Architecture des réseaux d'opérateurs

Les opérateurs ont pour objectif de satisfaire les besoins de leurs clients en matière de réseau. C'est la raison pour laquelle leur première tâche est de connaître le plus précisément possible les demandes des clients. Ces demandes s'effectuent par le biais de SLA (Service Level Agreement).

Les réseaux d'opérateurs doivent en outre être en mesure de transformer ces demandes en une configuration des équipements et des lignes de transmission. Afin d'adapter leur réseau à la demande, les opérateurs ont presque tous opté pour des architectures avec signalisation. Cela consiste, avant d'envoyer le moindre paquet d'un utilisateur, à mettre en place des chemins, éventuellement avec réservation explicite de ressources. Parmi les différentes techniques de signalisation, MPLS est la plus populaire.

Une autre caractéristique importante de ces réseaux concerne l'interconnexion avec les autres opérateurs pour desservir tous les points du globe. C'est normalement le rôle de la normalisation de l'UIT-T. Cependant, cette normalisation est moins bien respectée aujourd'hui, compte tenu de la suprématie de l'IETF, qui ne spécifie pas toujours parfaitement certaines options, rendant les interconnexions entre opérateurs plus délicates.

L'objectif des opérateurs est de vendre un maximum de services à leurs clients. Les premiers d'entre eux sont évidemment la bande passante et les temps de réponse, ainsi que, de plus en plus, la sécurité, la gestion de la mobilité, l'optimisation, etc. Les réseaux privés virtuels, ou VPN (Virtual Private Network), font partie de la panoplie de solutions proposées par les opérateurs. Ce chapitre se penche sur la mise en place de ces réseaux et sur l'apparition de routeurs virtuels. Les opérateurs doivent rendre ces services de façon fiable. Le taux de disponibilité est donc un facteur important.

SLA opérateur

Les réseaux deviennent de plus en plus complexes. Le développement des services s'appuie sur des modèles de plus en plus élaborés, comme si l'imagination concernant le développement de nouveaux services était illimitée.

Les utilisateurs souhaitent avoir accès à des services personnalisés, à travers des terminaux ou des technologies d'accès variés, tout en exigeant des garanties pour les services qu'ils achètent. La réalisation de ces attentes implique la coopération et la coordination entre les fournisseurs de services Internet, ou ISP (Internet Service Provider), les fournisseurs d'applications, ou ASP (Application Service Provider), et les opérateurs réseau, ou NSP (Network Service Provider). Cela implique d'assurer tout à la fois la qualité de service demandée, la gestion de la mobilité et la prise en compte de la sécurité. Pour garantir les droits et définir les obligations de l'utilisateur et du fournisseur de service, un contrat, appelé SLA, est écrit dans un langage de niveau business, compréhensible par ces derniers.

Les sections qui suivent examinent les différentes parties qui constituent un SLA ainsi qu'un ensemble de paramètres pour la qualité de service, la mobilité et la sécurité pouvant être négociés dynamiquement entre l'utilisateur et le fournisseur.

SLA, SLO et SLS

Les réseaux sont caractérisés par l'intégration de plusieurs technologies réseau en une unique technologie sous IP pour permettre le développement de nouveaux services en utilisant des modèles plus complexes. Ces services ne sont plus fournis par un seul fournisseur mais par plusieurs entités business que sont l'opérateur réseau, le fournisseur d'applications (ASP) et le fournisseur de services Internet (ISP). L'ASP et l'ISP peuvent être des clients de l'opérateur réseau. La relation entre ces entités n'intéresse généralement pas l'utilisateur final, qui se préoccupe plutôt du niveau de garantie des services qu'il paye.

Comme expliqué précédemment, la négociation entre l'utilisateur final et le fournisseur de service est spécifiée dans un SLA. Le SLA est ensuite traduit en objectifs, nommés SLO (Service Level Objectives). Chaque SLO est à son tour traduit en un ensemble de paramètres formant un SLS (Service Level Specification), comme illustré à la figure 25.1. Le SLO représente les objectifs à réaliser dans le cadre d'un SLA tandis que le SLS représente une interprétation technique du SLO et sert de guide opératoire afin d'aider le fournisseur à implémenter un objectif. Un SLA peut contenir plusieurs SLO pour plusieurs objectifs, tels le SLO pour la mobilité, le SLO pour la sécurité, le SLO pour la qualité de service, etc. Chaque SLO peut contenir à son tour plusieurs SLS.

Figure 25.1
Relations entre SLA, SLO et SLS

Paramètres d'un SLS de QoS

Cette section décrit les paramètres d'un SLS de qualité de service. Nous verrons un peu plus loin les paramètres à ajouter pour la gestion de la mobilité et de la sécurité.

Temps de service

Le temps de service, encore appelé service schedule, indique les temps de début et de fin de service. Ce paramètre spécifie le temps pendant lequel la QoS négociée doit être garantie. Le temps de service peut être l'instant précis du début et le temps précis de la fin du service. Par exemple, le service commence à 13 heures le 20 septembre 2005 et se termine à 17 heures le même jour. Le temps de service peut aussi être déterminé par des horaires périodiques spécifiés par l'heure du jour, le jour de la semaine, la date du mois et le mois de l'année. Par exemple, le service commence tous les jours de lundi à vendredi, de 8 heures à 17 heures, entre septembre et juin de chaque année.

Scope

Le scope est défini comme le point d'entrée et le point de sortie d'un domaine, par exemple, l'interface du routeur d'entrée par lequel le trafic entre dans le domaine et l'interface du routeur de sortie par lequel le trafic sort du domaine.

Paramètres de QoS

Les paramètres de QoS suivants sont définis :

- **Délai.** Délai de transmission d'un paquet IP entre le point d'entrée et le point de sortie du domaine.
- **Gigue.** Variation du délai de transmission des paquets IP entre le point d'entrée et le point de sortie du domaine.
- **Taux de perte.** Pourcentage des paquets perdus pendant la transmission des paquets IP entre le point d'entrée et le point de sortie du domaine.
- **Débit.** Nombre de paquets par seconde sur une interface.

Profil du trafic

Le profil du trafic, aussi appelé descripteur du trafic, est défini par les paramètres suivants :

- paramètres du token-bucket utilisé pour identifier les paquets dans le profil et hors profil ;
- taille maximale du paquet (MTU) ;
- taille minimale du paquet ;
- débit moyen et débit crête.

Traitement en excès

Le traitement en excès spécifie le traitement que le réseau applique aux paquets hors profil. Ce paramètre peut avoir les valeurs suivantes :

- **Dropping.** Le réseau jette les paquets hors profil.
- **Shaping.** Le réseau lisse les paquets hors profil pour les mettre dans le profil (in-profile).
- **Remarking.** Le réseau marque les paquets hors profil pour modifier la classe de service de ces paquets ou pour qu'ils puissent être rejetés avec une probabilité plus grande en cas de congestion.

Identification du trafic

L'identification du trafic, ou Flow Identification, est définie par les paramètres suivants :

- adresse IP de la source et de la destination ;
- numéro de port TCP ou UDP de la source et de la destination ;
- identification de protocole ;
- valeur du DSCP ;
- valeur de l'identificateur de flot (flow-label).

Identification du client

L'identification du client est utilisée pour les fonctions AAA (Authentication, Authorization, Accounting).

Marquage

Le paramètre de marquage spécifie la priorité qui est donnée aux paquets. Par exemple, dans DiffServ la valeur du DSCP est utilisée pour faire le marquage des paquets à l'entrée du réseau.

Mode de négociation

Le mode de négociation définit la manière avec laquelle la négociation est appliquée. En règle générale, il y a deux modes de négociation, le mode prédéfini (predefined-SLS mode) et le mode non prédéfini (non-predefined-SLS mode). Dans le mode non prédéfini, il n'y a pas de contrainte sur les valeurs des paramètres de SLS envoyées par le client. Dans le mode prédéfini, le fournisseur de service propose aux clients des SLS avec des paramètres à une valeur ou une plage de valeurs déterminées à l'avance. Dans ce cas, le client doit choisir le SLS le plus approprié à ses besoins.

