UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Y.1311.1

(07/2001)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION ET PROTOCOLE INTERNET

Aspects relatifs au protocole Internet – Transport

Réseau privé virtuel de type IP utilisant une architecture à commutation multiprotocolaire par étiquetage

Recommandation UIT-T Y.1311.1

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION ET PROTOCOLE INTERNET

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	**Y.1300–Y.1399**
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Y.1311.1

Réseau privé virtuel de type IP utilisant une architecture à commutation multiprotocolaire par étiquetage

Résumé

La présente Recommandation détaille les prescriptions relatives aux services, ainsi qu'un certain nombre de conceptions architecturales qui peuvent être appliquées par les fournisseurs de services pour mettre en place, en employant la technologie IP, des réseaux privés virtuels (VPN, *virtual private network*) dont l'infrastructure sous-jacente est de type commutation multiprotocolaire par étiquetage (MPLS, *multiprotocol label switching*).

Source

La Recommandation Y.1311.1 de l'UIT-T, élaborée par la Commission d'études 13 (2001-2004) de l'UIT-T, a été approuvée le 13 juillet 2001 selon la procédure définie dans la Résolution 1 de l'AMNT.

Mots clés

Commutation multiprotocolaire par étiquetage (MPLS), protocole interréseaux (IP), réseau privé virtuel (VNP), IP VPN.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T Y.1311.1

Réseau privé virtuel de type IP utilisant une architecture à commutation multiprotocolaire par étiquetage

1 Introduction

Il est essentiel de détailler les mécanismes destinés à la prise en charge des réseaux privés virtuels IP (VPN, *virtual private network*) qui utilisent une architecture à commutation multiprotocolaire par étiquetage (MPLS, *multiprotocol label switching*). Bien sûr, les Recommandations doivent aussi décrire et spécifier les différentes implémentations qui assurent l'interfonctionnement et la fourniture des services de bout en bout à travers les infrastructures des multiples vendeurs fournisseurs de services.

Les fournisseurs de services ont besoin dans les plus brefs délais de mettre en place des services IP VPN utilisant une infrastructure MPLS, et exigent que les implémentations incorporent des classes de transporteurs et garantissent l'interfonctionnement total.

2 Domaine d'application

La présente Recommandation donne une description générale des services VPN de type IP et des prescriptions, y compris en ce qui concerne les architectures de réseau et les aspects d'interfonctionnement dans un ensemble de conceptions possibles.

Les prescriptions relatives aux services IP VPN et les architectures de réseau prenant ceux-ci en charge sont destinées à donner les éléments nécessaires et les lignes directrices devant permettre au groupe de travail d'ingénierie Internet (IETF, *Internet engineering task force*) ou à d'autres organismes de normalisation de définir les améliorations qui pourront être apportées au protocole en ce qui concerne la prise en charge des réseaux IP VPN.

Bien que cette description concerne en premier lieu les réseaux de type MPLS, il est prévu que certaines prescriptions puissent aussi s'appliquer à d'autres architectures de réseau de type IP, par l'emploi d'autres technologies pour la mise en place des réseaux VPN de type IP. L'encapsulage générique pour le routage (GRE, *generic routing encapsulation*), l'introduction du protocole IP dans le protocole IP et la sécurité IP (IPSEC, *IP security*) en sont des exemples.

Une autre Recommandation, l'UIT-T Y.1311, en cours d'élaboration, fournira une architecture générique et des prescriptions relatives aux services pour les réseaux IP VPN.

3 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée.

3.1 Références normatives

[1] UIT-T Y.1241 (2001), *Prise en charge des services de type IP utilisant les capacités de transfert IP*.

[2] UIT-T Y.1310 (2000), *Transport des services IP sur des connexions ATM dans les réseaux publics*.

3.2 Références informatives

[3] IETF RFC 2764 (2000), Armitage, G., Malis, A., *Cadre général pour les réseaux privés virtuels de type IP*.

[4] IETF RFC 3031 (2001), *Architecture à commutation multiprotocole avec étiquette*.

[5] IETF RFC 2547 (1999), *Réseaux VPN à protocole BGP/à commutation MPLS.*

[6] IETF RFC 2917 (2000), A., *Architecture centrale des réseaux IP VPN à commutation MPLS.*

[7] IETF RFC 2998 (2000), *Cadre général pour l'exploitation de services intégrés dans les réseaux de services différenciés*.

[8] IETF RFC 2475 (1998), *Architecture pour les services différenciés*.

[9] IEEE802.1Q (1998), *Normes IEEE pour les réseaux locaux et métropolitains: réseaux locaux dérivés virtuels*).

[10] UIT-T Y.1311 (Projet), *Réseaux privés virtuels IP – Architecture générique et prescriptions de service.*

[11] UIT-T Y.iptc (Projet), *Régulation du trafic et des encombrements dans les réseaux IP*.

[12] UIT-T Y.1720 (Projet), *Commutation de protection pour les réseaux MPLS.*

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

AAA authentification, autorisation et comptabilité (*authentication, authorization and accounting*)

ATM mode de transfert asynchrone (*asynchronous transfer mode*)

BAS serveur d'accès à large bande (*broadband access server*)

BGP protocole de passerelle frontière (*border gateway protocol*)

CE bord client (*customer edge*) (dispositif)

CHAP protocole d'authentification par dialogue à énigme (*challenge handshake authentication protocol*)

CoS classe de service (*class of service*)

CR-LDP protocole de distribution avec étiquette de routage basé sur des contraintes (*constraint-based routing label distribution protocol*)

DHCP protocole de configuration dynamique de serveur (*dynamic host configuration protocol*)

DLCI identificateur de circuit de liaison de données (*data link circuit identifier*)

DNS serveur de nom de domaine (*domain name server*)

DS champ des services différenciés (*differentiated services*)

DSCP point de code des services différenciés (*differentiated service code point*)

DSL ligne d'abonné numérique (*digital subscriber line*)

DVMRP protocole de routage vectoriel multidestinataire à distance (*distance vector multicast routing protocol*)

EXP champ expérimental MPLS (*MPLS experimental field*)

FR relais de trames (*frame relay*)

FTP protocole de transfert de fichiers (*file transfer protocol*)

GRE encapsulage générique de routage (*generic routing encapsulation*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

IETF groupe de travail d'ingénierie Internet (*Internet engineering task force*)

IGP protocole de passerelle intérieure (*interior gateway protocol*)

IP VPN réseau privé virtuel IP (*IP virtual private network*)

IP protocole Internet (*Internet protocol*)

IPSEC sécurité IP (*IP security*)

IS-IS système intermédiaire à système intermédiaire (*intermediate system to intermediate system*)

L2TP protocole de tunnellisation de couche 2 (*layer 2 tunnelling protocol*)

LDAP protocole rapide d'accès à l'annuaire (*lightweight directory access protocol*)

LSP conduit commuté avec étiquette (*label switched path*)

LSR routeur à commutation avec étiquette (*label switching router*)

MD5 algorithme 5 de résumé de message (*message digest 5*)

MIB base d'informations de gestion (*management information base*)

MPLS commutation multiprotocolaire par étiquetage (*multiprotocol label switching*)

NAS serveur d'accès au réseau (*network access server*)

NAT traduction d'adresse de réseau (*network address translation*)

NNTP protocole de transfert d'informations dans le réseau (*network news transfer protocol*)

OAM gestion, exploitation et maintenance (*operation, administration and maintenance*)

OSPF premier itinéraire ouvert le plus court (*open shortest path first*)

P fournisseur (*provider*) (routeur principal)

PAP protocole d'authentification par mot de passe (*password authentication protocol*)

PE bord fournisseur (*provider edge*) (routeur)

PHB comportement par saut (*per hop behaviour*)

PHP avant-dernier saut produit (*penultimate hop popping*)

PIM multidiffusion indépendante du protocole (*protocol independent multicasting*)

POS paquet sur réseau Sonet/SDH (*packet over Sonet/SDH*)

PPP protocole point à point

QS qualité de service

RADIUS service d'authentification à distance des utilisateurs entrants (*remote authentication dial in user service*)

RGT réseau de gestion des télécommunications

RIP protocole d'information de routage (*routing information protocol*)

RNIS réseau numérique à intégration de services

RSVP protocole de réservation de ressources (*resource reservation protocol*)

RTPC réseau téléphonique public commuté

SLA accord de niveau de service (*service level agreement*)

SLS spécification de niveau de service (*service level specification*)

SMTP protocole simple de transfert de messages (*simple mail transfer protocol*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SP fournisseur du service (*service provider*)

TACACS système de commande de l'accès aux contrôleurs d'accès terminaux (*terminal access controller access control system*)

TCI information de contrôle des étiquettes (*tag control information*)

TE ingénierie du trafic (*traffic engineering*)

TOS type de service (*type of service*)

VCC connexion de voie virtuelle (*virtual channel connection*)

VCI identificateur de circuit virtuel (*virtual circuit identifier*)

VLAN réseau local virtuel (*virtual local area network*)

VoIP téléphonie utilisant le protocole Internet (*voice over IP*)

VPI identificateur de conduit virtuel (*virtual path identifier*)

VPN réseau privé virtuel (*virtual private network*)

VPN-ID identificateur de réseau VPN (*VPN identifier*)

VR routeur virtuel (*virtual router*)

5 Réseau privé virtuel de type IP utilisant un modèle de référence à commutation multiprotocolaire par étiquetage

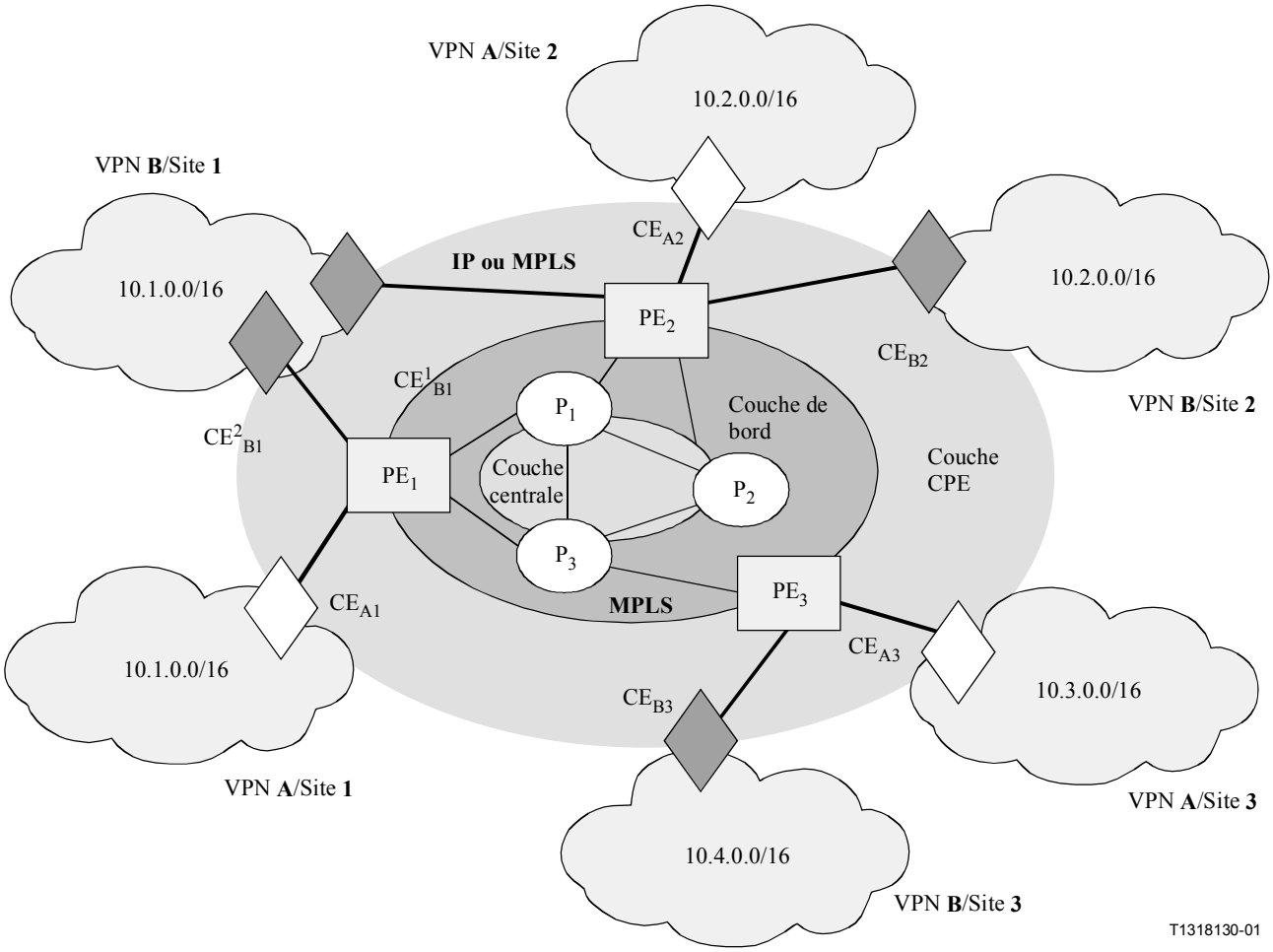


Figure 1/Y.1311.1 – Réseau VPN de type IP utilisant un modèle de référence MPLS

NOTE – La Figure 1 emploie pour la notation des préfixes le réseau d'adresses IPv4.

6 Définition des services

6.1 Définition fonctionnelle d'un "réseau privé virtuel de type IP (utilisant une architecture à commutation multiprotocolaire par étiquetage)"

Un réseau VPN de type IP fournit un service de couche 3 aux clients.

Le site d'un client est connecté au réseau VPN de type IP du fournisseur de services, et ce réseau assure le routage des paquets vers la destination exacte du client. Dans le cadre d'un tel réseau, les routeurs de bord fournisseur sont chargés de se renseigner sur la possibilité qu'a le client d'atteindre la couche 3 et d'en faire part aux autres routeurs.

Soit un ensemble de "sites" qui sont reliés à un réseau commun qu'on peut nommer "réseau dorsal". Lorsqu'on applique une certaine procédure pour créer un certain nombre de sous-ensembles dans cet ensemble, il faut observer la règle suivante: on ne peut établir une connexion IP entre deux sites, au moyen du réseau dorsal, que lorsqu'au moins l'un de ces sous-ensembles contient les deux sites. Les sous-ensembles résultants sont les "réseaux privés virtuels" (VPN, *virtual private network*). Une connexion IP entre deux sites au moyen du réseau dorsal ne peut donc être établie que lorsqu'un

certain réseau VPN contient les deux sites. On ne pourra pas établir de connexion au moyen de ce réseau dorsal entre deux sites qui n'appartiennent pas au même réseau VPN.

Si tous les sites dans un réseau VPN sont la propriété d'une même entreprise, ce réseau VPN est un "intranet" d'entreprise. Si, au contraire, les divers sites dans un réseau VPN sont la propriété de différentes entreprises, ce réseau VPN est un "extranet". Un site peut appartenir à plus d'un réseau VPN, par exemple, un intranet et plusieurs extranets. En général, l'emploi du terme réseau VPN ne permet pas de différencier les intranets des extranets.

Considérons le cas du réseau dorsal qui appartient à un ou à plusieurs fournisseurs de services (SP, *service providers*) et est exploité par les mêmes. Les propriétaires des sites sont les "clients" des fournisseurs de services. Les procédures qui permettent de déterminer si un ensemble particulier de sites est un réseau VPN sont des procédures qui sont appliquées par les clients. Certains clients souhaiteront peut-être que l'application de ces procédures soit entièrement à la charge des fournisseurs de services, tandis que d'autres pourraient souhaiter vouloir appliquer ces procédures eux-mêmes ou en partager la responsabilité avec les fournisseurs de services.

Les mécanismes qui peuvent être employés pour l'application de ces procédures sont l'objet principal de la présente Recommandation. Les mécanismes décrits sont suffisamment généraux pour que ces procédures puissent être appliquées par un fournisseur seul, ou par un client de site dans un réseau VPN aidé du fournisseur de services. L'analyse concerne toutefois principalement le premier cas.

Le cas intéressant ici est celui où le réseau dorsal commun offre un service IP. On ne s'attache pas au cas où ce réseau fait partie du réseau Internet public, mais plutôt à celui où il est le réseau dorsal d'un fournisseur de services ou d'un ensemble de fournisseurs de services avec lesquels le client entretient des relations contractuelles. Ce qui veut dire que le client achète explicitement au fournisseur de services un service VPN, plutôt qu'un accès au réseau Internet. (Le client peut vouloir acheter ou pas au même fournisseur de services un accès au réseau Internet aussi.)

Le client quant à lui peut être une seule entreprise, un ensemble d'entreprises ayant besoin d'un extranet, un fournisseur de services d'accès au réseau Internet, un fournisseur de services d'applications, ou même un autre fournisseur de services qui offre le même genre de services VPN à ses propres clients.

6.2 Définition quantitative d'un "réseau privé virtuel de type IP (utilisant une architecture à commutation multiprotocolaire par étiquetage)"

Les paramètres de dimensionnement caractérisant une offre de service VPN de type IP peuvent être exprimés en fonction du nombre de clients prévus, du nombre d'utilisateurs ou de sites (accès permanents ou temporaires) prévus par client, du nombre total de réseaux IP VPN à mettre en place (un site peut appartenir à plus d'un réseau VPN).

7 Prescriptions relatives aux services

La réalisation d'un réseau VPN devrait prendre en charge les prescriptions relatives aux services qui sont énumérées ci-après:

7.1 Interfonctionnement multivendeur

- Interfonctionnement multivendeur en ce qui concerne les éléments de réseau, le réseau et les niveaux de service.
- Prise en charge des normes Internet (y compris la compatibilité, la modularité, la compatibilité vers l'arrière, les extensions de protocole, etc.).

- La réalisation devrait permettre l'interfonctionnement multivendeur au sein de l'infrastructure de réseau des fournisseurs de services, et l'interfonctionnement avec l'équipement de réseau du client et les services employant le service VPN offert par le fournisseur de services.

7.2 Capacités de gestion des services

Les fonctions de gestion sont habituellement réparties suivant le modèle du réseau de gestion des télécommunications (RGT) qui prévoit quatre couches de macrogestion (gestion commerciale, gestion des services, gestion du réseau et gestion des éléments).

Dans le cas de la gestion d'un réseau VPN, qui se fait suivant ce modèle, il est nécessaire, lors de la mise en place du réseau et de la gestion des dispositifs déployés, de tenir compte des trois principaux aspects suivants:

- connectivité: configuration, dimensionnement et gestion des dispositifs, en particulier lorsque la topologie peut changer;
- surveillance du réseau (en particulier surveillance de la performance et de la capacité) afin de mesurer l'utilisation des ressources et de prévoir les problèmes de dimensionnement;
- sécurité: authentification, autorisation et politiques globales (y compris les risques en matière de sécurité introduits par des incohérences de politique).

Sont donnés ci-après quelques exemples de capacités de gestion des services:

- disponibilité des bases d'informations de gestion (MIB, *management information base*) par réseau VPN et par dispositif;
- gestion des dérangements pour chaque réseau VPN (par exemple, les défaillances du réseau central);
- gestion des accords de niveaux de service (SLA, *service level agreement*) pour chaque réseau VPN;
- gestion des profils de procédure pour chaque réseau VPN;
- gestion des profils de sécurité pour chaque réseau VPN;
- gestion des divers scénarios de connexion des sites clients;
- gestion des diverses topologies;
- gestion des divers scénarios de mise en place des services;
- gestion des divers types de trafic IP client (IPv4, IPv6, monodestinataire, multidestinataire, etc.);
- la configuration de chaque réseau VPN ne devrait pas avoir d'effet sur d'autres sites ou réseaux VPN;
  - l'adjonction ou la suppression d'un site ne devrait pas modifier la configuration des bords fournisseur (PE, *provider edge*) autres que celui auquel le site est connecté;
  - l'adjonction ou la suppression d'un site dans un réseau VPN donné ne devrait pas avoir d'effet négatif sur les autres réseaux VPN, y compris les réseaux VPN dont le ou les sites sont connectés au même bord fournisseur que le site qui a fait l'objet de l'adjonction ou de la suppression.

L'exploitation et l'interfonctionnement automatisés au moyen de plates-formes de gestion normalisées devraient être poursuivis.

NOTE – Bien que la spécification d'une base d'informations de gestion (MIB) décrivant en détail la configuration des éléments de réseau qui interviennent dans le dimensionnement des services VPN constitue une prescription essentielle en matière de configuration de réseau, elle ne sera pas abordée dans la présente Recommandation.

