche 1, incluant les réseaux de multiplexage à répartition dans le temps (MRT) et les réseaux optiques.

2. Terminologie

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].

Le lecteur est supposé être familiarisé avec la terminologie des [RFC3031], [RFC3209], [RFC3471], [RFC3473], [RFC4202], [RFC3945], [RFC4208], et [RFC4026].

Dans ce contexte, un réseau de couche 1 est tout réseau de transport qui a la connexité et/ou la commutation en utilisant la commutation spatiale (par exemple, accès ou fibre entrant à accès ou fibre sortant) la commutation lambda, ou la commutation en multiplexage à répartition dans le temps.

Un VPN de couche 1 (L1VPN) est un service offert par un cœur de réseau de couche 1 pour fournir la connexité de couche 1 entre deux sites consomateurs ou plus, et où le consommateur a un certain contrôle sur l'établissement et le type de connexité. Une autre définition est simplement de dire qu'un L1VPN est un VPN dont le plan des données opère à la couche 1. Plus de détails sur l'essence d'un L1VPN sont fournis à la Section 3.

De plus, les nouveaux termes suivants sont utilisés dans le présent document :

Liaison virtuelle : liaison d'ingénierie du trafic (TE, *Traffic Engineering*) d'un réseau de fournisseur annoncée aux consommateurs dans les informations d'acheminement pour des besoins qui incluent le calcul de chemin. Une liaison de données directe peut ou non exister entre les deux extrémités d'une liaison virtuelle.

Nœud virtuel : nœud logique d'un réseau de fournisseur annoncé aux consommateurs dans les informations d'acheminement. Un nœud virtuel peut représenter un seul nœud physique, ou plusieurs nœuds physiques et les liaisons entre eux.

Point d'extrémité de VPN : interface de plan des données d'un appareil de côté consommateur (CE, *Customer Edge*) qui est connecté à un appareil de côté fournisseur (PE, *Provider Edge*) et qui fait partie des membres du VPN. Noter qu'une interface de plan des données est associée à un point d'extrémité de liaison TE. Par exemple, si l'interface d'un routeur CE est une interface à canaux (définie dans SONET/SDH) un canal dans l'interface à canaux peut être une interface de plan des données.

Connexion de VPN (ou connexion dans le contexte de L1VPN) : connexion entre une paire de points d'extrémité de VPN. Noter que dans certains scénarios, une connexion peut être établie entre une paire d'appareils de consommateurs en utilisant cette connexion CE-CE de VPN comme un segment ou adjacence de transmission définie dans la [RFC4206].

Noter que les termes suivants sont en ligne avec la terminologie de VPN provisionné de fournisseur (PPVPN, *Provider Provisioned VPN*) [RFC4026], et que dans le présent document, ont une signification dans le contexte des L1VPN, sauf mention contraire.

Appareil CE : c'est un appareil de consommateur qui reçoit le service de L1VPN du fournisseur. Un appareil CE est connecté à au moins un appareil PE. Un appareil CE peut être divers appareils, par exemple, un commutateur de multiplexage à répartition dans le temps (MRT) un routeur, et un commutateur de couche 2. Un appareil CE n'a pas à avoir la capacité de commuter à la couche 1, mais il est capable de recevoir un signal de couche 1 et soit de le commuter soit de le terminer avec adaptation. Un appareil CE peut être rattaché à un ou plusieurs appareils de consommateur sur le site du consommateur, et it peut être un hôte utilisant directement une connexion de couche 1.

Appareil PE : c'est un appareil de fournisseur qui fournit le service L1VPN au consommateur. Un appareil PE est connecté à au moins un appareil CE. Un appareil PE de couche 1 est un commutateur MRT, un brasseur optique (OXC, *Optical Cross-Connect*) (voir la [RFC3945]) ou un brasseur photonique (PXC, *Photonic Cross-Connect*) (voir la [RFC3945]). Autrement, un appareil PE peut être un appareil de type ligne privée Ethernet (EPL, *Ethernet Private Line*) qui transpose des trames Ethernet en connexions de couche 1 (au moyen de Ethernet sur MRT, etc.).

Appareil P *(Provider)* : c'est un appareil de fournisseur qui est connecté seulement à d'autres appareils de fournisseur (appareils P ou PE). Un appareil P de couche 1 est un commutateur MRT, OXC, ou PXC.

Consommateur : un consommateur a autorité sur un ensemble d'appareils CE au sein du même VPN (par exemple, le propriétaire des appareils CE). Noter qu'un consommateur peut déléguer la gestion des appareils CE à d'autres organisations, incluant au fournisseur lui-même.

Fournisseur : un fournisseur a autorité sur la gestion du réseau du fournisseur.

Informations de membres : listes des adresses de liaisons TE de CE-PE qui appartiennent au même VPN. Les informations de membres contiennent l'association d'un CE, d'un PE, et d'un VPN.

3. Généralités

3.1 Topologie de réseau

Le réseau de couche 1, constitué de OXC, de commutateurs MRT, ou PXC peut être vu comme consistant en appareils PE qui donnent accès de l'extérieur du réseau, et en appareils P qui n'opèrent qu'au sein du cœur du réseau. De même, à l'extérieur du réseau de couche 1 se trouve le réseau consommateur consistant en appareils consommateurs avec accès au réseau de couche 1 effectué à travers les appareils CE.

Un CE et un PE sont connectés par une ou plusieurs liaisons. Un CE peut aussi être connecté à plus d'un PE, et un PE peut avoir plus d'un CE qui lui est connecté.

Une connexion de couche 1 est fournie entre une paire de CE. Une telle connexion suit la hiérarchie définie dans la [RFC4206]. C'est-à-dire, une connexion CE-CE peut être incorporée dans une connexion de couche inférieure (par exemple, une connexion VC3 sur une connexion STM1). De même, les capacités de commutation des interfaces des CE, PE, et P sur lesquelles une connexion est acheminée suivent la hiérarchie définie dans la [RFC4206].

3.2 Introduction aux VPN de couche 1

Le concept de PPVPN a été établi par de nombreux documents antérieurs comme les [RFC4664] et [RFC4110]. La terminologie pour les PPVPN est fixée dans la [RFC4026] avec une référence particulière aux VPN de couches 2 et 3.

La réalisation des L1VPN peut se fonder sur des extensions des concepts du PPVPN au réseau de couche 1. On doit comprendre que la satisfaction des exigences décrites dans le présent document peut nécessiter des extensions aux mécanismes existants à la fois au plan de contrôle au sein du réseau de couche 1 et pour le provisionnement de service à la bordure du réseau (appareils CE et PE). C'est à l'interface entre les appareils CE et PE que le service de L1VPN est fourni.

Noter que la différence fondamentale entre les L1VPN et les VPN de couche 2/3 est que dans les L1VPN, la connexité de plan des données ne garantit pas celle du plan de contrôle (et vice versa). Mais la connexité du plan de contrôle CE-PE est nécessaire pour les services de L1VPN provisionnés à travers le plan de contrôle, et la connexité du plan de données CE-CE est maintenue par des mécanismes de signalisation fondés sur cette connexité de plan de contrôle. De plus, le provisionnement de la connexité de plan de contrôle CE-CE sur le réseau fournisseur est aussi requise pour certains

niveaux de service de L1VPN, et cela peut être réalisé par l'échange de paquets de contrôle entre les CE sur le plan de contrôle du réseau fournisseur. Cet aspect est discuté plus en détails au paragraphe 10.2.

3.3 Technologies courantes pour le provisionnement dynamique de couche 1

Les efforts de normalisation pré-existants se sont concentrés sur la fourniture de connexions dynamiques au sein du réseau de couche 1 (signalisation et acheminement) et sur la définition des interfaces pour les services demandeurs entre l'utilisateur et le réseau de couche 1 sur l'interface utilisateur-réseau (UNI, *User-Network Interface*) et entre réseaux à travers l'interface réseau-réseau externe (E-NNI, *External Network-Network Interface*) (voir les [RFC3945], [RFC4208], [RFC4139], et [RFC4258]).

Les UNI courants incluent des caractériqtiques pour faciliter les demandes de services de bout en bout (c'est-à-dire, de CE à CE) qui incluent la spécification de contraintes comme les chemins explicites, les exigences de bande passante, les besoins de protection, et (bien sûr) les destinations.

Les E-NNI courants incluent des caractéristiques pour échanger des informations d'acheminement, ainsi que pour faciliter les demandes de services de bout en bout.

Les UNI et E-NNI peuvent être appliquées dans le contexte des L1VPN. Par exemple, l'UNI peut être appliquée entre le CE et le PE, et la E-NNI peut être appliquée entre des PE (L1VPN inter AS/SP) ou entre le CE et le PE.

Cependant, les spécifications existantes d'UNI et de E-NNI ne fournissent pas des paramètres suffisants pour prendre en charge les VPN sans quelques ajouts. Par exemple, il n'y a pas de moyen de distinguer les messages de contrôle reçus sur une liaison de contrôle partagée (c'est-à-dire, une liaison de contrôle partagée pas plusieurs VPN) à une UNI/E-NNI, et ces messages doit être distingués pour déterminer le L1VPN auquel ils s'appliquent. Une liaison de contrôle est une liaison IP utilisée pourr établir un canal de contrôle entre les nœuds.

Un autre exemple est qu'il n'y a pas de façon clairement définie de distribuer les informations de membres à utiliser en combinaison avec UNI/E-NNI. Cette fonction est nécessaire pour découvrir l'existence et la localisation des CE à connecter avec les connexions de couche 1. La distribution des informations d'appartenance est normalement faite par le fournisseur, et peut être réalisée par des mécanismes tels que le provisionnement statique, ou en les faisant porter par les protocoles d'acheminement (par exemple, voir le paragraphe 4.2.1 de la [RFC4110]). Noter que la méthode choisie pour la distribution des informations d'appartenance dépend de la solution utilisée pour prendre en charge les L1VPN, qui sort du domaine d'application du présent document.

