Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.1314

(10/2005)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

Aspects relatifs au protocole Internet – Transport

Décomposition fonctionnelle des réseaux privés virtuels

Recommandation UIT-T Y.1314

Union internationale des télécommunications

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE PROCHAINE GÉNÉRATION

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
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899

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

Recommandation UIT-T Y.1314

Décomposition fonctionnelle des réseaux privés virtuels

Résumé

La présente Recommandation décrit l'ensemble des fonctions requises pour établir, faire fonctionner et assurer la maintenance des réseaux privés virtuels (VPN, *virtual private network*) client/serveur et de niveau homologue. La fonctionnalité de réseau est décrite du point de vue du niveau réseau, en prenant en compte la structure en réseau de couche VPN, les informations caractéristiques de client, les associations client/serveur, la topologie de réseautage et la fonctionnalité de réseau de couche.

Les modèles fonctionnels sont décrits en utilisant la méthodologie de modélisation décrite dans les Recommandations UIT-T G.805 et G.809. La méthodologie de modélisation employée est indépendante de la technologie du réseau et donc les modèles fonctionnels et les fonctions associées décrites s'appliquent à toutes les technologies de réseau de couche VPN.

Source

La Recommandation UIT-T Y.1314 a été approuvée le 14 octobre 2005 par la Commission d'études 13 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

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.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

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 développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T Y.1314

Décomposition fonctionnelle des réseaux privés virtuels

1 Domaine d'application

La présente Recommandation décrit l'ensemble des fonctions requises pour établir, faire fonctionner et assurer la maintenance des réseaux privés virtuels (VPN, *virtual private network*) client/serveur et de niveau homologue. La fonctionnalité réseau est décrite du point de vue du niveau réseau, prenant en compte la structure de réseau de couche VPN, les informations caractéristiques de client, les associations client/serveur, la topologie de réseautage et la fonctionnalité de réseau de couche. Les modèles fonctionnels sont décrits en utilisant la méthodologie de modélisation indépendante de la technologie du réseau décrite dans les Recommandations UIT-T G.805 et G.809.

2 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. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

– Recommandation UIT-T G.805 (2000), *Architecture fonctionnelle générique des réseaux de transport*.

– Recommandation UIT-T G.809 (2003), *Architecture fonctionnelle des réseaux de couche sans connexion*.

– Recommandation UIT-T G.8010/Y.1306 (2004), *Architecture des réseaux de couche Ethernet*.

– Recommandation UIT-T Y.1311 (2002), *Réseaux virtuels privés fournis par le réseau – Architecture générique et prescriptions de service*.

3 Définitions

La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T G.805:

3.1 groupe d'accès

3.2 point d'accès

3.3 information adaptée (*adapted information*)

3.4 information caractéristique (*characteristic information*)

3.5 relation client/serveur (*client/server relationship*)

3.6 connexion (*connection*)

3.7 point de connexion (*connection point*)

3.8 couche de réseau (*layer network*)

3.9 liaison (*link*)

3.10 connexion de liaison (*link connection*)

3.11 matrice (*matrix*)

3.12 réseau (*network*)

3.13 connexion de réseau (*network connection*)

3.14 accès (*port*)

3.15 point de référence (*reference point*)

3.16 sous-réseau (*subnetwork*)

3.17 connexion de sous-réseau (*subnetwork connection*)

3.18 point de connexion de terminaison (*termination connection point*)

3.19 chemin (*trail*)

3.20 terminaison de chemin (*trail termination*)

3.21 transport (*transport*)

3.22 entité de transport (*transport entity*)

3.23 fonction de traitement de transport (*transport processing function*)

3.24 connexion unidirectionnelle (*unidirectional connection*)

3.25 chemin unidirectionnel (*unidirectional trail*)

La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T G.809:

3.26 point d'accès (*access point*)

3.27 groupe d'accès (*access group*)

3.28 information adaptée (*adapted information*)

3.29 information caractéristique (*characteristic information*)

3.30 relation client/serveur (*client/server relationship*)

3.31 chemin sans connexion (*connectionless trail*)

3.32 flux (*flow*)

3.33 domaine de flux (*flow domain*)

3.34 flux de domaine de flux (*flow domain flow*)

3.35 point de flux (*flow point*)

3.36 groupe de points de flux (*flow point pool*)

3.37 terminaison de flux (*flow termination*)

3.38 puits de terminaison de flux (*flow termination sink*)

3.39 source de terminaison de flux (*flow termination source*)

3.40 réseau de couche (*layer network*)

3.41 flux de liaison (*link flow*)

3.42 réseau (*network*)

3.43 flux de réseau (*network flow*)

3.44 accès (*port*)

3.45 point de référence (*reference point*)

3.46 unité de trafic (*traffic unit*)

3.47 transport (*transport*)

3.48 entité de transport (*transport entity*)

3.49 fonction de traitement de transport (*transport processing function*)

3.50 point de flux de terminaison (*termination flow point*)

La présente Recommandation utilise le terme suivant défini dans la Rec. UIT-T G.8010/Y.1306:

3.51 fragment de domaine de flux (*flow domain fragment*)

La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T Y.1311:

3.52 VPN de couche 1 (*Layer 1 VPN*)

3.53 VPN de couche 2 (*Layer 2 VPN*)

3.54 VPN de couche 3 (*Layer 3 VPN*)

La présente Recommandation définit les termes suivants:

3.55 réseau de couche client VPN: composant topologique dans un VPN client/serveur qui représente l'ensemble des points d'accès du même type associés pour les besoins du transfert des informations caractéristiques de couche client de VPN.

3.56 réseau de couche serveur VPN: composant topologique dans un VPN client/serveur qui représente l'ensemble des points d'accès du même type associés pour les besoins du transfert des informations adaptées de couche client de VPN.

3.57 réseau de couche homologue VPN: composant topologique qui représente l'ensemble des points d'accès du même type associés pour les besoins du transfert des informations caractéristiques de couche homologue de VPN.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

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

AAL couche d'adaptation ATM (*ATM adaptation layer*)

AG groupe d'accès (*access group*)

AI information adaptée (*adapted information*)

AIS signal d'indication d'alarme (*alarm indication signal*)

AP point d'accès (*access point*)

ASON réseau optique à commutation automatique (*automatically switched optical network*)

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

BFD détection d'émission bidirectionnelle (*bidirectional forwarding detection*)

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

CAC contrôle d'admission de connexion (*connection admission control*)

CBR débit binaire constant (*constant bit rate*)

CC vérification de connectivité (*connectivity check*)

CE extrémité client (*customer edge*)

CI information caractéristique (*characteristic information*)

CL-PS commutation de paquet sans connexion (*connectionless packet-switched*)

CO-CS commutation de circuit orientée connexion (*connection-orientated circuit-switched*)

CO-PS commutation de paquet orientée connexion (*connection-orientated packet-switched*)

CP point de connexion (*connection point*)

CV vérification de connexion (*connectivity verification*)

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

DLCI identificateur de connexion de liaison de données (*data link connection identifier*)

DSCP séquence codée de services différenciés (*differentiated services code point*)

DWDM multiplexage par répartition dense en longueurs d'onde (*dense wave division multiplexing*)

EBGP protocole de passerelle frontière externe (*external border gateway protocol*)

E-LMI interface de gestion locale externe (*external LMI*)

ES système terminal (*end system*)

FDF flux de domaine de flux (*flow domain flow*)

FDFr fragment de domaine de flux (*flow domain fragment*)

FDI indication de défaut vers l'avant (*forward defect indication*)

FP point de flux (*flow point*)

FPP groupe de points de flux (*flow point pool*)

FR relais de trames (*frame relay*)

FT terminaison de flux (*flow termination*)

FTP point de terminaison de flux (*flow termination point*)

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

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

IKE échange de clé Internet (*Internet key exchange*)

IPv4 protocole Internet version 4 (*Internet protocol version 4*)

IPv6 protocole Internet version 6 (*Internet protocol version 6*)

ISIS système intermédiaire à système intermédiaire (*intermediate system to intermediate system*)

L2TP protocole de création de tunnel de couche 2 (*layer 2 tunnelling protocol*)

LDP protocole de distribution d'étiquettes (*label distribution protocol*)

LF flux de liaison (*link flow*)

LMI interface de gestion locale (*local management interface*)

LOC perte de continuité (*loss of continuity*)

LOS perte du signal (*loss of signal*)

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

MAC commande d'accès au support (*media access control*)

MP2P multipoint à point (*multipoint-to-point*)

MP-BGP BGP multiprotocoles (*multi-protocol BGP*)

MPLS commutation multiprotocolaire par étiquetage (*multi-protocol label switching*)

MTU unité de transmission maximale (*maximum transmission unit*)

NE entité de réseau (*network entity*)

NF flux de réseau (*network flow*)

NMS système de gestion de réseau (*network management system*)

NSAP point d'accès au service de couche réseau (*network service access point*)

OAM opérations, administration et maintenance (*operations, administration and maintenance*)

OOB hors bande (*out of band*)

