UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Y.1311

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(03/2002)

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

Aspects relatifs au protocole Internet – Transport

Réseaux privés virtuels fournis par le réseau – Architecture générique et prescriptions de service

Recommandation UIT-T Y.1311

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

Réseaux privés virtuels fournis par le réseau – Architecture générique et prescriptions de service

Résumé

La présente Recommandation spécifie l'architecture générique et les prescriptions de service qui sont applicables à la fourniture de réseaux privés virtuels par des fournisseurs de services de réseau.

Source

La Recommandation Y.1311 de l'UIT-T, élaborée par la Commission d'études 13 (2001-2004) de l'UIT-T, a été approuvée le 16 mars 2002 selon la procédure définie dans la Résolution 1 de l'AMNT.

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

Réseaux privés virtuels fournis par le réseau – Architecture générique et prescriptions de service

1 Domaine d'application et objet

La présente Recommandation décrit un certain nombre d'aspects génériques relatifs à l'architecture et spécifie un certain nombre d'exigences génériques de service relatives à la fourniture de réseaux privés virtuels (NB-VPN, *network-based virtual private network*) par le réseau physique.

Les réseaux NB-VPN ont un ensemble commun d'exigences et sont associés par l'emploi d'un ensemble commun de mécanismes. La présente Recommandation décrit les définitions de service, le cadre et les exigences des réseaux NB-VPN.

Le domaine d'application de la présente Recommandation s'étend aux diverses implémentations essentielles d'un réseau NB-VPN ainsi qu'aux services offerts au client à l'interface d'accès.

Le domaine d'application est également décrit par la Figure 1, qui montre les principaux arrangements entres services et modes d'implémentation.

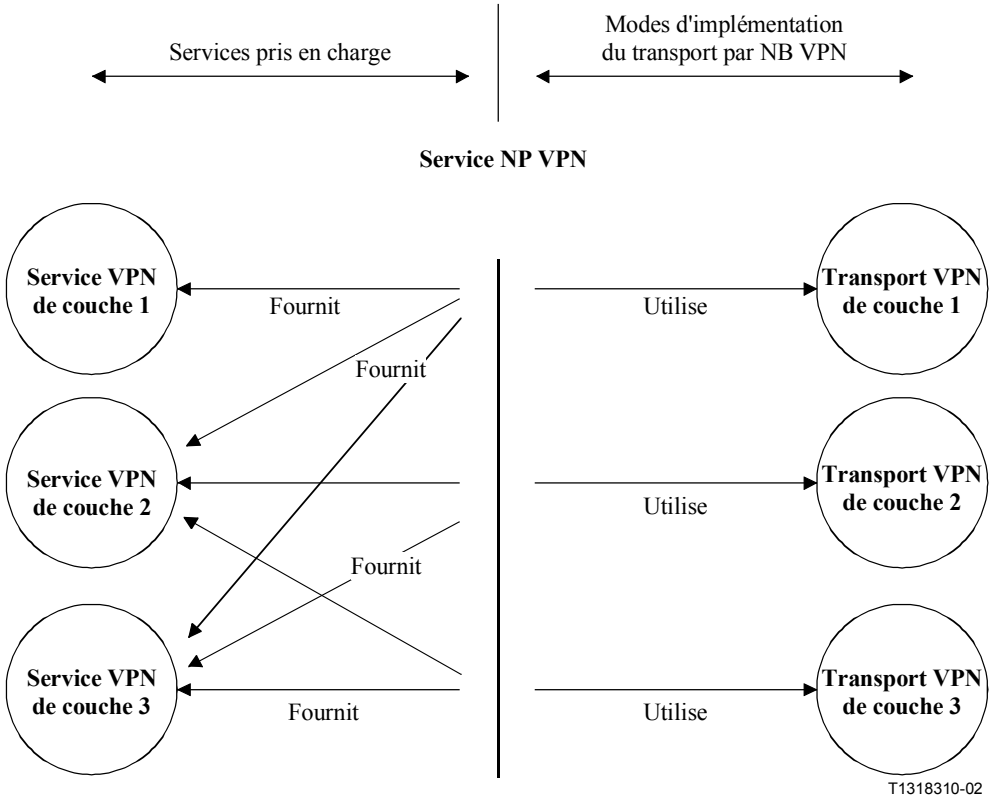


Figure 1/Y.1311 – Domaine d'application général

NOTE 1 – Les exemples indiqués ci-dessus ne sont pas exhaustifs.

NOTE 2 – Les combinaisons d'éléments indiquées dans cette figure ne sont pas toutes réalisables ni incluses dans le domaine d'application de la présente Recommandation.

Les paragraphes 5 et 6 développent les concepts représentés sur la Figure 1.

2 Références

2.1 Références normatives

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.

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

[2] Recommandation UIT-T Y.1311.1 (2001), *Réseau privé virtuel IP sur réseau utilisant l'architecture MPLS*.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 réseau privé virtuel fourni par le réseau (NB-VPN, *network-based virtual private network*)

Partie d'un réseau qui assure la connexité dans un sous-ensemble limité et spécifique de l'ensemble total des utilisateurs desservis par le fournisseur de réseau. Un VPN a l'apparence d'un réseau qui est dédié spécifiquement aux utilisateurs contenus dans le sous-ensemble. Cette affectation spéciale est réalisée par des moyens logiques plutôt que physiques, d'où l'usage du terme *virtuel*. Les utilisateurs contenus dans un VPN ne peuvent pas communiquer, en passant par le fournisseur du VPN, avec les utilisateurs non inclus dans le sous-ensemble VPN spécifique, et inversement.

NOTE – Le terme "fourni par le réseau" sert à distinguer les solutions de fourniture du réseau décrites dans la présente Recommandation des solutions VPN obtenues en ne faisant intervenir que les seuls équipements du client. Chaque fois que le terme "VPN" est utilisé dans la présente Recommandation, il doit être interprété comme signifiant "VPN fourni par le réseau".

3.2 réseau NB-VPN de couche 1

Réseau NB-VPN dont le service VPN fonctionne dans la couche 1 et fournit des connexions optiques ou TDM entre dispositifs clients appartenant au VPN, c'est-à-dire entre un accès d'un dispositif client donné et un accès d'un autre dispositif client.

3.2.1 réseau VPN optique

Réseau NB-VPN de couche 1 qui utilise des interconnexions optiques entre dispositifs clients comme base de fourniture des ressources VPN.

3.3 réseau NB-VPN de couche 2

Réseau NB-VPN dont le service VPN fonctionne dans la couche 2 et fournit un service de liaison de données entre dispositifs clients appartenant au VPN, par exemple au moyen des protocoles IEEE 802, FR ou ATM.

3.4 réseau NB-VPN de couche 3

Réseau NB-VPN dont le service VPN fonctionne dans la couche 3 et fournit un service de couche 3 entre dispositifs clients appartenant au VPN, par exemple au moyen de protocoles IP.

3.4.1 réseau NB-VPN en mode IP

Réseau NB-VPN de couche 3 qui utilise l'adressage IP, la retransmission et le routage IP, le protocole IP pour la commande et les données, et la technologie IP comme base de fourniture des ressources VPN.

3.5 réseau de services virtuels (VSN, *virtual services network*)

Représentation abstraite de l'ensemble des services qui peuvent être mis à la disposition d'un client de réseau NB-VPN. Ces services sont ceux qui permettent la commande, l'administration et la gestion du VPN.

3.6 réseau de transport virtuel

Représentation abstraite de l'ensemble des formes d'implémentation d'un réseau NB-VPN.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations suivantes:

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

CE extrémité client (*customer edge*)

FR relais de trames (*frame relay*)

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

IEEE Institut des ingénieurs électriciens et électroniciens (*Institute of electrical and electronic engineers*)

IETF Groupe de travail sur l'ingénierie Internet (*Internet engineering task force*)

IP protocole Internet (*Internet protocol*)

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

NB fourni par le réseau (*network based*)

P fournisseur (*provider*)

PE extrémité fournisseur (*provider edge*)

PPVPN réseau privé virtuel fourni par un tiers (*provider provisioned virtual private network*)

QS qualité de service

SLA convention sur le niveau de service (*service level agreement*)

TDM multiplexage par répartition dans le temps (*time division multiplex*)

VPN réseau privé virtuel (*virtual private network*)

VSN réseau de services virtuels (*virtual service network*)

VTN réseau de transport virtuel (*virtual transport network*)

5 Définition du service

5.1 Introduction

Le présent paragraphe donne une définition fonctionnelle générique d'un service de "réseau VPN fourni par le réseau". Les questions d'implémentation ainsi que les aspects de service propres à l'implémentation sont hors du domaine d'application de la présente Recommandation.

5.1.1 Types de service VPN

Les trois types de service suivants sont distingués.