Afin de faciliter la gestion des services, une image logique du réseau VPN est utile, sa topologie y étant indiquée en plus de celle du réseau dorsal. Elle peut être employée pour le dimensionnement et la vérification de la connectivité, la vérification de la configuration ou de la confidentialité, la gestion des dérangements et de la performance.

7.2.1 Connectivité du réseau

Lors de l'extension d'un réseau VPN, les nouveaux dispositifs doivent être configurés selon les modèles de services qui sont établis par le fournisseur, et cette tâche est assez répétitive. Le processus pourrait être centralisé par le système de gestion de manière à assurer la cohérence des paramètres et à accélérer la mise en place en rendant la configuration automatique.

Comme la configuration et la topologie d'un réseau VPN dépendent beaucoup de l'organisation du client, le dimensionnement des modèles doit satisfaire aux exigences spécifiques du client [accès distants, politique en matière de sécurité, qualité de service (QS)]. Le système de gestion pourrait reposer sur des informations centralisées afin de disposer de l'ensemble des paramètres nécessaires à une adaptation optimale des modèles aux besoins spécifiques. Il pourrait même optimiser certains conduits dans les tables de routage.

Un tel système peut renforcer la réactivité du réseau en cas de défaillance ou de violation de la procédure. Il peut réduire le temps du dimensionnement lorsque la configuration de réseau VPN demandée par le client est courante (adjonction, modification, suppression), tâche qui peut être très lourde en termes de mise à jour des tables de routage.

Dans un environnement multidomaine, la qualité de service de bout en bout dépend de celle qui est fournie dans chaque domaine. Lorsqu'un réseau VPN s'étend sur deux domaines, le dimensionnement de la qualité de service peut atteindre ses limites, et un tel problème semble difficile à résoudre.

7.2.1.1 Vérification de la connectivité

Il est souhaitable qu'il puisse être possible de vérifier la connectivité entre des sites d'utilisateur dans un réseau VPN. Si une image logique du réseau VPN est donnée et que le résultat de cette vérification y est indiqué, l'opérateur pourra aisément comprendre le résultat.

7.2.1.2 Vérification de la configuration et de la confidentialité

Il est souhaitable qu'il puisse être possible de vérifier la configuration et la confidentialité d'un réseau VPN. Par confidentialité, on entend ici le fait que le réseau VPN ne peut être atteint d'un endroit extérieur à lui. Si une image logique du réseau VPN est donnée et que le résultat de cette vérification y est indiqué, l'opérateur pourra aisément comprendre le résultat.

7.2.2 Surveillance des services

La surveillance du réseau dans le cadre des réseaux VPN inclut des tâches traditionnelles telles que la gestion des dérangements, la gestion des niveaux de service et la comptabilité.

7.2.2.1 Gestion des dérangements

Puisque les réseaux VPN sont fondés sur une infrastructure commune de réseau, le système de gestion des réseaux devrait permettre d'informer le fournisseur des conséquences pour les réseaux VPN d'une défaillance d'un dispositif qui a été pris en charge par celui-ci. Il devrait donner une image logique du réseau indiquant la topologie du réseau VPN en plus de celle du réseau dorsal. Il devrait fournir des pointeurs vers les configurations qui y sont associées et des informations sur les

exigences du client de manière à faciliter la localisation des dérangements et à prendre des mesures correctives, les effets sur l'ingénierie du trafic et les considérations de sécurité pouvant être importants.

Pour résumer, la gestion des dérangements comporte les éléments suivants:

- information des clients en ce qui concerne les défaillances;
- détection des dérangements (rapports d'incident, alarmes, visualisation des défaillances, violation des accords SLA);
- localisation des dérangements (analyse des rapports d'alarme, diagnostics);
- enregistrements des incidents, registres (établissement et suivi du ticket d'incident);
- mesures correctives (circulation, routage, ressources, etc.).

7.2.2.2 Gestion de la performance

Le système de gestion de la performance devrait être en mesure de surveiller le comportement du réseau afin d'évaluer la performance qui est par ailleurs prévue dans les accords de niveaux de service. Les clients s'abonnent à de nombreux services VPN différents et le système devrait pouvoir appliquer des techniques de mesure propres aux composantes de service sollicitées (sécurité, transfert multidestinataire, accès distant). Ces techniques peuvent être soit gênantes soit non gênantes selon les paramètres ou les services examinés.

La détermination de la qualité de service et la surveillance des accords SLA peuvent être reliés par des procédures de surveillance qui:

- décrivent les mécanismes garantissant la qualité de service et les mesures associées qui devraient être effectuées;
- commandent les ressources de surveillance telles que les sondes et les agents distants.

Les agents distants peuvent être les garants de la surveillance du réseau parce qu'ils permettent de recueillir des statistiques directement aux points d'accès du réseau employés par les clients et les utilisateurs mobiles. Une image logique du réseau VPN indiquant sa topologie aidera les opérateurs à comprendre le résultat des activités de gestion de la performance.

Pour résumer, la gestion de la performance comporte les éléments suivants:

- mesure en temps réel de la performance (initialisation et modification des indicateurs et des seuils, collecte de données);
- surveillance en temps réel (utilisation des ressources), état du réseau VPN (en amont et en aval);
- analyse (largeur de bande, temps de réponse, disponibilité, perte de paquets);
- statistiques et tendances à partir des mesures recueillies.

En outre, le système de gestion de la performance devrait pouvoir assumer la "gestion dynamique des largeurs de bande":

- la gestion dynamique des largeurs de bande devrait permettre la réponse en temps réel aux demandes des clients relatives aux modifications des largeurs de bande attribuées (le plan de commande devrait être assez souple pour s'adapter aux modifications en temps réel).

L'évolution de la performance (par exemple, l'attribution des largeurs de bande) devrait pouvoir être suivie.

NOTE – L'attribution des largeurs de bande devrait normalement se faire dans les gammes et dans les limites stipulées dans l'accord de niveau de service (SLA), éventuellement au moyen de mécanismes internes aux fournisseurs de services, qui permettent de vérifier l'exactitude de l'attribution.

7.2.2.3 Comptabilité

Le fait d'être en mesure d'associer les profils des services aux clients et aux ressources fournissant ces services peut faciliter la comptabilité, ce qui peut être important pour les services souscrits. Le système de comptabilité doit pouvoir trier les très nombreuses informations sur l'utilisation des services et relier ces informations aux informations sur la performance et la gestion des dérangements, de manière à pouvoir émettre une facture conforme aux services réellement fournis. Il convient de noter que les prescriptions relatives à la comptabilité peuvent aller à l'encontre des prescriptions en matière de sécurité.

Pour résumer, la procédure de comptabilité comporte les éléments suivants:

- mesure de l'utilisation des ressources;
- publication d'informations sur la comptabilité;
- enregistrement des mesures (création et administration de fichiers);
- contrôle des quotas par client (mise à jour de la consommation courante, vérification des autorisations de consommation).

7.2.3 Caractéristiques de gestion de la sécurité

Les caractéristiques du système de gestion de la sécurité d'une réalisation d'un réseau VPN doivent garantir la sécurité des connexions de réseau, ainsi que la confidentialité et l'intégrité des données.

7.2.3.1 Commande d'accès

La commande d'accès dicte le degré de liberté qu'a un utilisateur de réseau VPN, et contrôle l'accès des autres utilisateurs aux applications et aux différentes parties du réseau.

Un réseau VPN qui ne dispose pas de la commande d'accès ne garantit que la sécurité des données transportées mais pas le réseau. Les capacités de commande d'accès protègent l'ensemble du réseau de manière à garantir que les utilisateurs de réseau VPN ont un accès complet aux ressources que sont les applications, mais à elles seules uniquement.

Lorsque la largeur de bande du client a été négociée, la commande d'accès au niveau du réseau devrait garantir qu'aucun client ne viole son contrat.

7.2.3.2 Authentification

L'authentification est la procédure qui permet de vérifier que l'expéditeur est réellement celui qu'il dit être. Le système de gestion de la sécurité devrait la mettre en application.

La prise en charge de procédés d'authentification poussée est particulièrement importante pour garantir la confidentialité aussi bien des communications d'un point d'accès à un réseau VPN à un point d'accès à un réseau VPN (bord fournisseur à bord fournisseur) que de celles d'un point client à un point d'accès à un réseau VPN (bord client à bord fournisseur. Ceci est particulièrement important pour empêcher toute tentative délibérée de perturbation en un point d'accès à un réseau VPN (par exemple, un bord fournisseur simulant d'entrer dans un réseau VPN particulier ou dans un ensemble de réseaux) en présence de mécanismes de détection automatique.

L'accès itinérant impliquant une évolution dynamique des bords fournisseur desservant un réseau VPN spécifique est une autre situation qui nécessite de tels procédés d'authentification en présence de mécanismes de détection automatique. Diverses méthodes d'authentification sont disponibles afin de satisfaire aux besoins des mises en œuvre particulières de réseaux VPN, y compris l'authentification du nom de l'utilisateur et du mot de passe, les serveurs du service d'authentification à distance des utilisateurs entrants (RADIUS, *remote authentication dial in user service*) ou du système de commande de l'accès aux contrôleurs terminaux (TACACS, *terminal access controller access control system*), les serveurs du protocole allégé d'accès à l'annuaire (LDAP, *lightweight directory access protocol*), les certificats numériques X.509, les cartes à puce, etc.

Le dimensionnement devient critique lorsque le nombre de clients itinérants ou mobiles augmente. Le procédé d'authentification appliqué à ces implémentations doit être aussi bien gérable que facilement mis en place pour un grand nombre d'utilisateurs et de points d'accès à un réseau VPN.

7.2.3.3 Confidentialité des données

La réalisation d'un réseau VPN devrait assurer la protection de la confidentialité des données transmises. Le système de gestion de la sécurité pourrait y participer en faisant respecter la confidentialité des données.

La confidentialité des données pourrait être assurée au moyen du chiffrement ou d'autres mécanismes, par exemple la scission des données.

La réalisation peut prendre en charge plusieurs algorithmes et procédés de chiffrement, y compris ceux qui correspondent aux normes DES, 3DES et IPSec. Le chiffrement, le décryptage et la gestion des clés pourraient être incorporés dans les profils qu'un système de gestion de procédures peut appliquer. Il devrait être possible de mettre en œuvre le chiffrement pour des services particuliers.

7.2.3.4 Communication dynamique d'informations sur la sécurité

Le fait de pouvoir communiquer dynamiquement les mécanismes de sécurité à appliquer à un certain trafic particulier de données utilisateur (à travers un réseau VPN, le long d'une route, etc.) serait utile pour la gestion. Cette fonctionnalité devrait être assurée à toutes les échelles.

La communication automatique d'informations sur la sécurité se rapportant à une certaine partie du trafic de données valoriserait le processus de mise en place d'un réseau VPN. Cela voudrait dire qu'un dispositif de bord fournisseur qui est lié à un certain site client donnerait à ses dispositifs homologues de bord fournisseur des informations sur la sécurité (par exemple, le type de galerie) en ce qui concerne le trafic à envoyer vers le site en question.

La communication de ces informations sur la sécurité pourrait accompagner l'ensemble du trafic à travers les réseaux VPN qui est envoyé vers le bord fournisseur ayant fait la communication, le trafic qui est envoyé à un réseau VPN précis ou le trafic qui est envoyé vers une route donnée dans un réseau VPN.

7.2.4 Caractéristiques de gestion des accords de niveau de service et de la qualité de service

Les accords de niveau de service (SLA) pour chaque réseau VPN et/ou chaque site dans un réseau VPN et/ou chaque route dans un réseau VPN devrait comporter les éléments suivants [1]:

- objectifs de niveau de service comportant certains ou tous les éléments suivants:
  - capacité de transfert IP;
  - paramètres de qualité de service;
  - disponibilité;
  - fiabilité;
  - confirmation de fourniture de service;
  - prise en charge de la mobilité et de la portabilité;
  - sécurité;
  - largeur de bande;
  - priorité;
  - authentification;
  - protocoles pris en charge;

- souplesse – dimensionnement et connectivité;
- durée de l'accord SLA;

- objectifs de surveillance des services:
  - surveillance de la qualité de service – comparaison avec les objectifs;
  - suivi du flux;
  - rapports le cas échéant;
- objectifs de compensation financière:
  - options de facturation;
  - pénalités;
  - fixation des prix;
  - indemnités de cessation anticipée.

NOTE – Les prescriptions générales relatives aux accords SLA sont plus complètement décrites dans l'UIT-T Y.1241 [1].

La spécification du niveau de service fait partie de l'accord plus général de niveau de service. Elle contient les caractéristiques de transport entre la ou les interfaces données d'entrée et de sortie d'un réseau VPN, qui sont exigées par le client pour un ensemble corrélé de paquets.

Un client de site dans un réseau VPN devrait être en mesure de négocier les caractéristiques relatives à la performance d'un ou de plusieurs flux entre ses sites dans les réseaux VPN et le fournisseur de services VPN.

Sont énumérées ci-après un certain nombre de conditions qui devraient être remplies par une procédure de négociation sur la spécification de niveau de service (SLS, *service level specification*).

Cette procédure de négociation doit comporter les éléments suivants:

- demandes initiales de service, conformes aux composantes des spécifications SLS stipulées;
- accusé de réception du service, indiquant l'accord avec le niveau de service demandé;
- rejet du service indiquant toutefois la possibilité d'offrir un service semblable (ou portant l'indication d'un autre point de code des services différenciés (DSCP, *differentiated services code point*) à utiliser pour un service donné). Le message de réponse peut indiquer l'offre associée en remplaçant les attributs proposés des spécifications SPS (indices);
- rejet du service indiquant l'incapacité de fournir le service;
- modification du service aussi bien par l'utilisateur que par le fournisseur de services;
- la procédure de négociation devrait pouvoir tenir compte d'un retour d'information sur les événements liés au service, par exemple, la dégradation de la qualité de fonctionnement pouvant conduire à la renégociation des spécifications SLS.

De plus amples détails concernant les paramètres éventuels dans les spécifications SLS sont donnés au 7.4.

7.3 Fonctions de sécurité

7.3.1 Introduction

Les mécanismes de sécurité appliqués à la prise en charge de la fourniture des services IP VPN devraient être aussi transparents que possible pour l'utilisateur final, sauf peut-être pour les utilisateurs finals distants accédant au réseau IP VPN par l'intermédiaire du RNIS, du RTPC, des lignes d'abonné numérique (xDSL, *digital subscriber line*) ou du réseau Internet pour lesquels des services d'authentification, d'autorisation et de comptabilité (AAA, *authentication, authorization and accounting*) pourraient devoir être mis en place.

Les utilisateurs d'un réseau IP VPN devraient être en mesure et être autorisés à appliquer leurs propres mécanismes internes de sécurité, en plus de ceux qui sont mis en place par le fournisseur de service, afin de protéger des applications particulières ou le trafic interne au réseau IP VPN. Ces services de sécurité interne devraient idéalement être conformes aux prescriptions de l'opérateur, en particulier lorsqu'un accord SLA, notamment concernant la qualité de service, a été conclu entre le client et le fournisseur de services. Dans ce cas, la solution de sécurité appliquée par le client ne devrait pas occulter les informations employées par le fournisseur de services pour fixer les caractéristiques de qualité de service. En général, le fournisseur de services est contraint, conformément à la caractéristique de confidentialité des réseaux IP VPN, de garantir, dans la mesure du possible, que les mécanismes internes de sécurité qui pourraient être appliqués dans un réseau IP VPN ont toutes les chances d'être pris en charge de manière transparente par l'offre de service IP VPN.

Le réseau IP VPN sera en général protégé selon les exigences du client afin que la caractéristique de confidentialité de son réseau IP VPN puisse se traduire dans les faits. Cela implique que le fournisseur de services garantira en particulier que:

- tous les équipements (par exemple, les routeurs) intervenant dans la mise en place d'un réseau IP VPN seront en mesure de s'identifier et de s'authentifier mutuellement de manière que le trafic échangé au sein du réseau IP VPN puisse être routé. En fonction de la nature de ce trafic et de la nature de l'équipement impliqué dans son routage, cette identification et cette authentification pourraient devoir être faites entre les bords client (CE, *customer edge*), et/ou entre les bords client et les routeurs de bord fournisseur ou les fournisseurs, et/ou entre les routeurs de bord fournisseur ou les fournisseurs;
- les services de confidentialité seront fournis et intégrés par l'opérateur comme un élément du service. Les services de confidentialité et d'intégrité devront s'appliquer:
  - soit à tout le trafic échangé dans le réseau IP VPN au-dessus de la dorsale IP entre les différents sites;
  - soit à un certain trafic restreint dans le réseau IP VPN identifié par une combinaison d'adresses IP d'origine et/ou de destination et/ou de protocoles et/ou d'applications (par exemple, la sécurité entre les bords fournisseur et les fournisseurs, la sécurité le long de la route, etc.);
  - au trafic d'administration puisque celui-ci peut comporter des informations sensibles liées à la configuration, aux utilisateurs, à la sécurité ou à la comptabilité du réseau IP VPN;
- l'isolement de chaque réseau IP VPN sera rigoureusement assuré et l'opérateur pourra au moins observer les tentatives d'intrusion dans le but de mettre fin à celles-ci;
- de même, l'accès aux divers équipements mis en place pour la prise en charge des services IP VPN sera rigoureusement protégé afin d'empêcher que des utilisateurs non autorisés accèdent aux ressources IP VPN. Sera en particulier protégé l'accès aux ressources de commutation qui sont gérées par le fournisseur de services afin d'empêcher toute attaque malveillante pouvant être lancée par un quelconque pirate informatique (utilisateur Internet ou autre);
- les éléments des services de sécurité offerts présenteront une certaine souplesse afin de tenir compte du fait que certaines données pourraient nécessiter une protection plus forte que d'autres.

Il faudrait incorporer dans une offre de services IP VPN les fonctions de sécurité suivantes:

- isolement;
- identification de l'utilisateur;
- authentification de l'utilisateur;

- sécurité du flux;
- identification des homologues;
- authentification des homologues;
- protection du site.

Ces fonctions sont décrites ci-après.

7.3.2 Isolement du réseau VPN

Du point de vue du fournisseur de services et à un niveau élevé de description, la fonction d'isolement du réseau VPN consiste à assurer que tout le trafic échangé au sein du réseau IP VPN reste ignoré et protégé des autres utilisateurs de la dorsale, tout en étant insensible en ce qui concerne le trafic transporté au moyen de la dorsale IP le prenant en charge.

De ce point de vue, le fournisseur de services de service garantira, lors de la mise en place du service, que celui-ci est conforme aux caractéristiques suivantes:

- seul un ensemble d'utilisateurs désignés d'avance peut accéder au réseau IP VPN;
- l'accord SLA, notamment en ce qui concerne la qualité de service, sera garanti quel que soit l'état du trafic rencontré dans la dorsale IP le prenant en charge, et en particulier lorsque ce trafic est dû à d'autres clients dans le cadre du service IP VPN ou en dehors de celui-ci;
- la connectivité IP sera assurée de telle manière que seuls les sites enregistrés dans les réseaux IP VPN et les utilisateurs distants agréés peuvent échanger des informations dans le réseau IP VPN. En conséquence, les équipements homologues pourront être amenés à s'identifier ou à s'authentifier mutuellement à différents niveaux du service IP VPN;
- l'échange de trafic pourrait être protégé grâce aux fonctions de chiffrement et/ou d'authentification;
- les fonctions de gestion du réseau IP VPN n'affecteront pas d'autres réseaux IP VPN ou services.

Cette fonction d'isolement peut être obtenue en appliquant une combinaison de fonctions liées à l'architecture, à la qualité de service, à la sécurité et aux domaines fonctionnels d'administration. Cet ensemble de fonctions, correctement mis en place, forme une fonction générique nommée "isolement VPN". Cette fonction globale d'isolement est néanmoins classée dans le domaine de sécurité en raison des sérieuses conséquences des caractéristiques de sécurité dont il a été tenu compte lors de sa réalisation.

7.3.3 Identification de l'utilisateur du réseau VPN

Parmi les utilisateurs des réseaux IP VPN, il peut y avoir des personnes voyageant qui ne sont pas reliées de façon permanente à l'un des sites dans un réseau IP VPN. Afin de commander l'accès de ces utilisateurs au réseau IP VPN, il est nécessaire de les identifier. Cette identification s'appliquera aux différentes mises en place possible qui ont été indiquées (intranet, extranet, etc.), en gardant à l'esprit que certains de ces utilisateurs peuvent accéder à plusieurs réseaux IP VPN distincts. Cette fonction d'identification peut être employée pour automatiser ou lancer des interventions techniques, qui sont nécessaires pour établir la communication avec les réseaux IP VPN auxquels l'utilisateur désire se connecter.