De plus, les domaines d'adressage des consommateurs peuvent se chevaucher, et peuvent aussi se chevaucher avec le domaine d'adressage du fournisseur de service. Cela exige des mécanismes de transposition d'adresse, mais ces mécanismes ne sont pas bien définis dans les spécifiactions existantes d'UNI/E-NNI.

Enfin il n'y a pas de façon clairement définie de restreindre la connexité entre les CE (ou sur une UNI/E-NNI). De plus, les E-NNI permettent l'échange des informations d'acheminement, mais il n'y a pas de façon clairement définie de permettre un échange limité d'informations d'acheminement (c'est-à-dire, où un ensemble spécifique d'informations d'acheminement est distribué à un ensemble spécifique de CE).

Afin que les L1VPN soient pris en charge d'une manière pleinement fonctionnelle, ces capacités supplémentaires et les autres exigences mentionnées plus loin dans ce document doivent être traitées.

Noter que les L1VPN inter AS/SP exigent une analyse supplémentaire qui sort du domaine d'application du présent document.

3.4 Relations avec l'UIT-T

Le fondement du présent document est le travail réalisé par la question 11 du groupe d'études 13 de l'UIT-T, comme les Recommandations [Y.1312] et [Y.1313]. Ce groupe a fait des recherches et spécifié les exigences et l'architecture des L1VPN depuis un certain temps. Dans ce contexte, le fondement du présent document est une représentation des résultats de l'UIT-T, et une présentation de ces résultats dans des termes et un format familiers à l'IETF.

En particulier, le présent document se limite aux domaines qui concernent l'IETF. C'est-à-dire, il est limité aux réseaux de couche 1 qui utilisent IP comme support sous-jacent pour leur plan de contrôle.

Le présent document présente les exigences et les architectures développées au sein de l'UIT-T pour une meilleure compréhension au sein de l'IETF et pour poursuivre la coopération entre les deux organismes.

Un travail relatif à l'espace de solution de L1VPN a déjà été réalisé au sein de l'IETF.

4. Motifs

Les avantages généraux et le besoin des VPN ont été décrits de nombreuses fois et en de nombreux endroits ([RFC4110] et [RFC4664]). Le présent document ne s'attardera pas sur les mérites des VPN en tant que tels, mais se concentre entièrement sur l'applicabilité du concept de VPN aux réseaux de couche 1.

De même, l'utilité et la valeur d'un plan de contrôle pour la configuration, la gestion, et le fonctionnement d'un réseau de couche 1 est traitée dans la [RFC3945].

4.1 Services de base de couche 1

Les services de base de couche 1 peuvent être caractérisés en des termes qui incluent :
- Connexité : entre une paire de CE.
- Capacité : par exemple, le débit binaire pour un service de MRT ou la capacité d'un lambda.
- Transparence : par exemple, pour un réseau SDH, la transparence aux frais généraux.
- Disponibilité : le pourcentage de temps pendant lequel le service offert satisfait les critères que le fournisseur définit, éventuellement avec l'accord de chaque consommateur. Pour réaliser le niveau de disponibilité requis pour les connexions du consommateur, le réseau du fournisseur de service peut utiliser des ressources de restauration ou protégées [RFC4427].
- Performances : la qualité de service livrée aux consommateurs, par exemple, le nombre de secondes d'erreur par mois.

Les services de couche 1 peuvent être rangés en catégories sur la base de la combinaison des caractéristiques de connexité (plan des données) et des caractéristiques de capacité de contrôle du service (plan de contrôle) disponibles au consommateur. Un CE est associé à l'interface de service entre un site de consommateur et le réseau fournisseur, et la catégorisation peut être vue dans le contexte de cette interface de service comme suit :

1. Une seule connexion entre une paire de CE.
- Service statique : le service de ligne privée classique réalisé par une connexion permanente.
- Service dynamique : soit un service de connexion commutée, soit un service de connexion permanente logicielle contrôlée par le consommateur (c'est-à-dire, le consommateur contrôle quand la partie signalée est établie).

2. Plusieurs connexions parmi un ensemble de CE.
- Service statique : un service de réseau privé consistant en un maillage de connexions permanentes.
- Service dynamique : un service de réseau privé dynamique consistant en une combinaison de services de connexions commutées et de services de connexions permanentes logicielles contrôlées par le consommateur.

Pour les types de services 1 et 2, les connexions sont en point à point, et peuvent être permanentes, semi-permanentes, ou commutées. Pour un service statique, le plan de gestion du réseau fournisseur est responsable de la gestion de l'infrastructure réseau et des connexions de l'utilisateur d'extrémité. Pour les services dynamiques, le plan de gestion du réseau fournisseur est seulement responsable de la configuration de l'infrastructure ; les connexions de l'utilisateur d'extrémité sont établies de façon dynamique via le plan de contrôle du réseau fournisseur sur demande du consommateur.

Le présent document n'empêche pas la prise en charge d'autres services et topologie évoluées, comme des services de point à multipoints (P2MP) au titre des service de couche 1, mais ils feront l'objet d'études ultérieures.

4.1.1 L1VPN pour le provisionnement dynamique de couche 1

Des services de réseau privé de la seconde catégorie du paragraphe 4.1 peuvent être améliorés afin que plusieurs réseaux privés soient pris en charge à travers le réseau de couche 1 comme des réseaux privés virtuels. Ce sont des réseaux privés virtuels de couche 1 (L1VPN, *Layer 1 Virtual Private Network*). Noter que la première catégorie du paragraphe 4.1 inclurait les L1VPN avec seulement deux CE comme un cas particulier.

Comparé à la première catégorie de service, le service de L1VPN a des caractéristiques telles que la restriction de connexité, une politique séparée, et la distribution des informations d'appartenance appliquées à un groupe spécifique.

4.2 Mérites de L1VPN

4.2.1 Mérites du consommateur

Du point de vue du consommateur, il y a deux principaux avantages à un L1VPN. Ces avantages s'appliquent par dessus les avantages de l'accès à un réseau provisionné dynamiquement.

- Le consommateur peut déléguer la gestion directe d'un réseau de couche 1 en plaçant la gestion de VPN sous le contrôle d'un tiers. Cela libère le consommateur du besoin de configurer et gérer les informations de connexité pour les CE qui participent au VPN.

- Le consommateur peut faire une utilisation à petite échelle d'un réseau de couche 1. Ainsi, par exemple, en partageant l'infrastructure de réseau de couche 1 avec de nombreux autres utilisateurs, les sites de consommateur peuvent être connectés ensemble à travers le réseau de couche 1 sans supporter tout le coût du déploiement et de la gestion du réseau de couche 1.

Dans une certaine mesure, le consommateur peut aussi tirer parti des avantages du fournisseur (voir ci-dessous). C'est-à-dire, si le fournisseur est capable d'extraire plus de valeur du réseau de couche 1, le consommateur va bénéficier de services à moindre prix qui sont mieux adaptés aux besoins du consommateur.

4.2.2 Mérites du fournisseur

Le fournisseur bénéficie de la perception des bénéfices du consommateur.

En particulier, le fournisseur peut construire des services dynamiques à la demande en offrant de nouveaux services de VPN et en téléchargeant les exigences de configuration de CE à CE des consommateurs.

De plus, une structure de VPN plus souple appliquée au réseau de couche 1 permet au fournisseur de faire un usage plus complet de ressources épargnées (c'est-à-dire, non utilisées précédemment) au sein du réseau. Cela pourrait être réalisé en appliquant un modèle de réseau où le fournisseur est responsable de la décision sur la façon dont les ressources sont utilisées et pour provisionner la connexion à travers le réseau de couche 1.

4.3 Scénarios de déploiement de L1VPN

Dans les grands réseaux de transporteurs qui fournissent des services de diverses sortes, il est fréquent que des réseaux multi services soient pris en charge sur un réseau de transport partagé. En appliquant des L1VPN, plusieurs réseaux de service internes (qui peuvent être gérés et fonctionner séparément) peuvent être pris en charge sur un réseau de transport partagé de couche 1 contrôlé et géré en utilisant GMPLS. De plus, les L1VPN peuvent prendre en charge des capacités d'offrir des services innovants aux clients externes.

Des scénarios de déploiement plus spécifiques sont décrits ci-après.

4.3.1 Cœur de réseau multi services

Un cœur de réseau multi services est caractérisé par le fait que chaque département de service d'un transporteur qui reçoit le service de L1VPN du transporteur fournit un service de couche supérieure d'une sorte différente. Le consommateur qui reçoit le service L1VPN (c'est-à-dire, chaque département de service) peut offrir ses propres services, dont les charges utiles peuvent être à n'importe quelle couche (par exemple, ATM, IP, MRT). Le réseau de transport de couche 1 et chaque service réseau appartient à la même organisation, mais peut être géré séparément. Du point de vue du fournisseur de service de L1VPN, ces services ne sont pas visibles et ne font pas partie du service de L1VPN. C'est-à-dire, le type de service transporté dans la charge utile de couche 1 n'est pas connu du fournisseur de service.

L'avantage est que les mêmes ressources de réseau de transport de couche 1 sont partagées par de multiples services. Un cœur de réseau à grande capacité (au plan des données) peut être constuit de façon économique en partageant les ressources entre plusieurs services généralement avec la souplesse pour modifier les topologies, tout en séparant les fonctions de contrôle pour chaque département de service. Donc, chaque consommateur peut choisir un ensemble spécifique de caractéristiques nécessaires pour fournir son propre service.