5.1.1.1 Service VPN de couche 1

Dans un service VPN de couche 1, le dispositif d'extrémité client est connecté au fournisseur de réseau par l'intermédiaire d'une ou de plusieurs liaisons dont chacune se compose d'une ou de plusieurs voies ou sous-voies (par exemple, en longueur d'onde ou alternativement en longueur d'onde et en intervalle de temps, ou en intervalle de temps seulement). Le dispositif d'extrémité client et le dispositif d'extrémité fournisseur ne sont appariés que dans la couche de liaison physique du réseau d'accès.

Une liaison possède deux extrémités:

a) l'une au dispositif d'extrémité client (CE, *customer edge*), appelée *accès*;

b) l'autre au dispositif d'extrémité fournisseur (PE, *provider edge*), appelée *accès d'extrémité fournisseur*.

Le domaine d'application d'un service de couche 1 n'est associé qu'aux réseaux VPN équipés d'accès.

5.1.1.2 Service VPN de couche 2

Dans un service VPN de couche 2, le dispositif d'extrémité client reçoit le service de couche Liaison (c'est-à-dire de couche 2) provenant du fournisseur de réseau. Les dispositifs d'extrémité client et d'extrémité fournisseur sont appariés dans la couche Liaison de données du réseau d'accès. Le réseau assure la retransmission des paquets de données d'utilisateur sur la base des informations contenues dans les en-têtes de couche Liaison de données des paquets, par exemple les identificateurs DLCI en relais de trames, les circuits VCC en mode ATM ou les étiquettes VLAN en mode 802.1q.

5.1.1.3 Service VPN de couche 3

Dans un service VPN de couche 3, le dispositif d'extrémité client reçoit le service de couche Réseau (normalement sous la forme de paquets IP) provenant du fournisseur de réseau. Les dispositifs d'extrémité client et d'extrémité fournisseur sont appariés dans la couche Réseau du réseau d'accès. Le réseau assure la retransmission des paquets de données d'utilisateur sur la base des informations contenues dans les en-têtes de couche IP, comme une adresse de destination IPv4 ou IPv6. Le client voit le réseau comme un dispositif de couche 3 tel qu'un routeur IPv4 ou IPv6.

5.1.2 Vue du service NB-VPN

La Figure 2 décrit la vue de trois instances du service NB-VPN afin d'en illustrer différentes applications.

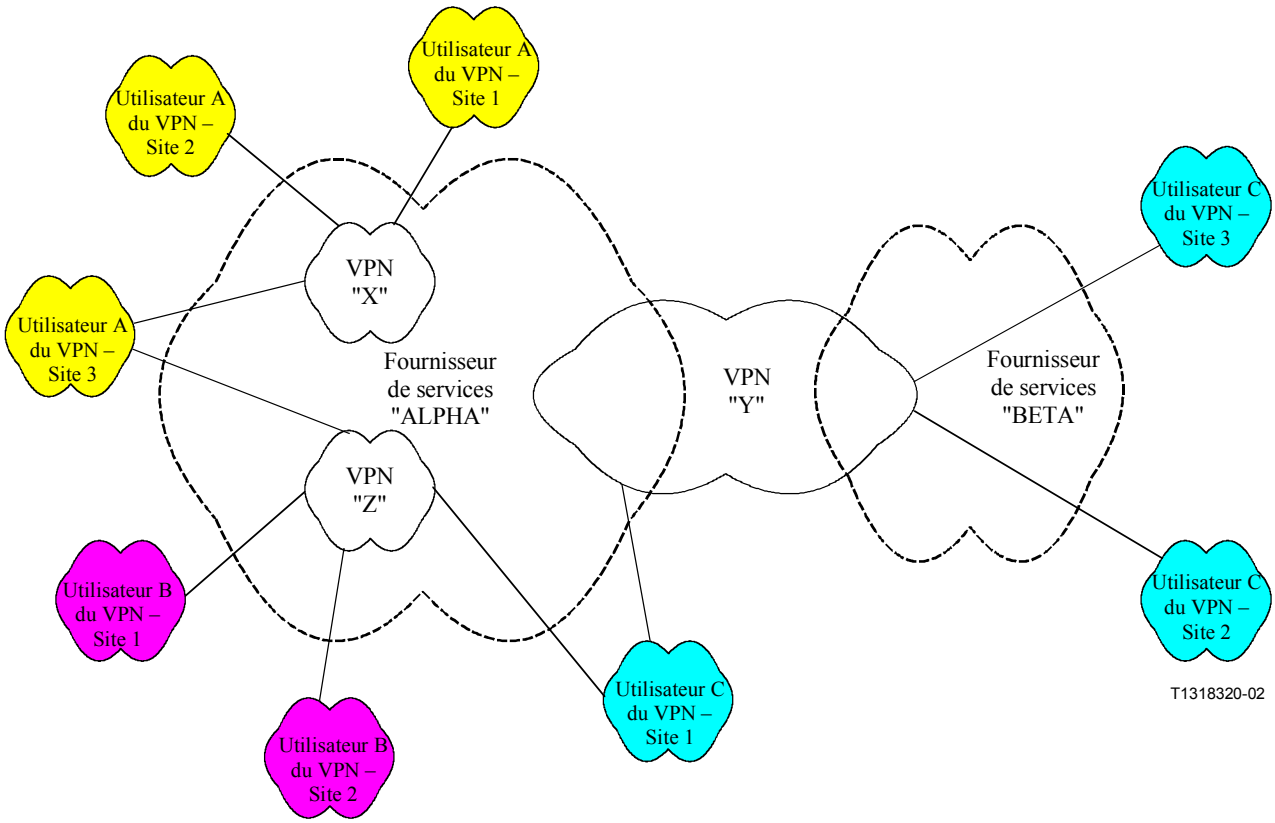


Figure 2/Y.1311 – Vue du service de réseau NB-VPN

5.1.3 Scénarios de déploiement du service NB-VPN

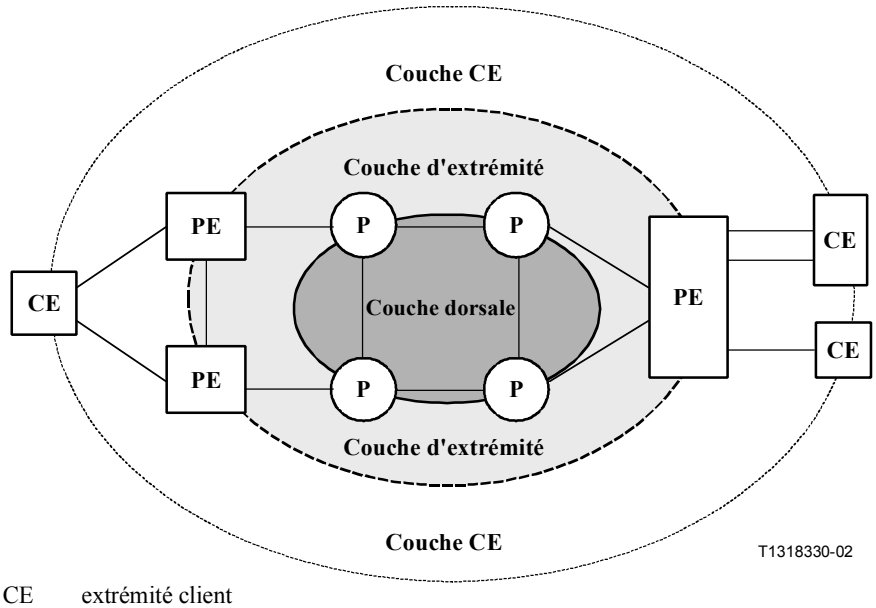
Un certain nombre de scénarios de déploiement du service générique sont envisagés pour les réseaux NB-VPN. Les Appendices I, II et III décrivent respectivement les VPN de couche 3, 2 et 1.

Il convient de noter qu'il s'agit des scénarios de déploiement envisagés le plus couramment et non pas d'une liste exhaustive de tous les scénarios devant être pris en charge par les services de réseau NB-VPN. Autrement dit, un fournisseur de services peut offrir un service VPN prenant en charge un sous-ensemble ou un surensemble des scénarios ci-dessus, en fonction des exigences du client et de limites techniques ou autres.

5.2 Modèle de référence du service NB-VPN

5.2.1 Désignation des éléments de réseau NB-VPN

Le modèle de référence générique du service VPN est représenté par la Figure 3 ci-dessous.