Il doit être tenu compte des deux cadres principaux d'identification suivants:

- identification en cas de "mobilité", que cette mobilité concerne les sites d'un intranet ou ceux d'un extranet;
- identification lorsque l'utilisateur tente d'atteindre son réseau IP VPN à partir d'un point d'accès public ou privé par l'intermédiaire d'un serveur d'accès au réseau (NAS, *network access server*) ou d'un serveur à large bande (BAS, *broadband access server*), ou même d'un réseau disposant d'un accès Internet auquel il a un accès temporaire.

Cette fonction peut être mise en œuvre dans sa totalité ou en partie par le fournisseur de services IP VPN. La possibilité d'itinérance devra probablement être prévue entre le fournisseur et le client qui pourrait décider de procéder à l'identification des utilisateurs du réseau IP VPN dans le cas où ceux-ci refuseraient d'utiliser le service d'identification ou d'authentification. En fait, cette authentification sera utilisée par le fournisseur du service d'accès qui doit identifier l'utilisateur en vue d'assurer la connexion IP et par le service d'identification des utilisateurs du réseau IP VPN dans le but d'accepter la connexion au réseau IP VPN. Les deux mécanismes peuvent être liés entre eux.

Dans ce cas, les ressources du fournisseur d'accès et celles du fournisseur de services IP VPN doivent travailler ensemble et un accord doit intervenir sur la spécification d'identification commune.

Toutes les informations nécessaires pour identifier les utilisateurs doivent être enregistrées et devraient idéalement être conservées par le client. Ces informations devraient être tenues à la disposition du fournisseur d'accès pour qu'il puisse commander l'accès IP.

7.3.4 Authentification de l'utilisateur du réseau VPN

Le domaine d'application de cette fonction d'authentification est le même que celui qui est décrit ci-dessus et concerne les utilisateurs qui veulent disposer d'un accès distant. Cette fonction d'authentification consistera à assurer, à un bon niveau de confiance, que l'utilisateur déclaré est celui qu'il déclare être.

Selon le niveau de sécurité souhaité par le client, divers protocoles d'authentification peuvent être utilisés à ces fins, mais les protocoles d'authentification par mot de passe (PAP, *password authentication protocol*) ou par dialogue à énigme (CHAP, *challenge handshake authentication protocol*) devraient au moins être pris en charge parce qu'ils sont actuellement très employés dans une large gamme d'équipements et de services.

Cette fonction d'authentification peut être exécutée complètement ou partiellement par le fournisseur de services IP VPN. Dans le second cas, le relais pour la phase d'authentification peut se faire au point d'accès du client, conformément aux clauses du contrat.

7.3.5 Protection des flux

Dans le cadre actuel de mise en place d'un réseau VPN au moyen d'une dorsale publique IP (qui fait partie du réseau Internet), les seules fonctions de routage ne suffisent pas à protéger les flux d'un client donné. En fait, même si les flux sont correctement acheminés entre les sites (y compris ceux d'utilisateurs distants), le trafic correspondant peut être intercepté et en conséquence lu ou altéré.

La protection des flux devrait être assurée au niveau de la couche Réseau afin que soient garanties les deux principales caractéristiques suivantes:

- confidentialité du trafic, de manière que seul l'équipement autorisé puisse le décrypter;
- intégrité, de manière à protéger les destinataires d'une altération qui aurait pu être introduite au cours du transport.

Ces deux fonctions s'appliqueront à ce qui est nommé ici "trafic de données" du client, qui comprend le trafic échangé entre deux sites, entre des utilisateurs distants et des sites et même entre des utilisateurs distants. Mais elles s'appliqueront aussi au "trafic de commande" qui n'est pas nécessairement perçu par le client mais est néanmoins essentiel pour la gestion de son réseau IP VPN.

Même s'il est fortement recommandé d'appliquer ces fonctions dans un cadre opérationnel, elles ne seront pas considérées comme obligatoires et devraient être activées seulement à la demande du client. Dans le même ordre d'idée, ces fonctions devraient être aussi souples que possible de manière à pouvoir être mises en place indépendamment les unes des autres et appliquées à certaines parties du trafic (le niveau de sécurité peut varier en fonction du trafic dont il est tenu compte, tandis que des considérations relatives à la qualité de fonctionnement peuvent aussi conduire à protéger des parties du trafic).

7.3.6 Identification des homologues

Le trafic échangé au sein d'un réseau IP VPN peut mettre en jeu plusieurs catégories d'équipements qui doivent travailler ensemble pour fournir le service. Ces éléments de réseau peuvent être des bords client, des coupe-feu, des routeurs de dorsale, des serveurs, des postes de gestion, etc.

Chaque fois que deux éléments de réseau doivent travailler ensemble, il est nécessaire que les homologues procèdent à une identification (se traduisant par une authentification le cas échéant, voir ci-après) avant d'accepter d'acheminer le trafic reçu ou de fournir le service demandé. Cette identification peut servir de point de départ à l'adaptation de la fourniture du service, si ce n'est, dans la plupart des cas, à la commande de l'accès aux ressources du réseau.

Cette fonction d'identification des homologues est destinée ici à ne s'appliquer qu'aux éléments de réseau qui participent à la mise en place du réseau IP VPN. Sont exclus tous les besoins d'identification liés aux applications des utilisateurs.

Ces identifications des homologues pourraient, par exemple s'appliquer:

- au trafic entre un bord client et un point d'accès d'un fournisseur de services (point d'accès fournisseur/bord fournisseur);
- au trafic entre des bords client appartenant au même réseau IP VPN;
- aux routeurs chargés de l'annonce de la route (ces routeurs pourraient être un routeur de bord client et un routeur de fournisseur/bord fournisseur ou deux routeurs de bord client s'échangeant des informations sur le routage);
- au serveur de procédure et à un élément de réseau;
- au poste de gestion et à un agent de protocole simple de gestion de réseau (SNMP, *simple network management protocol*).

Cette fonction d'identification ne sera pas considérée comme une fonction atomique parce qu'elle est plutôt distribuée et probablement appliquée différemment selon les éléments de réseau concernés. Mais globalement, le service IP VPN prévoira une fonction d'identification des homologues en définissant où cela est nécessaire comment elle sera appliquée, combien elle sera protégée et de quelle manière les informations d'identification nécessaires à l'exploitation du service seront mises à disposition et gérées.

7.3.7 Authentification des homologues

Cette fonction est la continuation, en termes de sécurité, de la fonction décrite ci-dessus. Elle vise à authentifier les homologues en suivant la même philosophie que celle qui est adoptée pour l'identification et l'authentification des utilisateurs.

7.3.8 Protection du site

Comme nous l'avons vu précédemment, un site peut appartenir à un réseau IP VPN de diverses façons. Il peut appartenir à un réseau IP VPN mis en place pour prendre en charge un réseau intranet (dans ce cas, il est interconnecté avec des sites appartenant à la même entreprise), à un réseau IP VPN mis en place entre différentes entreprises pour prendre en charge un réseau extranet, ou aux deux.

Dans ce cadre, un site pourrait faire l'objet de diverses attaques ayant des origines différentes. Les origines possibles sont les suivantes:

- utilisateurs connectés à la dorsale publique IP de prise en charge, puisque par définition un réseau IP VPN repose sur une infrastructure publique et sur une infrastructure IP partagée;
- utilisateurs provenant du réseau Internet, si la dorsale IP offre un accès Internet;
- utilisateurs provenant de sites distants appartenant au même réseau IP VPN.

Les risques qu'un site peut encourir sont les suivants:

- refus de service (lorsqu'un pirate informatique agit de telle manière qu'un service ne peut être employé. Envoi massif de courrier électronique non sollicité et surcharge de la ligne d'accès, par exemple);
- virus informatiques.

Intrusions

Afin d'éviter ces risques, le fournisseur de services IP VPN appliquera des fonctions qui commandent l'accès au site, grâce à la mise en place de fonctions de filtrage assurées par les coupe-feu, par exemple, mais aussi la surveillance, l'alerte et éventuellement la suspension de toutes les activités suspectes afin de détecter toutes les attaques possibles.

7.4 Prise en charge des diverses prescriptions relatives à la qualité de service

La spécification technique des paramètres de trafic correspondant et des engagements en ce qui concerne la qualité de service est indiquée comme étant la "spécification de niveau de service" (SLS, *service level specification*).

- Spécification SLS pour services avec meilleur effort.
- Spécification SLS pour modèles de services différenciés:
  - Spécification SLS point à nuage de points (modèle de tuyaux)

    La réalisation devrait prendre en charge une spécification SLS "point à nuage de points". Cela veut dire que les paramètres de trafic ainsi que les engagements en ce qui concerne la qualité de service sont spécifiés sur la base du trafic échangé entre un site dans un réseau VPN et le réseau dorsal VPN à commutation MPLS (contrairement au trafic échangé entre deux sites dans un réseau VPN). Ce modèle est aussi nommé modèle de "tuyaux". Un exemple de spécification SLS "point à nuage de points" est la spécification SLS concernant le réseau VPN à commutation MPLS qui définit la conformité avec le contrat de trafic à partir de la mesure de tous les paquets transmis d'un site donné dans réseau VPN vers le réseau dorsal VPN à commutation MPLS sur une base agrégée (à savoir quel que soit le site de destination dans un réseau VPN à commutation MPLS de chaque paquet).
  - Spécification SLS point à point (modèle de canalisation)

    La réalisation devrait prendre en charge une spécification SLS "point à point". Cela veut dire que les paramètres de trafic ainsi que les engagements en ce qui concerne la qualité de service sont spécifiés sur la base du trafic échangé entre deux sites dans un réseau VPN. Ce modèle est aussi nommé modèle de "canalisation". Les spécifications SLS "point à point" sont semblables aux spécifications SLS qui sont généralement prises en charge par des technologies de couche 2 telles que le relais de trames et le mode de transfert asynchrone (ATM, *asynchronous transfer mode*). Un exemple de spécification SLS "point à point" est la spécification SLS concernant le réseau VPN à commutation MPLS qui définit la conformité avec le contrat de trafic à partir de la mesure séparée des paquets transmis d'un site donné dans réseau VPN vers tous les sites de destination distants dans un réseau VPN.
  - Spécifications SLS point à multisite et multisite à point

    La réalisation devrait prendre en charge les spécifications SLS "point à multisite" et "multisite à point". Cela veut dire que les paramètres de trafic ainsi que les engagements en ce qui concerne la qualité de service sont spécifiés sur la base du trafic échangé entre un site dans un réseau VPN et un sous-ensemble d'autres sites dans ce réseau VPN.

– Transparence en matière de classe de service

  La réalisation devrait prendre en charge la transparence en matière de classe de service (CoS, *class of service*). Cela veut dire que le service public dans un réseau VPN à commutation MPLS devrait être en mesure d'attribuer au champ des services différenciés (DS, *differentiated services*) IP à la sortie du réseau VPN à commutation MPLS la même valeur qu celle qu'il avait à l'entrée du service. La justification de cette prescription est donnée au 10.3.

- Spécification SLS pour modèle de services intégrés.
- Accords SLA pour chaque réseau VPN (mesurable).

Les prescriptions générales des accords SLA pour les réseaux de type IP sont décrites dans l'UIT-T Y.1241 [1]. Certaines composantes de ces accords peuvent s'appliquer aux réseaux IP VPN.

- Qualité de service stricte (réseau VPN à largeur de bande garantie).
- Prise en charge de la qualité de service dans des scénarios plus complexes:
  – mappage de la classe de qualité de service d'un réseau VPN à un autre lors de l'interfonctionnement entre réseaux VPN;
  – mappage de la classe de qualité de service dans le cas de réseaux VPN partagés par plusieurs fournisseurs.

Sont décrits ci-après les paramètres des spécifications SLS qui devraient être spécifiés afin que le fournisseur de services puisse prendre en charge les types de spécifications SLS définis pour les réseaux VPN. L'ensemble corrélé de paquets forme un flux. Les moyens qui servent à corréler les paquets pour que ceux-ci fassent partie d'un flux sont décrits dans le "descripteur de flux".

Le service devant être assuré en ce qui concerne le flux à travers le réseau VPN dépend du domaine d'application du service, qui indique l'ensemble d'interfaces d'entrée et de sortie entre lesquelles les caractéristiques de transport doivent être garanties.

Afin que soient réalisées les caractéristiques de transport qui sont garanties, il faudrait que les paramètres de conformité en matière de trafic du flux soient les bons. Un trafic conforme recevra des garanties comme contractées quant à la performance. Le trafic excédentaire lors de l'essai de conformité du trafic recevra le traitement qui lui correspond.

Le service des transports peut encore être associé aux paramètres de programmation et de fiabilité des services.

On trouvera des informations plus détaillées dans les références à l'Appendice II.

7.5 Prise en charge des divers protocoles de routage (aux bords et au centre du réseau du fournisseur de services)

- Il ne devrait exister aucune restriction concernant les protocoles d'acheminement employés entre les routeurs des bords client et fournisseur.
- Le choix du protocole de passerelle intérieure (IGP, *interior gateway protocol*) du fournisseur de services ne doit pas dépendre du ou des protocoles d'acheminement employés entre les routeurs des bords fournisseur et client. En outre, ce choix devrait être souple, et non limité à un seul protocole d'acheminement.

7.6 Capacités de routage susceptibles d'être dimensionnées

- L'importance de la capacité de routage et/ou de programmation dans un routeur de fournisseur ne doit pas dépendre du nombre total de réseaux VPN pris en charge par un fournisseur de services ni du nombre de sites dans les réseaux VPN. Dans certains scénarios particuliers, il pourrait être envisagé de faire un compromis réduisant l'importance de la capacité de routage et/ou de programmation dans un routeur de fournisseur afin que le

fournisseur de services puisse disposer de capacités supplémentaires ou de valeurs ajoutées (par exemple, transfert multidestinataire à l'intérieur d'un réseau VPN).

- L'importance des informations concernant le routage (et/ou la configuration) au bord fournisseur peut ne dépendre que des réseaux VPN dont le ou les sites sont connectés à ce bord fournisseur.
- La réalisation devrait prendre en charge le filtrage d'informations concernant le routage dans les réseaux VPN dans des configurations de bord fournisseur à bord fournisseur et de bord client à bord fournisseur.

7.7 Autodécouverte

La réalisation devrait prendre en charge un mécanisme d'autodécouverte qui achemine dynamiquement les informations sur les réseaux VPN entre les bords fournisseur. Ce mécanisme peut être utilisé à des fins différentes, essentiellement à des fins de dimensionnement des services (un exemple fondé sur le protocole de passerelle limite (BGP, *border gateway protocol*) est donné dans les références à l'Appendice II).

7.8 Prise en charge des divers types de trafic IP client

- Trafic monodestinataire;
- Trafic multidestinataire;
- La réalisation devrait être en mesure (facilement extensible) de permettre à un fournisseur de services de disposer d'un réseau dorsal IPv4 ou IPv6 afin que ses clients puissent bénéficier de réseaux VPN tant IPv4 que IPv6.

7.9 Prise en charge des diverses topologies de réseaux VPN

– La réalisation devrait prendre en charge une large gamme de connexions intersites allant de celles reliant un point de concentration relais à une configuration partiellement ou totalement en maille.

7.10 Prise en charge des divers scénarios d'accès client

- Accès permanent et temporaire
  - rattachement multiple;
  - liaisons par entrées dérobées;
  - accès commuté.
- La prise en charge de la caractéristique d'acquisition du droit d'accès du client (le système de gestion pourrait reposer sur des informations centralisées afin de disposer de l'ensemble des paramètres nécessaires à une adaptation optimale des modèles aux besoins spécifiques. Cela pourrait réduire le temps du dimensionnement lorsque la configuration de réseau VPN demandée par le client est courante (adjonction, modification, suppression), tâche qui peut être très lourde en termes de mise à jour des tables d'accès).

7.11 Accès du bord client au bord fournisseur

La réalisation devrait prendre en charge les diverses technologies suivantes: RTPC, RNIS, lignes xDSL, câblomodem, lignes louées, mode ATM, relais de trames, boucle locale hertzienne, accès radio mobile, etc. (une vaste gamme de largeurs de bande devrait être prise en charge, conformément à la technologie particulière en usage).

7.12 Prescriptions relatives à l'adressage et prise en charge des divers plans de numérotage IP

- La réalisation doit admettre la non-unicité des adresses dans les réseaux VPN: les adresses IP ne doivent être uniques que dans un réseau VPN donné, pas dans l'ensemble des réseaux VPN.
- La réalisation devrait minimiser l'emploi des adresses IP.
- La réalisation ne devrait pas exclure la traduction d'adresse de réseau (NAT, *network address translation*).
- Prise en charge des plans de numérotage IP du client (privé, globalement unique, sans plan), prise en charge (à la demande) d'un mécanisme d'attribution dynamique d'une adresse IP, prise en charge d'une caractéristique d'acquisition du numérotage IP. (Prise en charge de la caractéristique d'acquisition du numérotage IP du client: le système de gestion pourrait reposer sur des informations centralisées afin de disposer de l'ensemble des paramètres nécessaires à une attribution optimale de la numérotation IP. Un tel système pourrait accroître la souplesse du réseau en cas d'extension de celui-ci. Cela pourrait réduire le temps du dimensionnement lorsque la configuration de réseau VPN demandée par le client est courante (adjonction, modification, suppression), tâche qui peut être très lourde en termes de mise à jour des tables de routage. Cela pourrait même permettre une optimisation rentable des ressources nécessaires à la numérotation IP.
- Un identificateur unique pour les réseaux VPN (ainsi que d'autres identificateurs, tels que ceux pour les tunnels dans les réseaux VPN) pourrait être approprié dans des scénarios particuliers.

7.13 Prise en charge des divers scénarios de mise en place des services

- Plusieurs réseaux VPN par site client.
- Service VPN couplé à un accès au réseau Internet par site client.
- La réalisation doit prendre en charge la connectivité entre sites appartenant au même ou à différentes entreprises (intranet/extranet).
- Réseau VPN entre systèmes autonomes.
- Réseau VPN entre fournisseurs (la réalisation doit permettre au réseau VPN de relier plusieurs fournisseurs de services).
- Multiplex de porteurs (un scénario consistant en des réseaux VPN hiérarchiques).

7.14 Prise en charge des alliances de réseaux VPN

NOTE – Le terme "alliance de réseaux VPN" peut faire l'objet d'un complément d'étude.

Les protocoles de gestion de réseau, de signalisation et de routage prendront en charge/admettront:

- la formation initiale (facile) d'une alliance de réseaux VPN;
- l'adhésion (facile) d'un nouveau réseau VPN membre de l'alliance;
- le départ (facile) d'un réseau VPN membre de l'alliance;
- la cessation (facile) de l'alliance entière de réseaux VPN.

Tout réseau VPN peut devenir membre d'une alliance de réseaux VPN.

Pendant que l'alliance existe, il peut éventuellement y avoir différents degrés de confidentialité en ce qui concerne la communication entre les membres intra-alliance et celle entre les membres interalliance.

Les réalisations devraient tenir compte d'éléments tels que:

- une connectivité défaillante entraînant l'éclatement de l'alliance de réseaux VPN;
- un emploi interne par les réseaux VPN membres de l'alliance de conceptions différentes en matière de réseau VPN;
- un emploi de conceptions différentes pour l'interconnexion des réseaux VPN membres de l'alliance;
- un emploi interne par les réseaux VPN membres de l'alliance de protocoles différents pour le routage et la signalisation;
- un emploi de l'adressage privé au sein des réseaux VPN membres de l'alliance.

Il est prévu que l'usage éventuel d'un identificateur unique de réseau VPN pour un réseau VPN particulier membre de l'alliance pourrait jouer un rôle dans l'identification des voies de routage/tunnels, au moins entre différents réseaux VPN (que les membres nomment peut-être le chef de l'alliance de réseaux VPN).