Noter qu'il est aussi possible de contrôler et gérer ces réseaux de service et le réseau de transport de couche 1 en utilisant GMPLS dans le modèle intégré [RFC3945] au lieu d'utiliser des L1VPN. Cependant, l'utilisation de L1VPN est bénéfique sur les points suivants :
- un espace d'adresses indépendant pour chacun des réseaux de service ;
- l'isolation du réseau (isolation des informations de topologie, isolation des fautes parmi les réseaux de service) ;
- vue indépendante des ressource de couche 1 pour chaque réseau de service ;
- politiques indépendantes qui pourraient être appliquées pour chacun des réseaux de service.

Ces points peuvent s'appliquer aux fonctions de plan de gestion aussi bien que de plan de contrôle.

4.3.2 Transporteur d'un transporteur

Un transporteur de transporteur est caractérisé par le fait qu'un transporteur qui reçoit un service L1VPN d'un autre transporteur fournit ses propres services. Dans ce scénario, deux transporteurs sont dans des organisations différentes. Il est donc supposé que les informations fournies aux points de démarcation de service sont plus limitées que dans le cas du cœur de réseau multi services. De même, moins de contrôle du service L1VPN est donné au point de démarcation de service. Par exemple, les consommateurs d'un service de L1VPN reçoivent :
- une vue plus limitée du réseau du fournisseur de service L1VPN,
- un contrôle plus limité sur le réseau du fournisseur de service L1VPN.

Un des mérites est que chaque transporteur peut se concentrer sur un service spécifique. Par exemple, le consommateur du service L1VPN peut se concentrer sur les services de couche 3, par exemple, pour fournir un accès sur à l'Internet, laissant le fournisseur de L1VPN se concentrer sur le service de couche 1, par exemple, en fournissant une large bande passante entre le villes. Le consommateur L1VPN peut construire son propre réseau en utilisant les ressources de couche 1 fournies par le fournisseur L1VPN, généralement avec de la souplesse pour modifier les topologies, tout en séparant les fonctions de contrôle pour chaque transporteur consommateur.

4.3.3 Compromis sur les ressouces de couche 1

En plus des scénarios où le fournisseur de service de second rang utilise un seul fournisseur de service de cœur comme mentionné au paragraphe 4.3.2, il est possible au fournisseur de second rang de recevoir des services de plus d'un fournisseur de service de cœur. Dans ce scénario, il y a quelques avantages pour le fournisseur de service de second rang comme la redondance de chemin et le choix dynamique du transporteur sur la base du prix. Le fournisseur de service de second rang peut prendre en charge une fonction qui permet un compromis sur les ressources de service de couche 1. En utilisant les informations de ressources publiées par ses fournisseurs de service de cœur, un fournisseur de service de second rang peut décider comment faire le meilleur usage des fournisseurs de cœur. Par exemple, si un fournisseur de service de cœur n'est plus capable de satisfaire les demandes de service, un autre fournisseur de service peut être utilisé. Ou le fournisseur de service de second rang pourrait choisir de répondre aux changements de prix d'un service au cours du temps.

Un autre exemple d'utilisation d'un fournisseur de service de second rang est de réduire l'exposition aux défaillances de chaque fournisseur (c'est-à-dire, d'améliorer la disponibilité).

4.3.4 L1VPN inter AS et inter SP

En plus des scénarios où une seule connexion entre deux CE est acheminée sur un seul fournisseur de service comme mentionné au paragraphe 4.3.2, il est possible qu'une connexion soit acheminée sur plusieurs AS au sein d'un fournisseur de service (appelé un L1VPN inter AS) ou sur plusieurs fournisseurs de service (appelé un L1VPN inter SP).

Le scénario de L1VPN inter AS peut être utilisé pour construire un seul L1VPN à partir de ressources réseau administrées par différents domaines d'un seul fournisseur de service. Ces domaines administratifs pourraient généralement ne pas avoir de relation de collaboration à la couche 1, et donc le L1VPN inter AS offre un nouveau modèle d'affaires pour la livraison conjointe de services à un consommateur. La considération des L1VPN inter AS requiert des analyses complémentaires qui sortent du domaine du présent document.

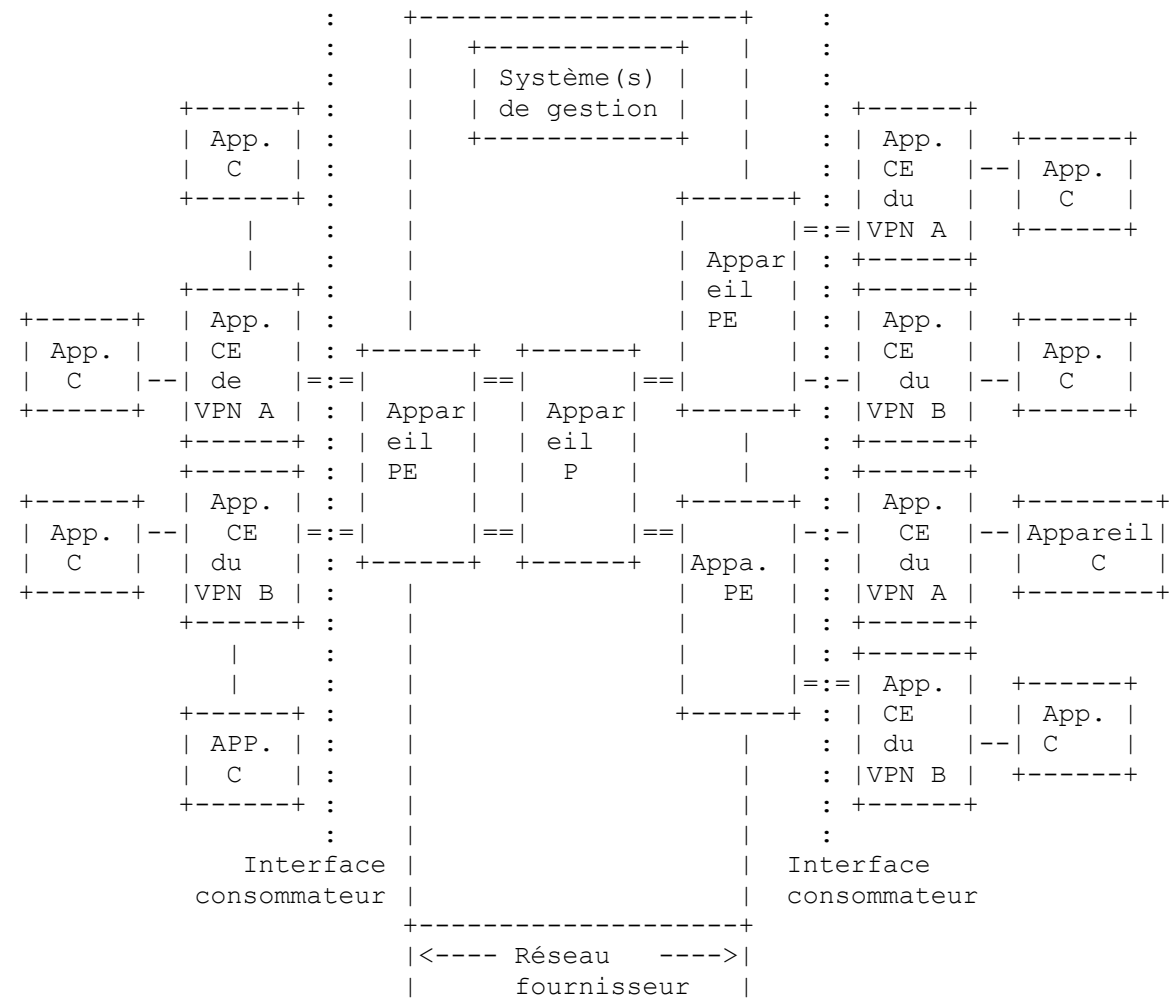
Le scénario inter SP peut être utilisé pour construire un seul L1VPN à partir de services fournis par plusieurs fournisseurs régionaux. Il pourrait y avoir diverses relations d'affaires parmi les fournisseurs et les consommateurs, et ce scénario contient plus de questions de gestion, de sécurité, de confidentialité et de politique commerciale que le cas plus simple de L1VPN inter AS. L'examen des L1VPN inter SP exige des analyses complémentaires qui sortent du cadre du présent document.

4.3.5 Service de programmation

Dans certains scénarios de déploiement, les consommateurs de services L1VPN peuvent souhaiter établir des connecxons de couche 1 non à la demande, mais à un instant programmé dans le futur. Ou, même quand les consommateurs de services L1VPN peuvent souhaiter utiliser des connexions de couche 1 à la demande, ils peuvent tolérer un certain délai, par exemple, à cause du manque de ressources à cet instant. Dans ces scénarios, le fournisseur peut réserver de la bande passante à un instant spécifié dans le futur, et peut établir les connexions de VPN conformément à ce programme. Cela rend possible d'utiliser plus efficacement la bande passante dans le temps (c'est-à-dire, de prendre en charge plus de demandes). Ce service, le service programmé, peut être utilisé pour prendre en charge les consommateurs qui utilisent des connexions de couche 1 pour des applications de sauvegarde de données, d'applications de livraison de contenu, et d'autres applications. De plus, les consommateurs peuvent être capables de spécifier à l'avance quand libérer les connexions de couche 1. En examinant ces informations, le fournisseur peut être capable de mieux agencer la programmation, ce qui conduit à une utilisation encore plus efficace de la bande passante. Noter que programmer des service de L1VPN exige une gestion de ressources dans le temps, ce qui n'est pas bien considéré dans les protocoles GMPLS actuels et exige la prise en charge du plan de gestion. De plus, l'offre de service de programmation et de service à la demande sur la même infrastructure doit être faite avec prudence.