CE extrémité client
PE extrémité fournisseur
P fournisseur

Figure 3/Y.1311 – Modèle de référence de réseau

Afin de faciliter la fourniture d'un VPN par un fournisseur de réseau, il est essentiel de tenir compte de l'adjonction, de la suppression, des déplacements et des modifications parmi les sites et les membres avec aussi peu d'intervention manuelle que possible. Un activateur déterminant pour la fourniture de VPN est l'établissement des "tunnels" qui séparent le trafic d'un réseau VPN donné de celui d'un autre VPN ainsi que du trafic du réseau ouvert dans une infrastructure commune. Si des éléments de réseau VPN essentiels peuvent annoncer leur présence les uns aux autres grâce à des techniques d'autodécouverte, les tunnels requis peuvent être configurés avec un minimum d'intervention manuelle. Le principe de l'autodécouverte s'applique à tous les types de VPN quelle que soit la couche dans laquelle le service est offert. Par exemple, la relation entre extrémités homologues CE-PE, établie pour le service VPN, peut s'établir dans la couche 1, 2, ou 3.

Les tunnels entre dispositifs PE pour VPN peuvent être construits de part et d'autre de la couche dorsale, dans la couche 1, 2 ou 3. Exemples de tunnels de couche 1: les trajets optiques ou TDM. Exemples de tunnels de couche 2: les conduits ATM, MPLS ou IEEE 802.2. Exemples de tunnels de couche 3: les conduits IP (fondés sur divers mécanismes protocolaires en mode IP).

NOTE – Le service de couche VPN offert à l'extrémité CE par l'extrémité PE peut fonctionner dans une couche différente de celle qui a été utilisée par la technique de mise en tunnel entre les extrémités PE. Si le service de couche CE-CE requis est différent du service de couche PE-PE, des techniques d'émulation et/ou d'encapsulage seront utilisées par les extrémités PE afin de résoudre cette différence.

L'extrémité PE est le dispositif contenu dans le réseau du fournisseur qui offre le service VPN au client. L'extrémité CE est le dispositif qui fournit l'interface au domaine client. Chaque CE peut être un dispositif d'entrée/de sortie pour un ensemble sous-jacent d'extrémités adressables/atteignables de client VPN dans une zone géographique donnée du domaine client. La connexité entre extrémités PE et CE peut être assurée de plusieurs façons. Par exemple, une extrémité CE donnée peut être connectée à une ou plusieurs extrémités PE et une extrémité PE donnée peut être connectée à une ou plusieurs extrémités CE qui peuvent appartenir ou ne pas appartenir au même site ou au même réseau VPN.

Le dispositif P est le routeur ou commutateur situé à l'intérieur de l'infrastructure dorsale afin d'interconnecter les extrémités PE. Les dispositifs P possèdent peu d'informations (si tant est qu'ils en aient) sur l'existence de réseaux VPN.

5.2.2 Autodécouverte entre éléments de réseau

Le degré d'autodécouverte entre éléments de réseau variera en fonction de la mise en œuvre technique et des décisions administratives. Théoriquement, le principe de l'autodécouverte peut être appliqué aux trois cas suivants.

5.2.2.1 Découverte PE-PE

Dans ce cas, les extrémités PE d'un réseau VPN donné sont informées de leur existence réciproque et établissent des informations de gestion de configuration appropriées.

5.2.2.2 Découverte CE-PE

Dans ce cas, les extrémités PE d'un réseau VPN donné sont informées de l'existence d'extrémités CE d'un réseau VPN donné et établissent des informations de gestion de configuration appropriées.

5.2.2.3 Découverte CE-CE

Dans ce cas, les extrémités CE d'un réseau VPN donné sont informées de leur existence réciproque et des adresses sous-jacentes desservies, puis établissent des informations de gestion de configuration appropriées.

6 Cadre abstrait de réseau NB-VPN

6.1 Environnement opérationnel

Il est essentiel que les opérateurs de réseau:

a) soient en mesure de répondre rapidement à diverses exigences de service client;

b) soient en mesure d'exploiter diverses technologiques dans le réseau afin de réaliser les services requis.

Il est possible de satisfaire à ces deux exigences en effectuant une dissociation entre les moyens internes de livraison de service et le service livré au point approprié. Une telle solution offre aux opérateurs de réseau:

c) un trajet dynamiquement évolutif;

d) un point de flexibilité facilitant les transitions et les adaptations entre techniques d'accès et techniques dorsales;

e) un moyen d'intégrer les systèmes existants;

f) des points précis d'interfonctionnement possible.

Etant donné que le service lui-même ou la technologie peut ne pas être homogène de bout en bout, l'on peut considérer l'ensemble du service et de la technologie comme étant constitué d'un réseau virtuel de service et d'un réseau de transport virtuel. Par ailleurs, le VPN possède l'apparence et les caractéristiques d'un réseau attribué à un client donné. Les techniques de service et de transport perçues par l'utilisateur ou les utilisateurs ultimes peuvent ne pas être les mêmes de bout en bout dans tous les éléments constituants du réseau; elles peuvent au contraire être simulées ou émulées par d'autres moyens, qui peuvent alors être considérés comme virtuels.

Génériquement, ces concepts peuvent être illustrés par un haut niveau d'abstraction, comme indiqué dans la Figure 4 ci-dessous. Ce modèle permet de définir les exigences génériques de service d'une façon indépendante de la technologie.

Dans la plupart des cas, le même service sera fourni de bout en bout d'un réseau VPN à chaque extrémité CE, par exemple IP à IP ou FR à FR. Des arrangements d'interfonctionnement pourront cependant faciliter la livraison de différents services à chaque extrémité, dans le cadre de certaines contraintes (par exemple du mode ATM au mode FR).

6.2 Aperçu général des réseaux VSN et VTN

6.2.1 Modèle général

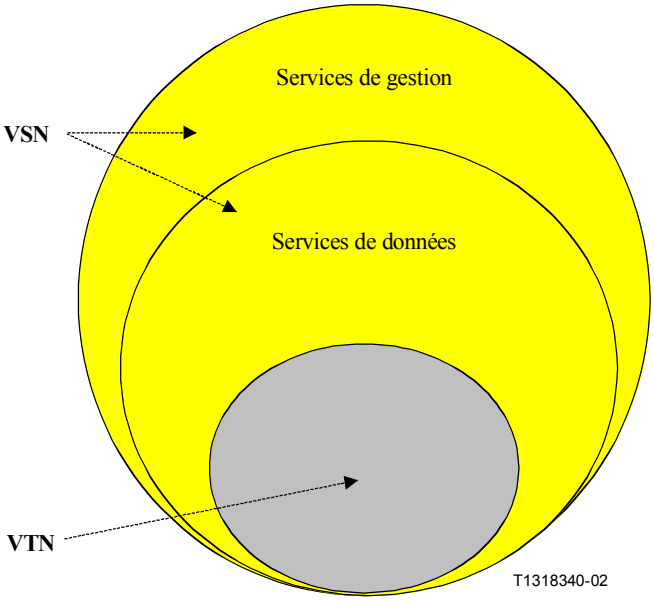


Figure 4/Y.1311 – Modèle VSN/VTN

6.2.2 Eléments constituants des réseaux VSN et VTN

Le réseau VPN est considéré comme constitué des éléments VSN et VTN.

L'élément VSN se compose d'un certain nombre de plates-formes de livraison de service qui livrent des services au client du transporteur. L'environnement de livraison de service inclut les éléments de gestion du réseau et de politique qui améliorent les possibilités de personnalisation et de spécialisation aussi bien pour les clients que pour les applications.

L'élément VSN offrira un ou plusieurs des services gérés de transporteur suivants:

- services gérés de couche 1;
- services gérés de couche 2;
- services gérés de couche 3 (accès Internet; services Intranet, services Extranet);
- services gérés d'accès distant;
- services gérés de sécurité.

L'élément VTN est l'infrastructure de transport proprement dite, vue en tant qu'image virtuelle de la dorsale du transporteur.

La fourniture et la nature d'un réseau VPN nécessite la séparation et l'isolation du trafic de ce réseau VPN par rapport au trafic d'autres réseaux VPN et au trafic public. Ces exigences nécessitent un certain mécanisme de mise en tunnel dans lequel les formats de capacité utile de données et/ou l'adressage utilisés dans un réseau VPN donné n'ont pas de relation avec ceux qui sont utilisés pour acheminer dans la dorsale les données mises en tunnel.

L'élément VTN offrira un ou plusieurs des modes de transport gérés de transporteur suivants:

- virtualisation de dorsale:
  - transport pour réseau VSN en couche 1, 2 ou 3;
- virtualisation d'accès:
  - accès d'abonné au réseau VSN en couche 1, 2 ou 3.

Les modes de réseau VTN selon des types de réseau VPN particulier sont décrits dans d'autres Recommandations de la série Y.1311 concernant les réseaux NB-VPN.

6.3 Gestion de réseau VPN

Un important aspect d'un réseau VPN est sa gestion. En plus de la connexité de transport assurée par le réseau VPN proprement dit, le fournisseur de services aura besoin de livrer à l'utilisateur des services fournis par le réseau, afin de faciliter l'administration, la commande et la gestion générale du réseau VPN. Les services de gestion peuvent en particulier être les suivants:

a) gestion de la configuration du VPN;

b) gestion de la performance du VPN;

c) gestion des dérangements du VPN;

d) gestion de la comptabilité du VPN;

e) gestion de la sécurité du VPN.