Intervalle de renégociation

L'intervalle de renégociation spécifie l'intervalle de temps pendant lequel un SLS négocié ne peut être renégocié.

Fiabilité

La fiabilité est définie par deux paramètres principaux :

- Le temps d'indisponibilité moyen du réseau par an (Mean Down Time).
- Le temps maximal de réparation (Time To Repair) lorsque le service tombe en panne.

Paramètres d'un SLS de mobilité

Les trois premiers paramètres que nous introduisons sont spécifiques du service de mobilité. Les quatre suivants se trouvent déjà dans les paramètres déterminés pour la qualité de service mais avec une vision légèrement différente.

Délai du handover

Cet attribut détermine le délai de rétablissement de la QoS sur le nouveau chemin après un handover. Ce délai peut être divisé en :

- temps nécessaire pour établir la nouvelle route vers le nœud mobile (Establishment time) ;
- temps pour recevoir le premier paquet transmis après établissement du nouveau chemin (Completion time).

Perte de paquet sur handover

Détermine le nombre de paquets que le réseau est autorisé à perdre au cours d'une session à cause d'un handover.

User-roaming

Permet à un utilisateur de demander certains services lors d'un roaming international, tels que cacher sa localisation, masquer son adresse IP, etc.

Scope-mobilité

Définit la région géographique dans laquelle la mobilité de l'utilisateur est prise en compte par son fournisseur de services. Par exemple, si le Scope-mobilité initial d'un utilisateur est la France, ce dernier peut le renégocier s'il doit se rendre aux États-Unis afin de l'étendre à une région géographique englobant ce pays.

Temps de service

Spécifie la période de temps pendant laquelle le service qui a été négocié pour la mobilité est disponible, en précisant la date et l'heure de début et de fin de période. Une période de temps minimale doit être définie dans le cas où le client ou le fournisseur de services désirerait mettre fin au contrat avant les dates prévues.

Marquage global

Donne la possibilité à l'utilisateur de demander un service de bonne qualité sans passer par la négociation du SLS. Une priorité est affectée à chaque client qui demande ce service selon certains critères, comme son profil utilisateur. Si plusieurs

clients demandent le même service et si la satisfaction de tous les clients engendre une surcharge pour le réseau, l'administrateur réseau doit repousser certaines demandes en fonction de leur priorité.

Profil du trafic

Donne la possibilité à l'utilisateur de connaître les charges liées au service de mobilité. Dans les réseaux de télécommunications, chaque type de technologie adopte un modèle spécifique pour calculer les charges. Par exemple, dans les réseaux GSM, le coût des appels dépend de la capacité du lien et non des données transmises, tandis que la charge du service paquet dans le GPRS ou l'UMTS est une combinaison de certains paramètres, comme le temps de connexion (time-based), le volume d'information (volume-based), l'heure de la journée (daytime) ou la QoS (délai, probabilité de perte, etc.) exigée pour la transmission des données. Par conséquent, les opérateurs doivent mettre des informations détaillées à la disponibilité de leur client sur les frais du roaming de façon que ces derniers puissent contrôler leur utilisation et vérifier l'exactitude de leur facture.

Les paramètres utilisés pour calculer les frais liés à la mobilité et au roaming spécifient si des tarifs d'une session, d'un appel ou d'un service seront présentés à l'utilisateur par l'intermédiaire de son écran. Ils indiquent également à quel moment ces tarifs seront affichés, par exemple, à la fin d'une session ou d'un appel.

Paramètres d'un SLS de sécurité

Le rôle d'un SLS de sécurité est de fournir les paramètres techniques du SLA pour la négociation de services de sécurité liés à la protection des données de l'utilisateur. Nous détaillons ci-après le SLS de sécurité lié à IPsec, qui est la solution la plus souvent mise en œuvre par les opérateurs.

Temps de service (schedule)

Comme pour le SLS de QoS, le temps de service (schedule) correspond à la durée en seconde pendant laquelle le service est assuré. Ici, le schedule peut aussi être défini en terme de quantité de trafic bénéficiant du service. Il s'exprime sous la forme de la durée divisée par la quantité d'information transportée.

Scope

Ce paramètre détermine les nœuds dans le réseau où l'opérateur peut appliquer le service de sécurité. La mise en place d'une association de sécurité, ou SA (Security Association), entre deux nœuds nécessite la configuration d'un service de sécurité sur ces deux nœuds.

L'application considérée ici est un VPN-IP *(voir le chapitre 32)* de groupe ou personnel, un des nœuds étant le terminal utilisateur. Les VPN peuvent être implémentés selon six modèles différents. La figure 25.2 illustre ces différents modèles. Parmi les nœuds, on trouve les équipements terminaux (End ou End Systems), les CE (Customer Edge) et les

PE (Provider Edge). CE et PE sont généralement des routeurs qui se trouvent chez le client ou l'opérateur.

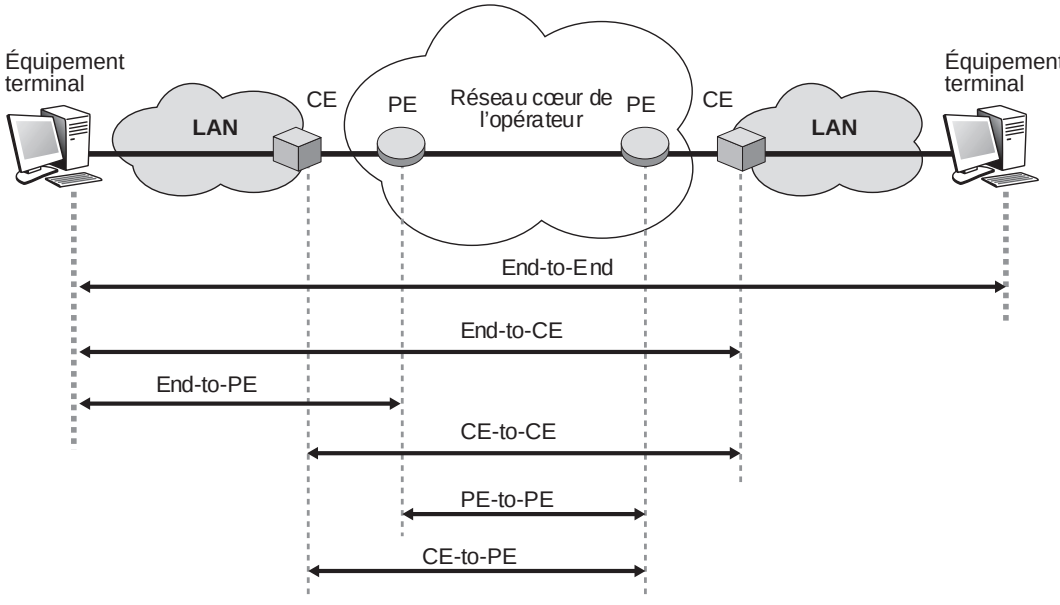


Figure 25.2
Les six modèles de VPN

Parmi ces modèles, le cas du bout-en-bout (End-to-End) n'est pas applicable dans le cadre de la négociation de SLS avec un opérateur. Dans la suite de cette section, nous avons regroupé les modèles End-to-CE et End-to-PE dans la partie VPN personnels. Les modèles CE-to-CE, CE-to-PE et PE-to-PE sont regroupés dans la partie VPN de groupe.

VPN personnel (End-to-CE ou End-to-PE)

Le VPN personnel commence au niveau d'un terminal et prend fin au CE du LAN distant, dans lequel se trouvent les équipements terminaux, ou au PE, qui peut se situer dans un POP (Point of Presence) de l'opérateur. Un équipement de VPN, associé à des fonctionnalités de VPN, disponible dans un CE ou dans un PE est responsable de l'application de services de sécurité entre lui et les équipements terminaux. L'approche End-to-PE peut éviter le besoin de déployer des matériels de VPN ou des fonctionnalités identiques dans le réseau du client. La plupart des VPN personnels sont implémentés selon le modèle End-to-CE.