5. Modèle de référence

La Figure 5.1 décrit le modèle de référence L1VPN.



Légende : == connexion de couche 1 ; -- liaison

Figure 5.1 : Modèle de référence L1VPN

Dans un L1VPN, les connexions de couche 1 sont fournies entre les interfaces de plan de données des CE dans le même VPN. Dans la Figure 5.1, une connexion est fournie entre le CE de gauche du VPN A et le CE supérieur droit du VPN A, et

une autre connexion est fournie entre le CE de gauche du VPN B et le CE inférieur droit du VPN B (montré avec "="). Ces connexions de couche 1 sont appelées des connexions de VPN.

Noter que comme mentionné au paragraphe 3.1, ces connexions de VPN suivent la hiérarchie définie dans la [RFC4206].

5.1 Systèmes de gestion

Comme montré dans le modèle de référence, un réseau fournisseur peut contenir un ou plusieurs systèmes de gestion. Un système de gestion peut prendre en charge des fonctions incluant le provisionnement, la surveillance, la facturation, et l'enregistrement. Les systèmes de gestion fournisseurs peuvent aussi communiquer avec les systèmes de gestion de consommateur afin de fournir des services. Les Sections 7 et 11 donnent plus de détails.

6. Description de service générique

Cette Section décrit les services génériques de L1VPN. Des descriptions détaillées sont fournies dans les modèles de service spécifiques à la Section 7.

6.1 Construction de CE

- L'appareil CE peut prendre en charge plus d'un VPN consommateur.
- Les liaisons de plan des données CE-PE (entre interfaces de plan des données) peuvent être partagées par plusieurs VPN.

Noter qu'il est nécessaire de préciser les mesages de plan de contrôle échangés entre CE et PE si la relation CE-PE est applicable à plus d'un VPN. Cela rend possible de déterminer à quel VPN ces mesages de plan de contrôle s'appliquent. Une telle précision peut être réalisée en allouant un canal de contrôle séparé à chaque VPN (en utilisant un canal physique séparé, un canal logique séparé comme un tunnel IP, ou en utilisant un adressage séparé).

Un domaine d'adressage de consommateur consiste en adresses de liaison TE de CE à PE et en adresses de canal de contrôle de CE à PE ainsi que des adresses de site de consommateur (adresses C et CE). Les domaines d'adressage de consommateur peuvent se chevaucher, et peuvent aussi chevaucher le domaine d'adressage du fournisseur de service.

Des NAT ou pare-feu pourraient raisonnablement être placés aux interfaces consommateurs, ou entre des domaines administratifs au sein du réseau cœur. L'adressage dans le modèle L1VPN doit traiter de telles éventualités. La traversée des NAT et pare-feu au sein du réseau consommateur pourrait avoir des implications pour les services de L1VPN qui connectent les appareils C, et fera l'objet d'études ultérieures.

6.2 Caractéristiques de service générique

Le L1VPN a les deux caractéristiques de service génériques suivantes :

- Restriction de connexité : la connexité de couche 1 est fournie à un ensemble limité d'interfaces de plan des données de CE, appelés des points d'extrémité de VPN. (Cet ensemble forme les membres du L1VPN.)
- Contrôle et gestion par VPN : un certain niveau de capacités de contrôle et de gestion est fourni au consommateur. Les détails diffèrent selon les modèles de service décrits à la Section 7.

7. Modèles de service

Cette Section décrit les modèles de service des VPN de couche 1 qui peuvent être pris en charge par les réseaux qui acceptent les protocoles GMPLS. Ces modèles sont dérivés de la description de service générique présentée ci-dessus.

De tels réseaux de couche 1 sont gérés et contrôlés en utilisant la signalisation GMPLS décrite dans les [RFC3471] et [RFC3473], et l'acheminement GMPLS décrit dans la [RFC4202]. On doit comprendre que satisfaire les exigences établies dans le présent document peut nécessiter des extensions aux protocole GMPLS existants pour le plan de contrôle au sein du réseau de couche 1 et pour le provisionnement de service à la bordure du réseau (appareils CE et PE). Un CE et un PE sont connectés par une ou plusieurs liaisons de données. Les extrémités de chaque liaison sont généralement représentées comme des interfaces à capacité GMPLS.

Noter que dans le présent document, les modèles de service sont classés par le sens des informations échangées sur l'interface de consommateur. L'interface de consommateur peut être instanciée par la communication du plan de contrôle

CE-PE et/ou la communication du plan de gestion entre le ou les sytèmes de gestion de consommateur et le ou les systèmes de gestion de fournisseur. Noter que la façon de réaliser un canal de contrôle CE-PE est discutée au paragraphe 10.1. Le ou les systèmes de gestion de consommateur et le ou les systèmes de gestion de fournisseur peuvent communiquer en utilisant le ou les canaux de contrôle CE-PE.

7.1 Modèle de service fondé sur la gestion

La Figure 7.1 décrit le modèle de service fondé sur la gestion.

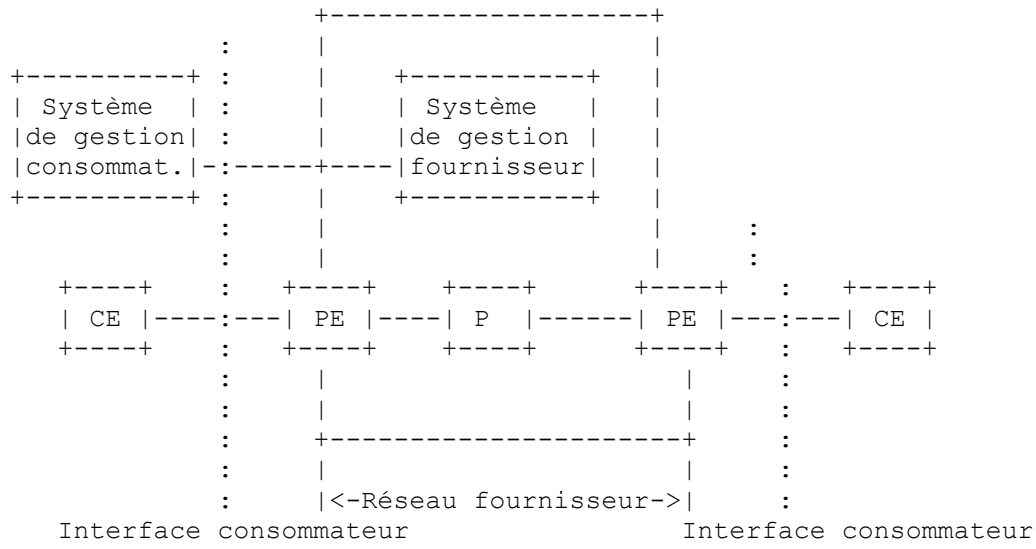


Figure 7.1 : Modèle de service fondé sur la gestion

Dans ce modèle de service, les systèmes de gestion consommateur et les systèmes de gestion fournisseur communiquent l'un avec l'autre. Les systèmes de gestion consommateur accèdent aux systèmes de gestion fournisseur pour demander l'établissement/suppression d'une connexion de couche 1 entre une paire de CE. Les systèmes de gestion consommateur peuvent obtenir, des systèmes de gestion fournisseur, des informations supplémentaires, comme des informations de disponibilité de ressources et des informations de surveillance. Il n'y a pas d'échange de messages de contrôle entre un CE et un PE.

Le réseau fournisseur peut être fondé sur GMPLS. Dans ce cas, des mécanismes pour prendre en charge les connexions permanentes logicielles peuvent être appliqués. Cependant, les interfaces entre les systèmes de gestion ne sont pas étudiées par le présent document.

7.2 Modèle de service fondé sur la signalisation (modèle de base)

Dans ce modèle de service, le répertoire fonctionnel des interfaces CE-PE est limité à la seule signalisation d'établissement de chemin. Le réseau du fournisseur n'est pas impliqué dans la distribution des informations d'acheminement du réseau consommateur.

Noter de plus qu'il peut y avoir une communication entre les systèmes de gestion de consommateur et les systèmes de gestion de fournisseur afin de fournir aux consommateurs une surveillance détaillée, des informations sur les fautes, etc.

7.2.1 Modèle de service en recouvrement

La Figure 7.2 décrit le modèle de service en recouvrement.

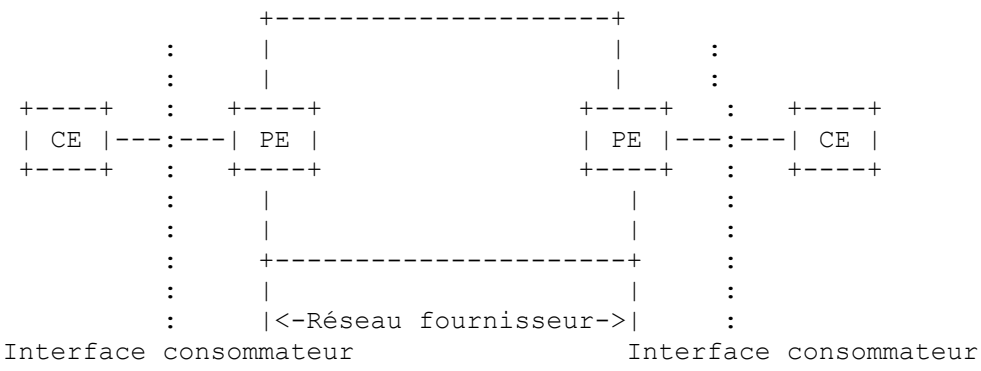


Figure 7.2 : Modèle de service en recouvrement

Dans ce modèle de service, l'interface de consommateur se fonde sur le recouvrement d'UNI GMPLS [RFC4208]. Le CE demande l'établissement/suppression de connexion de couche 1 à un CE distant. Aucun protocole d'acheminement ne fonctionne (c'est-à-dire, il n'y a pas de relation d'acheminement de voisin/homologue) entre un CE et un PE. Le CE ne reçoit pas d'informations d'acheminement des sites de consommateur distants, ni d'informations d'acheminement sur le réseau fournisseur.