Les services de gestion peuvent être répartis à l'intérieur du réseau du fournisseur. Ils appartiennent donc au réseau de services virtuels (VSN, *virtual services network*) comme indiqué dans la Figure 5.

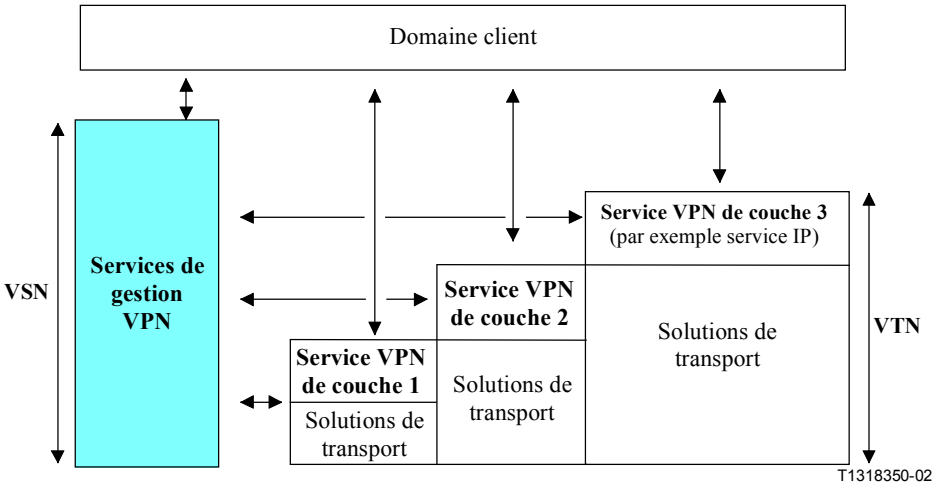


Figure 5/Y.1311 – Modèle de réseau VSN/VTN – Services de gestion

7 Exigences du service

Comme décrit au paragraphe 6, un réseau NB-VPN peut être modélisé comme étant composé d'un réseau de services virtuels et d'un réseau de transport virtuel. Ces deux éléments constituants peuvent être considérés comme ayant des exigences de service précises, représentant respectivement les aspects d'utilisateur et les aspects d'opérateur de réseau.

7.1 Exigences du service pour le réseau de services virtuels

Les paragraphes ci-après décrivent les exigences du service de réseau VSN.

7.1.1 Exigences générales du service de réseau VSN

- Moyens permettant à l'utilisateur de définir l'appartenance au réseau VSN.
- Prise en charge de systèmes d'adressage VPN définis par l'utilisateur.
- Transparence aux données d'utilisateur.
- Moyen permettant à un site client donné d'appartenir simultanément à plusieurs réseaux VPN.

- Capacité de définition arbitraire de topologies VPN par l'utilisateur (allant par exemple d'un réseau radial à maillage partiel à un réseau radial à maillage total).
- Prise en charge de protocoles multiples.
- Capacité de sites d'utilisateur à rattachements multiples.
- Prise en charge d'utilisateurs fixes et mobiles.
- Capacité d'interfaces normalisées (indépendantes du fournisseur du dispositif d'utilisateur).
- Prise en charge d'une large gamme de protocoles de routage entre routeurs d'extrémités CE et PE.
- Moyens de prise en charge de diverses exigences de trafic (QS) définies par l'utilisateur.
- Moyens de prise en charge de différents modes de communication tels que point à point (1:1), multidiffusion (1:N, M:N) et diffusion générale (1: tous).
- Moyens d'offrir, de prendre en charge et de maintenir des niveaux de service agréés (par exemple, au moyen de conventions sur le niveau de service).
- Moyens de répondre aux exigences de sécurité de l'utilisateur.
- Fourniture aux membres du réseau VPN d'un accès dynamique et sécurisé à ce réseau (par exemple, par circuit téléphonique commuté).
- Fourniture de services de gestion de réseau VPN appropriés (par exemple, configuration, dérangements, qualité, sécurité, etc.).
- Prise en charge de la croissance du ou des réseaux VPN donnés.

7.1.2 Gestion de la configuration

- Utilisation de gabarits de service définis par l'utilisateur afin de détecter les caractéristiques de site et de routage du réseau VPN.
- Vérification de compatibilité et de cohérence des informations de configuration d'utilisateur.
- Capacité de modifier facilement la topologie.
- Capacité d'ajouter, de supprimer ou de modifier facilement des dispositifs, des sites, des routes, des trafics, etc.
- Capacité de prendre en charge des exigences de croissance pour dispositifs, sites, routes, trafics, etc.

7.1.3 Gestion des dérangements

- Information du client en cas d'interruption et de rétablissement du service.
- Reprise dynamique "masquée" (sans interruption) dans la mesure du possible.
- Fourniture de comptes rendus et de résumés d'incident appropriés.

7.1.4 Gestion de la performance

- Conservation de la performance conformément aux conventions sur le niveau de service (SLA).
- Fourniture d'informations, de statistiques, etc. sur la performance.
- Capacité de fournir au client la démonstration de la performance.
- Prédiction de tendances, des probabilités de dérangement et/ou recommandations relatives aux conventions SLA actuelles, aux conformations du trafic, à la QS, etc.

7.1.5 Comptabilisation

- Fourniture aux clients/utilisateurs de factures détaillées.

- Ventilation personnalisée des informations de facturation.
- Corrélation avec la QS et/ou les conventions sur le niveau de service.
- Corrélation avec les informations de gestion de la performance et des dérangements.

7.1.6 Sécurité

- Contrôle d'accès.
- Authentification.
- Confidentialité des données.

7.1.7 Conventions sur le niveau de service et QS

- Conventions sur le niveau de service, par réseau VPN et/ou par site VPN et/ou par route VPN, devant contenir:
  - Les objectifs de niveau de service, composés de tout ou partie de ce qui suit:
    - capacité de transfert de données;
    - paramètres de QS;
    - disponibilité;
    - fiabilité;
    - confirmation de livraison;
    - prise en charge de la mobilité et de la portabilité;
    - sécurité;
    - largeur de bande;
    - priorité;
    - authentification;
    - protocoles pris en charge;
    - flexibilité – échelonnement et connexité;
    - durée de vie de la convention SLA.
  - Objectifs de surveillance du service
    - surveillance de la QS – comparaison aux objectifs;
    - suivi des flux;
    - comptes rendus si nécessaire.
  - Objectifs de compensation financière
    - option de facturation;
    - pénalités;
    - fixation des prix;
    - frais de terminaison anticipée.

NOTE – Les exigences générales relatives aux conventions SLA sont décrites plus en détail dans la Rec. UIT-T Y.1241.

7.2 Exigences du service pour le réseau de transport virtuel

Les paragraphes suivants décrivent les exigences du service VTN.

7.2.1 Fourniture générale du service

- Moyen d'attribuer à chaque VPN un identificateur VPN mondialement unique.
- Moyen de terminer les appartenances au réseau VPN.

- Capacité de prise en charge d'espace(s) d'adressage en chevauchement entre réseaux VPN.
- Capacité de réception d'informations d'accessibilité de liaison distante en provenance du site utilisateur et capacité de diffusion de ces informations vers les routeurs d'extrémité homologues et appropriés.
- Moyen de distribution d'informations d'accessibilité à l'intérieur d'un VPN.
- Moyen de construction de tunnels vers d'autres dispositifs nécessaires pour prendre en charge un VPN donné.
- Prise en charge de réseaux VPN recouvrant plusieurs réseaux de fournisseur.
- Utilisation d'interfaces normalisées pour l'interopérabilité à l'intérieur d'un réseau VPN.
- Utilisation de solutions échelonnables afin de permettre la croissance d'un VPN donné ou de plusieurs réseaux VPN.
- Moyen de détecter le trafic en boucle dans un VPN donné.
- Moyen d'éviter le trafic en boucle dans un VPN donné.
- Moyen de minimiser le trafic en boucle dans un VPN donné.

7.2.2 Gestion de la configuration

- Extraction automatique des informations de configuration à partir des informations d'utilisateur.
- Configuration automatisée des ressources du réseau.
- Utilisation de mécanismes d'autodécouverte pour l'accessibilité externe de l'utilisateur.
- Utilisation de mécanismes d'autodécouverte pour l'accessibilité à l'intérieur d'un VPN.
- Comparaison avec les conventions SLA.