7.15 La réalisation devrait permettre la sous-traitance des services IP [par exemple, les serveurs de noms de domaine (DNS) et les protocoles de configuration dynamique de serveur (DHCP)]

- La réalisation devrait permettre au fournisseur de services VPN lui-même ou à un autre fournisseur de services d'offrir des services IP supplémentaires, lorsqu'il s'agit de services tels que la mise à disposition de serveurs de noms de domaine (DNS, *domain name server*), de protocoles de transfert de fichiers (FTP, *file transfer protocol*), de protocoles de transfert hypertexte (HTTP, *hypertext transfer protocol*), de protocoles de transfert d'informations dans le réseau (NNTP, *network news transfer protocol*), de protocoles simples de transfert de messages (SMTP, *simple mail transfer protocol*), de protocoles rapides d'accès à l'annuaire (LDAP, *lightweight directory acces protocol*), de la téléphonie utilisant le protocole Internet (VoIP, *voice over IP*), de la visioconférence, du partage d'applications, de l'émission en continu, du commerce électronique et d'autres services tels que l'assistance technique.
- La réalisation devrait permettre la sous-traitance des services IP. (Le système de gestion pourrait reposer sur des informations centralisées afin de disposer de l'ensemble des paramètres nécessaires à une adaptation optimale des services IP aux besoins particuliers. Cela pourrait réduire le temps du dimensionnement lorsque la version ou la configuration de réseau VPN demandée par le client est nouvelle (adjonction, modification, suppression). Cela pourrait même permettre d'optimiser rentablement les ressources en offrant des services à une large gamme de clients).

7.16 Fiabilité et insensibilité aux dérangements

Il est demandé que la fiabilité du réseau soit grande lorsqu'un réseau VPN est construit sur le réseau public, la qualité étant égale à celle des lignes louées.

Les techniques de survie, telles que la commutation ou la restitution de protection, sont nécessaires à une récupération rapide lors de défaillances, afin d'augmenter la fiabilité du réseau VPN.

Les prescriptions relatives à la commutation de protection sont les suivantes:

- gestion des dérangements, telle que la détection des dérangements (voir le § 7.2.2.1);
- un premier calcul est fait concernant le routage et les ressources, qui sont attribués avant la défaillance à une entité de protection spécialisée, afin d'offrir de fortes garanties relatives au fait de pouvoir réobtenir après la défaillance les ressources de réseau nécessaires;

- temps de récupération court;
- un cadre plus général pour la commutation de protection dans les réseaux à commutation MPLS est donné dans la référence [12].

7.17 Efficacité (utilisation des ressources client et réseau)

- Ingénierie du trafic pour le réseau du fournisseur de services.
- Ingénierie du trafic pour chaque réseau VPN.

L'ingénierie du trafic est une technologie essentielle pour les réseaux IP de transport, qui est destinée à la commande et à l'optimisation des réseaux en général. Elle permet d'optimiser les ressources du réseau dans le but de satisfaire les objectifs de performance du service d'application, ces optimisations se faisant en tenant compte des caractéristiques particulières du réseau, qui peuvent influer sur les objectifs de niveaux de service.

Cela s'applique en particulier au service d'application des réseaux IP VPN configurés par le fournisseur. En effet, l'ingénierie du trafic pourrait contribuer à fournir des ressources et commander l'admission pour les réseaux VPN. Dans ce cas, elle pourrait vérifier si le service demandé pour les nouveaux réseaux VPN peut être fourni sans nuire à la qualité de service des réseaux VPN installés précédemment.

L'ingénierie du trafic joue également un rôle important dans la modification et l'adaptation en fonction de la demande des clients et des besoins des fournisseurs de services des ressources pour les réseaux VPN nouveaux et existants.

7.18 Absence de dépendance de la couche Physique ou liaison du réseau dorsal du fournisseur de services

La commutation MPLS est une technologie qui peut s'appliquer à diverses couches Physiques ou couches Liaison de données, telles que la hiérarchie numérique synchrone (SDH, *synchronous digital hierarchy*) [paquet sur réseau SONET à l'aide du verrouillage de trames conforme au protocole point à point (PPP)], le mode ATM, le relais de trames, Ethernet, etc. Il est souhaitable que les fonctions fournies dans les réseaux VPN de type MPLS, telles que la commande de la qualité de service, la fonctionnalité de gestion, d'exploitation et de maintenance (OAM, *operation, administration and maintenainance*), soient disponibles sans qu'il soit tenu compte de la couche Physique ou de la couche Liaison de données.

7.19 Transfert (économiquement et techniquement) graduel des clients à partir d'offres de services VPN préexistantes

- La réalisation devrait permettre le transfert des clients sans importante interruption de service.
- La réalisation devrait permettre divers scénarios de transfert des clients. Par exemple, un scénario de "transfert partiel": transfert de certains sites dans un réseau VPN donné vers un réseau VPN de type IP assurant la continuité des services avec d'autres anciens sites de ce réseau VPN.

7.20 Prise en charge des fonctions d'interfonctionnement entre la technologie VPN de type MPLS et les autres technologies VPN

La prescription concernant le plan de données pour les nœuds d'interfonctionnement est la suivante:

- mappage de toutes les informations pertinentes d'une technologie sous-jacente de transport VPN vers une autre technologie sous-jacente de transport VPN.

(Une méthode de mappage des informations est l'encapsulage: il existe diverses technologies de type VPN et dans chacune d'entre elles les paquets sont encapsulés par l'en-tête qui est propre à la technologie concernée. Un identificateur dans l'en-tête d'encapsulage est employé pour séparer dans le réseau la connexion de l'utilisateur du réseau VPN de celles des autres utilisateurs de réseaux VPN, et donc conserver l'intégrité des données de bout en bout. L'en-tête d'encapsulage possède aussi un champ qui présente la classe de qualité de service, tandis que chaque nœud de la connexion commande cette qualité de service en examinant ce champ.)

D'autres prescriptions pour le plan de données doivent faire l'objet d'un complément d'étude.

Dans certains cas (par exemple, les réseaux VPN fondés sur des technologies différentes), il peut être tenu compte des prescriptions suivantes:

- Interfonctionnement du protocole de signalisation qui est employé par chaque technologie de réseau VPN entre les réseaux VPN de type MPLS et les autres réseaux VPN (cette prescription peut également s'appliquer à l'interfonctionnement entre un réseau VPN de type MPLS et un autre réseau VPN de type MPLS dans lequel des protocoles de signalisation différents sont employés).
- Echange d'informations sur le routage entre un réseau VPN de type MPLS et d'autres réseaux VPN.

7.21 Quelques chiffres éventuels pour une offre de fourniture de services VPN de type IP

- Très grand nombre (par exemple, jusqu'à 10 000 000) de réseaux VPN par fournisseur de services.
- Large éventail du nombre de sites par client (en fonction de la taille ou de la structure de l'entreprise cliente): allant de quelques sites jusqu'à 10 000 sites par réseau VPN et par client.
- Large éventail du nombre de routes par réseau VPN: allant de quelques routes jusqu'à 100 000 routes par réseau VPN (ce nombre peut être limité par le choix du protocole de routage entre le bord client et le bord fournisseur).
- Plus d'un réseau VPN par site devrait être possible.
- Des valeurs élevées (à évaluer) du nombre de mises en place et de modifications de la configuration devraient être prises en charge (par exemple, le dimensionnement en temps réel d'un réseau VPN de visioconférence à la demande).

7.22 Une réalisation de réseau VPN peut prendre en charge les prescriptions suivantes relatives aux services

- Prise en charge d'autres scénarios de mise en place des services:
  - réseau VPN à commutation MPLS de bord client à bord client.

8 Architecture de la conception

Le modèle de réseau VPN de base est celui où les dispositifs de bord client sont connectés aux routeurs de bord fournisseur. La connexion doit assurer une connectivité IP directe (un seul saut IP) entre les dispositifs de bord client et les routeurs de bord fournisseur. Un dispositif de bord client peut être connecté à un routeur de bord fournisseur au moyen d'un type quelconque de liaison de données (par exemple, une connexion par voie virtuelle (VCC, *virtual channel connection*) en mode ATM, un circuit à relais de trames, Ethernet, un paquet sur réseau Sonet (POS, *packet over Sonet*), une session du protocole de tunnellisation de couche 2 (L2TP, *layer 2 tunnelling protocol*), un encapsulage GRE ou un tunnel de sécurité IPSEC, etc.).

Lorsqu'un site donné comporte un seul hôte, cet hôte peut être un dispositif de bord client. S'il comporte un seul sous-réseau IP, le dispositif de bord client peut être un commutateur. En général, on peut s'attendre que le dispositif de bord client est un routeur, que nous désignons par routeur de bord client. Les routeurs de bord fournisseur se renseignent sur les adresses IP accessibles sur chaque site client et distribuent ces informations entre eux. Ils établissent aussi entre eux et prennent en charge des tunnels d'un certain type, qui sont utilisés pour transmettre le trafic de données de réseau VPN à travers le réseau dorsal du fournisseur de services. Aux fins de la présente Recommandation, les tunnels sont des conduits à commutation avec étiquette (LSP, *label switched path*). Les routeurs dans le réseau dorsal du fournisseur de services qui ne prennent pas en charge d'état de réseau VPN sont nommés routeurs de fournisseur.

On peut distinguer les différents domaines suivants, traités ci-après:

- collecte d'informations sur l'accessibilité des sites client;
- distribution d'informations sur l'accessibilité dans les réseaux VPN;
- distribution limitée d'informations sur le routage;
- mise en place et utilisation des tunnels LSP.

8.1 Collecte d'informations sur l'accessibilité des sites client

Il est nécessaire de disposer de mécanismes pour permettre à un routeur de bord fournisseur de découvrir l'ensemble des adresses IP accessibles au moyen d'une liaison directe à un dispositif de bord client, et pour permettre à un routeur de bord client de découvrir l'ensemble d'adresses IP dans d'autres sites du réseau VPN auxquels ce dispositif de bord client est relié. Ces mécanismes comprennent notamment:

- l'exécution d'un protocole de routage (par exemple, le protocole d'information de routage (RIP, *routing information protocol*), le premier itinéraire ouvert le plus court (OSPF, *open shortest path first*) ou le protocole BGP);
- l'utilisation d'une configuration statique;
- le suivi des attributions dynamiques d'adresse lorsque le protocole de configuration dynamique de serveur (DHCP, *dynamic host configuration protocol*) ou le protocole point à point (PPP) est employé.

La gamme d'options est large en ce qui concerne la quantité d'informations sur le routage qu'un routeur de bord client reçoit du routeur de bord fournisseur auquel il est directement connecté. A l'une des extrémités du spectre, le routeur de bord fournisseur peut simplement annoncer une seule route, par défaut, au routeur de bord client. A l'autre extrémité du spectre, le routeur de bord fournisseur peut annoncer toutes les routes qu'il a reçues des autres sites.

8.2 Distribution d'informations sur l'accessibilité dans un réseau VPN

Lorsqu'un routeur de bord fournisseur a déterminé l'ensemble des destinations accessibles par l'intermédiaire du dispositif pour un réseau VPN de bord client auquel il est directement connecté, il doit ensuite distribuer ces informations vers d'autres routeurs de bord fournisseur auxquels sont reliés des sites client pour ce réseau VPN.

Les mécanismes disponibles à ces fins sont les suivants:

- exécution d'une version d'un protocole d'acheminement pour ce réseau VPN – l'option du routeur virtuel (VR, *virtual router*). Cette option du routeur virtuel est décrite de manière plus détaillée au 9.2;
- adjonction d'informations sur l'accessibilité dans un réseau VPN à un protocole BGP du réseau dorsal. Une option employant le protocole BGP est décrite au 9.1.

NOTE – En théorie, on pourrait joindre ces informations à un protocole IGP, mais des considérations de dimensionnement rendent cette option caduque.

8.3 Distribution limitée d'informations sur le routage

Afin d'atteindre les objectifs spécifiés en matière de dimensionnement, un routeur de bord fournisseur devrait être en mesure de prendre en charge seulement les routes pour les réseaux VPN dont les sites sont directement connectés à ce routeur de bord fournisseur. Cela oblige, en contrepartie, de limiter la distribution d'informations sur le routage dans les réseaux VPN.

Lorsqu'un routeur de bord fournisseur prend connaissance des informations sur l'accessibilité d'un site client dans un réseau VPN auquel il est relié localement, ces informations doivent être distribuées (sous réserve de filtrage et/ou de l'agrégation des routes) aux autres routeurs de bord fournisseur qui ont aussi des sites client reliés au réseau VPN. Un élément d'une réalisation de réseau VPN consiste en la question de savoir comment chaque routeur de bord fournisseur détermine pour chacun des réseaux VPN un ensemble d'autres routeurs auxquels il doit distribuer ces informations sur l'accessibilité.

Le mécanisme employé par le réseau VPN à protocole BGP/à commutation MPLS (voir 9.1) consiste en le filtrage des routes sur la base de l'attribut communautaire du protocole BGP. On peut trouver plus de détails dans la référence [5].

Des mécanismes qui peuvent éventuellement être employés dans l'option du routeur virtuel pour déterminer l'ensemble des autres routeurs qui sont considérés comme des homologues pour le routage sont les suivants:

- emploi d'un annuaire que les routeurs de bord fournisseur interrogent;
- configuration explicite au moyen de la gestion de la configuration;
- option multidiffusion;
- adjonction d'informations dans un protocole de routage employé par le réseau dorsal du fournisseur (par exemple, le protocole BGP).

Une autre éventualité est la connectivité intersites. Elle pourrait varier d'une configuration totalement en maille à un point de concentration relais, ou être une configuration intermédiaire (par exemple, une configuration partiellement en maille).

Une autre éventualité encore est une liaison entre un routeur de bord fournisseur et un dispositif de bord client qui pourrait être établie "à la demande" ou être relativement permanente. Une liaison "à la demande" pourrait par exemple être une session de protocole PPP, où le service RADIUS pourrait servir pour relier le dispositif de bord client à un réseau VPN particulier.

Dans l'option du réseau virtuel, la détermination pour un réseau VPN donné de l'ensemble des routeurs de bord fournisseur qui disposent de dispositifs de bord client dans ce réseau VPN est connue sous le nom de détermination de l'appartenance au réseau VPN. Aussi, dans cette option, est-il est nécessaire de construire une topologie pour chaque réseau VPN. Le mécanisme de construction d'une telle topologie peut différer du mécanisme qui est utilisé pour distribuer concrètement des informations sur l'accessibilité entre les routeurs de bord fournisseur. Tout mécanisme énuméré ci-dessus peut, par exemple, être employé à ces fins.

8.4 Mise en place et utilisation de la tunnellisation par conduit LSP

Un aspect important de la tunnelisation par conduit LSP concerne le fait de savoir si le conduit LSP est employé pour assurer le transport d'un seul réseau VPN ou s'il est employé pour transporter le trafic de plusieurs réseaux VPN. Ceci aboutit généralement à un compromis entre les ressources supplémentaires qui sont nécessaires pour mettre en place et prendre en charge des tunnels propres aux réseaux VPN, et la commande de la qualité de service à granulation fine ainsi que d'autres avantages qui pourraient être obtenus avec des conduits LSP spécialisés.

Un autre aspect de la tunnellisation par conduit LSP est qu'ils forment eux-mêmes un réseau, ce qui veut dire qu'ils peuvent constituer différentes topologies (allant d'un point de concentration relais à une configuration partiellement ou totalement en maille). Le choix de la topologie peut dépendre des exigences des différents clients et fournisseurs de services, telles que la prise en charge de conduits de remplacement de l'entrée à la sortie, ou la réduction au minimum du nombre de tunnels à gérer et à prendre en charge. Différents algorithmes sont disponibles pour déterminer les topologies des tunnels. On peut trouver des références supplémentaires à l'Appendice II.

9 Options de prise en charge des services VPN de type IP

9.1 Option pour les réseaux VPN à protocole de passerelle limite ou à commutation multiprotocolaire par étiquetage

L'option décrite dans le présent paragraphe figure dans la référence [5].

Cette option comporte les éléments suivants:

- configuration non perturbée des services dans le cas de l'adjonction ou de la suppression de nouveaux sites ou de partenaires sur extranet;
- utilisation optimale des protocoles de distribution avec étiquettes (LDP, *label distribution protocol*) pour la mise en place des conduits à commutation avec étiquette, la configuration étant minimale;
- fourniture de l'accès Internet aux clients lorsqu'une simple couche Liaison de données les sépare du routeur de bord fournisseur et que cette couche ne peut pas prendre en charge plusieurs adresses IP logiques;
- prise en charge de liaisons par entrées dérobées entre les sites dans des configurations particulières;
- emploi d'une topologie de point de concentration relais pour la construction d'un réseau de gestion;
- interaction dans le bord fournisseur entre le protocole BGP du fournisseur de services et les versions du protocole IGP (employées pour l'échange d'informations sur le routage entre le bord client et le bord fournisseur).

9.2 Option du routeur virtuel

Le présent paragraphe décrit une réalisation de réseau VPN fondée sur le concept de routeur virtuel, qui assure séparément le routage, la transmission et la qualité de service pour chaque réseau VPN.

Plusieurs réalisations ont été proposées, aboutissant à des niveaux de confidentialité de réseau différents lors de la construction de réseaux VPN à travers un réseau dorsal public partagé. La plupart de ces réalisations nécessitent des capacités de transmission distinctes pour chaque réseau VPN ou pour chaque site dans un réseau VPN et utilisent des tunnels IP ou LSP à travers le réseau dorsal. L'architecture de réseau VPN décrite dans le présent paragraphe est conforme au cadre de réseau IP VPN qui est décrit dans la référence [3].

Les routeurs virtuels emploient les mêmes mécanismes du point de vue du routage et de la transmission des données que les routeurs physiques, et sont faciles à mettre en place, à exploiter et à dépanner. La découverte de l'appartenance au réseau VPN est facilitée par l'emploi d'un certain nombre de mécanismes qui sont proposés dans le présent paragraphe. La présente option tente de séparer clairement le fournisseur de services du client du réseau VPN: le fournisseur de services possède et gère les services des couches 1 et 2, tandis que les services de couche 3 appartiennent au réseau VPN et peuvent être, à la discrétion du fournisseur de services, gérés par le client du réseau VPN. Les questions de sécurité des données sont abordées en employant, soit des conduits LSP privés, soit une superposition d'étiquettes sur des conduits LSP partagés pour confiner dans leurs domaines les données appartenant aux réseaux VPN particuliers.

Tout protocole de routage peut être employé dans le routeur virtuel. Cette souplesse s'applique aux segments de bord client à bord fournisseur ainsi qu'aux segments de bord fournisseur à bord fournisseur. Des données privées et des informations sur le routage sont échangées entre des sites dans un réseau VPN par l'intermédiaire de tunnels de type IP ou à commutation MPLS à travers le réseau dorsal.

9.2.1 Routeur virtuel

Un routeur virtuel est une émulation d'un routeur physique aux niveaux logiciel et matériel. Les routeurs virtuels possèdent des tables de routage et de transmission IP indépendantes et ils sont isolés les uns des autres. Cela veut dire qu'il peut y avoir un chevauchement entre l'espace d'adressage IP dans un réseau VPN et celui dans un autre réseau VPN. Les adresses IP ne doivent être uniques que dans un domaine de réseau VPN.

Un routeur virtuel a les deux fonctions principales suivantes:

- construction des tables de routage décrivant les conduits entre des sites dans des réseaux VPN à l'aide de protocoles de routage quelconques (par exemple, les protocoles OSPF, RIP ou BGP);
- transmission ou commutation des paquets vers les sauts suivants dans le domaine du réseau VPN.

Du point de vue de l'utilisateur, un routeur virtuel assure la même fonctionnalité qu'un routeur physique. De nombreux routeurs virtuels peuvent coexister dans le même routeur de bord fournisseur. Du point de vue du bord client, le routeur de bord fournisseur assure les fonctions de nombreux routeurs, en transmettant des paquets vers la destination exacte, tout en isolant le trafic dans le réseau VPN comme le font les différents routeurs. Des capacités de routeur distinctes donnent à chaque liaison de bord client dans un réseau VPN l'impression qu'un routeur spécialisé garantit son isolement d'autres trafics dans le réseau VPN, tout en employant la commutation partagée et les ressources de transmission.

Des réseaux privés virtuels sont créés en réalisant l'interconnexion des routeurs virtuels à travers le réseau dorsal et les dispositifs de bord client. L'administrateur du réseau attribue un routeur virtuel à chaque bord fournisseur où les sites sont reliés au réseau du bord client. Des routeurs virtuels appartenant au même domaine de réseau IP VPN doivent avoir le même identificateur de réseau privé virtuel (VPN-ID, *virtual private network identifier*). Les identificateurs VPN-ID indiquent pour les routeurs virtuels l'appartenance à un réseau VPN. Pour le dispositif d'accès de bord client, le routeur virtuel apparaît comme un routeur voisin dans le réseau de bord client, auquel il envoie tout le trafic devant être acheminé vers des destinations non locales dans des réseaux VPN. Chaque dispositif d'accès de bord client doit s'informer sur l'ensemble des destinations qui sont accessibles en étant connecté au routeur virtuel dans le routeur de bord fournisseur; ceci peut être aussi simple qu'une route par défaut. Les routeurs virtuels appartenant à un seul domaine de réseau VPN sont chargés de se renseigner sur les informations relatives à l'accessibilité et de les distribuer entre eux.