Considérons un utilisateur distant qui demande la mise en place d'un VPN d'accès distant selon un certain niveau de service auprès du CE ou de l'opérateur du PE. Une négociation peut être mise en place entre le terminal et l'opérateur. Si cette négociation se finalise par un accord d'un certain niveau de service, l'activation du service n'est effective qu'après configuration de l'équipement terminal et du CE ou du PE. Ce schéma de fonctionnement est décrit à la figure 25.3.

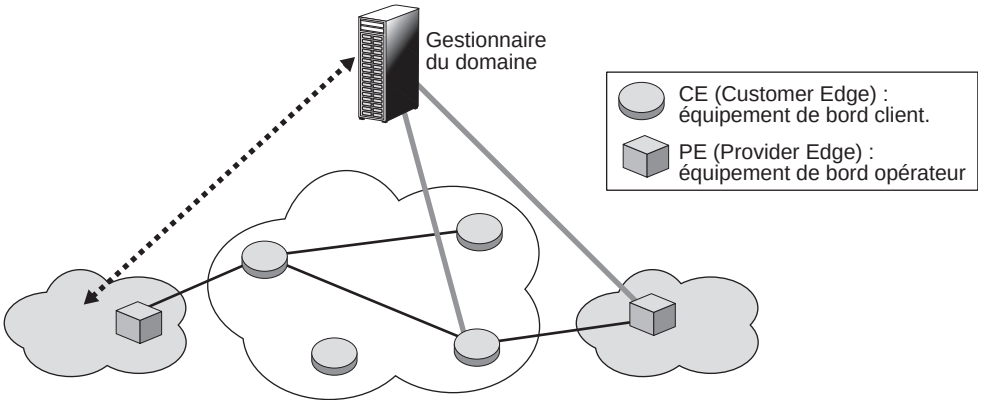


Figure 25.3
Schéma de fonctionnement d'un VPN personnel

VPN de groupe (CE-to-CE, CE-to-PE, PE-to-PE)

Avec un VPN de groupe, pour appliquer des services de sécurité, les équipements terminaux utilisent les équipements de VPN situés dans le périmètre du réseau d'entreprise (CE-to-CE ou CE-to-PE) ou dans le réseau de l'opérateur (CE-to-PE ou PE-to-PE). De cette façon, aucune fonction de sécurité n'a besoin d'être implémentée sur les terminaux. L'implémentation de services de sécurité leur est complètement transparente.

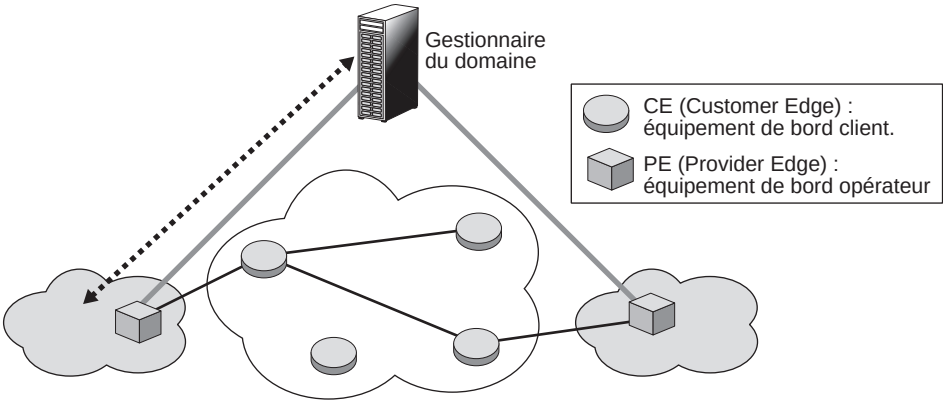


Figure 25.4
Schéma de fonctionnement d'un VPN de groupe

Dans le cas d'une négociation intradomaine, par exemple CE-to-CE, les CE sont gérés par un même opérateur. La négociation du SLS a lieu entre un client situé au niveau d'un réseau d'entreprise et l'opérateur. Si nous prenons l'exemple d'un client situé dans le réseau d'entreprise de gauche de la figure 25.4, le trait en pointillé indique la négociation du SLS pour un VPN à mettre en place entre le CE du réseau de gauche et le CE du réseau de droite.

Une fois la négociation terminée avec succès, l'opérateur peut mettre en place le service demandé en appliquant directement les politiques de sécurité adéquates sur les deux CE. Ce cas s'applique de façon similaire aux modèles CE-to-PE et PE-to-PE.

Le cas d'une négociation interdomaine, par exemple CE-to-CE, est illustré à la figure 25.5. Les CE étant gérés par deux opérateurs différents, la négociation a lieu en plusieurs phases. La première phase de négociation se passe entre le client situé au niveau d'un réseau d'entreprise et l'opérateur qui gère son CE.

Prenons l'exemple d'un client situé dans le réseau d'entreprise de gauche. Le trait en pointillé sur la gauche de la figure indique la négociation du SLS pour un VPN à mettre en place entre le CE du réseau de gauche et le CE du réseau de droite. Une fois cette demande de négociation reçue, l'opérateur de gauche s'aperçoit qu'il ne gère pas le CE distant. Dès lors, il retransmet la demande de négociation du SLS à l'opérateur qui gère le CE distant (les pointillés du centre de la figure). Ce dernier traite la demande de négociation de service.

Deux situations se présentent alors :

- Si l'opérateur de droite l'accepte, une réponse favorable est transmise à l'opérateur de gauche puis au client initiateur de la demande. Les deux opérateurs transmettent les politiques adéquates à leur CE respectif, et ces derniers appliquent les politiques de sécurité.
- Si l'opérateur de droite refuse la négociation, deux possibilités se présentent :

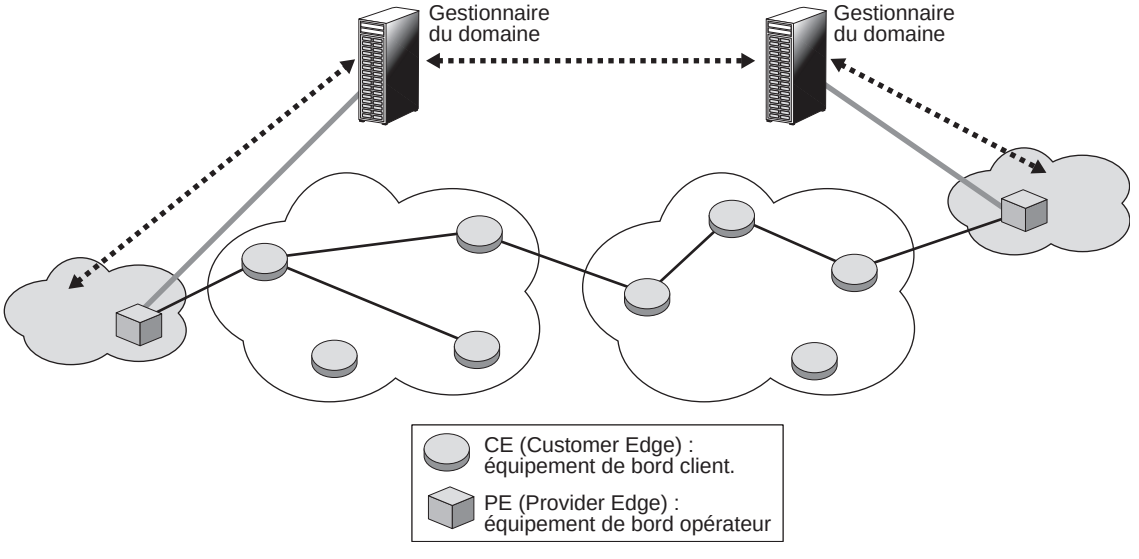


Figure 25.5
Cas d'une négociation interdomaine

  - L'opérateur distant (de droite) refuse catégoriquement la demande de négociation de service. Une réponse négative est transmise à l'opérateur de gauche puis au client. Le SLS ne peut être appliqué.
  - Le niveau de service demandé n'est pas applicable. Une renégociation du niveau du service de sécurité se met en place.