7.2.3 Gestion des dérangements

- Détection automatique des dérangements (par alarmes, comptes rendus d'incident, événements, violations de seuil de QS et de SLA, etc.).
- Localisation automatique des dérangements (par analyse d'alarmes, comptes rendus, diagnostics, etc.).
- Fourniture au client d'informations sur les dérangements.
- Enregistrement des incidents, journalisation (création et suivi des tickets de dérangement).
- Action correctrice automatisée (pour le rétablissement des nécessités du trafic, du routage, des ressources, etc.).
- Comparaison avec les conventions SLA.

7.2.4 Gestion de la performance

- Surveillance automatique du comportement d'un réseau VPN, soit:
  - les mesures de performance en temps réel;
  - la surveillance en temps réel de la situation des ressources et des éléments VPN.
- Activation des mécanismes de surveillance et des objets métrologiques appropriés aux exigences SLA et QS.
- Analyse des informations (par exemple, largeur de bande, temps de réponse, disponibilité, perte de paquets, etc.).
- Evaluation de la performance en fonction des conventions sur le niveau de service (SLA).
- Production de statistiques et de tendances fondées sur les informations recueillies.
- Analyse des informations de performance pour utilisation dans les comptes rendus clients.

7.2.5 Comptabilisation

- Mesurage du taux d'utilisation des diverses ressources applicables.
- Taux d'utilisation par rapport aux quotas/conventions SLA (cumul de consommation, autorisations, etc.).
- Stockage à long terme des informations de comptabilité (création/administration de fichiers).
- Traitement paramétré des informations de comptabilité afin de produire une ventilation des factures définie par le client.
- Moyen de corréler les informations de comptabilité avec les informations de gestion des dérangements et de la performance.
- Comparaison avec les conventions SLA.

7.2.6 Sécurité

- Mécanismes de contrôle d'accès au réseau VPN.
- Mécanismes d'authentification des utilisateurs accédant à un réseau VPN.
- Mécanismes de sécurisation des données transportées par le réseau VPN.
- Comparaison avec les conventions SLA.

Appendice I

Scénarios de déploiement du service pour réseaux NB-VPN en mode IP

Introduction

Le présent appendice décrit quelques importants scénarios génériques de déploiement du service (quel que soit le mécanisme de transport sous-jacent qui est utilisé dans le réseau du fournisseur de services). Les scénarios génériques suivants sont envisagés pour les services NB-VPN en mode IP:

– Intranet (connexité entre sites dans la même organisation);
– Extranet (connexité entre sites d'organisations différentes);
– réseaux VPN entre de multiples systèmes autonomes ou fournisseurs de services;
– accès simultané à un réseau VPN et à Internet;
– réseaux VPN hiérarchiques (VPN imbriqués dans des VPN);
– scénarios multiples d'accès distant (circuit téléphonique commuté, ligne DSL, radiotéléphonie à poste fixe, câble).

I.1 Intranet (connexité entre sites dans la même organisation)

Ce scénario est le plus simple et le plus courant. Dans ce cas, un réseau VPN est formé entre différents sites appartenant à la même organisation. Ce scénario pourrait par exemple être envisagé comme l'interconnexion de différentes filiales et/ou leur connexion supplémentaire au siège. C'est le scénario minimal/obligatoire qui doit être pris en charge par toute architecture de réseau VPN. Il est décrit en détail dans divers paragraphes de la présente Recommandation. Un scénario de déploiement Intranet de base est décrit dans la Figure I.1, où les sites clients sont connectés au dispositif d'extrémité fournisseur (PE) du service au moyen d'un dispositif d'extrémité client (CE). Les types de cette connexion peuvent être divers (par exemple, une route statique au moyen d'un protocole de routage, un circuit virtuel en mode ATM, ou tout mécanisme d'accès spécialisé comme une ligne DSL, un câblo-modem ou une station radioélectrique). Des tunnels sont construits dans le réseau dorsal du fournisseur de services. Le mécanisme de construction des tunnels est propre à

l'architecture utilisée pour construire le réseau VPN (comme décrit dans la présente Recommandation et dans la Rec. UIT-T Y.1311.1). Ces tunnels peuvent être soit construits séparément dans chaque réseau VPN comme indiqué dans la Figure I.1, ou être communs à plusieurs réseaux VPN avec une sorte de fonctionnalité de multiplexage afin de séparer le trafic de ces différents réseaux VPN. Il existe également la possibilité (non représentée sur la Figure I.1) qu'un même site client appartienne à plusieurs réseaux VPN.

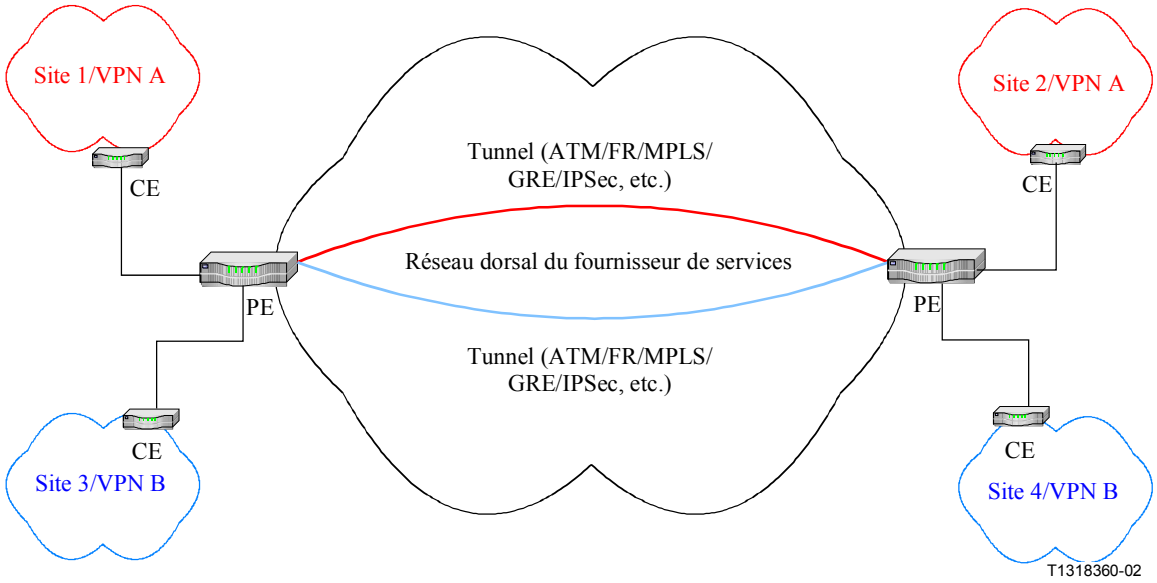


Figure I.1/Y.1311 – Exemple de scénario d'Intranet

I.2 Extranet (connexité entre sites de plusieurs organisations)

Dans un scénario d'Extranet, au moins deux organisations ont accès à un nombre limité de sites se trouvant chez les unes et les autres. Exemples de scénario d'Extranet: de multiples entreprises coopérant à la mise au point d'un logiciel commun, un fournisseur de services ayant accès aux informations issues des sites industriels du vendeur, différentes entreprises et universités participant à un consortium, etc. Un Extranet peut exister sur une seule dorsale de fournisseur de services ou sur de multiples dorsales ou systèmes autonomes. Le cas de dorsales ou systèmes autonomes multiples est examiné dans le scénario 3. La principale différence entre un Extranet et un Intranet est l'existence d'une sorte de mécanisme de contrôle d'accès à l'interconnexion entre différentes organisations. Ce contrôle d'accès peut être mis en oeuvre par un pare-feu, par des listes d'accès de routeur ou par des mécanismes similaires afin d'appliquer au trafic de transit un contrôle d'accès fondé sur une politique. Ce mécanisme de contrôle d'accès peut être réalisé au moyen de dispositifs distincts ou peut être intégré dans le dispositif PE. Ce scénario est décrit dans la Figure I.2. Dans cet exemple, deux réseaux VPN sont formés afin de connecter l'entreprise X et l'entreprise Y. Le mécanisme de contrôle d'accès utilisé entre ces deux entreprises est un pare-feu (bien qu'un autre mécanisme de contrôle d'accès approprié puisse être utilisé). L'on peut également utiliser, au besoin, des mécanismes d'authentification supplémentaires comme l'échange d'une autorité de certification. Il est possible, de nouveau, qu'un site appartienne à plusieurs réseaux VPN pouvant inclure un Intranet donné et un autre Extranet. Ces sous-scénarios doivent également être traités de façon appropriée lors de la mise au point d'une architecture de réseau VPN.