9.2.2 Modules de l'architecture de réseau VPN fondés sur des routeurs virtuels

Tout routeur virtuel est configuré de manière à prendre en charge un réseau VPN à un moment donné (même si le routeur virtuel pourrait être configuré pour la prise en charge de plusieurs d'entre eux).

Il est admis que tout réseau VPN (utilisant ou pas l'adjonction de l'accessibilité dans le protocole de routage) nécessite une certaine forme de tunnellisation (par exemple, la commutation MPLS).

La tunnellisation des sites dans un réseau VPN se fait au moyen de tunnels à commutation MPLS. Dans cette architecture, la commutation MPLS est utilisée comme un mécanisme de transport, même si d'autres types de tunnellisation ne sont pas exclus de cette architecture. En outre, selon le scénario de mise en place du réseau VPN, le mécanisme de superposition d'étiquettes peut être employé. Les tunnels peuvent être configurés statiquement ou mis en place dynamiquement (en employant les mécanismes existants). Le trafic envoyé à travers le tunnel est opaque pour la technologie sous-jacente du réseau dorsal.

Un réseau VPN de type IP (à commutation MPLS ou pas) assure la connectivité privée de site à site à travers une infrastructure de gestion centrale de réseau du fournisseur de services. Un réseau privé virtuel est composé de multiples sites reliés aux réseaux de bord client. Le dispositif de bord client (par exemple, un routeur) est connecté à un bord fournisseur.

Le bord fournisseur donne au réseau de bord client les capacités de routage et de transmission à travers le réseau dorsal. La technologie sous-jacente de liaison de données par le réseau dorsal peut employer le mode ATM, les circuits virtuels à relais de trames ou le protocole PPP.

Le réseau privé de bord client dont les sites sont reliés pour accéder au routeur de bord fournisseur se connecte à un routeur virtuel au moyen d'une liaison d'accès, pouvant employer le mode ATM, les circuits virtuels à relais de trames ou une connexion selon le protocole PPP. Les tables de routage associées à chaque routeur virtuel définissent la connectivité site à site pour ce réseau VPN.

9.2.3 Scénarios de mise en place des réseaux VPN fondés sur des routeurs virtuels

Des routeurs virtuels peuvent être mis en place dans différentes configurations. Sont donnés ci-après trois exemples fondamentaux de mise en place de réseaux VPN fondés sur des routeurs virtuels.

Exemple 1: connectivité directe des routeurs virtuels à l'aide de connexions de couche 2, voir Figure 2.

Des routeurs virtuels (VR, *virtual router*) peuvent être mis en place directement au moyen de connexions de couche 2.

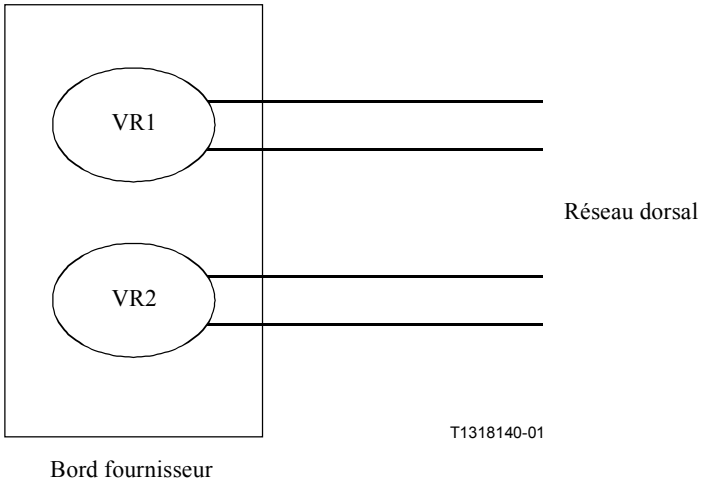


Figure 2/Y.1311.1 – Exemple 1: connectivité directe des routeurs virtuels à l'aide de connexions de couche 2

Exemple 2: emploi d'un routeur virtuel sur le réseau dorsal, voir Figure 3.

Un routeur virtuel peut être employé pour connecter tous les bords fournisseur à un réseau dorsal partagé.

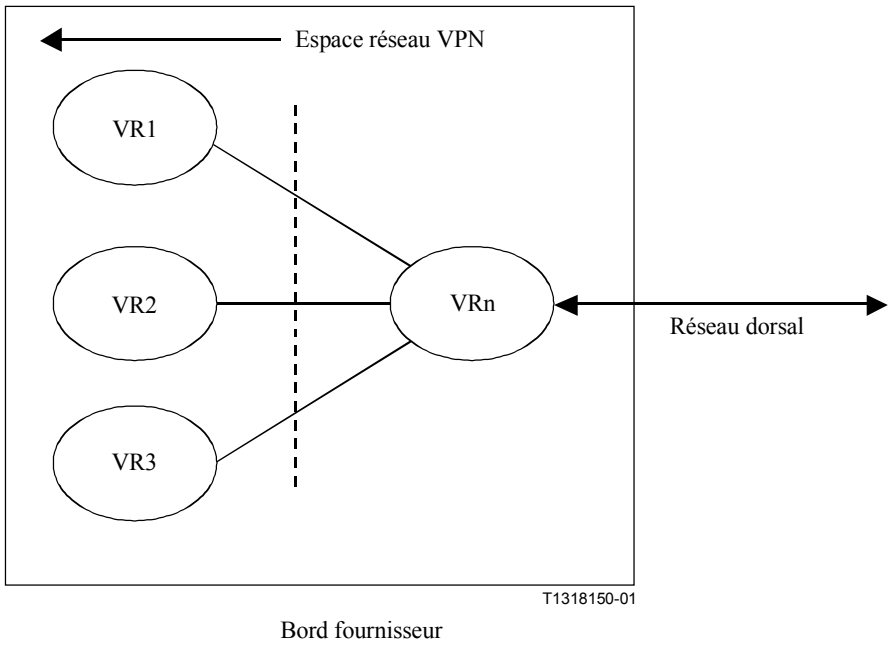


Figure 3/Y.1311.1 – Exemple 2: emploi d'un routeur virtuel sur le réseau dorsal

Exemple 3: emploi de plusieurs routeurs virtuels sur le réseau dorsal, voir Figure 4.

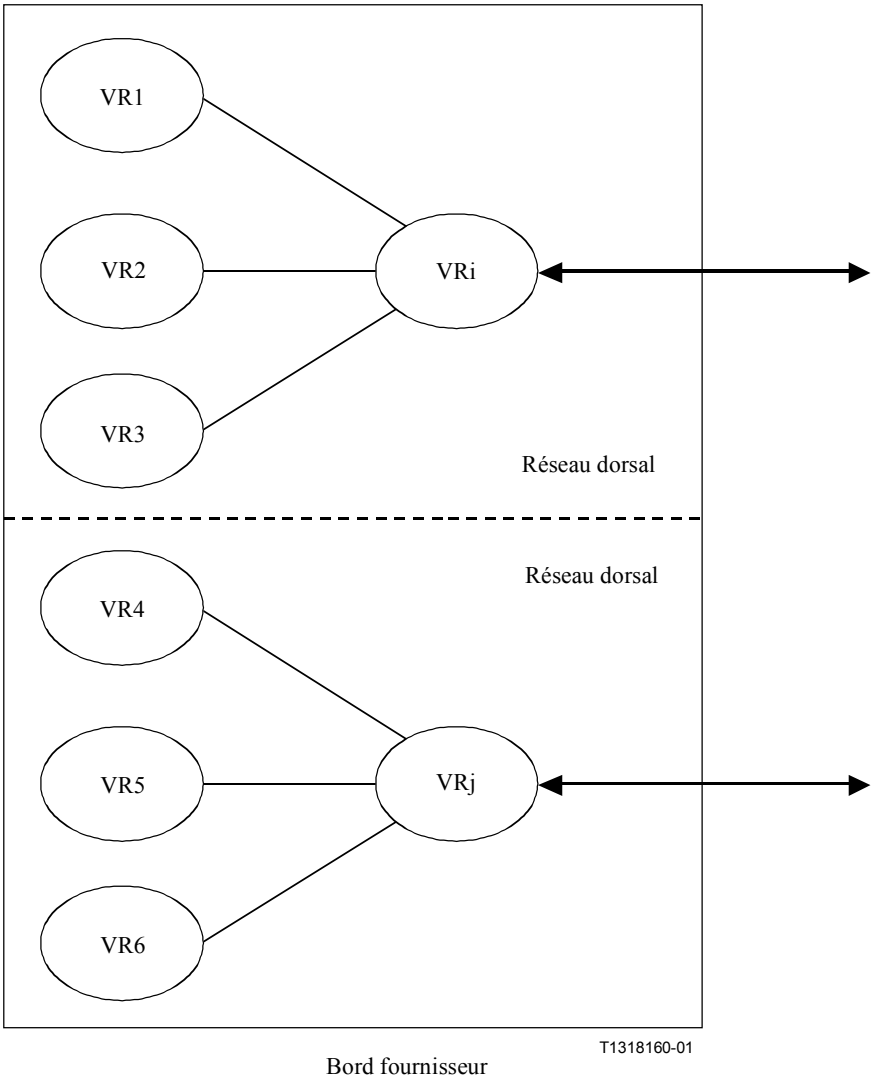


Figure 4/Y.1311.1 – Exemple 3: emploi de plusieurs routeurs virtuels sur le réseau dorsal

9.2.4 Détermination de l'accessibilité dans le réseau VPN

Par définition, les routeurs virtuels exécutent différentes versions de protocoles de routage pour chaque réseau VPN. Des informations concernant l'accessibilité sont transportées à travers des tunnels (par exemple, des conduits LSP à commutation MPLS). Le routeur virtuel ne maintient les routes que pour des réseaux VPN particuliers configurés pour lui. Cette architecture n'utilise pas l'adjonction au protocole de routage exécuté dans le réseau dorsal (par exemple, le protocole BGP) d'informations sur l'accessibilité dans les réseaux VPN.

Le paragraphe 9.2.4.1 ci-après décrit une méthode permettant de distribuer aux routeurs virtuels des informations sur l'accessibilité.

9.2.4.1 Liaison de diffusion entre routeurs virtuels

Les routeurs virtuels doivent envoyer des messages à tous les autres routeurs virtuels dans d'autres bords fournisseur d'un réseau VPN donné [par exemple, les routeurs virtuels doivent envoyer des datagrammes de diffusion comme demandé dans les protocoles de routage (mode de diffusion avec ouverture OSPF, protocole RIP V2, etc.)].

Dans les réseaux où le routage est traditionnel, lorsque des supports de diffusion tels qu'Ethernet sont disponibles et lorsque des protocoles de routage tels que le mode de diffusion avec ouverture OSPF ou le protocole RIP V2 sont configurés pour ces supports, les ressources en matière de liaison sont utilisées de manière efficace et les temps de convergence sont réduits au minimum.

Dans le cas de réseaux VPN fondés sur des routeurs virtuels, un système de diffusion pour qu'un routeur virtuel puisse envoyer efficacement des messages à tous les autres routeurs virtuels dans le réseau pourrait alors être utile, en particulier dans le cas de grands réseaux (par exemple, pour un grand nombre de réseaux VPN et de bords fournisseur par réseau VPN).

Ce système de diffusion peut être instauré au moyen de la multidiffusion. On peut trouver des informations plus détaillées dans la référence [6].

9.2.5 Détermination de l'appartenance aux réseaux VPN et de la topologie

Les réseaux VPN fondés sur des routeurs virtuels peuvent être mis en place dans différentes configurations. L'option de routeur virtuel sépare explicitement les mécanismes employés pour la distribution d'informations sur l'accessibilité de ceux qui sont employés pour déterminer l'appartenance et la topologie. L'architecture fondée sur des routeurs virtuels n'exclut pas la possibilité que, dans un bord fournisseur, plusieurs types de réseaux VPN fondés sur des routeurs virtuels peuvent coexister et employer différents mécanismes pour découvrir l'appartenance et la topologie.

Parmi ces mécanismes, on peut énumérer les options suivantes:

- option du serveur d'annuaire que les bords fournisseur interrogent pour déterminer leurs voisins;
- configuration explicite au moyen d'une plate-forme de gestion;
- option multidiffusion (on peut trouver des informations plus détaillées dans la référence [6]);
- adjonction de l'appartenance aux réseaux VPN et de la topologie au moyen des protocoles de routage disponibles [3] (par exemple, le protocole BGP).

9.2.6 Exploitation et gestion

L'élément clé dans le présent paragraphe est le fait que tous les outils et mécanismes existants d'exploitation et de gestion peuvent être employés dans le cadre d'une réalisation fondée sur des routeurs virtuels. En général, le fournisseur de services possède et gère les entités des couches 1 et 2. Pour être précis, le fournisseur de services commande les commutateurs ou les routeurs physiques, les liaisons physiques, les connexions logiques de couche 2 (et les identificateurs de circuit de liaison de données (DLCI, *data link circuit identifier*) dans le relais de trames, les identificateurs de conduit ou de circuit virtuels (VPI/VCI, *virtual path/circuit identifier*) en mode ATM) et les conduits LSP (ainsi que leur attribution à des réseaux VPN particuliers), Dans le cadre des réseaux VPN, le fournisseur de services est chargé de passer des contrats et d'attribuer des entités de couche 2 à des réseaux VPN particuliers. Les entités des réseaux VPN de couche 3 peuvent être gérées soit directement par le fournisseur de services ou, à la discrétion de celui-ci, par le client du réseau VPN. Ces entités sont par exemple des interfaces IP, un choix de protocoles de routage dynamique ou des routes statiques, ou des interfaces de routage. Il convient de noter que même si la configuration de la couche 3 relève logiquement du secteur de l'utilisateur du réseau VPN, il n'est pas nécessaire que celui-ci l'exécute. Il est assez faisable que l'utilisateur du réseau VPN confie l'administration IP des routeurs virtuels au fournisseur de services.

9.2.6.1 Surveillance des réseaux VPN au moyen d'une réalisation fondée sur des routeurs virtuels

Lorsqu'un utilisateur de réseau VPN se connecte à un bord fournisseur (directement ou indirectement) afin de configurer ou de surveiller son réseau, l'architecture fondée sur des routeurs virtuels lui permet de se connecter au routeur virtuel qui se rapporte à son réseau VPN particulier.

L'utilisateur de réseau VPN ne dispose pour le routeur virtuel que de privilèges pour la configuration et la surveillance de la couche 3. En particulier, il ne dispose pas de privilège de configuration du réseau physique. Cela garantit au fournisseur de services que l'administrateur du réseau VPN ne sera pas en mesure de modifier par inadvertance le réseau du fournisseur de services ou de nuire à celui-ci.

9.2.6.2 Mise à disposition des services VPN au moyen d'une réalisation fondée sur des routeurs virtuels

Dans l'architecture fondée sur des routeurs virtuels, le fournisseur de services a la possibilité de commander et de décider quels services VPN seront rétablis en premier lieu dans le cas d'une interruption des services de bord fournisseur (par exemple, la transition, les mises à niveau, les défaillances, etc.). La possibilité de ne pas se fonder sur l'adjonction au protocole de routage dans le réseau dorsal de l'accessibilité dans le réseau VPN permet à la réalisation fondée sur des routeurs virtuels de traiter pour chaque réseau VPN les prescriptions sur la disponibilité concernant l'exécution d'applications qui s'ajoutent au réseau VPN. Ce point particulier est important lorsqu'un grand nombre de réseaux VPN est pris en charge dans le bord fournisseur.

9.2.6.3 Dépannage des réseaux VPN

Dans le cadre des routeurs virtuels, le fournisseur de services (ou le client du réseau VPN) peut employer tous les outils de dépannage existants sans les modifier pour chaque réseau VPN (par exemple, le ping).

9.2.7 Considérations en matière de sécurité

Différents niveaux de sécurité concernant les données, le routage et la configuration peuvent être implémentés au moyen de l'architecture fondée sur des routeurs virtuels.

9.2.7.1 Sécurité de routage et des données

L'emploi de protocoles de routage existants tels que les protocoles OSPF et BGP implique que toutes les méthodes de chiffrement et de sécurité (telles que l'authentification par algorithme 5 de hachage de message (MD5, *message digest 5*) des voisins) sont entièrement disponibles dans les routeurs virtuels. En outre, les manipulations relatives au routage, à la transmission et à l'adressage privés se font dans le cadre des routeurs virtuels. Les connexions directes de couche 2 (en mode ATM ou relais de trames) ou les mécanismes de tunnellisation employés (par exemple, les conduits LSP à commutation MPLS) assurent différents niveaux de sécurité des données.

9.2.7.2 Sécurité de la configuration

Les routeurs virtuels semblent être des routeurs physiques pour l'utilisateur du réseau VPN. Les mécanismes de sécurité existants tels que les mots de passe, le service RADIUS, etc. peuvent être employés par l'utilisateur de réseaux VPN.

9.2.8 Qualité de service des réseaux VPN

L'architecture s'adapte aux différents mécanismes de qualité de service afin de préserver la qualité de service du transfert de site à site pour chaque réseau VPN. Les paquets reçus d'un site dans un réseau VPN peuvent recevoir un traitement en matière de qualité de service au niveau du routeur virtuel, qui implique directement quelle liaison de sortie du réseau dorsal est à employer. Dans ce cas, le routeur virtuel peut classer et ordonner les paquets pour chaque réseau VPN.

Ce modèle permet de séparer l'ingénierie de qualité de service pour les réseaux VPN de celle du réseau dorsal.

9.2.9 Dimensionnement

Dans cette architecture, seuls les bords fournisseur manipulent des informations de type VPN.

Les nœuds internes du réseau dorsal (par exemple, les routeurs) ne sont pas conscients de l'existence des réseaux VPN.

En outre, pour une réalisation fondée sur les réseaux VPN, il est souhaitable de simplifier la mise en place et la configuration des différents réseaux VPN, en plaçant plusieurs sites au même endroit géographique. Les routeurs virtuels permettent que plusieurs réseaux privés de bord client se connectent à un seul dispositif de fournisseur de services.

Un des avantages de la capacité de contenir l'espace d'adresse dans le réseau VPN, ainsi que des capacités de routage et de transmission dans un réseau VPN dans le routeur virtuel est la possibilité de répartir les ressources du système de bord fournisseur pour chaque réseau VPN. Cette répartition concerne par exemple l'application de différents mécanismes de programmation pour le traitement des activités de chacun des réseaux VPN dans le routeur de bord fournisseur. Cette répartition contribue à établir une vaste gamme de schémas de priorité dans les réseaux VPN.

9.2.10 Relations hiérarchiques entre les réseaux VPN fondés sur des routeurs virtuels

Le présent paragraphe décrit une technique destinée à la construction d'une hiérarchie entre des réseaux VPN fondés sur des routeurs virtuels. Une application de cette technique permet l'agrégation de nombreux réseaux VPN de fournisseurs de services à l'échelle régionale ou locale à travers une architecture de tunnellisation des réseaux VPN hiérarchiques. La démarche présentée ici n'exige aucune modification des protocoles de routage existants.

Un exemple simplifié montrant une relation hiérarchique entre des réseaux VPN fondés sur des routeurs virtuels est illustré dans la Figure 5.

NOTE – Les hiérarchies peuvent s'étendre sur plus de deux niveaux.

Les niveaux hiérarchiques sont repérés par un chiffre, le niveau supérieur correspondant au chiffre 0. Les niveaux hiérarchiques inférieurs sont désignés comme étant les niveaux 1, 2, etc. Les réseaux VPN de niveau supérieur transportent des réseaux VPN de niveaux inférieurs. Ainsi:

– le niveau 0 correspond au plus haut niveau hiérarchique. Un réseau VPN de niveau 0 transporte des réseaux VPN de niveaux inférieurs mais ne peut lui-même pas être transporté par un quelconque autre réseau VPN;

– le niveau 1 correspond à un réseau VPN qui est transporté par un réseau VPN de niveau 0, mais il ne peut pas lui-même être transporté par un quelconque réseau VPN de niveau égal ou inférieur au sien.