Une adresse publique ou privée peut être allouée à l'interface de CE, qui désigne les points d'extrémité de VPN.

Dans ce modèle, les informations de membres doivent être configurées sur les PE, afin qu'ils reçoivent un message Path provenant du CE d'entrée qui puisse identifier le PE distant connecté au CE de sortie. La distribution des informations sur les membres entre les PE est normalement faite par le fournisseur, et peut être réalisée par des mécanismes tels que le provisionnement statique, ou par portage par le protocole d'acheminement (auto-découverte).

Il y a plusieurs façon pour que les consommateurs perçoivent le réseau fournisseur. Dans un exemple, le réseau fournisseur entier peut être considéré comme un nœud -- le chemin spécifié et enregistré dans les messages de signalisation le reflète. Noter que ceci est distinct du modèle de service de nœud virtuel décrit au paragraphe 7.3.2 parce que ce modèle exige que le réseau soit représenté aux sites de VPN comme un nœud virtuel -- c'est-à-dire qu'une forme d'annonce d'acheminement est impliquée, et ceci sort du domaine du modèle de service fondé sur la signalisation.

7.3 Modèle de service de signalisation et d'acheminement (mode amélioré)

Dans ce modèle de service, l'interface CE-PE fournit les capacités de signalisation comme dans le modèle de base, et permet de plus un échange limité d'informations entre les plans de contrôle du fournisseur et du consommateur pour faciliter des fonctions telles que la découverte des informations d'acheminement du réseau consommateur (c'est-à-dire, les informations d'accessibilité ou de TE dans les sites de consommateur distants) ou des paramètres de la partie du réseau du fournisseur dédiée au consommateur.

En permettant aux CE d'obtenir les informations d'acheminement du réseau consommateur, un problème dit d'acheminement N au carré pourrait être résolu.

En plus, en utilisant les informations d'acheminement reçues fondées sur l'ingénierie du trafic, un consommateur peut utiliser les capacités d'ingénierie du trafic. Par exemple, un consommateur peut établir deux connexions disjointes entre une paire de CE. Un autre exemple est qu'un consommateur peut demander une connexion entre une paire d'appareils au sein des sites de consommateur, et pas nécessairement entre des CE, avec une ingénierie du traffic plus efficace.

À ce titre, l'interface de consommateur se fonde sur la signalisation et les mécanismes de GMPLS pour échanger les informations d'accessibilité/TE. Normalement, un protocole d'acheminement est utilisé entre un CE et un PE, ou plus précisément entre un CE et le contexte d'acheminement de VPN instancié sur le PE. Les informations d'acheminement d'état de liaison vont être nécessaires pour mettre en œuvre les deux exemples de scénarios ci-dessus. Certains scénarios peuvent être satisfaits avec les seules informations d'acheminement d'accessibilité.

Noter que ce modèle de service n'empêche pas l'utilisation de mécanismes autres que de protocole d'acheminement pour échanger les informations d'accessibilité/TE.

Comme avec le modèle de service fondé sur la signalisation, il peut y avoir une communication entre le ou les systèmes de gestion de consommateur et le ou les systèmes de gestion de fournisseur afin de fournir une surveillance détaillée, des informations sur les fautes, etc., aux consommateurs.

Quatre types spécifiques de modèle de service de signalisation et d'acheminement sont le modèle de service d'extension de recouvrement, le modèle de service de nœud virtuel, le modèle de service de liaison virtuelle et le modèle de service d'homologue par VPN, selon la façon dont les consommateurs perçoivent le réseau fournisseur dans l'acheminement et la signalisation (c'est-à-dire, le niveau de détail des informations qu'il est permis à un consommateur de recevoir dans l'acheminement et la signalisation).

7.3.1 Modèle de service d'extension de recouvrement

Le présent modèle de service complète le modèle de service de recouvrement. Dans ce modèle de service, un CE reçoit une liste des adresses de liaison TE CE-PE auxquelles il peut demander une connexion de VPN (c'est-à-dire, des informations de membre). Cela peut inclure des informations supplémentaires concernant ces liaisons TE (par exemple, le type de commutation). Des mécanismes autres que d'acheminement pourraient être utilisés pour échanger les informations d'accessibilité/TE entre le CE et le PE.

7.3.2 Modèle de service de nœud virtuel

La Figure 7.3 décrit le modèle de service de nœud virtuel.

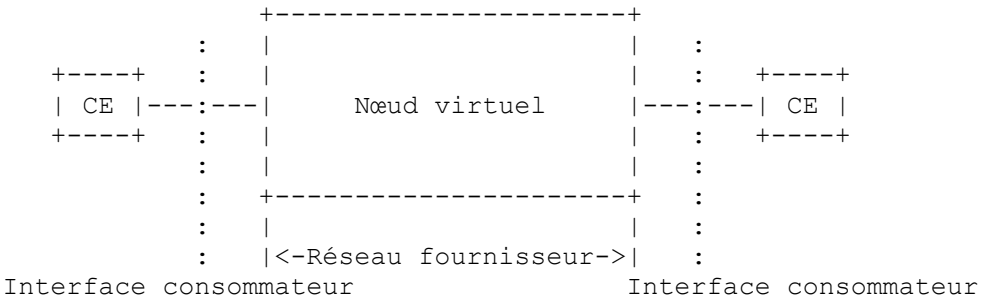


Figure 7.3: Virtual Node Service Model

Dans ce type de modèle de service, le réseau fournisseur entier est représenté comme un nœud virtuel (défini à la Section 2). Le consommateur perçoit le réseau fournisseur comme un seul nœud. Le CE reçoit les informations d'acheminement sur les liaisons CE-PE et le réseau consommateur (c'est-à-dire, les sites de consommateurs distants).

Noter que dans ce modèle de service, il doit y aroir un seul nœud virtuel, et ce nœud virtuel doit être connecté à chaque CE dans le VPN.

7.3.3 Modèle de service de liaison virtuelle

La Figure 7.4 décrit le modèle de service de liaison virtuelle.

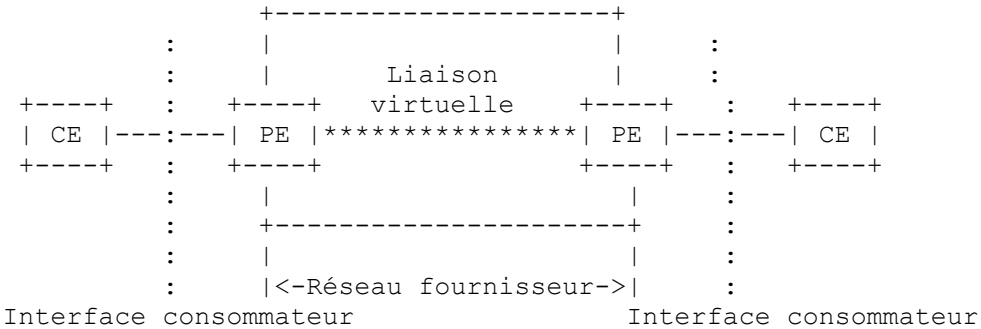


Figure 7.4 : Modèle de service de liaison virtuelle

Dans ce modèle de service, une liaison virtuelle est construite entre les PE. Pour la définition d'une liaison virtuelle, voir la terminologie à la Section 2. Une liaison virtuelle est allouée à chaque VPN et communiquée aux CE correspondants. À ce titre, le CE reçoit les informations d'acheminement sur les liaisons CE-PE, le réseau consommateur (c'est-à-dire, les sites de consommateurs distants) ainsi que les liaisons virtuelles allouées à chaque VPN. Une propriété particulière des liaisons virtuelles utilisées dans ce modèle de service est que le réseau fournisseur alloue des ressources de liaison de plan des données pour l'usage exclusif de chaque liaison virtuelle. Les attributs TE d'une liaison virtuelle sont déterminés en accord avec les ressources de liaison de plan de données allouées à cette liaison virtuelle. Les liaisons virtuelles sont une abstraction du réseau fournisseur aux consommateurs pour des besoins administratifs autant que pour exclure des informations "non nécessaires".

Noter que dans ce modèle de service, les deux points d'extrémité de chaque liaison virtuelle doivent être un appareil PE.

7.3.4 Modèle de service d'homologue par VPN

La Figure 7.5 décrit le modèle de service d'homologue par VPN.

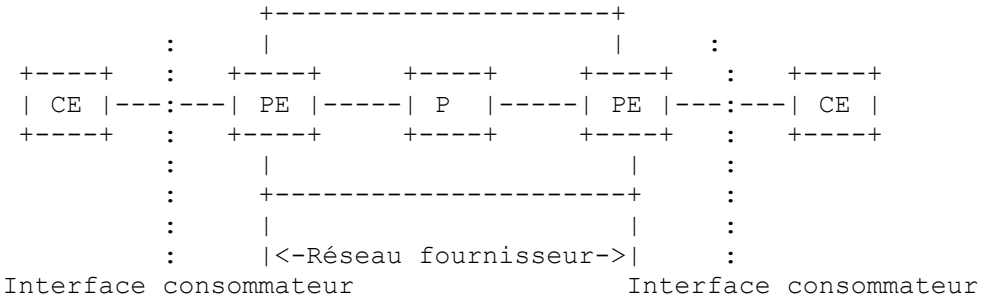


Figure 7.5 : Modèle de service d'homologue par VPN

Ce modèle de service est une généralisation et une combinaison du modèle de service de liaison virtuelle et du modèle de service de nœud virtuel mentionnés respectivement aux paragraphes 7.3.2 et 7.3.3.