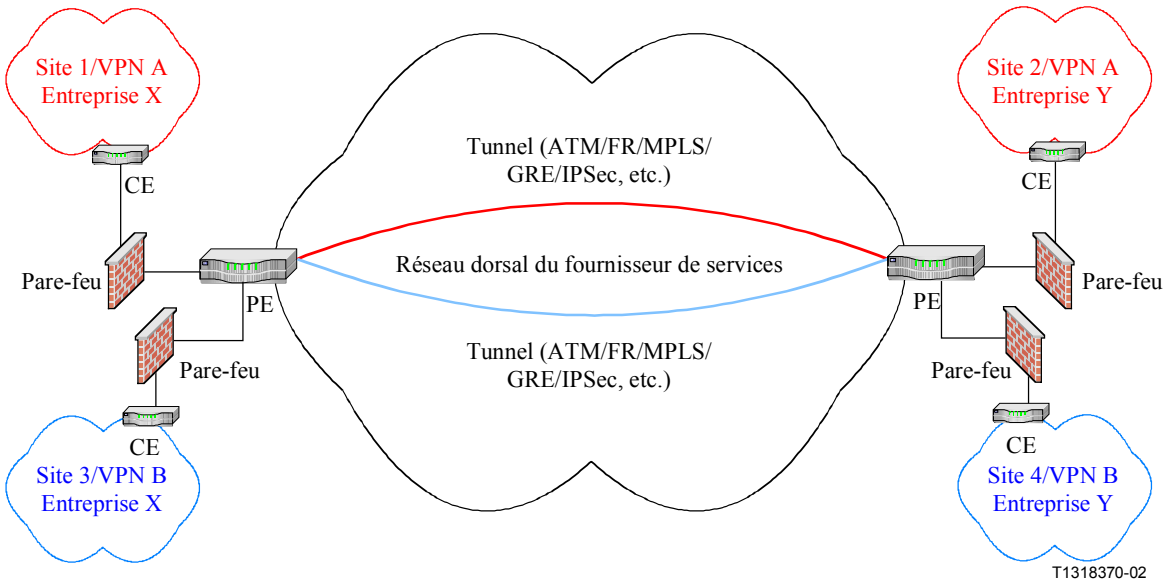


Figure I.2/Y.1311 – Exemple de scénario d'Extranet

I.3 Réseaux privés virtuels entre plusieurs systèmes autonomes ou plusieurs fournisseurs de services

Dans ce scénario, un seul réseau VPN peut s'étendre sur au moins deux réseaux de fournisseur de services ou sur au moins deux systèmes autonomes (AS, *autonomous system*). Le présent paragraphe décrira le scénario dans lequel plusieurs systèmes autonomes sont mis en jeu, car c'est un cas très général dans lequel les principales questions de connexité sont la communication et la sécurité entre les dispositifs PE appartenant aux différents systèmes autonomes. La communication entre dispositifs PE au moyen de systèmes autonomes peut être assurée de diverses façons, selon l'approche architecturale choisie pour construire le réseau NB-VPN en mode IP. Le problème de la sécurité entre dispositifs PE appartenant à différents systèmes autonomes peut être résolu au moyen de tunnels PE-PE (par exemple, des tunnels IPSec peuvent être utilisés afin d'assurer le cryptage dans les systèmes autonomes). Il convient d'effectuer la répartition des routes de réseau VPN dans les systèmes autonomes de façon qu'elle soit vue comme un seul tunnel allant du dispositif PE d'entrée dans un système autonome au dispositif PE de sortie dans un autre système autonome. Des solutions spécifiques pour ce scénario sont traitées dans la présente Recommandation et dans la Rec. UIT-T Y.1311.1. Ce scénario est décrit par la Figure I.3. Les traits discontinus de cette figure indiquent comment est "vu" un tunnel de PE d'entrée à un PE de sortie lorsque la communication entre systèmes autonomes est correctement réalisée. Il convient également de noter qu'une des conditions préalables à la construction d'un tel réseau VPN est l'existence d'un accord fiduciaire entre les fournisseurs de services en cause. Une autre observation à formuler dans ce modèle est la modularité globale du système, en particulier si un protocole comme EBGP est utilisé pour la communication entre systèmes autonomes. Une variante modulable consiste à utiliser des réflecteurs de route en protocole BGP afin de réduire le nombre de sessions EBGP entre dispositifs PE.

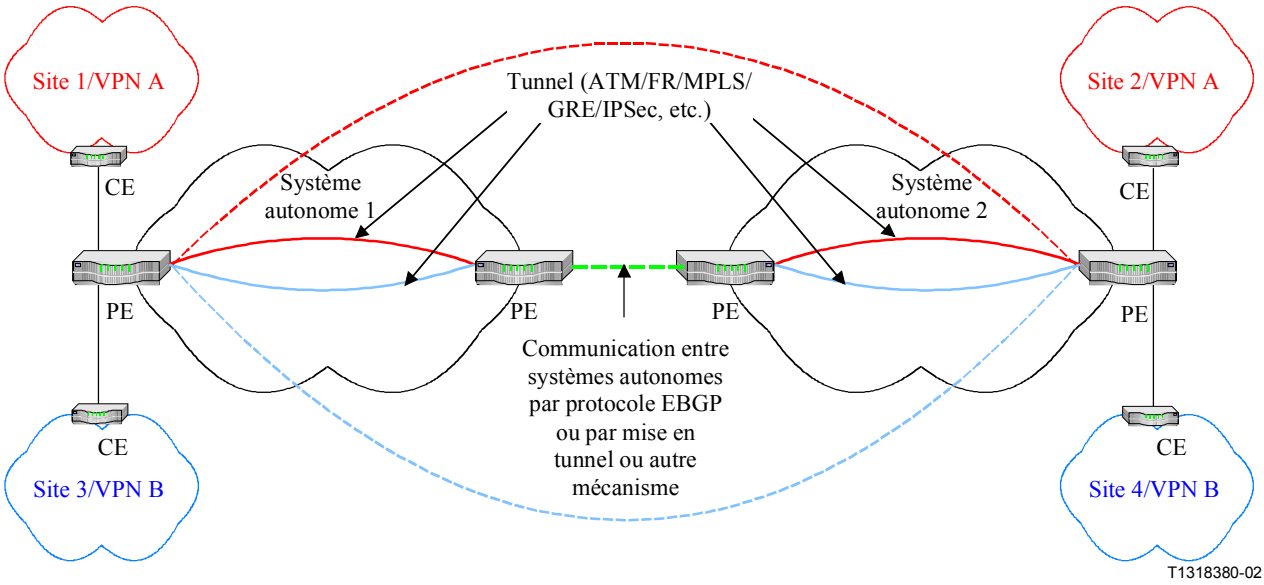


Figure I.3/Y.1311 – Réseaux VPN entre systèmes autonomes multiples

I.4 Accès simultané à un réseau privé virtuel et à Internet

Un important scénario de service VPN consiste à offrir un accès simultané à l'Internet mondial à partir de tout site appartenant à un réseau VPN donné. Plusieurs moyens peuvent de nouveau être utilisés à cette fin, selon le mécanisme VPN utilisé. Si le dispositif PE se compose de routeurs virtuels, il est possible d'accéder à l'Internet au moyen d'un routeur virtuel "mondial" spécialisé dans le dispositif PE. Une traduction d'adresse du réseau (NAT, *network address translation*) ou un mécanisme similaire peut ensuite être requis soit dans l'extrémité CE soit dans le dispositif PE afin de pouvoir distinguer les adresses VPN privées des adresses Internet mondiales. Si le dispositif PE n'emploie pas de routeurs virtuels, le trafic non VPN (Internet) peut être dirigé directement au moyen d'une route par défaut vers une passerelle Internet (Figure I.4). Cette route par défaut est répartie entre tous les sites contenus dans un VPN afin de leur donner accès à Internet. Le trafic Internet destiné à des sites particuliers dans les VPN doit être traité correctement par les fournisseurs ISP, qui répartiront ce trafic selon les routes Internet aboutissant aux sites contenus dans les VPN. La structure interne du réseau VPN sera invisible du réseau Internet. Une fonction de pare-feu peut être requise afin de limiter l'accès au VPN à partir de l'Internet. La Figure I.4 décrit l'accès simultané à Internet et à un réseau VPN. Les mécanismes spécifiques d'accès simultané à Internet et à un réseau VPN ne sont pas représentés dans cette Figure.