Identification du trafic

L'identification du trafic à sécuriser a lieu au point d'entrée de l'association de sécurité, ou SA (Security Association), IPsec. Cette information est stockée dans la base de données des politiques de sécurité SPD (Security Policy Database). À l'émission, une fois identifié, le trafic est encapsulé dans l'association de sécurité SA associée. Une SA est une connexion unidirectionnelle, ou simplex, qui apporte les services de sécurité au trafic qu'elle transporte. Deux SA sont nécessaires pour sécuriser une communication bidirectionnelle traditionnelle, une pour chaque direction. Dans ce cas, une identification du trafic à sécuriser a lieu au niveau des deux nœuds entre lesquels les SA sont mises en place.

Dans la réalité, le trafic à sécuriser entre deux points peut ne concerner que le trafic dans un sens, c'est-à-dire le trafic entrant ou sortant. On peut citer l'exemple d'un sous-réseau commercial dont la politique de sécurité est d'assurer le cryptage d'images en haute résolution à destination de ses clients. Dans ce cas, seuls les paquets IP sortants sont concernés. Les paquets IP entrants ne demandent aucune forme de cryptage. Dans ce cas, le client négocie auprès de son opérateur un niveau de service de sécurité pour le SA sortant. Aucun SA entrant n'est mis en place.

Les paramètres qui identifient le trafic à sécuriser, en unidirectionnel comme en bidirectionnel, sont les suivants :

- Adresse IP source (IPv4 ou IPv6) : peut être une adresse unique unicast, anycast ou broadcast (pour IPv4), un groupe multicast, une gamme d'adresses (valeurs inférieure et supérieure, adresse + masque de l'adresse) ou encore une adresse wildcard, c'est-à-dire une adresse réservée pour un invité.

- Adresse IP destination (IPv4 ou IPv6) : peut être une adresse unique unicast, anycast ou broadcast (pour IPv4), un groupe multicast, une gamme d'adresses (valeurs inférieure et supérieure, adresse + masque) ou une adresse wildcard.

- Nom : peut être un identifiant d'utilisateur ou un nom de système en fonction de la nature du nœud qui supporte IPsec. Le nom de système doit être applicable dans tout type de nœud IPsec. On peut se contenter d'un identifiant d'utilisateur au niveau des équipements terminaux, ainsi qu'au niveau des routeurs supportant IPsec pour le traitement du trafic entrant.

L'identifiant d'utilisateur et le nom de système peuvent être des noms d'utilisateur DNS ou des noms X.500.

Les réseaux en mode avec connexion

Les réseaux d'opérateurs sont généralement en mode avec connexion, la mise en place d'un chemin permettant de contrôler au mieux les ressources et de garantir la qualité de service. Au cours des années 80, les opérateurs de télécommunications ont beaucoup utilisé les circuits, non seulement pour la téléphonie mais également pour les données. La première évolution après la commutation de circuits pure a été le RNIS (Réseau numérique à intégration de services), qui utilise le circuit aussi bien pour la parole téléphonique que pour le transfert de paquets.

Les opérateurs sont ensuite passés à la commutation de paquets sur des circuits virtuels. Les réseaux X.25 comme Transpac ont connu un grand succès dans les années 80 et 90. Ils étaient les premiers réseaux en mode avec connexion à permettre un partage des ressources entre tous les paquets acheminés dans le réseau. Les réseaux en relais de trames ont pris le relais. Ces réseaux ont à peu près les mêmes propriétés que les réseaux X.25, si ce n'est qu'au lieu de se servir de circuits virtuels au niveau 3, ils ouvrent des liaisons virtuelles de niveau 2, beaucoup plus simples et moins onéreuses. Ces liaisons virtuelles de niveau 2 permettent en outre de ne pas décapsuler les trames lors des traversées des nœuds de commutation, au contraire des réseaux X.25.

Après le relais de trames, les opérateurs ont choisi la technique de transfert ATM pour proposer des services avec garantie aux utilisateurs. Les réseaux ATM étant des réseaux de commutation de niveau trame, ils sont puissants et peuvent prétendre à des débits importants. Cette technologie a connu un grand succès sans toutefois réussir à s'imposer en raison de son système de signalisation, à la fois spécifique et relativement complexe. Cette complexité provient du choix qui a été fait d'étendre les signalisations précédentes, en particulier celle provenant du RNIS. De surcroît, l'UIT-T s'est trouvée dans l'incapacité de normaliser une interface standard que les équipementiers auraient pu intégrer dans les équipements de réseau. De ce fait, la technologie ATM n'a jamais pu s'imposer sur l'interface utilisateur, où elle a été supplantée par Ethernet et son allié de toujours IP. N'ayant pu s'imposer complètement, la technologie ATM a été remplacée par MPLS. La raison essentielle de cette nouvelle donne est l'introduction d'une signalisation permettant de mettre en place les chemins simplement avec une signalisation IP, puisque IP est un réseau de routage aux adresses universelles.

La technologie MPLS permet d'utiliser les anciens réseaux introduisant de la qualité de service, comme ATM. Le passage d'ATM à MPLS ne pose donc pas vraiment de problème. L'avantage de cette solution MPLS est l'utilisation d'un réseau de signalisation fondé sur IP, assez simple à mettre en œuvre. MPLS peut également utiliser des réseaux Ethernet à partir du moment où Ethernet emploie le mode commuté introduit avec le shim-label.

La figure 25.6 illustre la traversée de plusieurs réseaux spécifiques formant un réseau MPLS afin d'illustrer la transition entre les réseaux de génération ATM et MPLS. La signalisation IP met en place un chemin de la façon suivante :

1. Lorsque le paquet de signalisation arrive au premier nœud, la technique de routage permet de déterminer le routeur suivant à atteindre après la traversée du réseau ATM. La traversée du réseau ATM par la signalisation est classique : un circuit virtuel ATM est ouvert en indiquant l'adresse ATM du routeur suivant, qui est obtenue par une traduction de l'adresse IP en une adresse ATM.

2. Une fois ouvert, le circuit virtuel ATM permet de transporter les différents fragments du paquet de signalisation, qui est reformé au nœud suivant.

3. Les fragments sont réassemblés au routeur suivant grâce à la couche AAL.

4. De nouveau, une fois déterminé le routeur suivant, il faut ouvrir un circuit virtuel ATM pour y transporter le paquet de signalisation IP.

5. De même, pour traverser le réseau Ethernet, un chemin est mis en place, sur lequel les trames Ethernet sont commutées grâce aux références de type shim-label.