Dans ce modèle de service, le fournisseur partage les liaisons TE au sein du réseau fournisseur par VPN, et divulgue les informations de liaison TE par VPN aux CE correspondants. À ce titre, un CE reçoit les informations d'acheminement sur les liaisons CE-PE, le réseau consommateur (c'est-à-dire, les sites de consommateur distants) ainsi que sur les portions partagées du réseau fournisseur.

Noter que les PE peuvent annoncer aux CE des informations d'acheminement abstraites sur le réseau fournisseur pour des besoins administratifs ainsi que pour exclure des "informations non nécessaires". En d'autres termes, des liaisons virtuelles peuvent être construites entre deux nœuds lorsque de liaisons de données directes n'existent pas, ou des nœuds virtuels peuvent être construits pour représenter plusieurs nœuds et les liaisons physiques entre eux

Dans le modèle de service d'homologue par VPN, au moins un nœud virtuel correspondant aux appareils P (un seul P ou un ensemble de P) doit être visible aux consommateurs.

8. Modèles de service et exigences de service

Les modèles de service mentionnés à la Section 7 se rapportent aux informations échangées entre CE et PE. De plus, les modèles de service diffèrent quant aux ressources de plan des données allouées pour chaque VPN.

Noter que dans les documents de l'UIT-T, le terme de" plan U" est utilisé à la place de "plan des données".

- Allocation de ressources au plan des données : partagées ou dédiées. Partagé signifie que les liaisons du plan des données du réseau fournisseur sont partagées par plusieurs VPN (c'est-à-dire, n'importe lequel, ou un ensemble spécifique de VPN). (Les liaisons du plan des données sont allouées dynamiquement à un VPN quand une connexion de VPN est demandée, et les liaisons de plan des données allouées à un VPN à un moment donné peuvent être allouées à un autre VPN à un autre moment.) Des moyens dédiés signifient que les liaisons de plan des données du réseau fournisseur sont partagées entre les VPN. (Les liaisons de plan des données sont allouées statiquement à un VPN et ne peuvent pas être utilisées par d'autre VPN.)

o Informations échangées entre CE et PE :
Signalisation :
- Informations sur les membres (incluent facultativement les information de TE des liaisons TE CE-PE associées)
- Informations d'acheminement de réseau consommateur (accessibilité seule, ou peuvent inclure des informations de TE)
- Informations d'acheminement de réseau fournisseur (informations de TE).

Noter que les informations de gestion de liaison (par exemple, LMP [RFC4204]) peuvent être échangées entre un CE et un PE, mais ceci est orthogonal à la définition des modèles de service.

Le tableau 1 montre la combinaison des exigences de service et des modèles de service.

	Plan de données partagé	**Plan de données dédié**
Signalisation	Recouvrement	Recouvrement
Signalisation + informations de membres	Extension de recouvrement	Extension de recouvrement
Signalisation + informations de membres + informations d'acheminement de réseau consommateur	Nœud virtuel	Nœud virtuel
Signalisation + informations de membres + informations d'acheminement de réseau consommateur + informations d'acheminement de réseau fournisseur	Non applicable	Liaison virtuelle d'homologue par VPN

Tableau 1 : Combinaison des exigences de service et des modèles de service

Comme décrit dans les paragraphes précédents, la différence entre les modèles de service de liaison virtuelle et d'homologue par VPN est si les consommateurs ont la visibilité des appareils P. Dans le modèle de service de liaison viruelle, les points d'extrémité des liaisons virtuelles doivent être des appareils PE, donc les appareils P ne sont pas visibles aux consommateurs. Dans le modèle de service d'homologue par VPN, au moins un nœud virtuel correspondant aux appareils P (un seul P, ou un ensemble de P) est visible aux consommateurs.

Noter que quand les consommateurs reçoivent des informations d'acheminement de réseau fournisseur sous la forme d'une liaison virtuelle, les consommateurs doivent être capables de spécifier de telles liaisons pour une connexion de VPN sur le réseau fournisseur dans la signalisation.

8.1 Exigences détaillées de niveau de service

En plus des exigences mentionnées dans le tableau 1, des exigences de service plus détaillées sont fournies ci-dessous. Elles sont généralement communes aux divers modèles de service, sauf quand c'est indiqué.

- Choix de la classe de service 1 : il PEUT être permis aux consommateurs de spécifier une classe de service de couche 1 (par exemple, niveau de disponibilité) pour une connexion de VPN. Plus de détails sont fournis à la Section 9.

- Réception d'informations de performances : il PEUT être permis aux consommateurs de recevoir des informations de performances pour leurs connexions de VPN (par exemple, des données de surveillance de performances). Quand des liaisons de plan des données sont dédiées, il PEUT être permis aux consommateurs de recevoir des informations de performances pour les liaisons qui leur sont dédiées.

- Réception d'informations de faute : il PEUT être permis aux consommateurs de recevoir des informations de fautes pour leurs connexions de VPN (par exemple, notification de défaillance par RSVP-TE, notification d'alarme du plan des données à travers le plan de gestion, notification des causes de rejet d'établissement de connexion). Noter que cela n'empêche pas les consommateurs d'utiliser des mécanismes de fonctionnement et de gestion (OAM, *Operations and Management*) pour, ou sur, leurs connexions de VPN. Quand des liaisons de plan des données sont dédiées, il PEUT être permis aux consommateurs de recevoir des informations de faute pour les liaisons qui leur sont dédiées.

- Réception d'informations de connexion : il PEUT être permis aux consommateurs de recevoir des informations pour les connexions de VPN en cours (par le plan de gestion).

- Réception d'information comptables : les consommateurs DOIVENT être capables de recevoir des informations de comptabilité pour chaque VPN.

- Spécification de politique : il PEUT être permis aux consommateurs de spécifier des politiques (par exemple, des politiques de calcul de chemin, des politiques de récupération incluant des paramètres) pour chaque VPN.

- Sécurité : la communication entre le consommateur et le fournisseur DOIT être sûre. Plus de détails sont donnés à la Section 12.

- Filtrage : des informations inutiles (par exemple, des information concernant d'autres VPN) NE DOIVENT PAS être fournies à chaque consommateur. Cela s'applique particulièrement au modèle de service de signalisation et d'acheminement, mais est aussi pertinent pour le modèle de service fondé sur la signalisation et le modèle de service fondé sur la gestion. Plus de détails sont décrits à la Section 12.

9. Aspects de récupération

9.1 Portée de récupération

GMPLS fournit diverses techniques de récupération à utiliser dans différents scénarios de récupération [RFC4427]. Le réseau fournisseur peut appliquer ces techniques de récupération pour protéger les connexions de VPN au titre du service L1VPN, par exemple comme suit :

o Récupération de PE à PE : le réseau fournisseur constitue un domaine de récupération, et la portée de récupération est la partie PE-PE de la connexion CE-CE de VPN. Il devrait être possible au réseau fournisseur de cacher l'opération de récupération du réseau fournisseur au consommateur. À savoir qu'il devrait être possible de configurer le réseau fournisseur à ne pas notifier au consommateur quand une défaillance se produit et à une opération de récupération de PE-PE de réparer avec succès la défaillance. De plus, quand la récupération de PE-PE échoue et que la défaillance devrait être notifiée au consommateur, il devrait être possible que le réseau fournisseur cache sa topologie interne.

o Récupération de CE à PE : la portée de récupération est l'une des liaisons d'entrée et de sortie de CE à PE ou les deux de la connexion CE-CE de VPN.

o Récupération de CE à CE : la portée de récupération est la connexion CE à CE de VPN entière. Quand une défaillance doit être notifiée à un consommateur afin qu'il puisse initier l'opération de rcupération, il devrait être possible au réseau fournisseur de cacher sa topologie interne.

Ces schémas de récupération peuvent être appliqués combinés.

Il peut être permis aux consommateurs de spécifier le niveau de récupération désiré dans une demande d'établissement de connexion. De plus, il peut être permis au consommateur de spécifier le niveau de récupération désiré d'une façon qui ignore la technique de récupération (par exemple, quand l'opération de récupération n'exige pas de coopération entre le réseau fournisseur et le réseau consommateur). Dans ce cas, le réseau fournisseur doit traduire le niveau de récupération spécifié en des techniques de récupération spécifiques, sur la base des politiques de fonctionnement. Cela permet des techniques de récupération améliorées au dessus et au delà des spécifications GMPLS à utiliser dans le réseau fournisseur.

9.2 Schémas de partage de ressource de récupération

Le réseau fournisseur peut prendre en charge divers schémas de partage de ressources de récupération, comme les suivantes :

o Récupération partagée : quand le réseau fournisseur prend en charge la récupération partagée (par exemple, restauration de maillage partagé [RFC4427]) le réseau fournisseur peut fournir des ressources de restautation partagées entre les connexions de VPN qui serveent seulement le même VPN, un ensemble spécifique de VPN, ou tous les VPN. Le mode par défaut est le partage des ressources de récupération avec tous les VPN.

o Extra traffic : les mécanismes de récupération de GMPLS prennent en charge le trafic supplémentaire. Le trafic supplémentaire permet le transfert du trafic préemptable sur les ressources de récupération quand ces ressources ne sont pas utilisées pour la récupération de trafic protégé normal [RFC4427].

Dans le contexte des L1VPN le trafic supplémentaire est appliqué pour les connexions CE-CE de VPN, ou la partie PE-PE des connexions CE-CE de VPN. Ce dernier cas ne peut être appliqué que quand il y a une hiérarchie (c'est-à-dire, quand la connexion CE-CE de VPN est incorporée au dessus de la connexion PE-PE). Dans ce paragraphe, ce dernier aspect est analysé.