OSI interconnexion des systèmes ouverts (*open systems interconnection*)

OSPF plus court chemin ouvert en premier (*open shortest path first*)

OSS système d'assistance à l'exploitation (*operational support system*)

P fournisseur (nœud) (*provider (node)*)

P2MP point à multipoint (*point-to-multipoint*)

P2P point à point (*point-to-point*)

PCR débit cellulaire maximal (*peak cell rate*)

PE extrémité fournisseur (*provider edge*)

PHP saut de l'avant-dernier bond (*penultimate hop popping*)

PM surveillance des performances (*performance monitoring*)

PNNI interface réseau privé à réseau public (*private network-to-network interface*)

PW pseudo circuit (*pseudo wire*)

QS qualité de service

RADIUS service d'accès commuté entrant d'utilisateur distant (*remote authentication dial in user service*)

RIP protocole d'informations d'acheminement (*routing information protocol*)

RMON surveillance à distance (*remote monitoring*)

RPR anneau de paquet résilient (*resilient packet ring*)

RSVP-TE protocole de réservation de ressources avec extensions d'ingénierie de trafic (*resource reservation protocol (with) traffic engineering (extensions)*)

SCR débit de cellules soutenu (*sustained cell rate*)

SDH hiérarchie numérique synchrone (*synchronous digital hierarchy*)

SES seconde gravement erronée (*severely errored second*)

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

SNC connexion de sous-réseau (*subnetwork connection*)

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

SONET réseau optique synchrone (*synchronous optical network*)

SPVC circuit virtuel permanent commuté (*switched permanent virtual circuit*)

SSL couche des numéros de connexion logique sécurisés (*secure socket layer*)

STP protocole d'interconnexion arborescente (*spanning tree protocol*)

SVC circuit virtuel commuté (*switched virtual circuit*)

TCP point de connexion de terminaison (*termination connection point*)

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

TFP point de flux de terminaison (*termination flow point*)

TTL durée de vie (*time-to-live*)

TTSI identificateur de source de chemin (*trail termination source identifier*)

UNI interface utilisateur-réseau (*user-to-network interface*)

VC circuit/canal virtuel (*virtual circuit/channel*)

VCCV vérification de connectivité de circuit virtuel (*virtual circuit connectivity verification*)

VCI identificateur de canal virtuel (*virtual channel identifier*)

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

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

VPN réseau privé virtuel (*virtual private network*)

WDM multiplexage par répartition en longueurs d'onde (*wavelength division multiplexing*)

5 Les VPN client/serveur

Les VPN client/serveur ont une hiérarchie à deux couches dans laquelle une couche serveur de VPN sert à prendre en charge une ou plusieurs couches client de VPN.

La Rec. UIT-T Y.1311 décrit les VPN client/serveur en termes de types de service VPN et de types de transport VPN, où le terme type de service VPN se réfère à la couche client de VPN et le terme type de transport VPN se réfère à la couche serveur de VPN. Les différents types de service (client) et de transport (serveur) VPN sont classés dans la Rec. UIT-T Y.1311 comme décrit ci-dessous au Tableau 5-1.

Tableau 5-1/Y.1314 – Types de service de Y.1311

Type de service	Description
Couche 1	Fournit un service de couche physique entre les sites d'utilisateur appartenant au même VPN. Les connexions peuvent être fondées sur des accès physiques, des longueurs d'onde optiques, des circuits/canaux virtuels SDH/SONET, des canaux de fréquence, ou des intervalles de temps.
Couche 2	Fournit un service de couche Liaison de données entre les nœuds d'utilisateur appartenant au VPN. La transmission des paquets de données d'utilisateur est fondée sur les informations des en-têtes de couche Liaison des données des paquets (par exemple, DLCI, ATM VCI/VPI, ou adresses MAC).
Couche 3	Fournit un service de couche réseau entre les nœuds d'utilisateur appartenant au VPN. La transmission des paquets de données d'utilisateur est fondée sur les informations d'en-tête de couche 3 (par exemple, adresse de destination IPv4 ou IPv6).

Un inconvénient de la méthode de classification utilisée dans la Rec. UIT-T Y.1311 est que MPLS ne rentre dans aucune de ces catégories et doit donc être traité comme une technologie unique de réseau de couche. Un autre inconvénient est que, d'un point de vue fonctionnel, les technologies de réseau au sein de la même couche peuvent avoir des caractéristiques et exigences très différentes. Par exemple, Ethernet et ATM sont tous deux des technologies de couche 2, cependant Ethernet est une diffusion fondée sur des technologies sans connexion alors que ATM est une technologie orientée connexion non diffusée.

Une autre méthode de classement des technologies réseau est de les classer par le mode de réseau auquel elles appartiennent. Toutes les technologies de réseau peuvent être transposées dans un des trois modes suivants: commutation de paquet sans connexion (CL-PS, *connectionless packet-switched*), commutation de paquet orientée connexion (CO-PS, *connection-orientated packet-switched*), et commutation de circuit orientée connexion (CO-CS, *connection-orientated circuit-switched*). Les exigences fonctionnelles de chaque mode sont différentes car chaque mode a des caractéristiques différentes. Le Tableau 5-2 donne des exemples de technologies de réseau de couche VPN et indique le mode auquel elles appartiennent.

Tableau 5-2/Y.1314 – Modes de fonctionnement de réseau et exemples

Mode de fonctionnement	Exemples
Commutation de paquet sans connexion	IP, Ethernet, MPLS MP2P (Note 1)
Commutation de paquet orientée connexion	Relais de trames, MPLS P2P/P2MP (Note 2), ATM
Commutation de circuit orientée connexion	SDH/SONET, TDM
NOTE 1 – Des LSP MPLS multipoint à point (MP2P) établis en utilisant LDP en mode aval non sollicité ou en mode contrôle ordonné traversant directement les homologues LDP adjacents. NOTE 2 – Des LSP MPLS point à point (P2P) ou point à multipoint (P2MP) établis en utilisant RSVP-TE traversant des homologues RSVP-TE, ou des LSP P2P établis en utilisant un LDP ciblé/dirigé entre des homologues LDP non adjacents.	

5.1 Combinaisons client/serveur

Il y a neuf combinaisons client/serveur possibles sur la base des trois modes réseau, quoique certaines combinaisons soient plus compatibles que d'autres. Le Tableau 5-3 décrit les combinaisons client/serveur possibles et fournit des informations sur leur compatibilité.

Une couche serveur de VPN doit prendre en charge le multiplexage/démultiplexage pour fournir la séparation du plan de données entre plusieurs couches client de VPN. Les couches serveur de VPN doivent aussi prendre en charge l'adaptation du trafic client, qui est spécifique du client/serveur et dépendante des modes de couche client et serveur de réseau VPN et des technologies spécifiques employées. Une exigence d'adaptation importante pour les clients VPN en circuit commuté transportés par une couche serveur de VPN à commutation de paquets est que la fonction d'adaptation doit fournir le découplage de débit (c'est-à-dire rempli par inactif) et le dessin des paquets de la couche client de VPN. Une exigence clé pour les situations où le client/serveur sont tous deux en commutation de paquets (CO ou CL) est que la fonction d'adaptation doit prendre en charge la fragmentation et le séquençage si l'unité de trafic de couche serveur de VPN (c'est-à-dire la MTU de paquets) est plus petite que l'unité de trafic de la couche client de VPN. D'autres fonctions d'adaptation peuvent être nécessaires selon les technologies spécifiques du client/serveur de VPN employées, y compris le codage, le changement de débit, et l'alignement.

Tableau 5-3/Y.1314 – Combinaisons client/serveur de mode réseau

	Couche client de VPN CL-PS	**Couche client de VPN CO-PS**	**Couche client de VPN CO-CS**
Couche serveur de VPN CL-PS	– Idéal, quoique la fourniture de garanties de livraison sur la base du flux introduise des problèmes d'échelle. – Une approche commune, qui ne donne pas de garanties de livraison sur la base du flux, est d'utiliser le surprovisionnement et la classe sur la base de la file d'attente avec priorité (pour gérer les pointes de trafic et les encombrements). *Exemple: une couche serveur Ethernet qui prend en charge une couche client IP.*	– La fourniture de garanties de livraison sur la base du flux introduit des problèmes d'échelle. – Une approche commune, qui ne donne pas de garanties de livraison sur la base du flux, est d'utiliser le surprovisionnement et la classe sur la base de la file d'attente avec priorité. – La couche client de VPN doit être capable de récupérer en présence d'unités de trafic hors séquence (dues à la possibilité de remise en ordre de paquets à la couche serveur). *Exemple: une couche serveur IP prenant en charge une couche client ATM.*	– La fourniture de garanties de livraison sur la base du flux introduit des problèmes d'échelle. – Une approche commune, qui ne donne pas de garanties de livraison sur la base du flux, est d'utiliser le surprovisionnement et la classe sur la base de la file d'attente avec priorité. – La récupération de la synchronisation des horloges est un défi technique. – La couche client de VPN doit être capable de récupérer en présence d'unités de trafic hors séquence. *Exemple: une couche serveur IP prenant en charge une couche client TDM.*
Couche serveur de VPN CO-PS	– Coût associé à la maintenance de l'état de connexion pour les VPN à la demande avec courts temps de garde, par exemple, SPVC. *Exemple: une couche serveur ATM prenant en charge une couche client IP.*	– Idéal. *Exemple: une couche serveur P2P MPLS prenant en charge une couche client ATM.*	– La récupération de la synchronisation d'horloge est un défi technique. *Exemple: une couche serveur ATM prenant en charge une couche client TDM.*
Couche serveur de VPN CO-CS	– Pas de multiplexage statistique entre agrégats. – L'allocation permanente de bande passante aux incréments en cours donne une médiocre utilisation du réseau. – Les temps de réponse d'établissement de connexion des VPN à la demande avec des temps de garde courts sont lents. *Exemple: une couche serveur SDH prenant en charge une couche client Ethernet.*	– Pas de multiplexage statistique entre agrégats. – L'allocation permanente de bande passante aux incréments en cours donne une médiocre utilisation du réseau. – Les temps de réponse d'établissement de connexion des VPN à la demande avec des temps de garde courts sont lents. *Exemple: une couche serveur ATM prenant en charge une couche client TDM.*	– Idéal. *Exemple: une couche serveur optique (par exemple, un canal DWDM) prenant en charge une couche client SDH/SONET.*