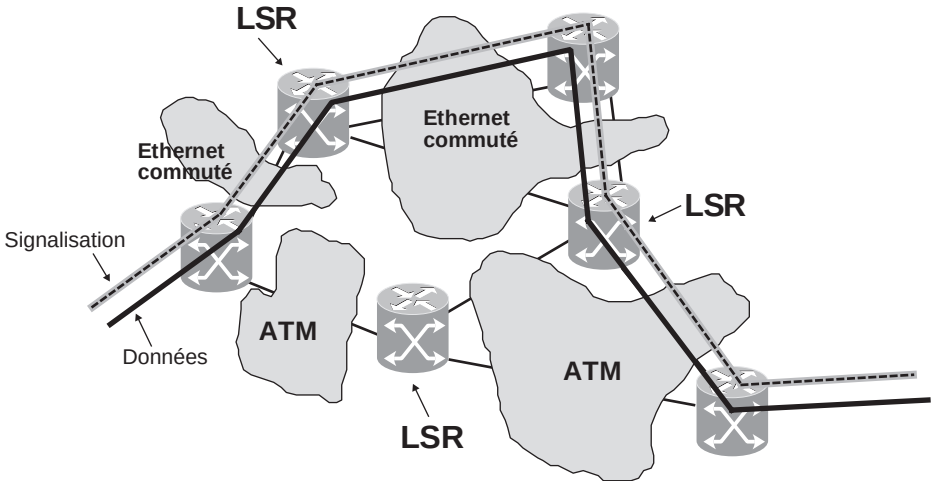
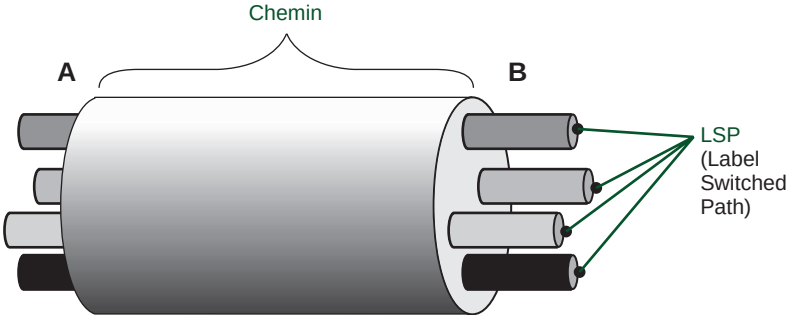


Figure 25.6
Réseau MPLS de transition

La figure 25.7 représente un réseau MPLS de façon conceptuelle. Les opérateurs n'attendent pas l'arrivée d'un client pour ouvrir un LSP mais l'ouvrent dès l'initialisation du réseau. De la sorte, lorsqu'un client se présente, il suffit de regarder l'adresse de sortie du réseau à partir de son adresse IP de destination et d'affecter le client au LSP approprié. Par exemple, entre les deux interfaces A et B, quatre circuits virtuels peuvent proposer un service EF, deux services AF, comme Gold et Bronze, et un service best-effort. Bien d'autres solutions peuvent être mises en œuvre pour affecter les chemins à des services particuliers. Par exemple, à chaque LSP pourrait correspondre une application particulière.

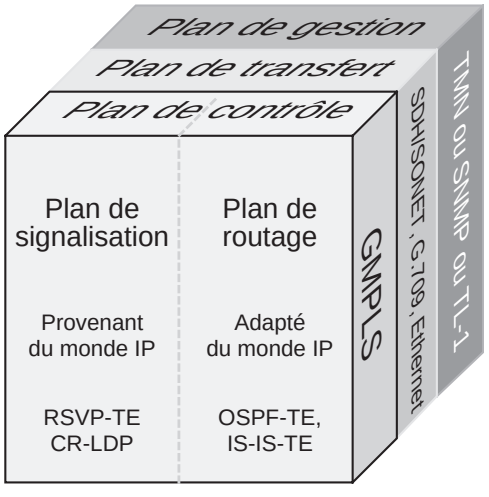
Figure 25.7
Représentation conceptuelle d'un réseau MPLS



La figure 25.7 représente un cas simple. Dans la réalité, MPLS fait appel à une solution de signalisation formant des FEC (Forwarding Equivalency Classes). Toutes les communications qui ont une même destination se rassemblent sur un même circuit virtuel. Au lieu d'être point-à-point, le chemin se présente sous la forme d'un arbre, dont la racine se trouve chez le destinataire et les feuilles chez les émetteurs.

Les réseaux MPLS seront eux-mêmes remplacés peu à peu par des réseaux GMPLS (Generalized MPLS), qui forment un surensemble de MPLS introduisant des techniques de commutation supplémentaires. L'architecture de GMPSL est illustrée à la figure 25.8. Le plan de gestion utilise des standards classiques, comme SNMP ou le TMN de l'UIT-T. Le plan de transfert est issu principalement de l'UIT-T et de l'IEEE, avec SONET/SDH, G.709 et la commutation Ethernet. Le plan de contrôle provient quant lui de l'IETF et comporte deux parties, le plan de signalisation, avec pour principaux protocoles RSVP-TE (RSVP-Traffic Engineering) et CR-LDP (Constraint-based Routing/Label Distribution Protocol), et le plan de routage, avec pour principaux algorithmes de routage OSPF-TE (OSPF-Traffic Engineering) et IS-IS-TE.

Figure 25.8
Architecture de GMPLS



Les réseaux partagés

Les réseaux des opérateurs doivent être partagés entre les clients de telle sorte que chaque client puisse croire qu'il est seul à utiliser les ressources mises à sa disposition par l'opérateur et puisse avoir confiance dans la capacité de l'opérateur à sécuriser ses communications.

De ces principes sont nés les réseaux privés virtuels, que nous étudions en détail au chapitre 32. Un réseau privé virtuel, ou VPN, est, du point de vue de l'entreprise cliente, un ensemble de réseaux de site reliés par un réseau d'opérateur garantissant une forte sécurité des communications. En particulier, aucun autre client que le personnel de l'entreprise ne peut y accéder de l'extérieur.

Du point de vue de l'opérateur, un VPN est un réseau dont les ressources sont partagées entre les différentes entreprises clientes de telle sorte que chaque client ait l'impression d'avoir un réseau dédié et non partagé. Pour l'opérateur, l'avantage de cette solution est énorme. Lorsque les entreprises n'utilisent les ressources qui leur sont affectées que pendant un temps restreint, l'opérateur peut les réaffecter au fur et à mesure des besoins réels des autres entreprises clientes. En d'autres termes, nous avons un multiplexage statistique des équipements logiciels et matériels. Si la probabilité de manquer de ressources est parfaitement calculée, de façon à demeurer infime, le gain financier pour l'opérateur est très important.

Pour garantir le partage, il faut que le réseau se prête à une ingénierie simple, d'où le choix de MPLS et GMPLS.

Une structure de réseau VPN-MPLS est illustrée à la figure 25.9, dans laquelle trois VPN d'entreprise sont représentés. Un VPN-MPLS est un ensemble de chemins, ou LSP, d'un réseau MPLS dédiés aux entreprises se connectant en VPN. Ces VPN d'entreprise sont connectés au réseau de l'opérateur par des points d'accès, ou PE (Provider Edge), appartenant à l'opérateur. Les réseaux d'entreprise sont raccordés au PE par un équipement CE (Customer Edge). Nous avons examiné ces éléments à la section précédente. Sur la figure 25.9, on voit que certains sites peuvent appartenir à plusieurs VPN simultanément.