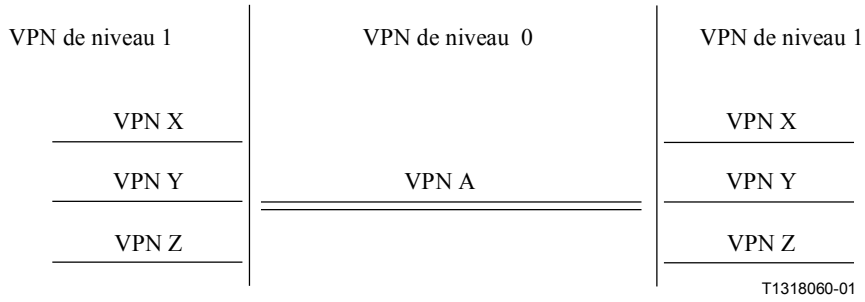


Figure 5/Y.1311.1 – Niveaux hiérarchiques des réseaux VPN

En attribuant aux réseaux VPN représentés dans la Figure 5 des niveaux hiérarchiques différents, on crée une relation hiérarchique entre eux. Par exemple, le niveau hiérarchique le plus élevé est désigné comme étant le "niveau 0". Dans cet exemple, le réseau VPN A est un réseau de niveau 0. De même, les réseaux VPN X, Y et Z appartiennent au niveau hiérarchique suivant inférieur, désigné comme étant le "niveau 1". Les données dans un réseau VPN de niveau 1 sont transportées de manière transparente à travers le réseau de niveau 0.

Une réalisation possible d'un réseau VPN hiérarchique (semblable à celui qui est représenté dans la Figure 5) peut maintenant être décrite au moyen du modèle des routeurs virtuels. Cette réalisation ne fait pas l'hypothèse d'un unique fournisseur de services impliqué. Plus précisément, dans les exemples qui suivent, les fournisseurs de services SP1 et SP2 ne représentent pas nécessairement le même fournisseur de services. Les techniques de superposition d'étiquettes avec commutation MPLS sont employées pour créer des niveaux hiérarchiques et expliquer comment les données sont transportées.

La Figure 6 donne un exemple de réseau VPN hiérarchique comportant deux fournisseurs de services. Dans cet exemple, on suppose que le fournisseur de services SP1 met à disposition un réseau dorsal international, utilisé par un fournisseur de services SP2 pour connecter ses réseaux régionaux (ou locaux) isolés géographiquement. Le fournisseur de services SP2 y dessert deux réseaux VPN client, X et Y. Un réseau VPN hiérarchique à deux niveaux est mis en place afin de permettre aux réseaux VPN X et VPN Y (à savoir, des réseaux VPN de niveau 1 dans cette hiérarchique) d'être transportés (au niveau 0) à travers le réseau VPN A.

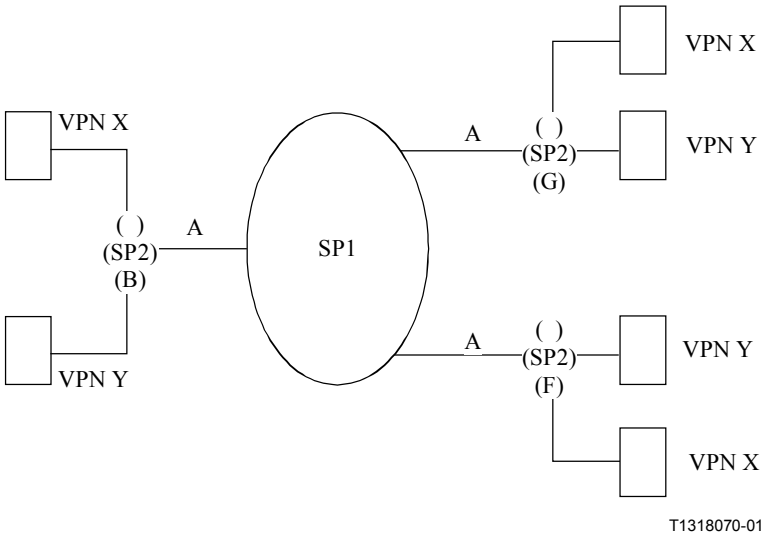


Figure 6/Y.1311.1 – Réseau VPN hiérarchique

La Figure 7 détaille le diagramme et illustre la relation entre les fournisseurs de services SP1 et SP2. On y observe que le fournisseur de services SP2 dessert les réseaux VPN client aux deux bouts, et qu'il doit aussi être informé sur le réseau dorsal (réseau VPN A) qu'il utilise pour le transport de la hiérarchie, tandis que le fournisseur de services SP1 ne doit s'intéresser qu'au réseau VPN A de niveau 0.

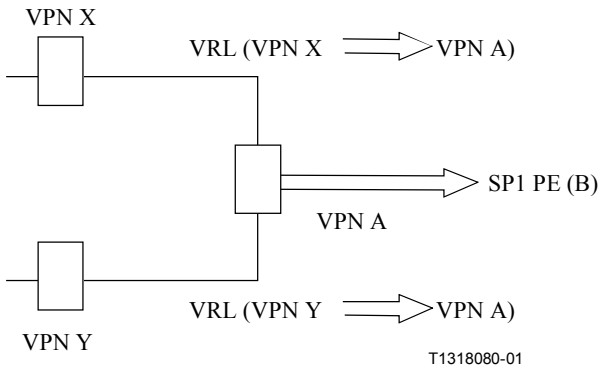


Figure 7/Y.1311.1 – Relation hiérarchique des liaisons entre routeurs virtuels

La Figure 7 montre aussi la relation entre un réseau VPN de niveau 1 (par exemple, le réseau VPN X) et un réseau VPN de niveau 0 (par exemple, le réseau VPN A). Une liaison entre routeurs virtuels (VRL, *virtual router link*) est employée entre les réseaux VPN de niveau 1 et de niveau 0. Cette liaison VRL est expliquée de manière plus détaillée dans le paragraphe suivant.

Dans la Figure 7, la relation hiérarchique est indiquée par des flèches (à savoir, VPN X => VPN A). La flèche pointe du réseau VPN X de niveau inférieur vers le réseau VPN A de niveau supérieur comme dans la relation VPN X => VPN A.

9.2.10.1 Liaison entre routeurs virtuels

Un routeur virtuel peut être connecté à d'autres routeurs virtuels par une "liaison entre routeurs virtuels (VRL)".

Chaque extrémité d'une liaison VRL est reliée logiquement à un routeur virtuel. Du point de vue du routeur virtuel, la liaison VRL ressemble à l'une de ses nombreuses liaisons, dont certaines pourraient être des liaisons physiques.

L'utilisateur peut définir un ensemble de règles pour cette liaison VRL afin de commander la relation entre deux réseaux VPN. Cette relation peut être une relation hiérarchique ou une relation d'appariement.

Dans le cas des réseaux VPN hiérarchiques, les liaisons VRL sont configurées entre des routeurs virtuels, l'une des extrémités étant l'extrémité supérieure de la hiérarchie et l'autre étant l'extrémité inférieure.

NOTE – L'examen de la question de savoir si les liaisons VRL peuvent être étendues de manière à englober les connexions point à point entre des routeurs virtuels pour l'échange des informations de commande doit encore faire l'objet d'un complément d'étude.

9.2.10.2 Distribution des étiquettes

Les réseaux VPN peuvent utiliser un quelconque protocole de distribution d'étiquettes. La seule restriction est que, dans un réseau VPN donné, on utilise le même protocole dans tous les dispositifs de bord fournisseur, de manière que ceux-ci puissent interfonctionner. Cette restriction est due à la nature du protocole de distribution et non aux réseaux VPN.

En se reportant à la Figure 6, on observe que le fournisseur de services SP1 fournit le service VPN de niveau 0 (nommé VPN A) au fournisseur de services SP2 (B/G/F).

La distribution des étiquettes se fait indépendamment à chaque niveau de la hiérarchie des réseaux VPN. La distribution des étiquettes pour le réseau VPN de niveau 0 est indépendante de celle des étiquettes pour le réseau VPN de niveau 1. Le texte suivant décrit la distribution des étiquettes pour chaque niveau de la hiérarchie des réseaux VPN.

Distribution des étiquettes au niveau 0 (réseau VPN A)

Les bords du fournisseur de services SP1 se partagent les informations sur le routage dans le réseau VPN A. En d'autres termes, des informations sur l'accessibilité des routeurs de bord du fournisseur de services SP2 sont échangées. Les tunnels LSP sont mis en place dans le réseau VPN A entre les routeurs de bord du fournisseur de services SP2. Par exemple, on peut établir un tunnel LSP à partir du fournisseur de services SP2 (routeur de bord B) vers ce même fournisseur de services SP2 (routeur de bord G).

Distribution des étiquettes au niveau 1 (réseau VPN X)

Les bords du fournisseur de services SP2 se partagent les informations sur le routage dans le réseau VPN X. En d'autres termes, des informations sur l'accessibilité des routeurs de bord client des réseaux VPN X sont échangées. Les tunnels LSP sont mis en place dans le réseau VPN X entre les routeurs de bord client du fournisseur de services SP2.

L'emploi de l'avant-dernier saut produit (PHP, *penultimate hop popping*) nécessite que l'avant-dernière et la dernière étiquette en provenance du même espace d'étiquettes soient attribuées (dans ce cas, par exemple, l'attribution se fait en provenance de l'espace d'étiquettes du réseau VPN A). Cela implique que, dans le cas de réseaux VPN hiérarchiques, une étiquette supplémentaire (à savoir, l'avant-dernière étiquette) sera nécessaire entre l'étiquette du protocole IGP (à savoir, la dernière étiquette) pour le bord fournisseur et l'étiquette de destination du réseau VPN. Ceci est illustré dans le paragraphe 9.2.10.3 sur la transmission.

Dans cet exemple, il est indiqué que A2 est l'étiquette entre le routeur de bord client G du fournisseur de services SP2 et le routeur de bord client B de ce même fournisseur de services SP2, et il est mentionné au 9.2.10.3 comment A2 est employé (voir la Figure 8). Cette étiquette est choisie dans l'espace d'étiquettes du réseau VPN A.

Sur le plan architectural, les réseaux VPN X et Y de niveau 1 sont connectés au réseau VPN A de niveau 0 par une liaison entre routeurs virtuels. Il convient de noter que les routeurs de bord du fournisseur de services SP2 doivent être informés sur l'ensemble des trois réseaux VPN (à savoir, les réseaux VPN X, Y et A). Lorsque la liaison VRL est configurée pour une relation hiérarchique, le réseau VPN de niveau supérieur attribuera une étiquette en provenance de son espace d'étiquettes pour chaque liaison VRL, c'est-à-dire à chaque réseau VPN.

9.2.10.3 Transmission

Les données d'utilisateur provenant des réseaux VPN de niveau inférieur (par exemple, le niveau 1 dans la Figure 8) sont transmises par des tunnels LSP du réseau VPN de niveau supérieur (par exemple, le niveau 0 dans la Figure 8). Le codage des étiquettes illustré dans la Figure 8 est expliqué ci-après.

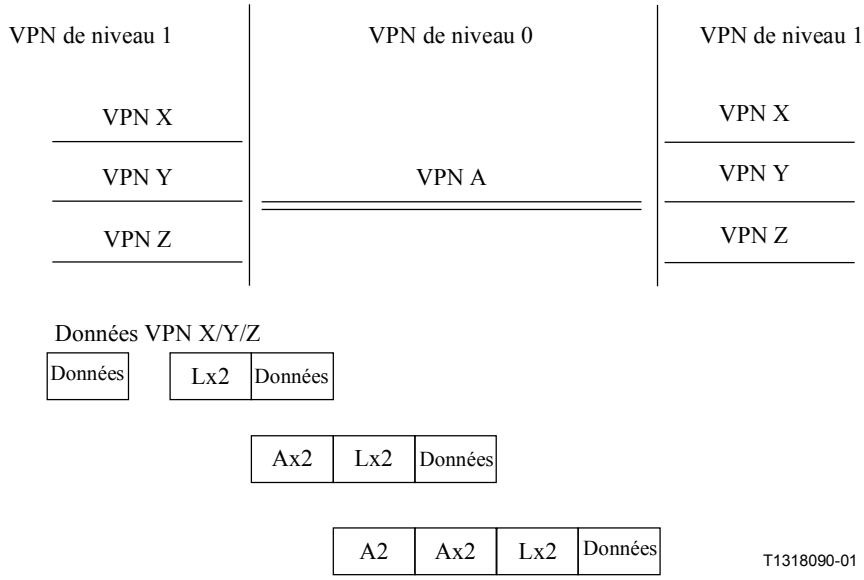


Figure 8/Y.1311.1 – Codage des étiquettes

1) Les données client arrivent au niveau du routeur de bord client pour le réseau VPN X du fournisseur de services SP2 (B) et sont encapsulées dans une trame à commutation MPLS.
2) L'étiquette Lx2 est envoyée sur la pile d'étiquettes. Lx2 est l'étiquette homologue du bord client du réseau VPN X employée pour transmettre des données du réseau VPN X vers le routeur de bord client pour ce même réseau VPN X du fournisseur de services SP2 (G).
3) L'étiquette suivante Ax2 est envoyée sur la pile d'étiquettes. Ax2 est l'étiquette homologue d'attache du réseau VPN X au réseau VPN A, provenant de l'espace d'étiquettes du réseau VPN A. Cette étiquette est employée par le réseau VPN A pour transmettre des données sur la liaison VRL du fournisseur de services SP2 (G) entre les réseaux VPN A et VPN X.
4) Finalement, l'étiquette A2 est envoyée sur la pile d'étiquette. Ceci est l'étiquette homologue du réseau VPN A employée pour transmettre des données en provenance du routeur de bord fournisseur pour le réseau VPN A du fournisseur de services SP2 (B) vers le routeur de bord fournisseur pour le même réseau VPN A de ce même fournisseur de services SP2 (G).

En résumé, le conduit LSP dans son entièreté, destiné à transporter des données client sur le réseau VPN X du bord client du fournisseur de services SP2 (B) au bord client de ce même fournisseur de services SP2 (G), assure les tâches suivantes:

a) transport des données à travers le réseau VPN A de niveau 0 à l'aide de l'étiquette A2;
b) transport des données à travers la liaison VRL du niveau 0 au niveau 1 du fournisseur de services SP2 (G) à l'aide de l'étiquette Ax2;
c) transport des données à travers le réseau VPN X de niveau 1 du fournisseur de services SP2 (B) vers ce même fournisseur de services SP2 (G) à l'aide de l'étiquette Lx2.

10 Options relatives à la qualité de service

Les options suivantes ont été proposées.

10.1 Spécification de niveau de service "point à nuage de points"

L'architecture de l'IETF relative aux services différenciés définit les mécanismes que sont le conditionnement du trafic DiffServ et le comportement par saut (PHB, *per hop behaviour*) Diffserv. Elle établit aussi que les divers services différenciés de bout en bout peuvent être mis en place au moyen de la combinaison d'une manière donnée de certains sous-ensembles de ces mécanismes et de l'application de procédures particulières d'attribution des ressources.

Il est prévu que les procédures d'attribution des ressources (pour chaque service DiffServ) pourraient être élaborées par des administrateurs de réseau qui permettraient, au moyen des mécanismes DiffServ de conditionnement du trafic et de comportement PHB, de prendre en charge les spécifications SLS "point à nuage de points".

A titre d'exemple, un administrateur de réseau peut prendre en charge une spécification SLS "point à nuage de points":

- en activant le conditionnement du trafic à chaque début ou fin de service sur la base des paramètres de trafic des différentes spécifications SLS correspondantes;
- en activant les comportements PHB et en attribuant des ressources à chaque liaison d'accès (pour chaque comportement PHB) sur la base des paramètres de trafic des différentes spécifications SLS correspondantes;
- en activant les comportements PHB dans le centre du réseau et en attribuant des ressources pour chaque comportement PHB sur une base agrégée (c'est-à-dire indépendamment des différentes spécifications SLS), sur la base des cycles monitoring and provisioning en cours, ou pour chaque liaison.

Le conditionnement du trafic DiffServ ainsi que les comportements PHB peuvent être pris en charge par les dispositifs à commutation MPLS. En conséquence, au moyen d'une infrastructure de réseau VPN à commutation MPLS, les fonctions de conditionnement du trafic et les comportements PHB peuvent être activés en tout point du réseau (par exemple, les dispositifs des bords client, des bords fournisseur ou des fournisseurs) d'une manière cohérente sans qu'il soit tenu compte du fait de savoir si le dispositif fonctionne au moyen de la commutation MPLS ou du protocole IP normal. Mais cela signifie que les services DiffServ de bout en bout peuvent être mis en place sur un réseau dorsal VPN à commutation MPLS disposant des capacités DiffServ de la même manière qu'ils peuvent être mis en place sur un réseau à capacités DiffServ n'étant pas à commutation MPLS. Et cela signifie aussi que les spécifications SLS "point à nuage de points" peuvent être prises en charge sur un réseau dorsal VPN à commutation MPLS disposant des capacités DiffServ exactement comme elles peuvent être assurées sur les réseaux dorsaux IP (sans commutation MPLS).

10.2 Spécification de niveau de service "point à point"

Il est envisagé que certaines applications, qu'il est prévu de transporter dans le cadre des services VPN à commutation MPLS, nécessitent des spécifications SLS "point à point".

10.2.1 Spécification de niveau de service "point à point" faisant intervenir des procédures d'attribution des ressources

Bien que les services DiffServ de bout en bout doivent encore faire l'objet d'une définition précise par l'IETF, il est prévu que, dans certains environnements, les procédures d'attribution des ressources (pour chaque service DiffServ) pourraient être élaborées par des administrateurs de réseau qui permettraient, au moyen des mécanismes DiffServ de conditionnement du trafic et de comportement PHB, de prendre en charge les spécifications SLS "point à point". A titre d'exemple, un administrateur de réseau peut prendre en charge une spécification SLS "point à point":

- en activant le conditionnement du trafic à chaque début ou fin de service sur la base des paramètres de trafic des différentes spécifications SLS correspondantes;
- en activant les comportements PHB et en attribuant des ressources à chaque liaison d'accès (pour chaque comportement PHB) sur la base des paramètres de trafic des différentes spécifications SLS correspondantes;

- en activant les comportements PHB dans le centre du réseau et en attribuant des ressources pour chaque comportement PHB sur une base agrégée (c'est-à-dire indépendamment des différentes spécifications SLS), sur la base d'un important surdimensionnement combiné aux cycles monitoring and provisioning en cours, ou pour chaque liaison.

A nouveau, parce que les mécanismes DiffServ peuvent être pris en charge par la commutation MPLS d'une façon transparente, dans des environnements où les procédures d'attribution des ressources peuvent être élaborées de manière à assurer des spécifications SLS "point à point", celles-ci peuvent être appliquées de la même manière exactement aux réseaux dorsaux VPN à commutation MPLS disposant des capacités DiffServ.

10.2.2 Spécification de niveau de service "point à point" faisant intervenir des procédures d'attribution des ressources et des mécanismes supplémentaires (commande d'admission explicite dans la bande, routage fondé sur des contraintes)

Il est prévu que, dans certains environnements, les spécifications SLS "point à point" ne peuvent être prises en charge efficacement au moyen des seuls mécanismes DiffServ combinés aux procédures d'attribution des ressources. Par exemple, lorsque des services intégrés (IntServ) doivent être pris en charge selon des engagements individuels "point à point" entre un site donné dans un réseau VPN et un autre site donné dans un réseau VPN, et lorsque les ressources dans le réseau dorsal sont limitées de manière que le surdimensionnement ne peut être envisagé, des mécanismes supplémentaires, tels que la commande d'admission explicite dans la bande ainsi que le routage fondé sur des contraintes, sont nécessaires.

La référence [7] fournit un cadre pour la prise en charge des services IntServ de bout en bout lorsqu'un nuage de points à capacités DiffServ est employé dans le réseau central. Une des options décrites est le contrôle d'admission sur une base agrégée dans le réseau central pour les ressources DiffServ.

Les mécanismes DiffServ peuvent être pris en charge par un réseau dorsal à commutation MPLS d'une manière qui est compatible avec les protocoles de signalisation à commutation MPLS de l'ingénierie du trafic, *traffic engineering*. En particulier, on peut établir des conduits commutés MPLS avec étiquette (LSP, *label switched path*) au moyen de ces protocoles. Dans ce cas, ces protocoles peuvent signaler les prescriptions relatives aux largeurs de bande de manière que la réservation de la largeur de bande ainsi que la commande d'admission peuvent être faites lors de l'établissement des conduits LSP. Par ailleurs, le routage dans ces conduits LSP à capacités DiffServ peut être fondé sur des contraintes.