5.2 Transparence de couche client de VPN

Dans un VPN client/serveur, les composants fonctionnels (tels que l'acheminement, la signalisation, la gestion OAM, etc.) appartenant à la couche client de VPN devraient être complètement indépendants des composants fonctionnels appartenant à la couche serveur de VPN.

Bien qu'il soit possible de concevoir des solutions de VPN client/serveur où les composants fonctionnels de couche serveur de VPN interagissent avec les composants fonctionnels de couche client de VPN, cette approche conduit à un certain nombre de conséquences indésirables, par exemple:

1) le service VPN peut se rompre si l'utilisateur change un des composants fonctionnels de la couche client de VPN;
2) le fournisseur de services VPN a besoin de suivre à la trace les développements de la technologie de la couche client de VPN de l'utilisateur et implémenter en conséquence les mises à niveau de son réseau;
3) dans des conditions de faute, il devient difficile d'établir si la faute est dans la couche client de VPN ou dans la couche serveur de VPN.

En demandant que les couches client et serveur de réseau VPN soient capables de fonctionner indépendamment l'une de l'autre, il s'ensuit naturellement que la couche serveur de VPN devrait transférer la couche client de VPN de façon transparente. Par exemple, si la couche client de VPN est en ATM, la couche client de VPN peut implémenter une caractéristique propriétaire (par exemple, AAL, acheminement et signalisation non-PNNI, OAM) qui, si elle n'est pas transportée de façon transparente, romprait le service VPN.

La transparence de couche client n'est pas seulement une exigence technique, mais elle a aussi des implications commerciales parce qu'un fournisseur de services VPN va vraisemblablement considérer que les détails de son réseau sont commercialement sensibles et va donc souhaiter cacher ces détails à toute couche client de VPN. Par exemple, il ne serait pas souhaitable pour la couche serveur de VPN d'être l'homologue de l'acheminement et de la signalisation de la couche client de VPN dans l'exemple ci-dessus.

6 Couche homologue de VPN

Dans le paragraphe 5, les topologies de VPN décrites étaient fondées sur une relation client/serveur entre une couche client de VPN et une couche serveur de VPN. Dans le modèle VPN client/serveur, la fonction source d'adaptation de couche serveur de VPN adapte les informations caractéristiques de la couche client de VPN en informations adaptées dans la couche serveur de VPN, et la fonction puits d'adaptation de couche serveur de VPN adapte les informations adaptées de couche serveur de VPN aux informations caractéristiques de couche client de VPN. Fondamentalement, cette adaptation se réfère à l'encapsulation de la trame/signal de couche client dans une trame/signal de couche serveur de VPN.

Cependant, toutes les topologies VPN ne sont pas fondées sur le modèle client/serveur. Les VPN peuvent aussi être fournis avec des technologies de réseau CL-PS fondées sur un modèle dans lequel l'isolation de l'accessibilité au VPN au sein d'un domaine partagé est réalisée via d'autres moyens que l'encapsulation client/serveur. La présente Recommandation se réfère à ce type de VPN sous le nom de VPN à niveau d'homologue *(peer level VPN)*. Le terme de niveau d'homologue se réfère au fait que le fournisseur transporte les paquets VPN de l'utilisateur à travers son infrastructure partagée à la même couche de réseau que celle à laquelle il reçoit les paquets de l'utilisateur. Il ne se réfère pas à l'homothétie du plan de contrôle utilisateur/fournisseur, l'utilisateur et le fournisseur peuvent avoir des relations d'homologue à homologue dans le plan de contrôle indépendamment du type de VPN. Seul le mode réseau CL-PS prend en charge ce type de VPN parce que dans les cas de CO-PS et CO-CS la nature orientée connexion de la technologie met en

application l'isolation d'accessibilité, c'est-à-dire que les entités de réseau ne peuvent communiquer qu'avec les entités de réseau qui appartiennent à la même connexion P2P ou P2MP.

Afin de prendre en charge les VPN à travers un domaine partagé, la technologie de réseau utilisée doit avoir des moyens de fournir l'isolation de VPN, c'est-à-dire que les entités de réseau doivent être seulement capables de communiquer avec les autres entités de réseau qui appartiennent au même VPN ou être capables de décrypter les paquets provenant des entités de réseau qui appartiennent au même VPN.

6.1 Filtrage de paquet/route

Une façon d'implémenter l'isolation de VPN à travers un domaine partagé est d'utiliser des filtres de paquet avec des extrémités fournisseur qui sont partagées entre plusieurs utilisateurs. Dans cette approche, tous les nœuds dans le réseau du fournisseur de services connaissent toutes les routes des utilisateurs. Cela inclut les nœuds d'extrémité fournisseur (PE) qui font face aux sites des utilisateurs, et les nœuds fournisseurs (P) dans le cœur de réseau. Dans cette architecture, les nœuds d'extrémité fournisseur sont partagés par des utilisateurs différents. Le fournisseur de services alloue une portion de son espace adresse à un utilisateur et gère les filtres de paquets sur les routeurs d'extrémité fournisseur pour s'assurer de la pleine accessibilité entre les sites d'un même utilisateur, et de l'isolation entre les utilisateurs.

Pour surmonter le besoin d'assurer la maintenance de tableaux d'acheminement cohérents et de filtres de paquets utilisateur par utilisateur et site par site, une voie de rechange consiste à implémenter une solution fondée sur le filtrage de route, plutôt que sur le filtrage de paquet, avec les extrémités fournisseur, c'est-à-dire une PE par VPN. Dans cette architecture les nœuds fournisseur contiennent toutes les routes des utilisateurs, mais les nœuds de PE ne contiennent que les routes pour un seul utilisateur. L'isolation des routes des utilisateurs est réalisée par le filtrage de route. Les nœuds PE sont configurés avec des filtres de route qui permettent seulement aux utilisateurs d'être informés des routes qui leur appartiennent. Le protocole de passerelle frontière (BGP, *border gateway protocol*) est un exemple de protocole communément utilisé à cette fin à l'intérieur du réseau dorsal du fournisseur du fait de ses outils versatiles de filtrage de route. Une solution de remplacement au filtrage de route serait d'utiliser une instance de protocole d'acheminement différente pour chaque VPN. Cependant, à utiliser cette approche, le réseau partagé serait seulement capable de prendre en charge un petit nombre de VPN, du fait que les nœuds fournisseur ne sont capables de prendre en charge qu'un nombre limité d'instances de protocole d'acheminement, et du fait de la complexité de fonctionnement d'une gestion à plusieurs instances de protocole.

Pour surmonter le besoin d'utiliser un nœud d'extrémité fournisseur différent pour chaque VPN, une autre approche est d'utiliser des routeurs virtuels (VR, *virtual router*). Dans cette approche, un nœud physique est effectivement séparé en un certain nombre de routeurs virtuels. Un ou plusieurs routeurs virtuels peut être alloué à un utilisateur particulier. De cette façon, un nœud peut fournir des instances d'acheminement compartimentées pour plusieurs utilisateurs. Les routeurs virtuels individuels se comportent exactement comme des nœuds d'extrémité fournisseur séparés dédiés à un VPN particulier. Comme avec l'approche de filtrage de route, les nœuds fournisseur contiennent toutes les routes de l'utilisateur et donc le filtrage de route est nécessaire dans les extrémités fournisseur.[1]

---

[1] Une évolution naturelle de cette approche est d'utiliser MPLS ou d'autres approches de tunnelage afin que les routes spécifiques de VPN n'aient pas à être entretenues sur les routeurs de réseau dorsal. Cependant, cela crée une topologie de VPN client/serveur et donc cette approche est plutôt applicable au paragraphe 5 qu'au présent paragraphe.