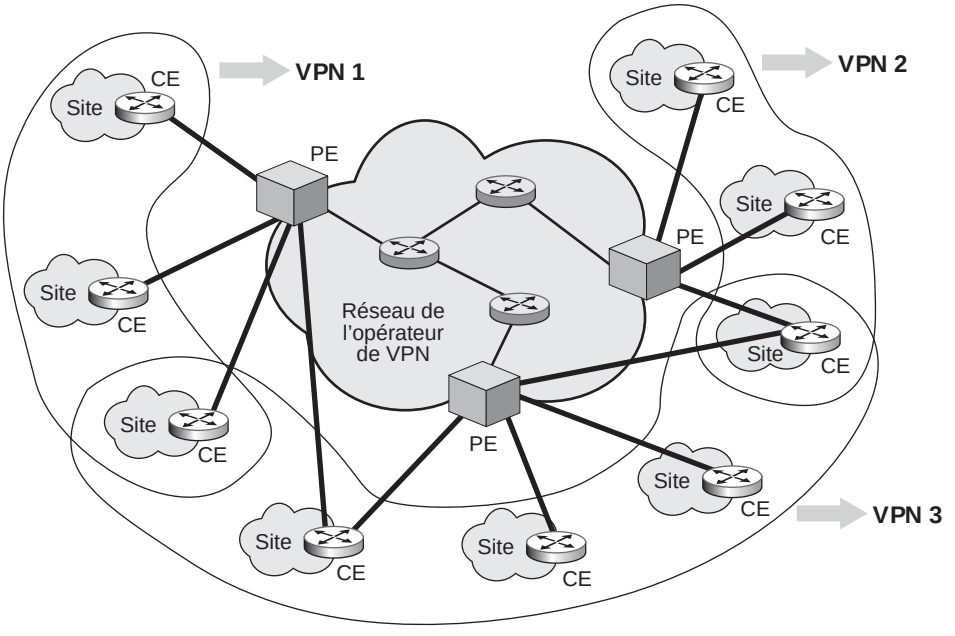


Figure 25.9
Trois VPN d'entreprise sur un réseau d'opérateur

Les routeurs extrémité PE et CE peuvent gérer différents types de services. Le plus important pour les entreprises est la sécurité. Le VPN peut être sécurisé en chiffrant les paquets entrants dans le réseau de l'opérateur. Ce chiffrement peut s'effectuer dans le routeur extrémité de l'opérateur ou de l'entreprise. Bien que les opérateurs présentent cette solution comme une valeur ajoutée à leur offre de VPN, beaucoup d'entreprises préfèrent gérer elles-mêmes leur sécurité et chiffrer les données à l'entrée et à la sortie de leurs sites, en dépit du coût induit.

D'autres fonctionnalités peuvent être prises en charge par l'opérateur, notamment la qualité de service, la gestion de la mobilité ou d'autres types de services de sécurité que la simple confidentialité. Pour cela, la structure du VPN peut avoir son importance.

Deux structures de VPN-MPLS peuvent être mises en place : un VPN selon le modèle overlay et un VPN selon le modèle peer. Dans le modèle overlay, les LSP sont ouverts directement de site à site, tandis que, dans le modèle peer, le routeur de bord se trouve chez l'opérateur. Dans le premier cas, les LSP sont ouverts directement entre CE, de telle sorte que le

VPN de l'opérateur ne fasse que multiplexer les LSP sur son propre réseau. Le réseau de l'opérateur ne peut apporter de forte valeur ajoutée puisque l'information est chiffrée chez l'utilisateur. Dans le second cas, l'opérateur a à sa charge la gestion des extrémités des LSP et peut effectuer un multiplexage de plusieurs flots d'entreprise dans des LSP communs, garantissant au réseau de l'opérateur la scalabilité, ou passage à l'échelle.

La figure 25.10 illustre le premier cas de figure, où le VPN démarre dans l'équipement extrémité, ou CE, de l'entreprise. Ce dernier gère les fonctionnalités de routeur, de sécurité IPsec, de terminaison de tunnel IPsec et de pare-feu mais peut aussi gérer des logiciels antivirus, antispam, etc. Le routeur PE de l'opérateur peut également jouer le rôle de pare-feu mais en proportion très limitée puisque les flots du client sont chiffrés. Seuls les paquets de gestion et de contrôle peuvent être vérifiés à ce niveau.

Cette solution revient relativement cher à l'entreprise, car elle doit gérer elle-même toutes les fonctionnalités de l'interconnexion de réseau.

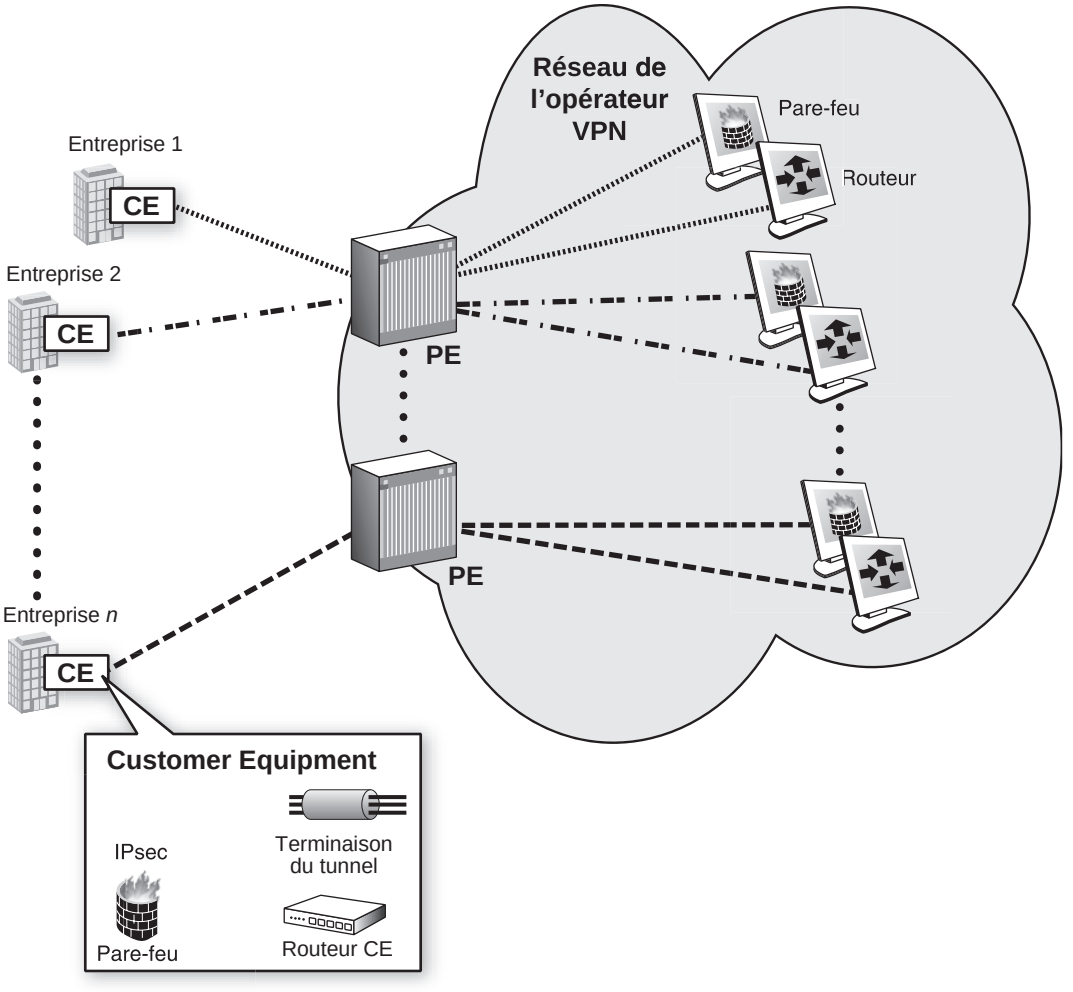


Figure 25.10
VPN géré à partir de l'entreprise cliente

La figure 25.11 illustre un VPN géré par l'opérateur. Cette solution est beaucoup plus flexible puisque les équipements de routage, de pare-feu, de gestion d'IPsec, etc., sont partagés par les clients connectés au routeur PE.