Quand le réseau fournisseur permet qu'une connexion CE-CE de VPN soit établie comme "extra traffic", cela signifie que la connexion de VPN peut utiliser une connexion PE-PE qui protège une autre connexion CE-CE de VPN. Dans ce cas, le

réseau fournisseur peut restreindre le trafic CE-CE de connexion de VPN à utiliser des ressources (c'est-à-dire, les connexions PE-PE) qui :
- protègent les connexions de VPN du même VPN comme la connexion de trafic supplémentaire,
- sont utilisées pour un ensemble spécifique de VPN,
- sont disponibles pour tout VPN.

Le mode par défaut est de prendre en charge le trafic préemptable sur les ressource de récupération réservéees pour tout VPN.

10. Connexité de plan de contrôle

10.1 Connexité de plan de contrôle entre un CE et un PE

Dans le modèle de service fondé sur la signalisation et le modèle de service de signalisation et acheminement, il doit y avoir un canal de contrôle (connexité de niveau IP) entre un CE et son PE. L'instanciation du canal de contrôle peut être différente selon l'adressage et la sécurité.

Comme mentionné au paragraphe 6.1, il est nécessaire de préciser les messages de plan de contrôle échangés entre le CE et le PE si la relation CE-PE est applicable à plus d'un VPN. De plus, des adresses privées peuvent être allouées aux canaux de contrôle CE-PE.

Les aspects de sécurité du canal de contrôle CE-PE sont discutés à la Section 12.

10.2 Connexité de plan de contrôle entre CE

Un réseau consommateur connecté par des connexions de VPN peut être contrôlé par MPLS ou GMPLS, et les connexions de VPN peuvent être traitées comme des liaisons TE au sein du réseau consommateur. Dans ce cas, il doit y avoir connexité du plan de contrôle (niveau IP) entre les CE, afin que les messages de contrôle, comme les messages de signalisation et d'acheminement, puissent être échangés entre les CE. De plus, dans certaines techniques de récupération, un échange de messages Notify est nécessaire entre l'entrée et la sortie de la connexion de VPN, ce qui exige la connexité de plan de contrôle entre les CE. Il y a potentiellement plusieurs façon de faire cela :

- Utilisation de connexions de VPN comme canaux de contrôle dans la bande : si les CE sont capables d'injecter des messages de contrôle dans les connexions de VPN et d'extraire les messages à l'extrémité distante des connexions de VPN, des messages de contrôle peuvent alors être échangés dans la bande. Par exemple, quand une connexion de VPN est une liaison TE à capacité de commutation de paquet (PSC, *Packet Switch Capable*) dans le réseau consommateur, cette opération est transparente au fournisseur de service L1VPN.

- Utilisation des frais généraux associés aux connexions de VPN : si la connexion de VPN assure la connexité dans le réseau consommateur à une capacité de commutation différente (impliquant une couche de technologie réseau) de celle utilisée par le réseau fournisseur pour prendre en charge la connexité CE-PE et PE-PE, alors le réseau consommateur peut utiliser tous les frais généraux disponibles au sein de la connexion de VPN comme canal de contrôle pour connecter les CE. Par exemple, si une connexion de VPN fournit une liaison TE MRT dans le réseau consommateur mais est prise en charge par une technologie telle que lambda ou de fibre, alors les CE peuvent utiliser les frais généraux (DCC, *data control channel*) comme canal de contrôle, si le réseau prend en charge le transfert transparent de ces frais généraux. Cette opération est transparente au fournisseur de service L1VPN.

- Utilisation de connexions de VPN spécifiques du canal de contrôle : un consommateur établit des connexions de VPN dédiées comme canaux de contrôle. Cette opération est transparente au fournisseur de service L1VPN, mais comme le trafic de plan de contrôle va probablement être relativement faible comparé à la capacité des connexions de VPN, ce peut être une solution coûteuse pour le consommateur.

- Utilisation d'un réseau séparé : un consommateur peut utiliser un autre réseau et service réseau, comme un service de lignes privées, un service L3VPN, un service L2VPN, ou un service d'accès Internet, pour établir la connexité de canal de contrôle CE-CE. Cette opération est transparente pour le fournisseur de service L1VPN.

- Utilisation de canaux de contrôle CE-PE : dans le modèle de service fondé sur la signalisation, et le modèle de service de sigalisation et acheminement, il doit y avoir connexité de plan de contrôle (au niveau IP) entre le CE et le PE, comme décrit au paragraphe 10.1.

En utilisant cela, l'échange de message de contrôle CE-CE pourrait être réalisé au titre du service fourni par le fournisseur de service L1VPN. À savoir que le réseau fournisseur transfère les messages de contrôle reçus sur le canal de contrôle CE-PE à l'autre côté du réseau fournisseur et les livre à travers le canal de contrôle PE-CE. La réalisation de cela dans le réseau fournisseur relève de l'opérateur, mais lorsque le réseau fournisseur utilise un plan de contrôle GMPLS, les messages du plan de contrôle du consommateur pourraient être transmis à travers le plan de contrôle du fournisseur, peut-être en utilisant des tunnels IP.

Il faut faire attention à protéger le réseau fournisseur et les autres consommateurs des attaques de déni de service (DoS, *Denial of Service*). La saturation du trafic sur le plan de contrôle réseau doit aussi être gérée avec soin. Noter que si des adresses privées sont allouées aux canaux de contrôle CE-PE, le réseau fournisseur doit prendre ene charge l'acheminement et la transmission de portée VPN des messages de contrôle.

11. Considérations de gestion

Les considérations de gestion pour GMPLS sont décrites dans les documents existants, comme la [RFC3945]. Aussi, les considérations de gestion pour L3VPN sont décrites dans les documents existants, comme la [RFC4176]. Ces considérations de gestion devraient aussi être appliquées dans les L1VPN, et ces aspects sont décrits dans cette section. De plus, il y a des considérations de gestion spécifiques des L1VPN, comme de configuration et de comptabilité.

- Gestion des fautes : le réseau fournisseur DOIT prendre en charge la gestion des fautes. Il DOIT prendre en charge la détection de vie, et la surveillance et la vérification du fonctionnement correct. Quand une défaillance survient, le réseau fournisseur DEVRAIT corréler la défaillance. Aussi, il DEVRAIT être capable de détecter quel consommateur est affecté par la défaillance. Si le réseau fournisseur peut résoudre des défaillances sans intervention du réseau consommateur, il DOIT être possible de configurer le réseau fournisseur à ne pas faire rapport des défaillances aux consommateurs. Cependant, il PEUT faire partie d'un accord entre un consommateur et fournisseur que les défaillances soient néanmoins rapportées au consommateur.

- Gestion de configuration : le réseau fournisseur DOIT prendre en charge la gestion de configuration, comme ce qui suit :
  - mode/modèle de configuration de service ;
  - configuration de représentation de réseau : configuration de nœud virtuel et de liaison virtuelle ;
  - configuration d'allocation de ressource : dédiée, partagée, voir les détails à la Section 8 ;
  - configuration de politique de récupération : par exemple, schémas de partage de ressource de récupération, comme la récupération partagée, le trafic supplémentaire, voir les détails à la Section 9 ;
  - configuration des membres ;
  - configuration de niveau réseau/élément : par exemple, configuration de liaison TE.

  Il DEVRAIT être possible au réseau fournisseur de vérifier que la configuration est faite correctement.

- Gestion de la comptabilité : le réseau fournisseur DOIT prendre en charge la gestion de la comptabilité. Il DOIT être capable d'enregistrer l'utilisation des connexions de VPN pour chaque consommateur.

- Gestion des performances : le réseau fournisseur DOIT prendre en charge la gestion des performances. En particulier, il DOIT prendre en charge la surveillance des performances des paramètres associés à l'accord de niveau de service (SLA, *Service Level Agreement*) comme le taux d'erreurs binaires par connexion de VPN, et la vérification du SLA. De plus, il DOIT prendre en charge la surveillance des performances et l'analyse des paramètres relatifs au réseau et aux équipments non directement associés au SLA, comme l'utilisation des ressources du réseau.

- Gestion de la sécurité : le réseau fournisseur DOIT prendre en charge la gestion de la sécurité. Voir les détails à la Section 12.

- Systèmes de gestion : afin de prendre en charge diverses fonctions de gestion, le réseau fournisseur s'appuie sur des systèmes de gestion et des outils en rapport. Les protocoles GMPLS et les extensions potentielles à GMPLS DOIVENT être capables de fonctionner avec des systèmes, et les outils qui s'y rapportent, pour fournir de telles fonctionnalités. En particulier, les modules de MIB pour les protocoles GMPLS et leurs extensions potentielles DOIVENT être pris en charge.

- Gestion des réseaux consommateurs : les consommateurs PEUVENT déléguer la gestion de leur réseau (en particulier les CE et les liaisons CE-CE) au réseau fournisseur. Dans ce cas, le fournisseur DOIT être capable de gérer le réseau consommateur, ainsi que le réseau fournisseur.

12. Considérations sur la sécurité

La sécurité est clairement une des exigences essentielles dans les L1VPN. Dans cette section sont soulignées les exigences clés pour la sécurité. Les considérations sur la sécurité des L3VPN et L2VPN sont décrites dans les documents existants, les [RFC4110], [RFC4111], et [RFC4664]. Ces considérations sur la sécurité devraient aussi être s'appliquer dans les L1VPN, et ces aspects sont décrits dans cette section. De plus, il y a quelques considérations sur la sécurité spécifiques des L1VPN, comme la restriction de connexité et les liaisons à contrôle partagé.

Cette section décrit d'abord les types d'informations à sécuriser. Ensuite sont décrites les caractéristiques ou aspects de sécurité. Finalement on décrit les considérations concernant les scénarios où des mécanismes de sécurité sont appliqués.