6.2 Chiffrement

Une alternative au filtrage de route/paquet est de fournir une accessibilité complète entre tous les utilisateurs connectés à une infrastructure partagée, en conjonction avec le chiffrement des paquets. Le chiffrement de paquet assure que si les utilisateurs reçoivent des paquets d'un VPN auquel ils n'appartiennent pas, ils ne peuvent pas accéder aux informations contenues dans le paquet. L'utilisateur peut chiffrer les paquets VPN avant que le trafic ne passe sur le réseau partagé et donc l'utilisateur est responsable de la gestion du VPN. Dans cette approche, le trafic au sein du réseau du fournisseur de services est acheminé de la même façon que tout autre trafic IP, et le fournisseur de services n'a pas de visibilité dans le tunnel. Le réseau du fournisseur de services n'a pas non plus besoin d'être configuré de façon particulière. Autrement, les paquets VPN peuvent être cryptés en utilisant des équipements gérés par le fournisseur (c'est-à-dire des extrémités fournisseur ou des extrémités client gérées par le fournisseur) à la bordure du réseau partagé du fournisseur. Dans cette approche, le fournisseur est responsable de la gestion du VPN.

Un exemple d'architecture prenant en charge le chiffrement est celui de la RFC 2401 – Architecture de sécurité pour le protocole Internet (IPsec). IPsec définit des algorithmes cryptographiques, des routines d'authentification et de gestion de clé[2] pour la création de tunnels de trafic IP sécurisés entre les passerelles/clients IPsec. IPsec garantit la confidentialité, l'intégrité et l'authentification d'origine des données dans un VPN lorsque les informations traversent une infrastructure partagée. IPsec est particulièrement utile pour fournir des VPN à travers des réseaux publics tels que l'Internet pour les VPN de site à site et d'accès distant. La fonction IPsec peut être fournie par une extrémité fournisseur, une extrémité client, ou un appareil terminal d'utilisateur (par exemple, un ordinateur portatif faisant tourner un client IPsec).

Les VPN à couche des numéros de connexion logique sécurisés (SSL, *secure socket layer*) sont un autre type de VPN qui utilise le chiffrement pour fournir l'isolation de VPN. Une utilisation typique de VPN à SSL est de permettre aux utilisateurs d'accéder en toute sécurité aux applications et aux fichiers sur l'Internet. L'avantage de cette approche est qu'elle n'exige aucun changement de configuration de la part des systèmes terminaux d'utilisateur, et seules les applications standards doivent être prises en charge (par exemple, les navigateurs de la toile, la messagerie électronique de client, etc.). Ainsi, les VPN à SSL sont transparents à la couche homologue de VPN (car le chiffrement est effectué à la couche Application) et donc la configuration des nœuds d'acheminement/commutation n'est pas nécessaire pour prendre en charge les VPN à SSL.

6.3 VLAN Ethernet

La norme IEEE 802.1Q définit le fonctionnement des ponts de LAN virtuel (VLAN) qui permet la définition, le fonctionnement et l'administration des topologies de LAN virtuel au sein d'une infrastructure de LAN ponté. Les VLAN permettent à des stations terminales sur plusieurs segments de LAN physique de communiquer comme si elles étaient connectées au même segment de LAN. Les utilisateurs finaux et les concentrateurs/commutateurs peuvent être passés à des VLAN différents en changeant la configuration du VLAN sur le port/interface de l'appareil de commutation compatible 802.1Q auquel la station terminale ou concentrateur/commutateur est connectée. Les trames en diffusion et multidiffusion sont contraintes par les frontières de VLAN de sorte que les stations terminales vont seulement recevoir des trames en diffusion/multidiffusion pour le VLAN auquel elles appartiennent. Ceci, conjointement avec la façon dont fonctionne l'acquisition d'adresse MAC, garantit que seules les stations terminales appartenant au même VLAN peuvent communiquer les unes avec les autres, et peuvent donc être considérées comme membres du même VPN.

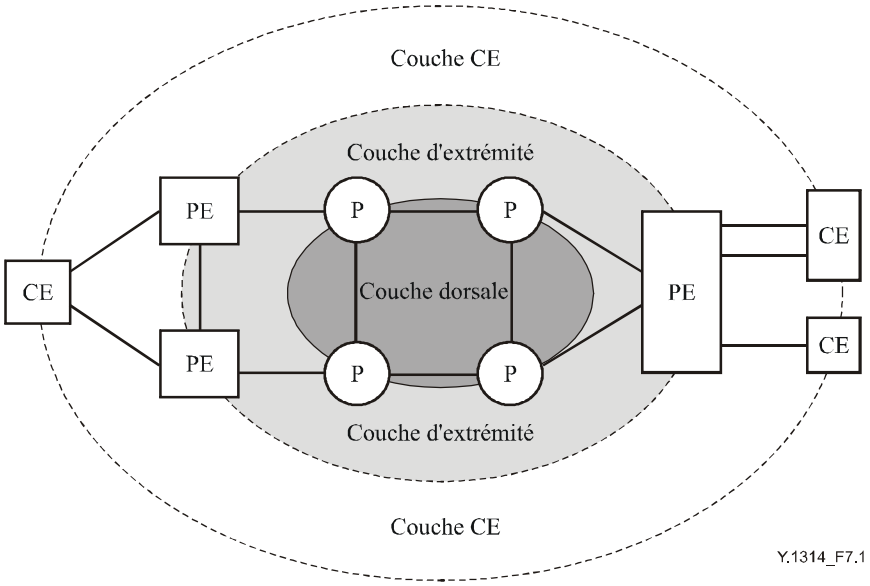
---

[2] Une clé est une information qui contrôle le fonctionnement de l'algorithme de chiffrement/déchiffrement.

La séparation du trafic pour les trames appartenant à des VLAN différents à travers une infrastructure partagée est réalisée en insérant une étiquette avec un identificateur de VLAN (VID) dans chaque trame. Un VID doit être alloué pour chaque VLAN (1 à 4 096) et doit être globalement unique au sein de la même infrastructure physique. Un des inconvénients de cette approche est que les consommateurs utilisent aussi les VLAN au sein de leur propre réseau, ce qui introduit des problèmes d'allocation et de limitation de VID. Pour résoudre ce problème, une seconde étiquette IEEE 802.1Q peut être ajoutée aux paquets étiquetés IEEE 802.1Q de l'utilisateur qui entre dans le réseau du fournisseur (Q-in-Q comme défini dans IEEE 802.1ad). Cela sépare l'espace VLAN du fournisseur de l'espace VLAN de l'utilisateur et permet au consommateur d'utiliser les VID qu'il veut[3].

7 Architecture fonctionnelle des VPN

Le modèle de référence de VPN tiré de la Rec. UIT-T Y.1311 est donné à la Figure 7-1.



CE extrémité client
PE extrémité fournisseur
P fournisseur

Figure 7-1/Y.1314 – Modèle de référence de VPN de la Rec. UIT-T Y.1311

Bien que ce modèle montre la topologie physique et les différents composants du réseau, il ne montre pas les différentes topologies de couche serveur et client de VPN ou la localisation des fonctions d'adaptation intercouches.

Une autre méthode de représentation d'un réseau VPN client/serveur est d'utiliser la modélisation fonctionnelle. L'architecture fonctionnelle des réseaux de couches orientées connexion (CO-PS/CO-CS) et sans connexion (CL-PS) peut être décrite en utilisant respectivement la Rec. UIT-T G.805, "Architecture générique fonctionnelle des réseaux de transport" et la Rec. UIT-T G.809, "Architecture fonctionnelle des réseaux de couche sans connexion".

---

[3] Une autre option est d'utiliser une approche MAC-in-MAC (comme défini dans IEEE 802.1ah) dans laquelle un fournisseur ajoute un second en-tête Ethernet au paquet de l'utilisateur. Cependant, cette option crée un VPN client/serveur plutôt qu'un VPN de niveau homologue parce que la trame d'utilisateur est incorporée dans une trame fournisseur.

Les Recommandations UIT-T G.805 et G.809 fournissent des méthodes génériques utiles pour la modélisation de réseau dans une perspective d'architecture fonctionnelle et structurelle. La terminologie définie est indépendante de la technologie et peut être utilisée pour décrire les composants physiques et logiques pour tout réseau donné. Ceci est particulièrement utile pour l'inventaire et la gestion de réseau car une vision complète du réseau peut être modélisée depuis les fibres optiques dans leur enveloppe jusqu'aux services VPN qui passent sur elles.