L'ingénierie du trafic pour la commutation MPLS peut être renseignée sur les capacités DiffServ de manière que le routage fondé sur des contraintes puisse se faire séparément pour les différentes classes qui exigent que soient respectées des contraintes différentes.

En conséquence, en combinant la prise en charge des capacités DiffServ par la commutation MPLS avec les mécanismes existants de routage à commutation MPLS fondé sur des contraintes conformément à l'option définie dans la référence [7], ou les options d'ingénierie du trafic renseignée sur les capacités DiffServ, les spécifications SLS "point à point" concernant les capacités IntServ de bout en bout peuvent être prises en charge par un réseau dorsal VPN à commutation MPLS possédant les capacités DiffServ ou les options de l'ingénierie du trafic. Cette option proposée peut être employée dans des environnements où le surdimensionnement ne peut être envisagé.

Dans le cas de réseaux dorsaux hétérogènes comme à l'Annexe A (réseaux dorsaux à commutation MPLS non complète), des mécanismes supplémentaires tels que l'agrégation des protocoles de réservation de ressources (RSVP, *resource reservation protocol*) pour les réservations à travers le réseau dorsal sans commutation MPLS peuvent être utilisés pour offrir des garanties en ce qui concerne les spécifications SLS de bout en bout.

10.3 "Transparence en matière de classe de service"

La référence [8] indique que les points de code du champ des services différenciés peuvent être modifiés au sein d'un domaine de services différenciés, à l'intérieur de celui-ci ou aux nœuds de ses frontières. On suppose que le même principe s'applique aux champs qui sont employés dans le cadre des capacités DiffServ pour l'option à commutation MPLS (par exemple, le champ expérimental MPLS (EXP, *MPLS experimental field*) dans l'en-tête de remplissage MPLS).

La modification de ces champs, ajoutée à la configuration des réseaux IP VPN, n'est pas suffisante, parce qu'il n'a pas été tenu compte des spécifications particulières pour les réseaux IP VPN. Ces spécifications sont les suivantes:

- les clients des réseaux VPN qui utilisent des applications incorporant des solutions internes, relatives à la classe de service, devraient avoir la possibilité d'employer des solutions indépendantes de la solution relative à la classe de service, qui est prise en charge par l'infrastructure du fournisseur de services;
- les clients des réseaux VPN qui prennent en charge plus de classes de service que le fournisseur de services devraient avoir la possibilité d'utiliser ces classes sur les sites dans leurs réseaux privés physiques;
- un service de transport d'un transporteur, assuré par un fournisseur d'accès à un réseau, peut permettre à un fournisseur de services (client du fournisseur d'accès au réseau susmentionné) d'offrir des services IP VPN à ses clients. Le non-changement au cours du transport de la classe de service indiquée est une prescription essentielle pour les fournisseurs d'accès à un réseau et pour les fournisseurs de services. Au moyen de la propriété de transparence de la classe de service, le fournisseur de services peut offrir à ses clients sa propre solution en matière de classe de service, sans tenir compte de la solution relative à la classe de service qui est prise en charge par le fournisseur d'accès au réseau.

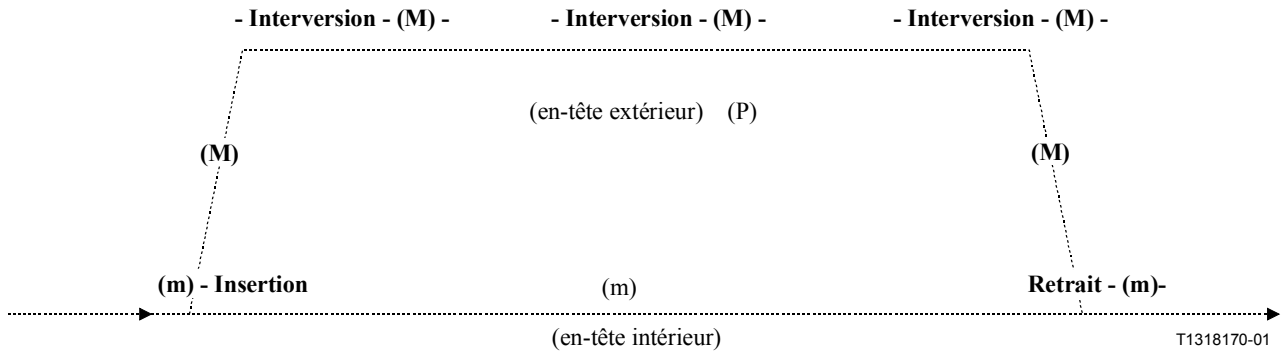
Même si un réseau IP VPN peut en quelque sorte être considéré comme une émulation d'un réseau privé physique, il n'est pas faisable que le fournisseur d'accès à un réseau prenne en charge toutes les différentes solutions du client et du fournisseur de services en matière de classe de service. La prise en charge de la transparence en matière de classe de service garantit donc que la classe de service indiquée par un client ou un fournisseur de services soit transmise sans changement dans le réseau à commutation MPLS du fournisseur d'accès au réseau.

Les modèles de tunnellisation à capacités DiffServ pour la commutation MPLS sont notamment:

- le modèle de tunnellisation uniforme;
- le modèle de tunnellisation par canalisation.

Le modèle de canalisation est tel que les informations sur les capacités DiffServ des paquets transportés à travers le tunnel ne sont pas affectées par les informations sur les capacités DiffServ employées sur la longueur du tunnel.

Les opérations du modèle de canalisation sans avant-dernier saut PHP sont illustrées dans la Figure 9.



(M) représente les "informations DiffServ transmises par conduit LSP"
(m) représente les "informations DiffServ transmises par tunnel"

Figure 9/Y.1311.1 – Modèle de canalisation sans avant-dernier saut PHP

Une des applications du "modèle de tunnelisation par canalisation" est la prise en charge de la transparence en matière de classe de service dans un réseau dorsal VPN à commutation MPLS.

11 Réseau VPN entre systèmes autonomes (fournisseurs de services)

Les réseaux VPN de type IP peuvent comporter plusieurs systèmes autonomes ou fournisseurs de services. L'exemple le plus courant est celui d'une société internationale, dont les bureaux sont répartis dans plusieurs pays dans le monde, qui voudrait confier ses services IP à un fournisseur de services. En réalité, il est peu probable qu'une telle société puisse acquérir les services d'un fournisseur de services qui serait présent à proximité de presque tous les sites qu'elle possède. Généralement, certains fournisseurs de services couvrent des régions ou des pays, tandis que d'autres sont présents au niveau international. Cela veut dire que la société doit acquérir les services VPN auprès de différents fournisseurs de services, en fonction des besoins de ses bureaux locaux ou succursales. Cela signifie en outre que l'interconnexion de ces îlots VPN séparés géographiquement revêt une grande importance aux yeux du fournisseur dont la présence est mondiale. Bien sûr, une présence mondiale peut vouloir dire la présence internationale d'un fournisseur de services permettant d'assurer la connectivité de fournisseurs nationaux dans diverses parties du monde; elle pourrait aussi vouloir dire la présence nationale d'un fournisseur de services permettant d'assurer la connectivité de fournisseurs régionaux dans un pays donné. Il est donc indispensable de disposer de l'interfonctionnement.

L'une des manières de fournir des services VPN à une société par l'intermédiaire de plusieurs systèmes autonomes (fournisseurs de services) consiste à employer le mécanisme hiérarchique entre réseaux VPN décrit au 9.2.10.

Toutefois, il n'est actuellement envisagé aucune contrainte qui empêcherait d'étendre cette méthode de manière à englober des scénarios d'interconnexion de systèmes autonomes (de fournisseurs de services), fondés sur d'autres conceptions en matière de réseaux VPN.

Il conviendrait également de noter que les capacités pour les scénarios concernant les réseaux VPN entre systèmes autonomes (fournisseurs de services), fondés sur les conceptions en matière de réseaux VPN à protocole BGP/à commutation MPLS, sont données dans la référence [5].

12 Interfonctionnement

12.1 Interfonctionnement entre différentes réalisations

Le présent paragraphe donne les grandes lignes d'une réalisation possible permettant d'assurer l'interfonctionnement entre des conceptions décrites dans la présente Recommandation.

Il est tenu compte des éléments suivants:

- motivation pour l'interfonctionnement entre réseaux VPN (voir 12.1.1);
- hypothèses pour les réseaux VPN à commutation MPLS en tant qu'éléments assurant l'interfonctionnement (voir 12.1.2);
- capacités fonctionnelles pour l'interfonctionnement, telles que la garantie de la sécurité, la projection de la classe de qualité de service, la distribution d'informations sur le routage dynamique (voir 12.1.3).

Des restrictions en matière de dimensionnement pour cette réalisation peuvent en limiter l'applicabilité. En conséquence, cette réalisation doit faire l'objet d'un complément d'étude.

12.1.1 Motivation pour l'interfonctionnement entre réseaux VPN

Deux cas peuvent se présenter:

cas 1: les réseaux VPN s'étendent sur plusieurs réseaux à commutation MPLS implémentés différemment et appartenant à différents fournisseurs de services VPN. Ce cas répond aux prescriptions et aux attentes normales en ce sens que chaque fournisseur de services VPN choisit, parmi plusieurs implémentations pour les réseaux VPN, celle qui lui convient le mieux.

cas 2: les réseaux VPN s'étendent sur plusieurs réseaux à commutation MPLS implémentés différemment mais appartenant à un fournisseur de services VPN. Un fournisseur de services VPN peut mettre en place plusieurs réseaux à commutation MPLS (par exemple, un ancien et un nouveau réseau à commutation MPLS). L'interfonctionnement entre réseaux VPN permet de lever la prescription qui stipule que tous les sites d'utilisateur dans un réseau VPN doivent être connectés au même réseau à commutation MPLS.

Dans les deux cas, l'interfonctionnement permet aux fournisseurs de services VPN de fournir des services VPN de manière souple. Cela profite également aux utilisateurs de réseaux VPN.

12.1.2 Hypothèses

La structure suivante pour le réseau à commutation MPLS qui est illustrée dans la Figure 10 est supposée être présente en tant qu'élément de base pour la fourniture des services VPN.

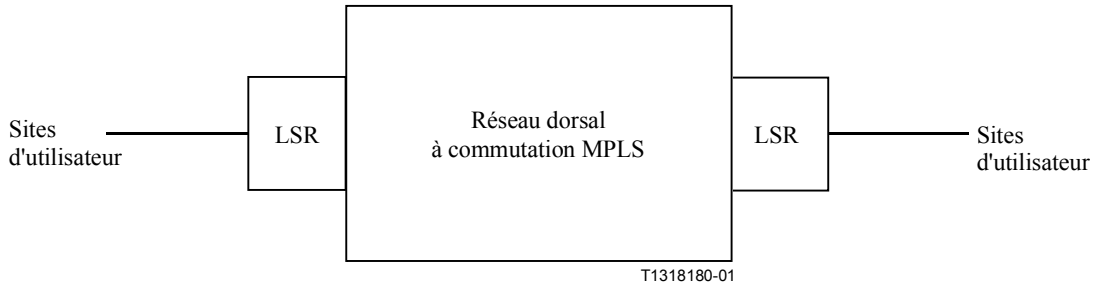


Figure 10/Y.1311.1 – Structure du réseau à commutation MPLS (LSR, *label switching router:* routeur à commutation avec étiquette)

La Figure 11 illustre le modèle d'interfonctionnement.

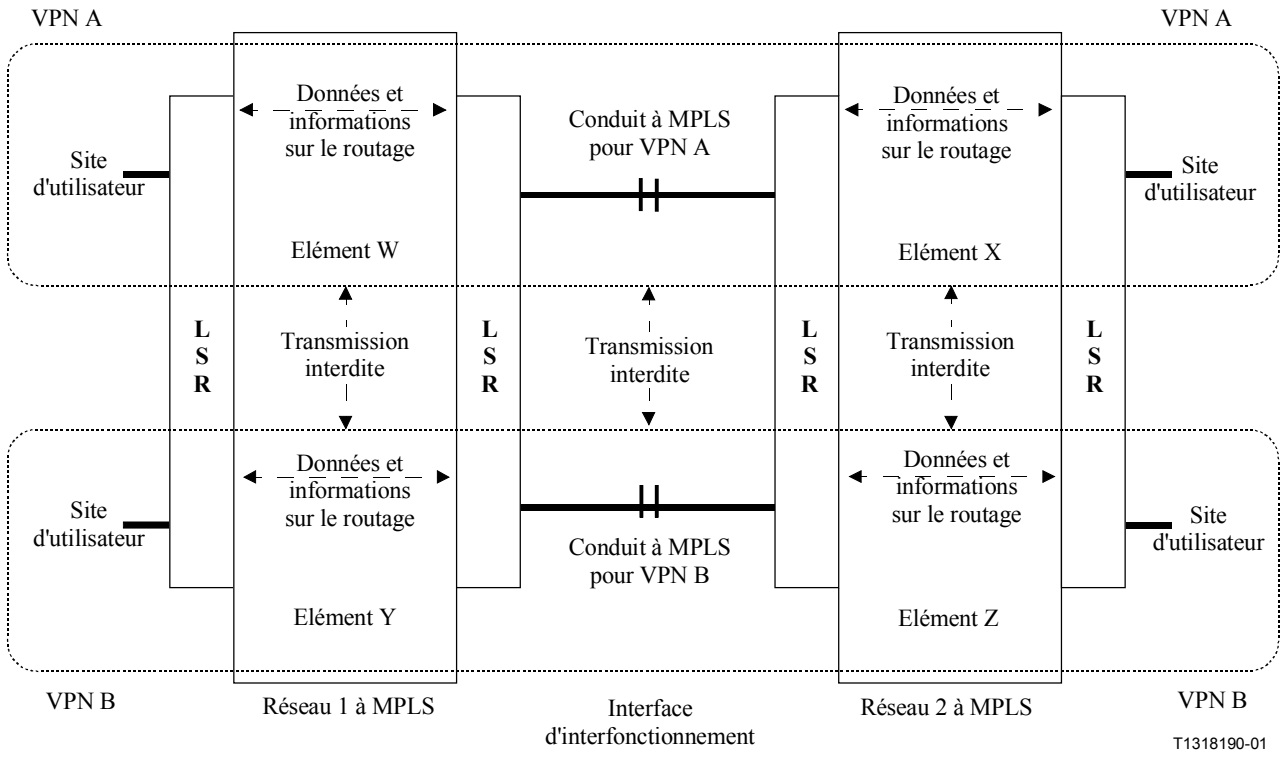


Figure 11/Y.1311.1 – Modèle d'interfonctionnement

Un "élément" est toute partie d'un réseau VPN qui est séparé par un réseau à commutation MPLS. Lorsqu'un réseau VPN s'étend sur plusieurs réseaux (domaines) à commutation MPLS, la partie du réseau VPN qui appartient à un seul réseau à commutation MPLS est nommée un "élément".

12.1.3 Capacités fonctionnelles pour l'interfonctionnement entre réseaux VPN à commutation multiprotocolaire par étiquetage

12.1.3.1 Capacités fonctionnelles pour l'interfonctionnement

Les deux types suivants d'interfonctionnement entre réseaux VPN peuvent se présenter:

- type (1): interfonctionnement lorsque les réseaux à commutation MPLS sont raccordés et que l'en-tête IP est consulté au niveau d'un routeur LSR de sortie/entrée;
- type (2): interfonctionnement lorsque les réseaux à commutation MPLS ne sont pas raccordés et que l'en-tête IP n'est pas consulté au niveau des routeurs LSR de sortie/entrée.

Puisque l'implémentation de chaque réseau VPN existant à commutation MPLS est unique, il est difficile de réaliser le type (2).

Le type (1) par contre est facilement réalisable puisqu'il emploie la fonction du routeur LSR qui consiste à consulter l'en-tête IP. La description qui suit se concentrera donc sur le type (1).

Il est supposé que les connexions à l'interface d'interfonctionnement sont assurées au moyen du protocole Internet ou de la commutation MPLS.

Il est nécessaire pour la prise en charge de l'interfonctionnement entre réseaux VPN de disposer des trois capacités fonctionnelles suivantes:

- garantie de la sécurité;
- mappage de la classe de qualité de service;
- distribution d'informations sur le routage dynamique détaillées ci-après dans les paragraphes 12.1.3.2, 12.1.3.3 et 12.1.3.4, respectivement.

12.1.3.2 Garantie de la sécurité

Lorsque des réseaux VPN à commutation MPLS s'étendent sur plusieurs réseaux à commutation MPLS, chaque réseau VPN dispose d'une "connexion" définie au préalable (par exemple, un circuit virtuel en mode ATM, un conduit à commutation MPLS, etc.) aux frontières d'interconnexion des réseaux à commutation MPLS. Il n'est pas permis de transmettre des paquets entre une connexion donnée quelconque et un autre réseau VPN quelconque à commutation MPLS (sauf lorsque des accords particuliers entre réseaux VPN ont été conclus). Ce mécanisme permet d'assurer la sécurité. Les procédures qui permettent une telle attribution sont propres à la réalisation employée pour l'implémentation du réseau à commutation MPLS, associée à la connexion.

L'identité du réseau VPN à chaque extrémité n'a de sens que dans le cadre du réseau particulier à commutation MPLS qui est associé à la connexion. Il est supposé que les connexions ne sont pas communes à plusieurs réseaux VPN.

Dans la Figure 11 ci-dessus, on observe qu'il existe une connexion logique entre le réseau 1 à commutation MPLS et le réseau 2 à commutation MPLS employés pour construire le réseau VPN qui s'étend sur ceux-ci. La connexion avec le réseau VPN est attribuée à l'élément "W" qui n'a de sens que dans le cadre du réseau 1 à commutation MPLS. L'autre extrémité de la connexion est attribuée à l'élément "X" qui n'a de sens que dans le cadre du réseau 2 à commutation MPLS.

NOTE – Il est recommandé que la largeur de bande d'une connexion n'interfère pas avec la largeur de bande des autres connexions. Les spécifications détaillées relatives à la qualité de service de la connexion doivent faire l'objet d'un complément d'étude.

12.1.3.3 Mappage de la classe de qualité de service

Toute connexion peut se voir attribuer des attributs d'une classe de qualité de service. Cela permet la configuration dans chaque réseau VPN de plusieurs classes de qualité de service. L'identification de la classe dans la couche IP ne doit être faite qu'une seule fois.

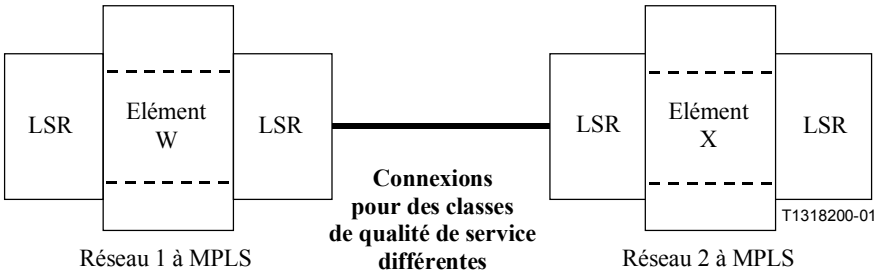


Figure 12/Y.1311.1 – Emploi de connexions multiples pour des classes de qualité de service multiples pour chaque réseau VPN

Une autre méthode consiste à employer le champ de la classe de service, à savoir une configuration binaire dans un champ tel que EXP dans l'en-tête de remplissage ou le point DSCP [type de service (TOS, *type of service*)] de l'en-tête IP, pour identifier une classe de qualité de service au cours de la transmission d'un paquet sur cette connexion. La connexion est commune à plusieurs classes de qualité de service. Les capacités DiffServ sont un exemple typique de cette méthode de projection. Cette méthode peut réduire le nombre de connexions, mais la commande de la qualité de service de la connexion est difficile.