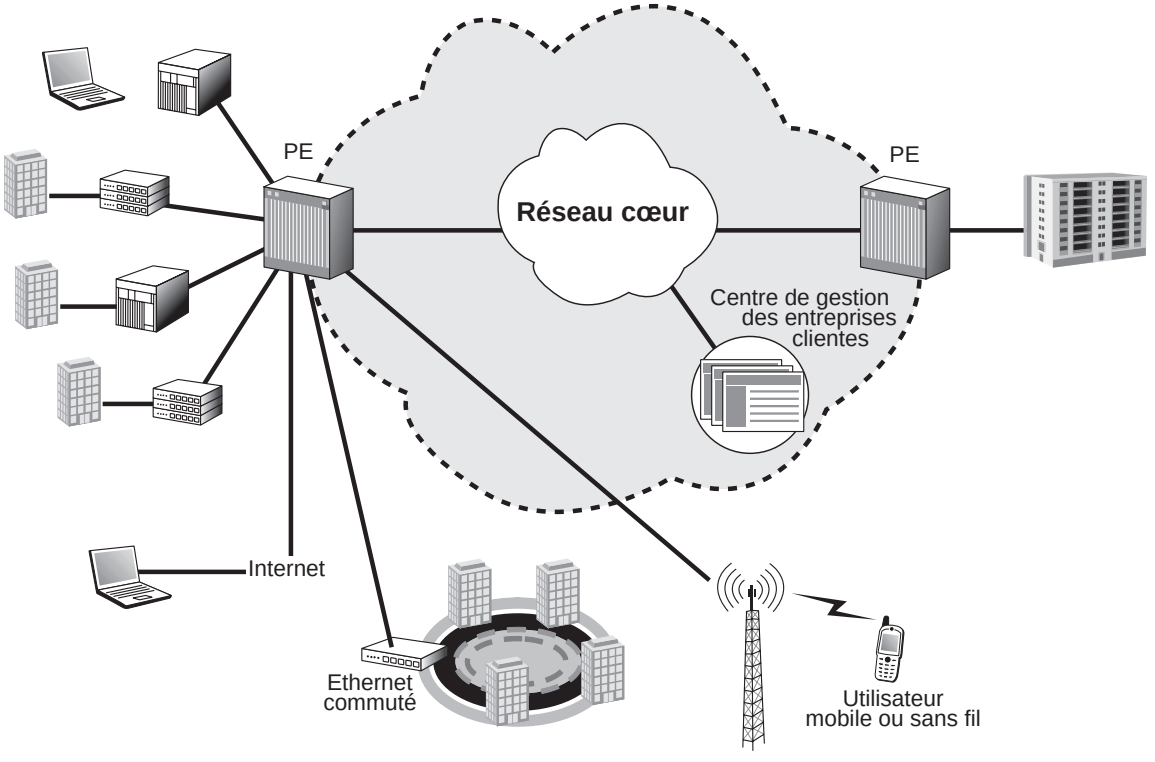


Figure 25.11
VPN géré par l'opérateur

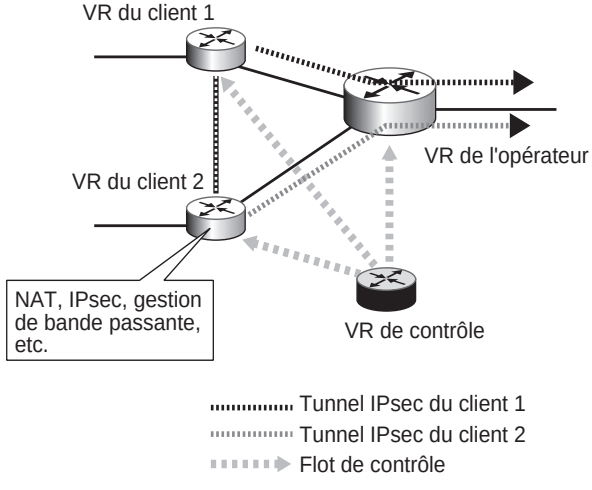
On voit que les machines de l'entreprise peuvent être connectées au routeur extrémité PE par un très grand nombre de solutions, alors que, dans la technique de raccordement au routeur CE, il faut que les matériels de l'entreprise soient connectés directement à l'entreprise. Dans la solution de gestion opérateur, les connexions peuvent s'effectuer par des lignes *x*DSL, des liaisons spécialisées, des réseaux en relais de trames ou ATM ou même par des accès *via* des ISP permettant la connexion de terminaux mobiles ou sans fil. Des connexions Ethernet directes sont également possibles.

L'opérateur peut offrir des services supplémentaires, comme la gestion des équipements de l'entreprise cliente à partir de serveurs situés dans son réseau. Des services de gestion de messagerie électronique, d'impression, de gestion de logiciels ou de programmes métier peuvent être proposés à partir du réseau de l'opérateur. Cette solution apporte un gain à la fois au client et à l'opérateur. Le client n'a plus à gérer de façon privée un ensemble d'équipements. Il a de surcroît la possibilité de se connecter beaucoup plus facilement à ses sites par le biais d'ISP intermédiaires et d'ajouter des clients mobiles ou nomades. Pour l'opérateur, le gain statistique est toujours le maître mot. Il est obtenu en partageant des équipements entre plusieurs clients.

Une autre solution qui se développe consiste, pour l'opérateur, à faire appel à des routeurs virtuels, ou VR (Virtual Router). Cette solution est illustrée à la figure 25.12. Un routeur virtuel est l'équivalent d'un routeur matériel, mais avec ses propres algorithmes de routage et la possibilité de mettre en œuvre des fonctionnalités telles que NAT ou DHCP, des gestionnaires de bande passante, etc. Un routeur virtuel est donc un logiciel en technologie objet susceptible d'être implémenté sur une machine de sortie de l'entreprise ou plus généralement sur l'équipement PE de connexion de l'opérateur. Les fonctionnalités supplémentaires se présentent sous la forme d'objets spécifiques, qui peuvent être mis en route ou non. Plusieurs routeurs virtuels peuvent être créés à l'intérieur d'un même équipement. Si le routeur virtuel est situé sur le PE de l'opérateur, chaque client peut disposer de son propre routeur, avec ses propres fonctionnalités, même si, physiquement, l'équipement de réseau PE est unique.

L'opérateur peut agréger les flots sortant des différents routeurs virtuels sur des LSP uniques de façon à permettre la scalabilité de son réseau. L'opérateur possède un contrôleur de routeurs virtuels pour effectuer les modifications de configuration et la gestion du logiciel.

Figure 25.12
Réseau d'opérateur à routeurs virtuels



Les opérateurs Ethernet

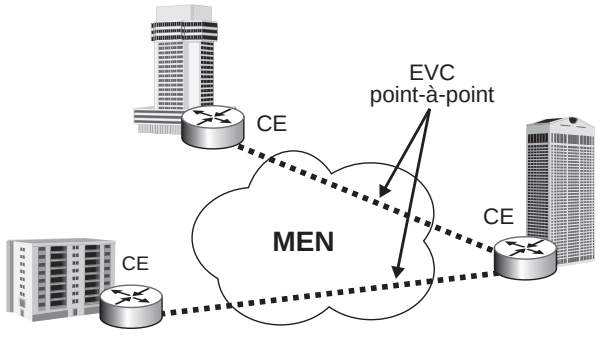
Ethernet devenant le standard de transport des paquets IP, du fait de la forte coopération entre IP et Ethernet, de nombreux opérateurs commencent à implémenter Ethernet à la place d'ATM ou du relais de trames. La solution Ethernet n'est pas incompatible avec MPLS, bien au contraire, puisque l'Ethernet commuté utilise un shim-label, ou référence, au fonctionnement classique, entrant parfaitement dans ce cadre.

Les solutions Ethernet actuelles permettent de mettre en place cette technologie dans de nombreux contextes, allant du réseau métropolitain au réseau étendu. Les débits vont de 1 à 10 Gbit/s et bientôt 40 et 160 Gbit/s. Les avancées les plus importantes se situent surtout au niveau des réseaux métropolitains, avec la poussée du MEF (Metropolitan Ethernet Forum) et la possibilité de gérer des boucles haut débit à forte fiabilité, comme

sur SONET, avec la norme RPR (Resilient Packet Ring), normalisée par le groupe de travail IEEE 802.17.

La figure 25.13 illustre un réseau d'opérateur Ethernet utilisant un réseau privé virtuel Ethernet construit à partir d'EVC (Ethernet Virtual Connection). Grâce à cette solution, les VPN-IP ou MPLS sont parfaitement compatibles avec le monde Ethernet.

Figure 25.13
Réseau privé virtuel Ethernet à base d'EVC



Un EVC peut être soit point-à-point, soit point-à-multipoint, soit encore multipoint-à-multipoint. Un réseau privé virtuel Ethernet peut donc avoir toutes les propriétés des VPN classiques mais avec une efficacité supérieure, puisque le système se trouve au niveau 2, et à un coût bien inférieur grâce aux matériels Ethernet utilisés.