Un réseau VPN peut être décomposé en un certain nombre de réseaux de couches indépendantes avec une relation client/serveur entre les réseaux de couches adjacentes. Comme noté dans la Rec. UIT-T G.805, les couches de réseau définies comme utilisant la modélisation fonctionnelle ne devraient pas être confondues avec les couches du modèle OSI (interconnexion de systèmes ouverts) (Rec. UIT-T X.200). Chaque couche du modèle OSI offre un service spécifique et les protocoles définis à chaque couche effectuent une fonction spécifique correspondant à cette couche, par exemple, la couche Transport (couche 4) accepte les données de la couche Session, et les passe à la couche Réseau fournissant un service de livraison de bout en bout. Au contraire, chaque réseau de couche dans un modèle fonctionnel fondé sur la Rec. UIT-T G.805 ou G.809 offre le même service, c'est-à-dire, le transport de bits/trames entre entrées et sorties. L'abstraction est communément utilisée pour seulement cacher les détails et se concentrer sur les couches/composants de réseau intéressants, mais les réseaux peuvent être modélisés jusqu'aux éléments de réseau, par exemple, les commutateurs Ethernet, les paires de cuivre, les interconnexions SDH, etc.

7.1 Réseau de couches VPN orientées connexion

Les couches client et serveur de réseau VPN ont chacune leur propre ensemble d'entrées et de sorties de connectivité connu sous le nom de points d'accès (AP, *access point*). Ceux-ci peuvent être associés chacun l'un à l'autre pour transférer des informations de façon transparente à travers le réseau de couche d'entrée à sortie. Les constructions de topologie valide d'association entre points d'accès pour les réseaux de couche CO sont le point à point (P2P) et le point à multipoint (P2MP).

Les points d'accès de réseau de couche VPN marquent les frontières fonctionnelles entre les couches serveur et client de réseau VPN. Du point de vue des couches serveur de VPN, un point d'accès de couche serveur de VPN représente une destination d'acheminement qui peut prendre en charge un chemin. Du point de vue des couches client de VPN, un point d'accès de couche serveur de VPN représente un point auquel il est possible de fournir une capacité de liaison. Les composants fonctionnels et les points de référence dans un réseau de couche CO sont illustrés à la Figure 7-2.

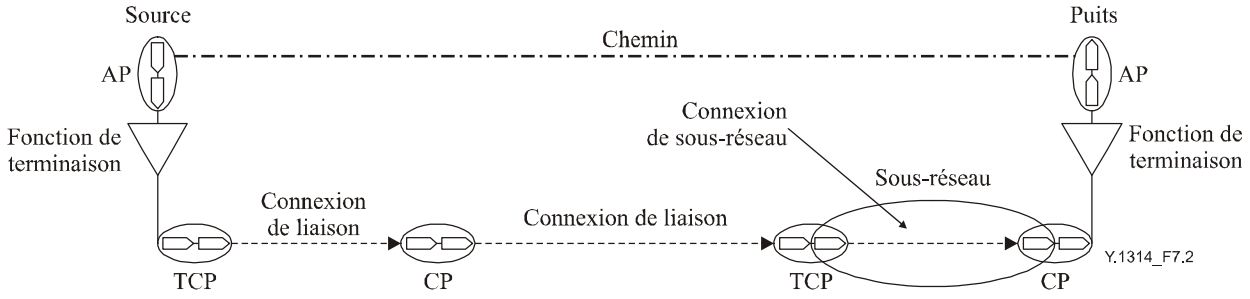


Figure 7-2/Y.1314 – Composants fonctionnels et points de référence CO

Les connexions sont des entités de transport dans les réseaux de couches orientées connexion qui consistent en une paire associée de connexions unidirectionnelles capables de transférer simultanément des informations dans des directions opposées entre leurs entrées et sorties respectives. Une connexion de réseau est une entité de transport dans un réseau de couche orientée connexion formée par une série de connexions de liaisons contiguës et/ou de connexions de sous-réseau entre des points de terminaison de connexion (TCP, *termination connection point*).

Un sous-réseau est un composant topologique dans un réseau de couche orientée connexion utilisé pour effectuer l'acheminement d'informations caractéristiques spécifiques, et il contient un ensemble de points associés à une fonction de gestion sur un seul réseau de couche orientée connexion. Une connexion de sous-réseau transfère des informations à travers un sous-réseau, et elle est formée par une association d'accès *(de ports)* (sortie de source/entrée de terminaison de chemin d'un puits de terminaison de chemin) sur la frontière du sous-réseau.

Les connexions de liaison interconnectent des sous-réseaux topologiquement adjacents qui ont un sous-ensemble commun de points. Le point auquel l'entrée d'une connexion de liaison est rattachée à la sortie d'une autre connexion de liaison est un point de connexion (CP, *connection point*). Le point auquel une sortie de source de terminaison de chemin dans un réseau de couche orientée connexion est rattachée à l'entrée de la connexion de réseau est un TCP de source, et le point auquel une entrée de puits de terminaison de chemin est rattachée à une sortie de connexion de réseau est un TCP puits. Les points de connexion et les points de terminaison de connexion (TCP) ont un objet géré associé, et il est donc possible de grouper les TCP et les CP appartenant au même VPN pour les besoins de la gestion.

7.2 Réseau de couches VPN sans connexion

A la différence des réseaux de couches orientées connexion, les réseaux de couches sans connexion prennent en charge les topologies multipoint à multipoint (MP2MP) ou les topologies tout point à tout point. Les réseaux de couches sans connexion utilisent des flux plutôt que des connexions, qui sont une agrégation d'une ou plusieurs unités de trafic avec un élément d'acheminement commun. Les flux peuvent être unidirectionnels ou bidirectionnels, un flux bidirectionnel consistant en deux flux unidirectionnels de direction contraire. Un flux de réseau est une entité de transport dans un réseau de couche sans connexion formée d'une série de flux contigus entre des points de flux de terminaison (TFP, *termination flow point*). Les composants fonctionnels et les points de référence dans un réseau de couche sans connexion sont illustrés à la Figure 7-3.

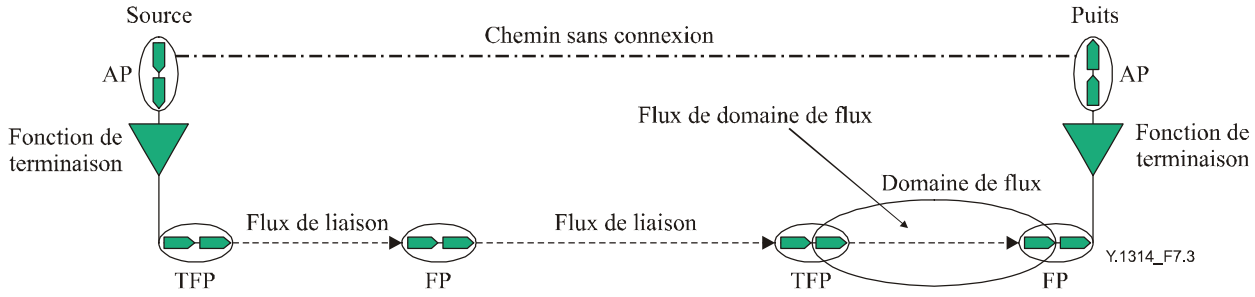


Figure 7-3/Y.1314 – Composants fonctionnels et points de référence CL

Un domaine de flux est un composant topologique dans un réseau de couche sans connexion utilisé pour effectuer l'acheminement d'informations caractéristiques spécifiques. Un flux de domaine de flux est une entité de transport qui transfère des informations à travers un domaine de flux, et il est formé par l'association d'accès *(ports)* sur la frontière du domaine de flux. Un domaine de flux contient un ensemble de points associés à une fonction de gestion au sein d'un seul réseau de couche sans connexion.

Les flux de liaison s'interconnectent topologiquement aux domaines de flux adjacents qui ont un sous-ensemble de points communs. Le point auquel l'entrée d'un flux de liaison est rattaché à la sortie d'un autre flux de liaison est un point de flux (FP). Le point auquel une sortie de source de terminaison de chemin sans connexion dans un réseau de couche sans connexion est rattaché à l'entrée du flux de réseau est un TFP de source, et le point auquel une entrée de puits de terminaison de chemin sans connexion est rattaché à une sortie de flux de réseau est un TFP puits. Comme avec les points de connexion et les points de connexion de terminaison dans le cas orienté connexion, dans le cas sans connexion, les points de flux et les points de flux de terminaison ont un objet géré qui leur est associé, et donc il est possible de grouper ensemble les TFP et les FP qui appartiennent au même VPN pour les besoins de la gestion.

7.3 Relations client/serveur de VPN

En termes fonctionnels, une couche client de VPN est un composant topologique dans un VPN client/serveur qui représente l'ensemble des points d'accès du même type associés pour transférer des informations caractéristiques de couche client de VPN, qui sont prises en charge par un chemin de couche serveur de VPN ou un chemin sans connexion. Les TCP/TFP source/puits pour les connexions/flux de couche client de VPN peuvent être localisés dans des nœuds d'extrémité client, ou dans des nœuds/systèmes d'extrémité ailleurs dans le réseau de l'utilisateur. Par exemple, les TCP dans une couche client de VPN en ATM seront vraisemblablement localisés dans des nœuds d'extrémité client, alors que des TFP dans une couche client de VPN d'Ethernet seront vraisemblablement localisés dans des ordinateurs ou serveurs d'utilisateur final. La localisation des TFP/TCP de flux/connexion de client VPN est importante du point de vue du consommateur, car c'est le point où, dans le réseau de ce consommateur, doit prendre place l'adaptation entre la couche client de VPN et la couche supérieure. Il est aussi important du point de vue OAM, car c'est là que sont situés les points d'accès de source et puits pour le chemin/chemin sans connexion associé à un flux/connexion de couche client de VPN. Des exemples de VPN client/serveur où les TFP/TCP sont localisés en des endroits différents sont fournis à l'Appendice I.