12.1 Types d'informations

Il DOIT être possible de sécuriser les informations échangées entre le consommateur et le fournisseur. Cela inclut des informations de plan des données, de plan de contrôle, et du plan de gestion.

À la couche 1, les informations de plan des données sont normalement supposées être sécurisées une fois que les connexions sont établies, car ces connexions sont dédiées à chaque VPN. C'est-à-dire, il n'est pas possible de communiquer si il n'y a pas de connexion. Donc, dans les L1VPN, le principal souci de sécurité du plan des données est de restreindre les connexions de VPN à n'être utilisées que dans le même VPN, comme décrit au paragraphe 6.2. Noter qu'un consommateur peut souhaiter assurer la sécurité des informations de plan des données contre non seulement les autres consommateurs, mais aussi le fournisseur. Dans ce cas, le consommateur peut souhaiter appliquer ses propres mécanismes de sécurité pour les informations de plan des données (sécurité de CE à CE) comme on le décrit plus loin.

De plus, les informations contenues dans le réseau fournisseur DOIVENT être sécurisées. Cela inclut des informations de contrat de service de VPN, des informations courantes de connexion de VPN, des informations sur les membres du VPN, et des informations de système. Noter que ces types d'informations PEUVENT être accessibles aux entités autorisées.

12.2 Caractéristiques de sécurité

Les caractéristiques de sécurité incluent ce qui suit :

- Intégrité des données : les informations échangées entre le consommateur et le fournisseur DOIVENT être livrées inchangées.

- Confidentialité : les informations échangées entre le consommateur et le fournisseur NE DOIVENT PAS être divulguées à un tiers.

- Authentification : l'entité qui demande le service au fournisseur DOIT être identifiée et avoir son identité authentifiée, et le fournisseur du service DOIT aussi être identifié et avoir son identiré authentifiée.

- Contrôle d'accès : l'accès aux informations contenues dans le réseau fournisseur, qui peuvent être des informations sur les réseaux consommateurs ou l'existence des consommateurs, ainsi que sur le réseau fournisseur, DOIVENT être restreintes à l'entité autorisée.

- Détection et protection contre les attaques de déni de service : le réseau fournisseur DOIT avoir des mécanismes pour détecter les attaques de déni de service et pour protéger contre elles de façon réactive et proactive.

12.3 Scénarios

Il y a deux scénarios (ou occasions) dans lesquelles les mécanismes de sécurité sont appliqués. Un est la phase de contrat de service, où les mécanismes de sécurité sont appliqués une fois. L'autre est la phasee d'accès au service, où les mécanismes de sécurité sont appliqués chaque fois que le service est demandé.

- Scénario de contrat de service (statique) : ce scénario inclut l'ajout de nouveaux appareils physiques, comme des appareils CE, des liaisons de données et des liaisons de contrôle. Il DOIT être garanti que ces appareils physiques sont connectés à la bonne entité. De plus, l'autorité pour accéder à des informations spécifique PEUT être donnée à chaque consommateur au titre du contrat de service.

- Scénario d'accès de service (dynamique) : ce scénario inclut la réception des demandes de connexion, des demandes d'échange d'informations d'acheminement (par exemple, des tentatives d'établir une relation de voisinage dans le protocole d'acheminement, ou une demande de commande via l'interface de plan de gestion) et des demandes de restitution d'informations de gestion. Si un canal de communication entre le consommateur et le fournisseur (canal de contrôle, interface de gestion) est physiquement séparé par consommateur, et si l'entité connectée sur ce canal de communication est identifiée dans la phase de contrat de service, le fournisseur peut s'assurer de qui demande le service. Aussi, le canal de communication pourrait être considéré comme sûr. Cependant, quand le canal de communication est physiquement partagé parmi les consommateurs, des mécanismes de sécurité DOIVENT être disponibles et DEVRAIENT être appliqués. Des exemples de ces mécanismes de sécurité incluent IPsec [RFC4302] et [RFC4303]. Noter que même dans le cas de canaux de communication physiquement séparés, les consommateurs peuvent souhaiter appliquer des mécanismes de sécurité pour assurer une plus forte sécurité, et de tels mécanismes DOIVENT être disponibles.

Quand l'entité qui demande le service est identifiée, le fournisseur DOIT s'assurer que la demande est autorisée pour cette entité. Cela inclut de s'assurer que la demande de connexion est entre les points d'extrémité de VPN qui appartiennent au même VPN.

Noter aussi que les consommateurs peuvent souhaiter appliquer leurs propres mécanismes de sécurité pour les informations de plan des données (sécurité de CE à CE). Cela inclut IPsec [RFC4302] et [RFC4303] pour le trafic IP.

13. Remerciements

Les matériaux de ce document se trouvent dans les travaux du groupe d'étude 13 de l'UIT-T. Merci à Dimitri Papadimitriou, Deborah Brungard, Yakov Rekhter, Alex Zinin, Igor Bryskin, Adrian Farrel, et Ross Callon de leurs utiles commentaires et suggestions. Merci à Mark Townsley, Dan Romascanu, et Cullen Jennings de leurs utiles apports durant la revue de l'IESG.

14. Contributeurs

Les fondements de ce document se trouvent dans les travaux du groupe d'études 13 de l'UIT-T, question 11. Le SG13/Q11 a investigué les exigences et l'architecture de service pour les VPN de couche 1 pendant un certain temps, et la base du présent document est un sommaire et le développement des conclusions auxquelles il est arrivé. Sur la base de ces matériaux, l'IETF et le groupe de travail L1VPN en particulier, ont développé ce cadre et les exigences pour la prise en charge des L1VPN par l'utilisation des protocoles GMPLS.

Les détails de ce document sont le résultat des contributions de plusieurs auteurs mentionnés ici par ordre alphabétique. Les détails de contact pour ces auteurs se trouvent un peu plus loin vers la fin du document.

Raymond Aubin (Nortel)
Marco Carugi (Nortel)
Ichiro Inoue (NTT)
Hamid Ould-Brahim (Nortel)
Tomonori Takeda (NTT)

15. 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)

[RFC3031] E. Rosen, A. Viswanathan, R. Callon, "Architecture de commutation d'étiquettes multi protocoles", janvier 2001. *(P.S.)* (*MàJ par la* RFC6790)

[RFC3209] D. Awduche, et autres, "RSVP-TE : Extensions à RSVP pour les tunnels LSP", décembre 2001. (*Mise à jour par* RFC3936, RFC4420, RFC4874, RFC5151, RFC5420, RFC6790)

[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)

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

[RFC4026] L Andersson et T. Madsen, "Terminologie des réseaux privés virtuels (VPN) approvisionnés par le fournisseur", mars 2005.

[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.)*

[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.)*

[Y.1312] Recommandation UIT-T Y.1312, "Exigences génériques et éléments d'architecture de réseau privé virtuel de couche 1", septembre 2003, disponible à <http://www.itu.int>.

16. Références pour information

[RFC4110] R. Callon, M. Suzuki, "Cadre pour les réseaux privés virtuels approvisionnés par le fournisseur (PPVPN) de couche 3", juillet 2005. *(Information)*

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

[RFC4139] D. Papadimitriou et autres, "Exigences pour l'utilisation de la signalisation de MPLS généralisé (GMPLS) et extensions pour les réseaux optiques à commutation automatique (ASON)", juillet 2005. *(Information)*

[RFC4176] Y. El Mghazli et autres, "Cadre du fonctionnement et de la gestion de la couche 3 des réseaux privés virtuels (L3VPN)", octobre 2005. *(Information)*

[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.)*

[RFC4258] D. Brungard, éd., "Exigences pour l'acheminement de la commutation généralisée d'étiquettes multiprotocoles (GMPLS) pour les réseaux optiques à commutation automatique (ASON)", novembre 2005. *(Information)*

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

[RFC4303] S. Kent, "Encapsulation de charge utile de sécurité dans IP (ESP)", décembre 2005. (*Remplace* RFC2406) *(P.S.)*

[RFC4427] E. Mannie et autres, "Terminologie de récupération (protection et restauration) pour le protocole généralisé de commutation d'étiquettes multiprotocoles (GMPLS)", mars 2006. *(Information)*

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

[Y.1313] Recommandation UIT-T Y.1313, "Architectures de service et de réseau de réseau privé virtuel de couche 1", juillet 2004, disponible à <http://www.itu.int>.

Adresse des auteurs

Raymond Aubin
Nortel Networks
P O Box 3511 Station C
Ottawa, ON K1Y 4H7 Canada
téléphone : +1 (613) 763 2208
mél : aubin@nortel.com

Marco Carugi
Nortel Networks S.A.
Parc d'activites de Magny-Chateaufort
Les Jeunes Bois - MS CTF 32B5 - Chateaufort
78928 YVELINES Cedex 9 - FRANCE
téléphone : +33 1 6955 7027
mél : marco.carugi@nortel.com

Ichiro Inoue
NTT Laboratories, NTT Corporation
3-9-11, Midori-Cho
Musashino-Shi, Tokyo 180-8585 Japan
téléphone : +81 422 59 6076
mél : inoue.ichiro@lab.ntt.co.jp

Hamid Ould-Brahim
Nortel Networks
P O Box 3511 Station C
Ottawa, ON K1Y 4H7 Canada
téléphone : +1 (613) 765 3418
mél : hbrahim@nortel.com

Tomonori Takeda
NTT Laboratories, NTT Corporation
3-9-11, Midori-Cho
Musashino-Shi, Tokyo 180-8585 Japan
téléphone : +81 422 59 7434
mél : takeda.tomonori@lab.ntt.co.jp

Déclaration complète de droits de reproduction

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