Tout comme les environnements DiffServ, les réseaux d'opérateurs Ethernet permettent d'introduire des priorités, à cette différence près que le champ IEEE 802.1p, qui sert à l'introduction de ces priorités, n'a que 3 bits. Ces 3 bits ne permettent que 8 niveaux de priorités, à comparer aux 14 niveaux définis par l'IETF pour les services DiffServ.

Les niveaux de priorités proposés par le MEF sont les suivants :

- 802.1p-6 DiffServ Expedited Forwarding.
- 802.1p-5/4/3 DiffServ Assured Forwarding.
- 802.1p-5, qui présente la perte la plus faible.
- 802.1p-3, qui présente la perte la plus forte.
- 802.1p-2 DiffServ Best Effort.

Dans l'environnement Ethernet, le contrôle de flux est généralement un problème délicat. Diverses propositions ont été faites pour l'améliorer. En particulier, les méthodes de backpressure proposent l'envoi de messages de contrôle de la part des commutateurs surchargés, qui permettent aux commutateurs connexes de stopper leur émission vers le nœud congestionné pendant un temps indiqué dans la primitive de contrôle.

Le choix effectué par le MEF est un contrôle de type relais de trames, où l'on retrouve exactement les mêmes paramètres :

- CIR (Committed Information Rate)

- CBS (Committed Burst Size)
- PIR (Peak Information Rate)
- MBS (Maximum Burst Size)

Ces différentes propositions montrent que le monde Ethernet est en train de grignoter petit à petit des parts de marché et devrait devenir la technologie numéro un des opérateurs de réseau dans un avenir qui se rapproche.

Disponibilité d'un réseau d'opérateur

Dans un réseau d'opérateur, la fiabilité est une qualité essentielle. Nous avons représenté au tableau 25.1 les temps d'indisponibilité d'un réseau en fonction du taux de disponibilité, c'est-à-dire la proportion du temps pendant lequel le réseau est disponible. La première colonne indique le taux de disponibilité et les colonnes suivantes le temps d'indisponibilité du réseau par mois et par an.

Les réseaux de télécommunications pour la téléphonie sont actuellement des réseaux « cinq neuf », c'est-à-dire avec un taux de disponibilité de 99,999. Ce taux représente des coupures du service téléphonique égales au total à 5 minutes par an. Actuellement, les réseaux des ISP n'offrent que « trois neuf » et donc un temps de panne de l'ordre de 9 heures par an, un temps beaucoup trop important pour un service téléphonique de qualité. Les opérateurs de télécommunications en mode IP doivent donc faire un énorme effort pour atteindre des taux de deux ordres supérieurs.

Plusieurs solutions pour atteindre des taux de disponibilité acceptables pour les applications utilisateur sont envisageables et même déjà en grande partie implémentées dans les grands réseaux d'opérateurs. La solution la plus utilisée est la réservation de chemins supplémentaires ou chemins de back-up. Les chemins supplémentaires peuvent être soit réservés et disponibles en permanence, soit réservés mais utilisés par des flots qui cèdent leur place aux flots à sauvegarder.

1	90 %	36,5 j/an	3 j/m	
2	99 %	3,65 j/an	7,3 h/m	
3	99,9 %	8,8 h/an	44 min/m	Bon ISP
4	99,99 %	53 min/an	4,4 min/m	
5	99,999 %	5 min/an	25 s/m	Téléphone
6	99,9999 %	32 s/an	3 s/m	

TABLEAU 25.1 • Taux d'indisponibilité d'une ligne ou d'un réseau

Une protection 1:*N* indique qu'une ligne en back-up est réservée pour *N* lignes en cours d'utilisation, la ligne en back-up pouvant elle-même être utilisée. Une protection 1+*N* indique qu'une ligne en back-up est réservée pour *N* lignes en cours d'utilisation, la ligne en back-up ne pouvant être utilisée que par les lignes à protéger. Plus généralement, une protection *M*:*N* ou *M*+*N* indique que *M* lignes en back-up sont réservées pour *N* lignes actives.

Pour arriver au « cinq neuf » dans un grand réseau où les paquets doivent passer par plusieurs routeurs, il faut protéger très fortement les chemins. En effet, le taux de panne pour une liaison en fibre optique de 1 000 kilomètres est de l'ordre de 0,3 p. 1 000. Les pannes peuvent avoir de nombreuses raisons, dont la plus importante est la coupure pour travaux de génie civil. Si l'on compte un temps de réparation de 12 heures par panne, qui est déjà une valeur excellente, une redondance de 1:1 ne suffit pas à atteindre les « cinq neuf » car la probabilité que les chemins primaire et secondaire soient tous deux en panne est supérieure à 5 minutes par an. Il faut donc que la ligne de protection soit elle-même protégée.

Dans les réseaux traditionnels, la boucle locale est protégée dans le cadre de SONET par une reconfiguration qui s'effectue en 50 ms. Dans le réseau cœur, il y a toujours un chemin de rechange pour un chemin en panne. Quant à la partie entre le réseau métropolitain et l'utilisateur, sa fiabilisation s'effectue comme pour la téléphonie classique par le biais d'une alimentation indépendante du réseau électrique. Dans ce cas, il est facile d'atteindre les 99,999 p. 100. Cependant, le prix de revient de cette fiabilisation du réseau est assez important, et les opérateurs IP hésitent du fait de la concurrence acharnée sur les prix.

Conclusion

Les réseaux d'opérateurs sont en pleine mutation du fait du passage de la technologie circuit à la technologie IP en utilisant des infrastructures en mode avec connexion, qu'elles soient de type MPLS ou, d'ici peu, Ethernet/MPLS. Vers les années 2010, beaucoup de réseaux d'opérateurs ne travailleront plus qu'en mode paquet IP. Les technologies de réseaux privés virtuels devraient continuer à se développer avec un partage des ressources de plus en plus prononcé pour atteindre les prix les plus bas possibles.

Une autre vision, qui apparaît fortement chez les grands opérateurs, concerne le statut d'opérateur intégré. Cette proposition a pour objectif de mettre à disposition du client les différents réseaux de l'opérateur intégré comme si c'était un réseau unique, même si pour le moment ces réseaux ne sont pas intégrés. Par exemple, un opérateur qui possède un réseau de téléphonie en mode circuit, un réseau pour ses mobiles et un réseau pour le transport des données peut devenir un opérateur intégré en apparaissant auprès de ses clients comme opérant un seul et même réseau. Lorsqu'il téléphone de son combiné fixe, de son portable ou en utilisant de la voix sur IP à partir de son ordinateur personnel, l'utilisateur doit avoir l'impression que les informations sont véhiculées sur le même réseau. La facture est alors unique, ce qui fait la force de ces opérateurs intégrés.

L'intégration complète des réseaux demandera encore quelques années. Des opérateurs comme France Télécom ou British Telecom se sont lancés dans cette direction, avec une intégration complète du réseau sous forme de paquets IP espérée pour la fin de la décennie.

Références

Les services rendus par les réseaux d'entreprise peuvent être classifiés en niveaux en fonction de la qualité de service requise. Le livre suivant fait le point sur ces différents niveaux :

L. LEWIS – *Service Level Management for Enterprise Networks*, Artech House, 1999

Une présentation simple des réseaux privés virtuels pour permettre la connexion intersite et favoriser la sécurité des communications :

M. S. MERKOW – *Virtual Private Networks for Dummies*, For Dummies, 2000

La sécurité d'un réseau d'entreprise dépend beaucoup des fonctions de la passerelle qui permet d'entrer et de sortir. En particulier, une zone dite démilitarisée, la DMZ, permet de mettre en place ce no man's land :

R. J. SHIMONSKI, W. SCHMIED, V. CHANG, T. W. SHINDER – *Building DMZs for Enterprise Networks*, Syngress Publishing, 2003