Une couche serveur de VPN est un composant topologique dans un VPN client/serveur qui représente l'ensemble des points d'accès du même type associés pour les besoins du transfert des informations adaptées de couche client pour un ou plusieurs flux ou connexions de couche client de VPN. La couche serveur de VPN contient des fonctions d'adaptation de source/puits qui adaptent les informations caractéristiques dans la couche client de VPN en informations adaptées dans la couche serveur de VPN et réciproquement. Les couches client et serveur VPN peuvent appartenir au même mode (c'est-à-dire lorsque les couches serveur et client sont toutes deux orientées connexion ou lorsque les couches serveur et client sont toutes deux sans connexion), mais des combinaisons des deux sont aussi possibles, c'est-à-dire que des couches serveur de VPN orientées connexion peuvent prendre en charge des couches client sans connexion, et de même des couches serveur sans connexion peuvent aussi prendre en charge des couches client orientées connexion. La Figure 7-4 montre un exemple de couche serveur de VPN sans connexion qui prend en charge une couche client de VPN sans connexion dans une perspective fonctionnelle fondée sur la topologie physique du modèle de réseau tiré de la Rec. UIT-T Y.1311 montré à la Figure 7-1. La couche inférieure montrée dans le modèle est la couche serveur de VPN et la couche supérieure est la couche client de VPN. Seules les couches client/serveur VPN sont illustrées par souci de simplification; la couche client d'utilisateur au-dessus de la couche client de VPN, et la couche serveur en dessous de la couche serveur de VPN ne sont pas montrées. Dans cet exemple, la couche serveur de VPN est orientée connexion (par exemple, ATM) alors que la couche client de VPN est sans connexion (par exemple, Ethernet), bien que toutes combinaisons de paires orientées connexion ou sans connexion soient possibles.

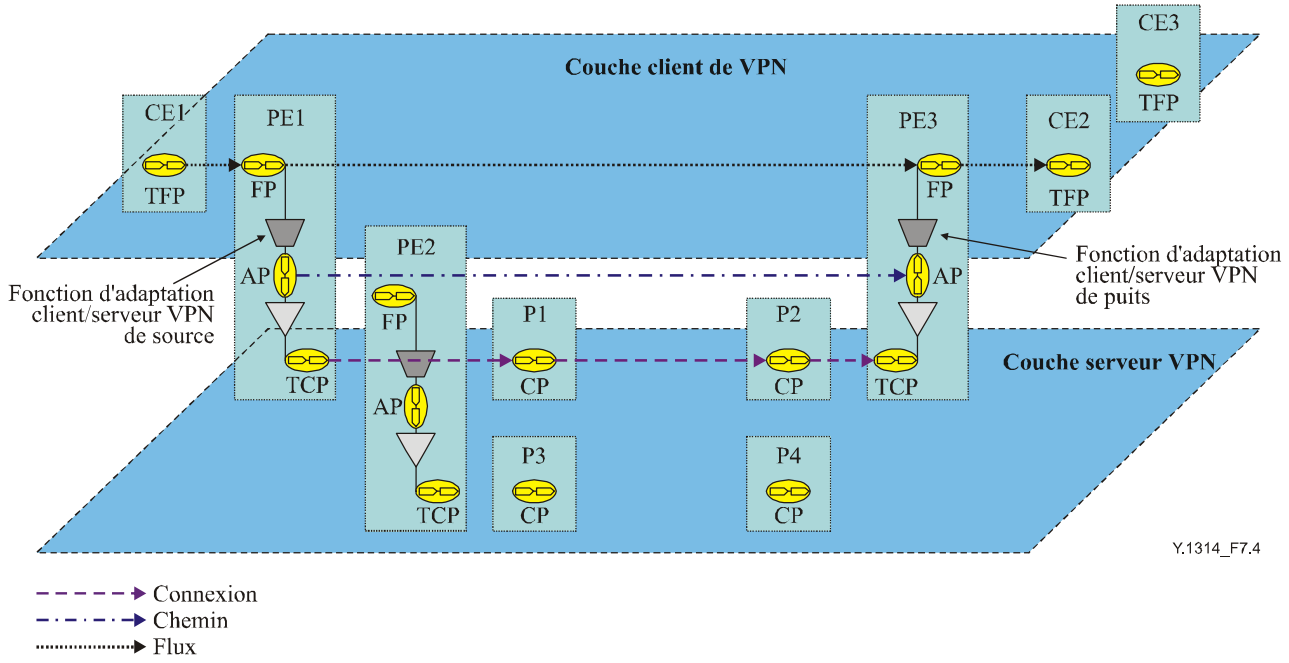


Figure 7-4/Y.1314 – Modèle fonctionnel de VPN client/serveur

La Figure 7-4 montre comment le modèle fonctionnel se rapporte au diagramme de réseau de la Figure 7-1 en soulignant quelles fonctions et points de référence réseau existent dans les différents éléments de réseau (c'est-à-dire les nœuds d'extrémité client, d'extrémité fournisseur ou les nœuds fournisseur). Les nœuds d'extrémité client et les nœuds fournisseur appartiennent respectivement aux couches client et serveur VPN, alors que les nœuds d'extrémité fournisseur appartiennent aux deux couches. Les TFP dans la couche client de VPN identifient où commence (dans ce cas, à quel nœud d'extrémité client) le flux de la couche client de VPN point à point (sa source) et se termine (son puits), et les points de flux identifient à travers quels nœuds d'extrémité fournisseur passe le flux point à point. De même que les TFP dans la couche serveur de VPN identifient la source et le puits pour la connexion de couche serveur de VPN, et que les points de flux identifient à travers quels nœuds fournisseur passe le flux. Les points d'accès dans la couche serveur de VPN identifient la source/puits pour le chemin de couche serveur de VPN.

Les paragraphes suivants présentent chacun les quatre combinaisons client/serveur de VPN possibles en utilisant les modèles fonctionnels et décrivent le rôle des fonctions d'adaptation client/serveur de VPN.

7.3.1 Couche client de VPN CO prise en charge par une couche serveur de VPN CO

Un exemple de couche client de VPN orientée connexion qui est prise en charge par une couche serveur de VPN orientée connexion est illustré à la Figure 7-5.

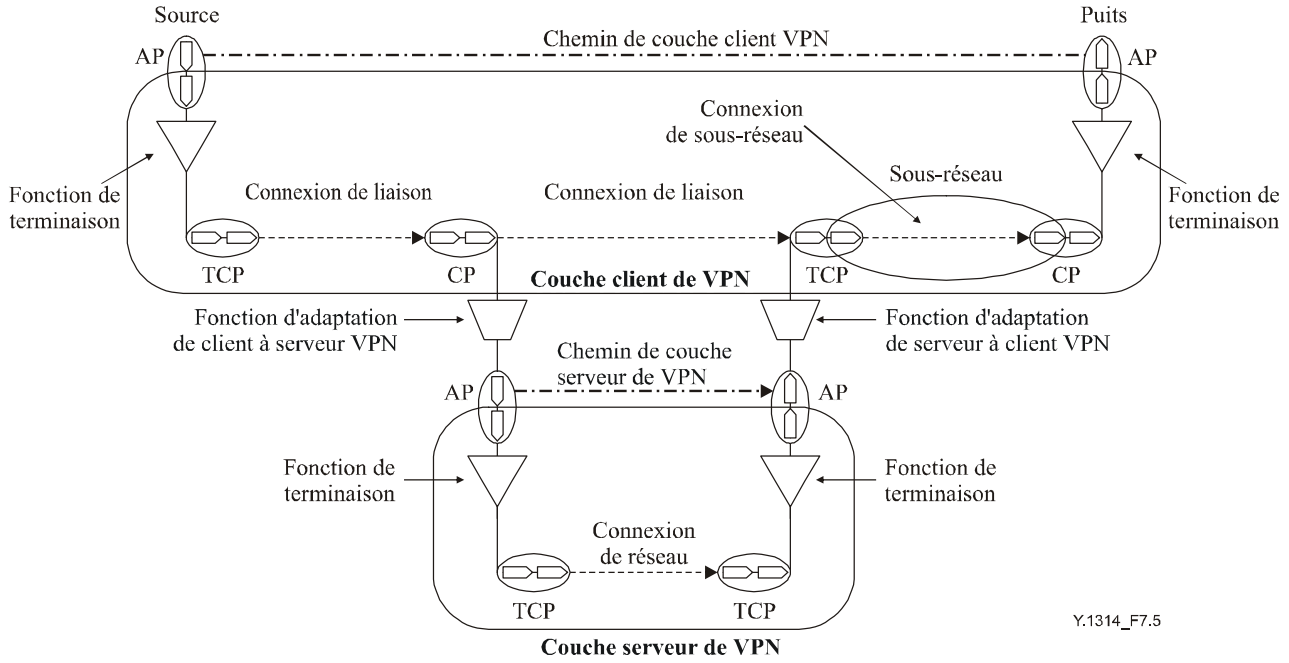


Figure 7-5/Y.1314 – Couche serveur CO VPN avec une CO VPN client

Dans cet exemple, la connexion de couche client de VPN orientée connexion est prise en charge par un chemin de couche serveur de VPN orientée connexion. La fonction de source d'adaptation de couche serveur de VPN orientée connexion adapte les informations caractéristiques (CI) de la couche client de VPN orientée connexion en informations adaptées (AI) dans la couche serveur de VPN orientée connexion. La fonction puits d'adaptation de couche serveur de VPN orientée connexion adapte les informations adaptées de couche serveur de VPN orientée connexion en informations caractéristiques de couche client de VPN orientée connexion.