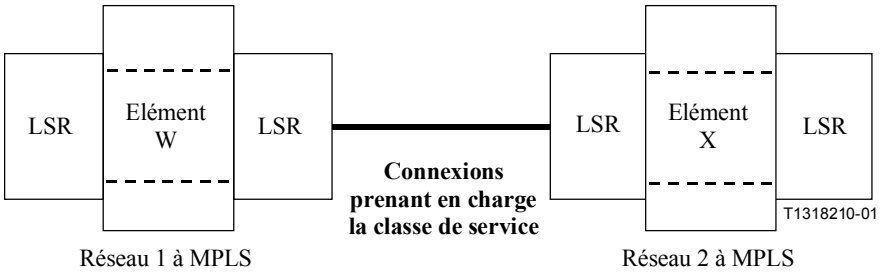


Figure 13/Y.1311.1 – Emploi de la classe de service dans une connexion unique pour la prise en charge de classes de qualité de service multiples pour chaque réseau VPN

12.1.3.4 Distribution d'informations sur le routage dynamique

Certains mécanismes des réseaux VPN de commande de routage sont nécessaires dans les routeurs LSR de sortie/entrée. La connexion représentée dans la Figure 11 entre le réseau 1 à commutation MPLS et le réseau 2 à commutation MPLS ne transmet que des paquets destinés au routage IP normalisé. Les informations sur le routage sont alors transmises par la capacité fonctionnelle qui est décrite au 12.1.3.2 ainsi que par les données. Cela permet la distribution d'informations sur le routage dynamique dans chaque réseau VPN. Des protocoles normalisés de routage tels que les protocoles BGP, OSPF, RIP, le protocole de routage vectoriel multidestinataire à distance (DVMRP, *distance vector multicast routing protocol*) ou la multidiffusion indépendante du protocole (PIM, *protocol independent multicast*) peuvent être utilisés dans les connexions de tous les réseaux VPN.

12.1.3.5 Considérations sur le dimensionnement de la réalisation proposée d'interfonctionnement

Les capacités fonctionnelles de l'interfonctionnement entre réseaux VPN à commutation MPLS par l'intermédiaire du protocole Internet en mode ATM sont récapitulées dans la Figure 14. Il convient de noter que cette réalisation ne nécessite aucun nouveau protocole ni aucune nouvelle modification des protocoles existants.

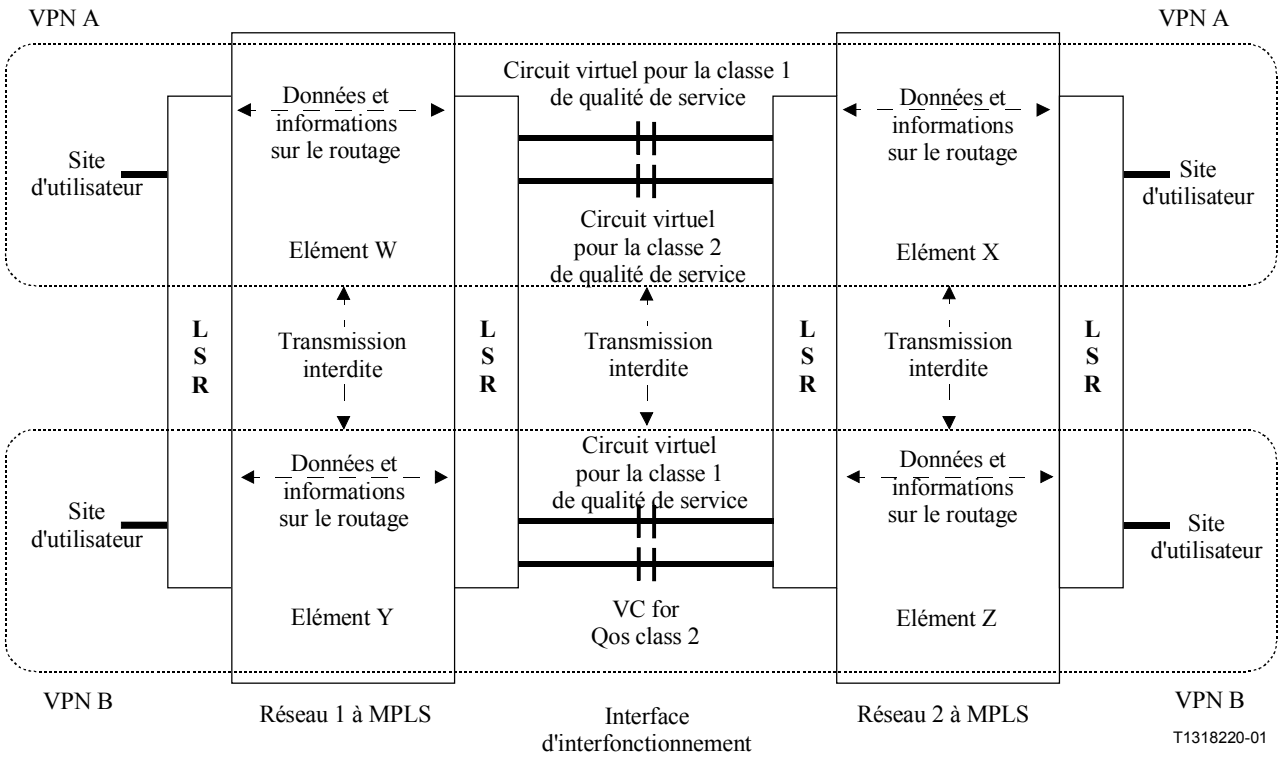


Figure 14/Y.1311.1 – Proposition d'interfonctionnement entre réseaux VPN au moyen du protocole Internet en mode ATM

La réalisation exposée dans le paragraphe 12 est axée sur l'interfonctionnement statique (à savoir l'interfonctionnement dans le plan utilisateur) à mettre en place rapidement. L'interfonctionnement dynamique (à savoir l'interfonctionnement dans le plan de commande ou dans le plan de gestion) devrait être examiné afin de réduire dans un avenir proche la configuration manuelle, et d'améliorer ainsi le dimensionnement.

12.2 Interfonctionnement des services avec d'autres architectures VPN

Il devrait être tenu compte des aspects suivants pour l'interfonctionnement des services:

- interfonctionnement dans le plan de données;
- interfonctionnement dans le plan de commande;
- interfonctionnement dans le plan de gestion.

L'Appendice I donne des informations sur ce sujet.

ANNEXE A

Réseaux VPN à commutation MPLS s'étendant sur des infrastructures de réseau central sans commutation MPLS

La présente Recommandation aborde la prise en charge des services IP VPN dans une architecture à commutation MPLS qui ne nécessite pas une infrastructure de réseau à commutation MPLS complète.

Un scénario générique de mise en place d'une infrastructure de réseau à commutation MPLS non complète est présenté dans la Figure A.1.

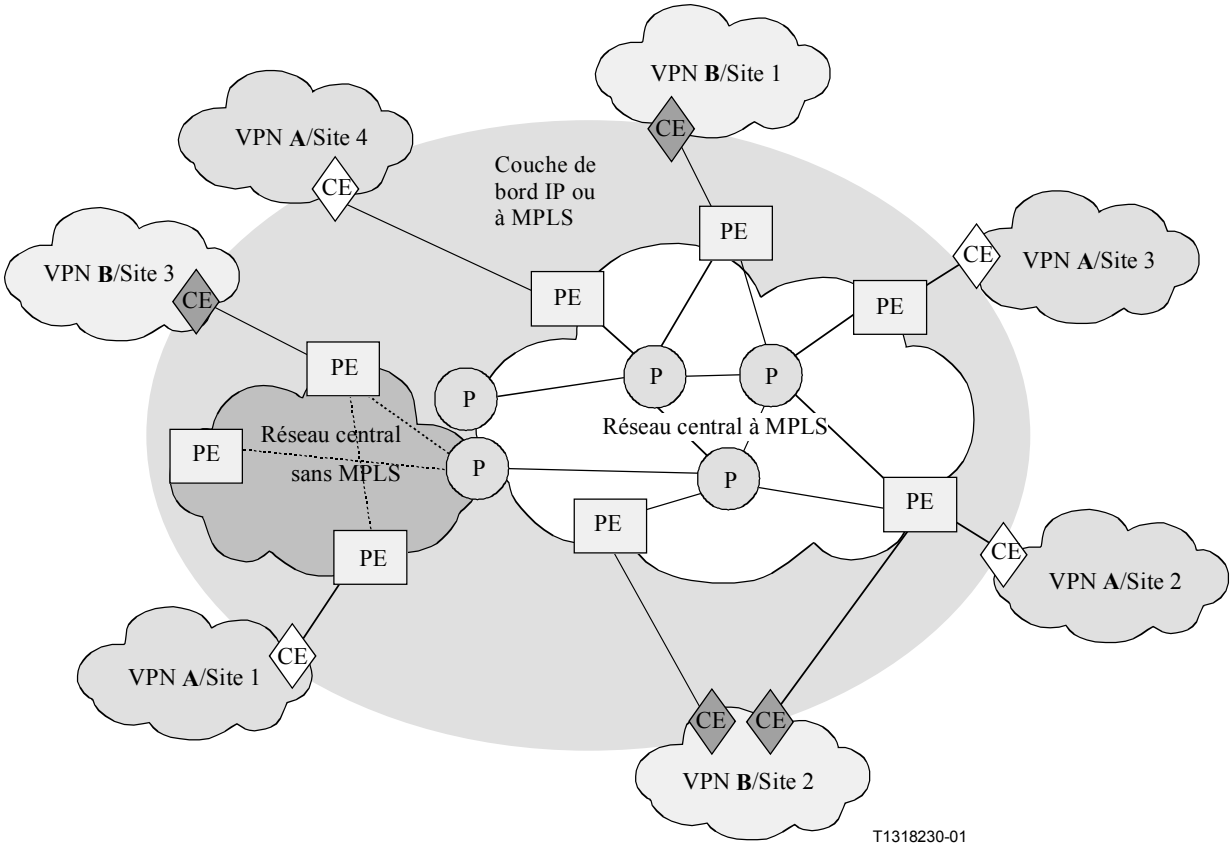


Figure A.1/Y.1311.1 – Infrastructure de réseau à commutation MPLS non complète

L'emploi de mécanismes tels que la commutation MPLS au moyen de l'encapsulage GRE ou IP est un exemple de scénario particulier de mise en place, dans lequel la partie sans commutation MPLS de l'infrastructure du réseau est purement de type IP.

NOTE – Dans le cas d'une infrastructure de réseau à commutation MPLS non complète, les effets particuliers sur la capacité de satisfaire à toutes les prescriptions décrites dans la présente Recommandation doivent faire l'objet d'un complément d'étude.

APPENDICE I

Exemples d'interfonctionnement des services avec d'autres architectures de réseau VPN

Il devrait être tenu compte des aspects suivants:

- interfonctionnement dans le plan de données;
- interfonctionnement dans le plan de commande;
- interfonctionnement dans le plan de gestion.

Interfonctionnement dans le plan de données

Pour l'interfonctionnement dans le plan de données, l'information de l'en-tête d'encapsulage propre à l'architecture de réseau VPN du paquet reçu est mappée sur celle du paquet transmis afin de satisfaire à la prescription relative au service, décrite dans le paragraphe 7.

La Figure I.1 ci-après montre l'exemple de l'en-tête d'encapsulage employé par plusieurs architectures de réseau VPN afin d'identifier les utilisateurs de réseaux VPN.

Architecture de réseau VPN	En-tête	Identificateur
MPLS	En-tête de remplissage	Etiquette
VLAN (IEEE802.1Q)	TCI	ID VLAN
IP en mode ATM	En-tête de cellule	VPI/VCI
IP en mode relais de trames	En-tête de relais de trames	DLCI
L2TP	En-tête L2TP	ID tunnel/ID session

Figure I.1/Y.1311.1 – Exemple d'en-têtes employés par les réseaux VPN

Il convient de noter que la longueur des champs d'identificateur pour les différentes architectures de réseau VPN ne sont pas les mêmes, et qu'en conséquence un mappage précis devrait être défini.

Les informations de l'en-tête d'encapsulage et les informations de l'en-tête de couche 3 (c'est-à-dire l'en-tête IP) doivent être mappées afin de préserver l'identification de l'utilisateur de réseau VPN.

Par exemple, on peut mapper l'identificateur de l'en-tête d'encapsulage joint à l'adresse IP de destination de l'en-tête IP du paquet reçu dans l'identificateur du paquet transmis.

En outre, les informations sur la classe de qualité de service d'un paquet ne peuvent être transmises d'une extrémité à une autre. A titre d'exemple, dans le cas de l'interfonctionnement entre un réseau VPN à commutation MPLS et un réseau VLAN (dont l'explication est donnée ci-après dans le présent appendice), le nœud peut projeter la priorité de l'utilisateur contenue dans l'information de contrôle d'étiquette dans le champ EXP de l'en-tête de remplissage MPLS (ou dans le champ approprié d'un en-tête MPLS ne servant pas au remplissage).

Interfonctionnement dans le plan de commande

Des informations sur le routage, propres à chacune des différentes architectures de réseau VPN, doivent être échangées entre celles-ci afin de réaliser la projection des informations d'en-tête.

Interfonctionnement dans le plan de gestion

Afin d'améliorer l'interfonctionnement, il est souhaitable que les systèmes de gestion des différentes architectures de réseau VPN puissent fonctionner les unes avec les autres.

Exemple d'interfonctionnement entre des architectures de réseau VPN à commutation MPLS et un réseau VLAN

Le texte ci-après décrit l'interfonctionnement entre différentes architectures de réseaux et, à titre d'exemple, entre un réseau VPN à commutation MPLS et un réseau VLAN spécifié dans la référence IEEE802.1Q [9].

La Figure I.2 montre un modèle de réseau pour l'interfonctionnement entre un réseau VPN à commutation MPLS et un réseau VLAN. Dans ce modèle, les réseaux VLAN A sont situés en des lieux physiquement séparés et connectés entre eux par un réseau VPN à commutation MPLS, tout comme les réseaux VLAN B qui sont aussi situés en des endroits physiquement séparés et connectés entre eux par un réseau VPN à commutation MPLS.

1) *Passage du réseau VLAN au réseau à commutation MPLS*

Le nœud à l'entrée du réseau VPN à commutation MPLS mappe l'identificateur du réseau VLAN attribué à chacun d'entre eux dans l'étiquette MPLS afin de séparer dans le réseau VPN à commutation MPLS ses utilisateurs, et il mappe le préfixe de l'adresse IP de destination dans l'étiquette MPLS afin de router le paquet vers la bonne destination.

2) *Passage du réseau à commutation MPLS au réseau VLAN*

Le nœud à la sortie du réseau VPN à commutation MPLS mappe l'étiquette MPLS dans l'identificateur du réseau VLAN attribué à chacun d'entre eux, et route le paquet vers la bonne destination après avoir examiné l'adresse IP de destination.

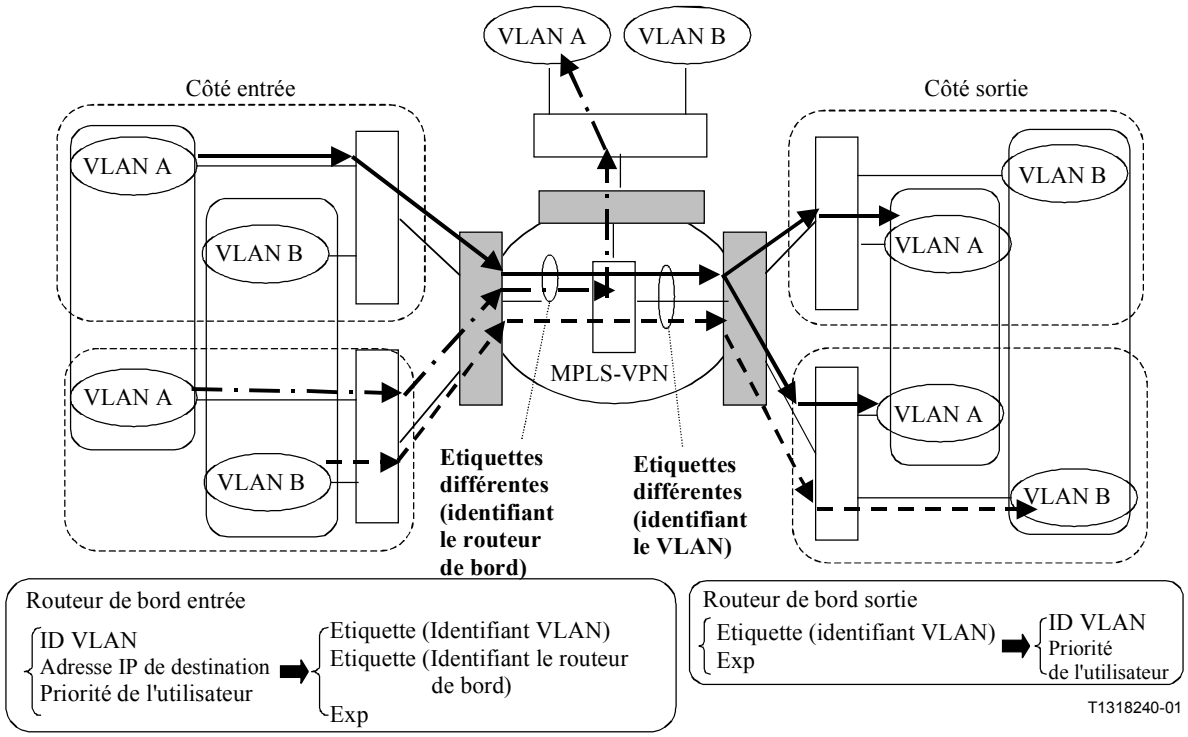


Figure I.2/Y.1311.1 – Modèle de réseau pour l'interfonctionnement entre un réseau VPN à commutation MPLS et un réseau VLAN

APPENDICE II

Bibliographie

[1] CARUGI (M.) *et al., Service requirements for Provider Provisioned Virtual Private Networks*, travail en cours de l'IETF.

[2] CALLON (R.) *et al., A Framework for Provider Provisioned Virtual Private Networks*, travail en cours de l'IETF.

[3] JACQUENET (C.), *Functional needs for the deployment of an IP VPN service offering: a service provider perspective*, travail en cours de l'IETF.

[4] ROSEN (E.) *et al., BGP/MPLS VPNs* (draft-rosen-rfc2547bis-03.txt), travail en cours de l'IETF.

[5] OULD-BRAHIM (H.) *et al., Network based IP VPN Architecture using Virtual Routers*, travail en cours de l'IETF.

[6] OULD-BRAHIM (H.) *et al., BGP/VPN: VPN Information Discovery for network based VPNs*, travail en cours de l'IETF.

[7] MUTHUKRISHNAN (K.) *et al., A Core MPLS IP VPN architecture*, (draft-muthukrishnan-rfc2917bis-00.txt), travail en cours de l'IETF.

[8] KATHIRVELU (C.) *et al., Hierarchical VPN over MPLS Transport,* travail en cours de l'IETF.

[9] LE FAUCHEUR (F.) *et al., MPLS Support of Differentiated Services*, travail en cours de l'IETF.

[10] SUMIMOTO (J.), SUZUKI (M.), TABATA (O.), ESAKI (Y.), DOUKAI (M.), *MPLS VPN Interworking*, travail en cours de l'IETF.

[11] WORSTER (T.) *et al., MPLS Label Stack Encapsulation in IP*, travail en cours de l'IETF.

[12] GODERIS (D.) *et al., Service Level Specification Semantics and Parameters*, travail en cours de l'IETF.

[13] REKHTER (Y.), TAPPAN (D.), ROSEN (E.), *MPLS Label Stack Encapsulation in GRE*, travail en cours de l'IETF.

[14] LE FAUCHEUR (F.) *et al., Requirements for support of DiffServ-Aware MPLS Traffic Engineering*, travail en cours de l'IETF.

[15] LE FAUCHEUR (F.) *et al., Extensions to IS-IS, OSPF, RSVP and CR-LDP for support of DiffServ-Aware MPLS Traffic engineering*, travail en cours de l'IETF.

[16] BAKER (F.), ITURRALDE (C.), LE FAUCHEUR (F.), DAVIE (B.), *Aggregation of RSVP for IPv4 and IPv6 Reservations*, travail en cours de l'IETF.

[17] AWDUCHE (D.), BERGER (L.), GAN (D.), LI (T.), SWALLOW (G.), SRINIVASAN (V.), *RSVP-TE: Extensions to RSVP for LSP Tunnels*, travail en cours de l'IETF.

[18] JAMOUSSI (B.) *et al., Constraint-Based LSP Setup using LDP*, travail en cours de l'IETF.

[19] HUMMEL (H.), *Tree/Ring/Meshy VPN tunnel systems*, travail en cours de l'IETF.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données et communication entre systèmes ouverts
Série Y	**Infrastructure mondiale de l'information et protocole Internet**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Genève, 2001