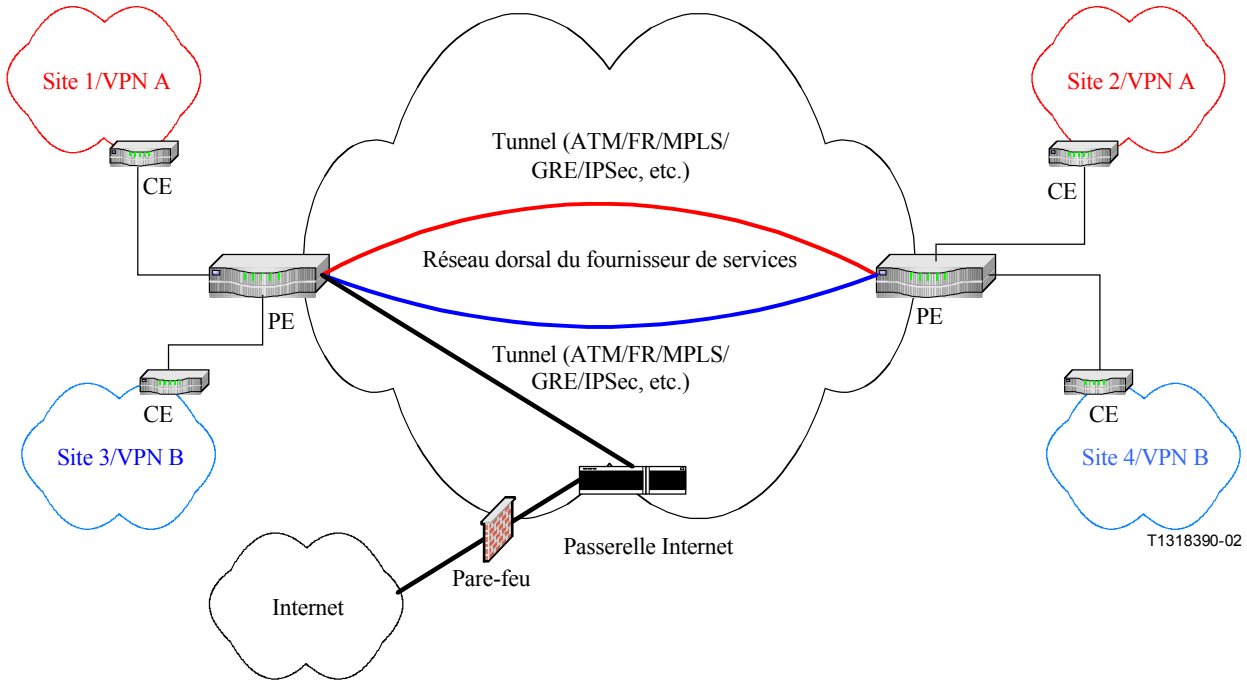


Figure I.4/Y.1311 – Accès simultané à un VPN et à Internet

I.5 Réseaux privés virtuels hiérarchiques (réseaux VPN intégrés dans des réseaux VPN)

Dans ce scénario, un fournisseur de services offrant des services VPN peut en fait être un client d'un fournisseur de services plus important. Un tel réseau de fournisseur de services peut être considéré comme un grand réseau VPN contenant de multiples réseaux VPN plus petits. Par souci de simplicité, un tel réseau de fournisseur de services peut être appelé *VPN de niveau 1*. De même, les réseaux VPN contenus dans ce réseau de fournisseur de services peuvent être appelés *VPN de niveau 2*. Ce scénario est décrit dans la Figure I.5. Les dispositifs CE et PE aux niveaux 1 et 2 sont étiquetés en conséquence. D'après la Figure I.5, il ressort que le dispositif PE du réseau VPN de niveau 2 (PE2) est le dispositif CE du réseau VPN de niveau 1 (CE1). L'on peut également observer qu'afin de fournir un service de réseau NB-VPN en mode IP au niveau 2, le réseau VPN de niveau 1 sera surtout un VPN fourni par équipement CPE en raison de l'établissement d'un tunnel de bout en bout entre les dispositifs CE1 (c'est-à-dire identiques aux dispositifs PE2). Les tunnels logiques du réseau VPN de niveau 2 sont indiqués en traits discontinus, tandis que les traits pleins représentent les tunnels réels de CE1 à CE1 (c'est-à-dire de PE2 à PE2) dans le réseau du grand fournisseur de services. Les dispositifs CE du VPN de niveau 1 devront donc être associés au mécanisme d'établissement du réseau VPN. Le grand fournisseur de services sera surtout un transporteur de transporteur.

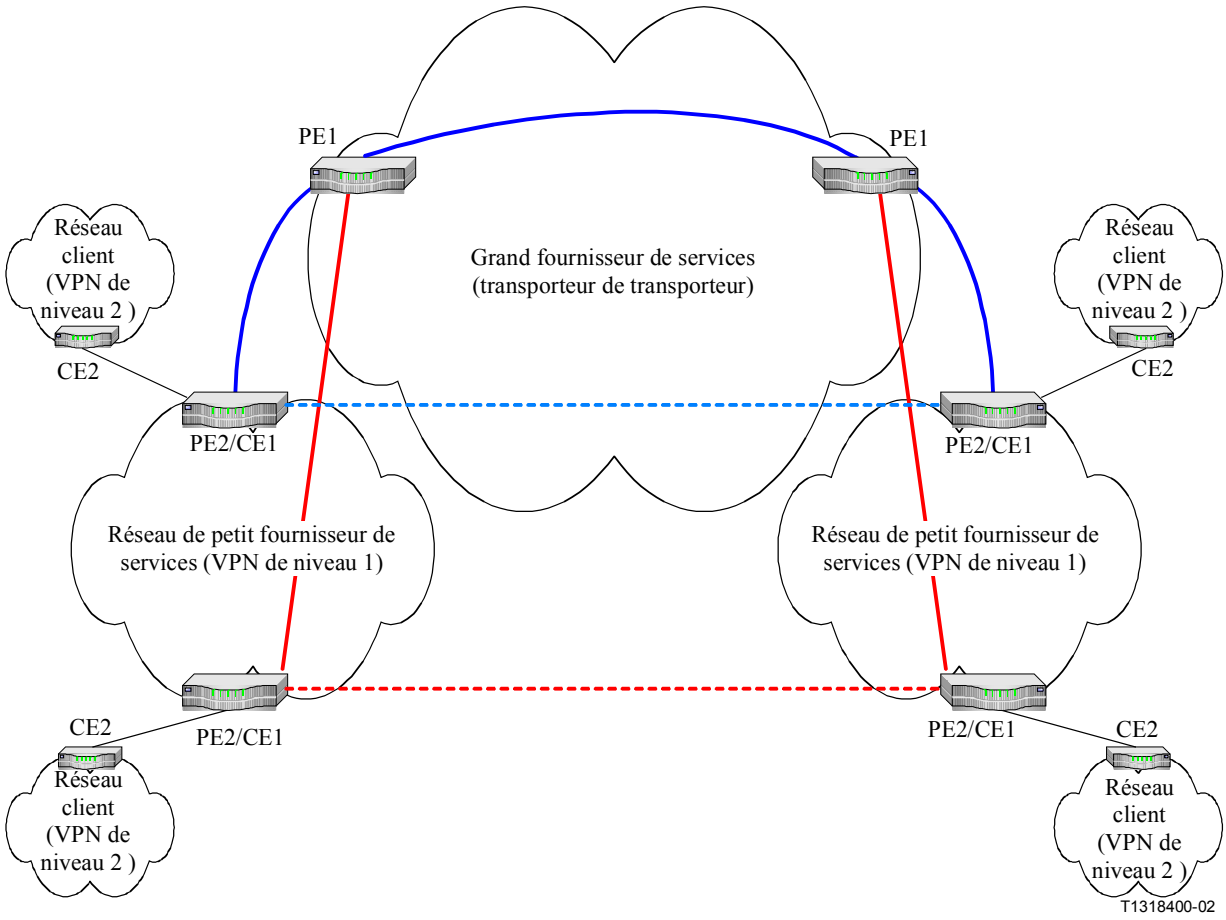
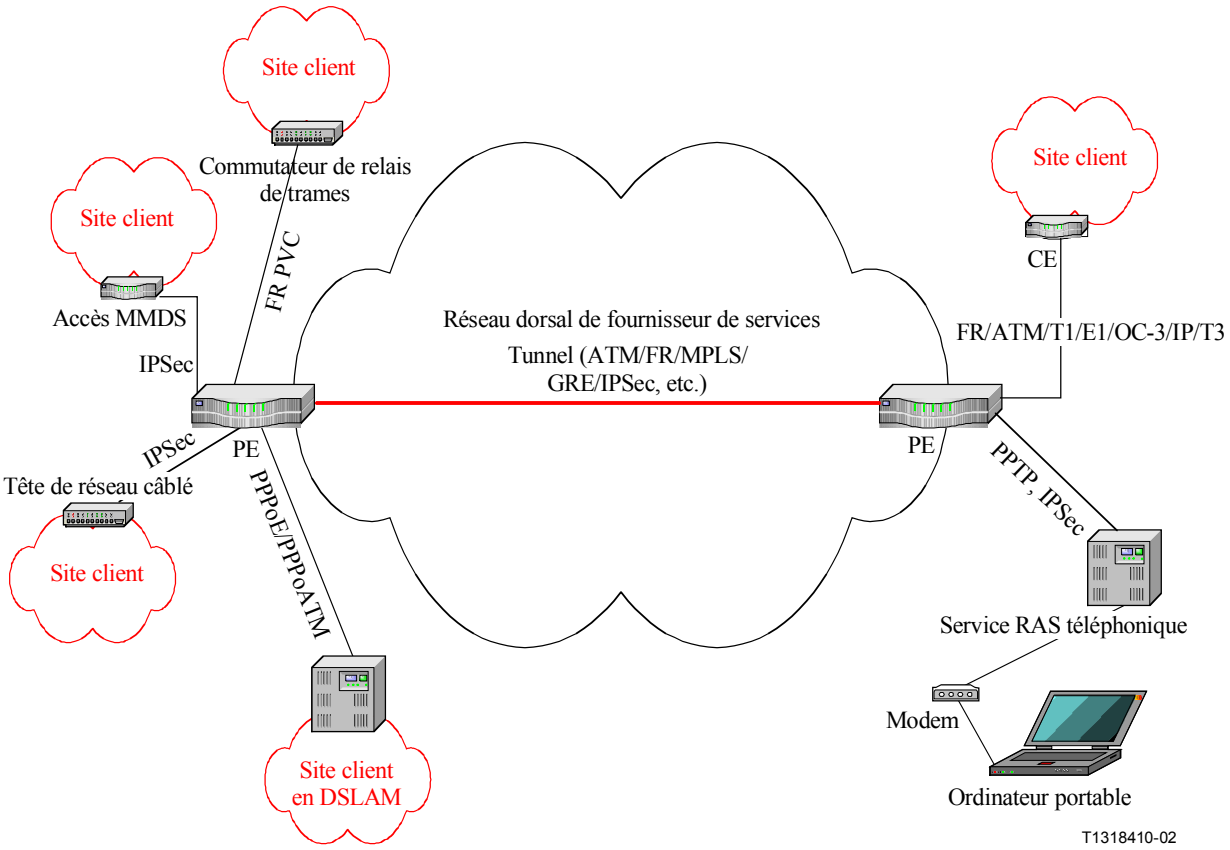