7.3.2 Couche client CL VPN prise en charge par une couche serveur CL VPN

Un exemple de couche client de VPN sans connexion qui est prise en charge par une couche de serveur de VPN sans connexion est illustré à la Figure 7-6.

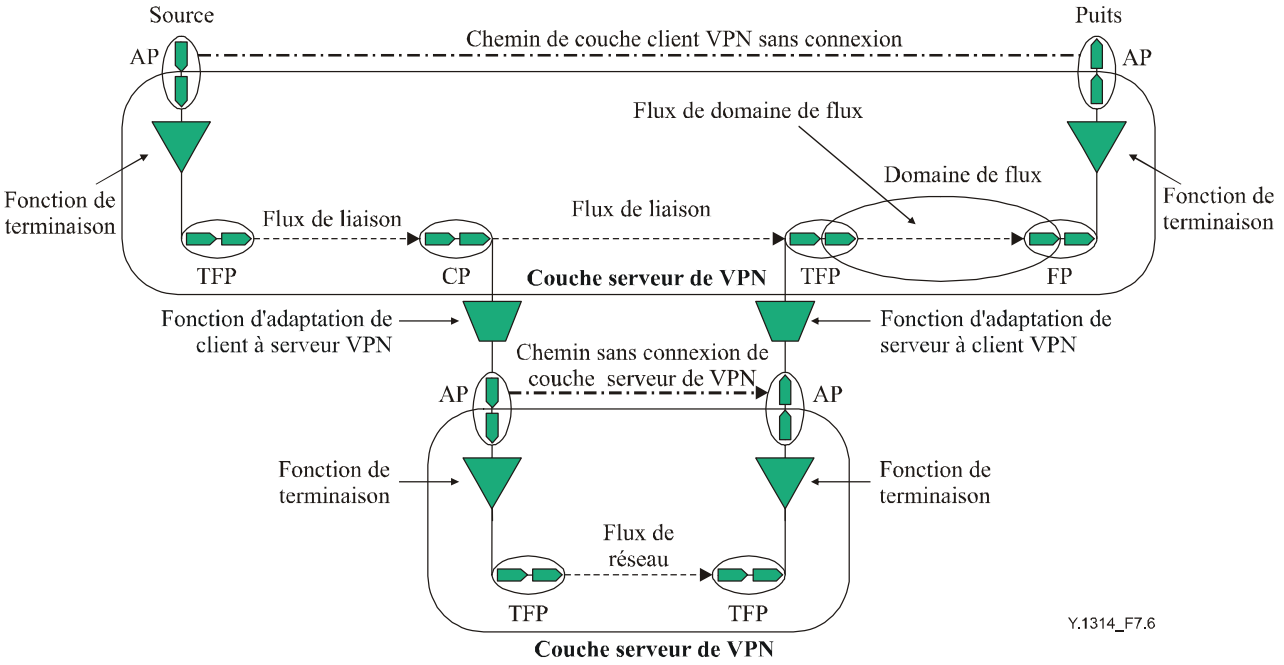


Figure 7-6/Y.1314 – Couche serveur de CL VPN avec CL VPN client

Dans cet exemple, le flux de couche client de VPN sans connexion est pris en charge par un chemin sans connexion de couche serveur de VPN sans connexion. La fonction de source d'adaptation de couche serveur de VPN sans connexion adapte les informations caractéristiques (CI) de la couche client de VPN sans connexion en informations adaptées (AI) dans la couche serveur de VPN sans connexion. La fonction de puits d'adaptation de couche serveur de VPN sans connexion adapte les informations adaptées de la couche serveur de VPN sans connexion aux informations caractéristiques de couche client de VPN sans connexion.

7.3.3 Couche client de VPN CO prise en charge par une couche serveur de VPN CL

Un exemple de couche client de VPN orientée connexion qui est prise en charge par une couche serveur de VPN sans connexion est illustré à la Figure 7-7.

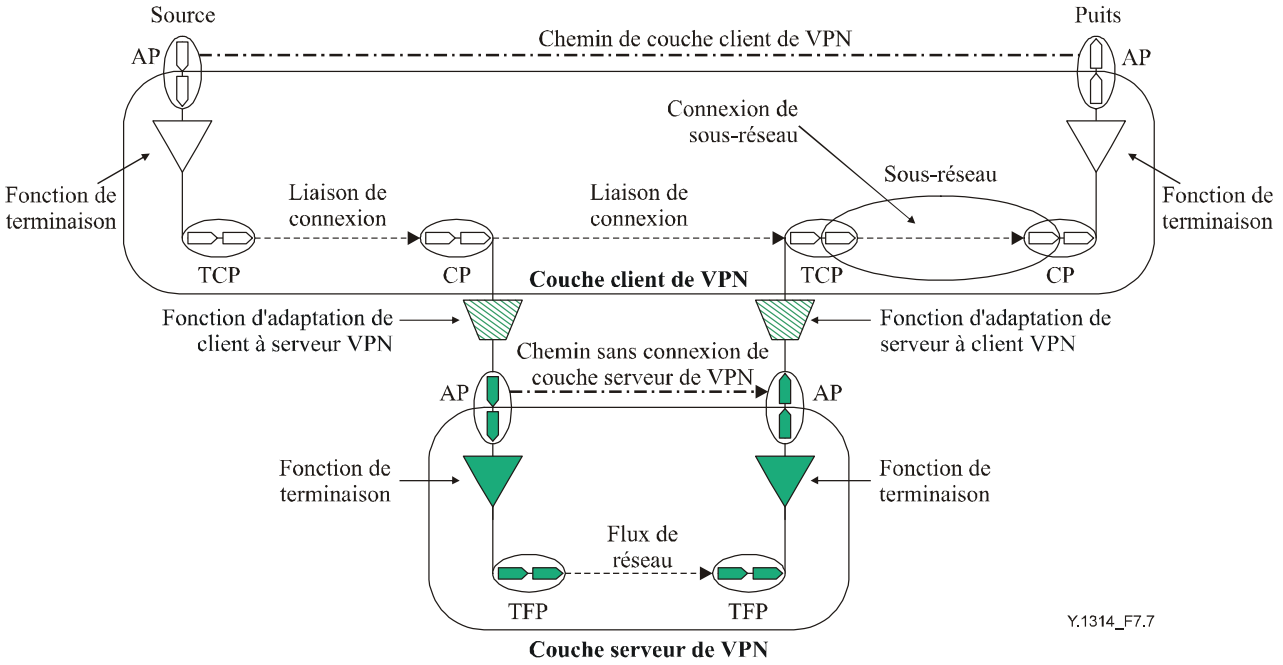


Figure 7-7/Y.1314 – Couche serveur de VPN CL avec client CO

Dans cet exemple, la connexion de couche client de VPN orientée connexion est prise en charge par un chemin de couche serveur de VPN sans connexion. La fonction de source d'adaptation de couche serveur de VPN sans connexion adapte les informations caractéristiques (CI) de la couche client de VPN orientée connexion en informations adaptées (AI) dans la couche serveur de VPN sans connexion. La fonction de puits d'adaptation de couche serveur de VPN sans connexion adapte les informations adaptées de couche serveur de VPN sans connexion aux informations caractéristiques de couche client de VPN orientée connexion.

7.3.4 Couche client de VPN CL prise en charge par une couche serveur de VPN CO

Un exemple d'une couche client de VPN sans connexion qui est prise en charge par une couche serveur de VPN orientée connexion est illustré à la Figure 7-8.