Figure I.5/Y.1311 – Réseaux VPN hiérarchiques

I.6 Scénarios multiples d'accès distant (circuit téléphonique commuté, ligne DSL, radiotéléphonie à poste fixe, câble)

En plus de tous les scénarios ci-dessus, le réseau NB-VPN en mode IP devra prendre en charge de multiples scénarios d'accès. Les deux types d'accès, spécialisé (par exemple par route statique, par circuit PVC en mode ATM, par protocoles de routage, par ligne xDSL, par câblo-modem, par radiotéléphonie à poste fixe, etc.) et non spécialisé (téléphonique) devront être pris en charge. Des dispositifs appropriés pourront être utilisés aux extrémités des différents types de mécanisme d'accès ou bien la fonctionnalité requise pourra être intégrée dans les dispositifs PE. La Figure I.6 décrit un réseau NB-VPN en mode IP prenant en charge divers mécanismes d'accès.



DSLAM Multiplexeur d'accès de ligne d'abonné numérique (*digital subscriber line access multiplexer*)

Figure I.6/Y.1311 – Scénarios d'accès multiple

Appendice II

Scénarios de déploiement du service pour NB-VPN de couche 2

Pour étude complémentaire.

Appendice III

Scénarios de déploiement du service pour NB-VPN de couche 1

Pour étude complémentaire.

Appendice IV

Exemples de réalisations pratiques de modèles de réseau VTN pour réseau NB-VPN en mode IP

Les réseaux NB-VPN (y compris ceux qui sont en mode IP) peuvent être construits selon diverses architectures de base, comme cela a déjà été indiqué dans la Figure 1.

La Figure IV.1 ci-dessous montre une réalisation pratique de l'architecture de réseau cadre illustrant les concepts de façon plus approfondie. Il existe un certain nombre de types d'architectures de réseau de transport permettant de prendre en charge des réseaux VPN. Une architecture de commutation MPLS peut être utilisée afin de prendre en charge des tunnels à commutation MPLS et une architecture en mode ATM ou relais de trames peut être utilisée afin de prendre en charge des connexions virtuelles en mode ATM ou relais de trames. Les services VPN en mode IP peuvent aussi être superposés à l'une ou l'autre de ces architectures de réseau.

La Figure IV.1 donne un exemple d'implémentation d'un réseau NB-VPN générique en mode IP. Le nœud contient une architecture de routeur virtuel (VR, *virtual routeur*) qui à son tour donne accès à un tunnel IPSec ou à un tunnel à commutation MPLS pour implémenter des réseaux VP en mode IP utilisant le protocole BGP, lequel peut également être implémenté par des tunnels MPLS sans faire appel à un routeur virtuel.

Le nœud contenant l'architecture de routeur virtuel peut être atteint à partir du côté client, au moyen d'un réseau d'accès en mode ATM, relais de trames, X.25, SDH ou d'éventuels autres moyens d'accès.

La figure montre d'autres modes de réalisation.

Les services IP sont pris en charge dans le nœud du réseau au moyen de fonctions de stockage, d'extraction et de traitement transactionnel. Les exemples de services IP indiqués dans la figure sont la conversion d'adresse, l'authentification et la commande d'admission.

Le modèle de réseau VSN/VTN décrit dans les paragraphes 6.2 et 6.3 peut être superposé à la réalisation pratique afin de montrer ses rapports avec les concepts VSN/VTN indiqués dans la Figure IV.1.

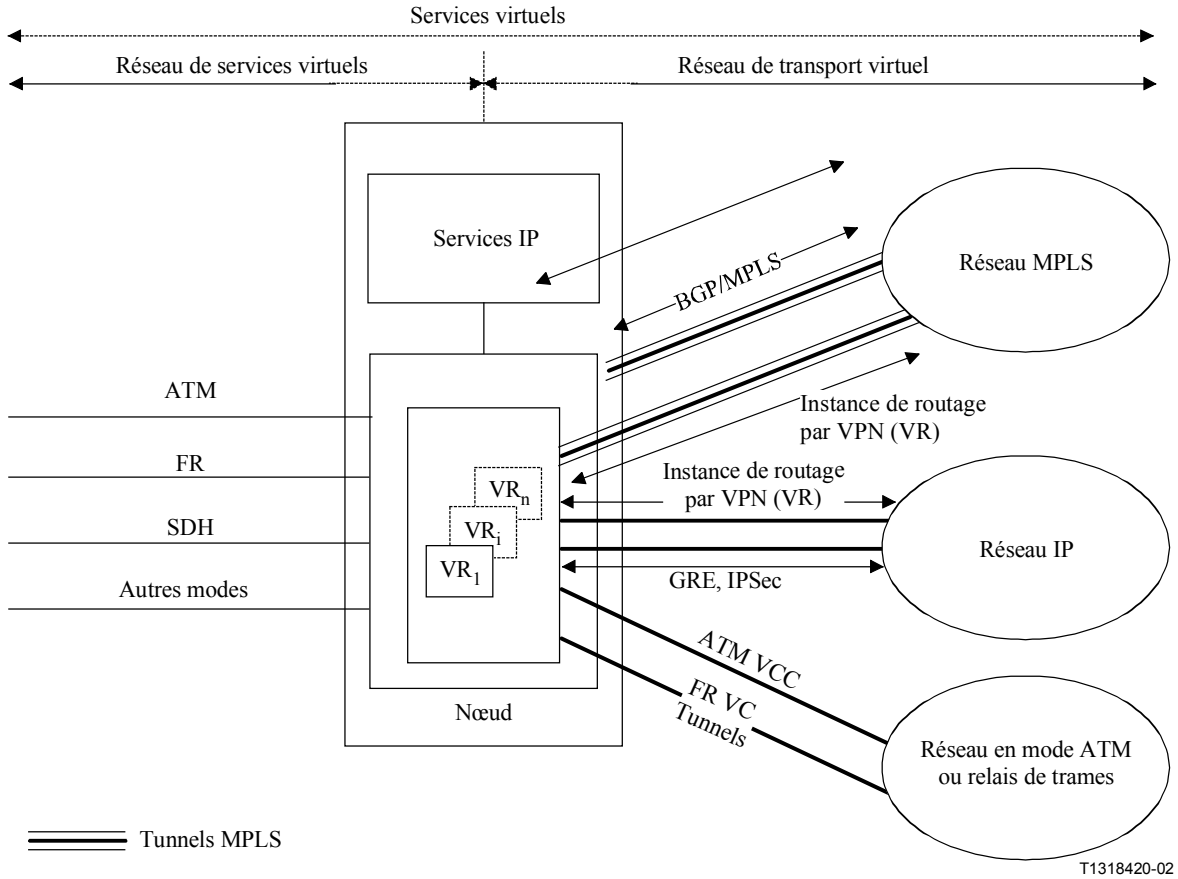


Figure IV.1/Y.1311 – Exemples de réalisation pratique de réseaux VTN

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, 2002