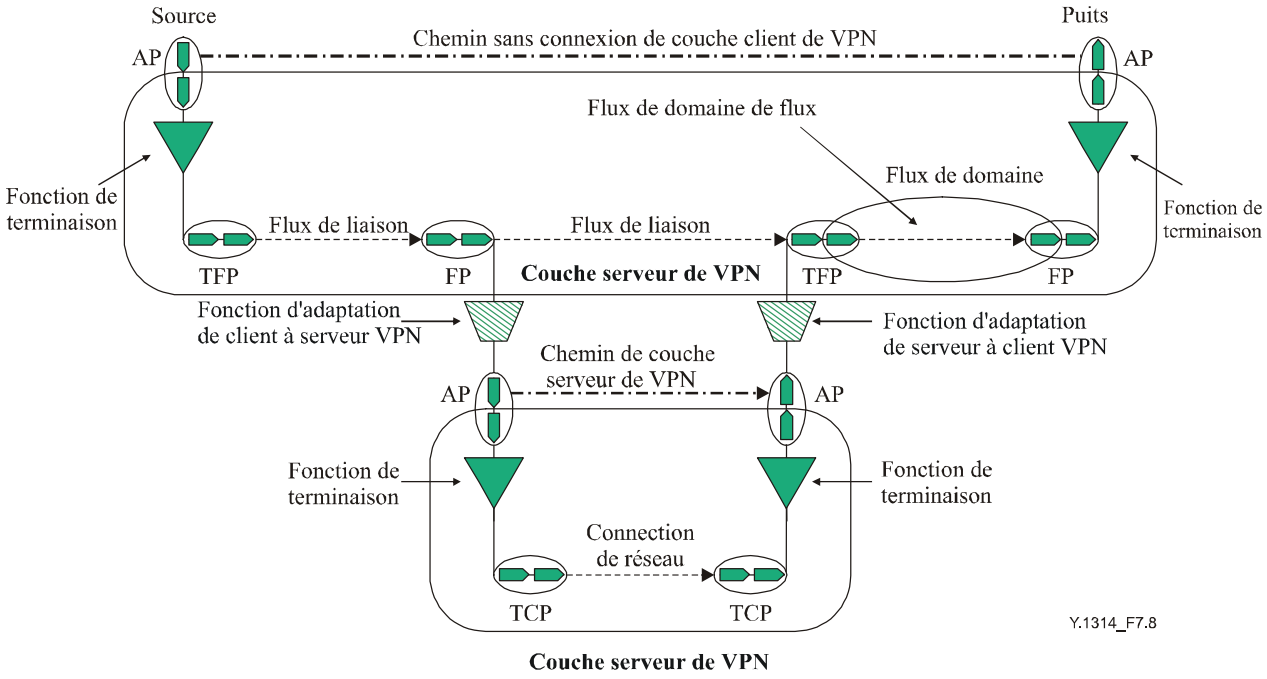


Figure 7-8/Y.1314 – Couche serveur de VPN CO avec un client CL

Dans cet exemple, le flux de couche client de VPN sans connexion est pris en charge par un chemin de couche serveur de VPN orientée connexion. La fonction de source d'adaptation de couche serveur de VPN orientée connexion adapte les informations caractéristiques (CI) de la couche client de VPN sans connexion en informations adaptées (AI) dans la couche serveur de VPN orientée connexion. La fonction de puits d'adaptation de couche serveur de VPN orientée connexion adapte les informations adaptées de couche serveur de VPN orientée connexion aux informations caractéristiques de couche client de VPN sans connexion.

7.4 Couches client de VPN multiples

Dans les exemples donnés jusqu'à présent dans le présent paragraphe, une seule couche client de VPN a été utilisée de bout en bout. Cependant, cela peut n'être pas toujours le cas, et un consommateur peut souhaiter utiliser un type de couche client de VPN d'un côté d'un VPN, et un type différent de client VPN de l'autre côté d'un VPN. Par exemple, d'un côté la couche client de VPN pourrait être IP et de l'autre côté elle pourrait être MPLS, ou un côté pourrait être en relais de trames (FR, *frame relay*) et l'autre côté pourrait être en ATM. Dans de tels cas, les deux différents réseaux de couche client VPN doivent être réseautés sur la base de niveaux homologues.

A noter que le terme "couche client de VPN" utilisé ici se réfère à un composant topologique dans un VPN client/serveur qui représente l'ensemble des points d'accès du même type associés pour les besoins du transfert des informations caractéristiques de couche client de VPN. Il ne se réfère pas à la mise en réseau de couche au sens des couches 1, 2, 3, c'est-à-dire que les deux technologies de réseau qui interfonctionnent à la couche client de VPN peuvent être toutes deux des technologies de couche 2 (par exemple, une peut être de l'ATM et l'autre du relais de trames), mais elles sont considérées comme des réseaux de couches différents car elles contiennent des points d'accès différents, qui sont aussi d'un type différent.

La fonction d'interfonctionnement peut prendre place soit avant la fonction d'adaptation de source de couche serveur de VPN soit après la fonction d'adaptation de puits de couche serveur de VPN. La Figure 7-9 montre la topologie physique de réseau client/serveur de VPN qui utilise des couches client de VPN différentes de chaque côté du VPN.

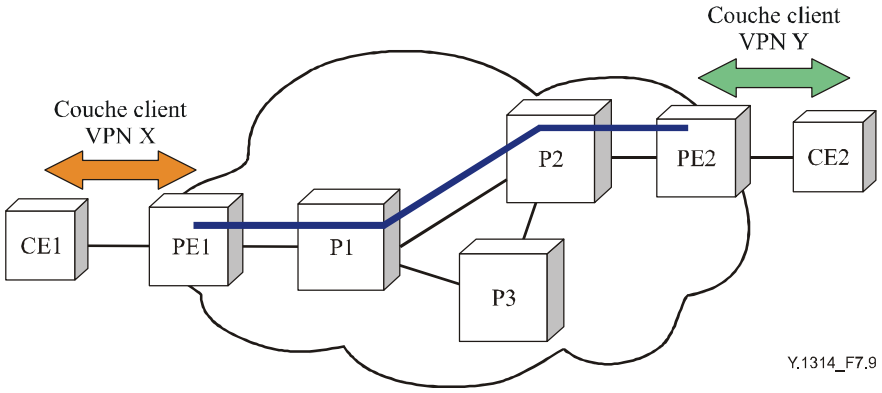


Figure 7-9/Y.1314 – Topologie physique d'interfonctionnement de niveau homologue de VPN client

La Figure 7-10 présente un modèle fonctionnel générique pour l'interfonctionnement de VPN client de niveau homologue fondé sur la topologie physique de la Figure 7-9, où la fonction d'interfonctionnement prend place avant la fonction d'adaptation de source de couche serveur de VPN.

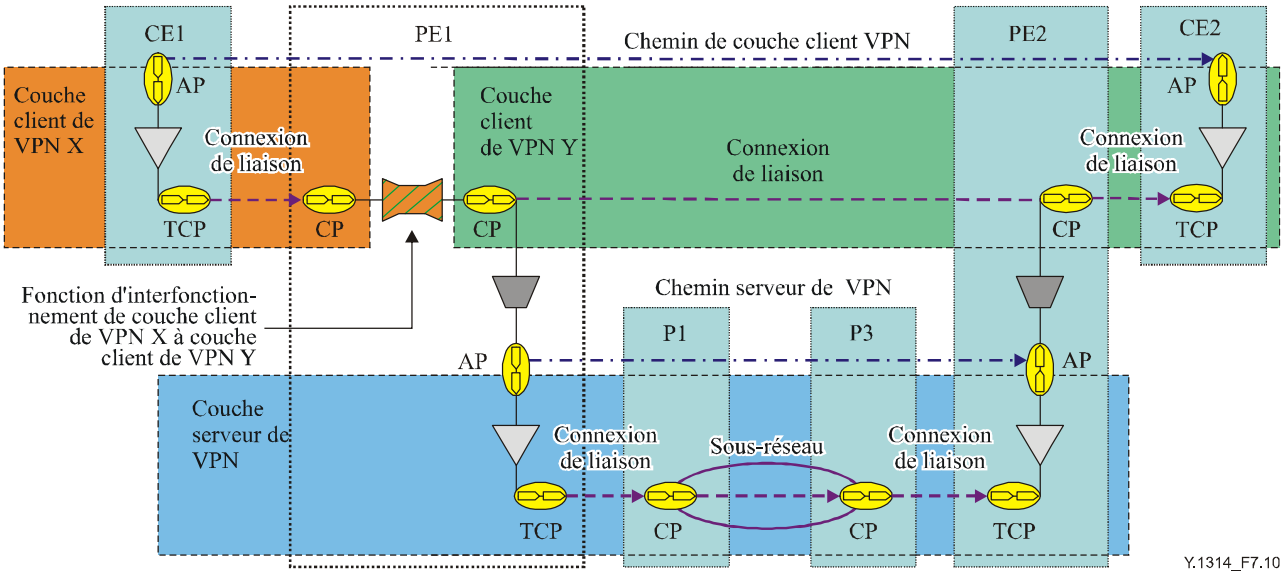


Figure 7-10/Y.1314 – Interfonctionnement de niveau homologue de VPN client (préadaptation de source de VPN serveur)

Les deux couches client de VPN hétérogènes dans ce modèle sont la couche client de VPN X et la couche client de VPN Y. Dans cet exemple l'extrémité fournisseur effectue la fonction d'interfonctionnement mais elle pourrait aussi être effectuée en utilisant un appareil distinct. La fonction d'interfonctionnement convertit les informations caractéristiques de la couche client du VPN X en informations caractéristiques de couche client du VPN Y. La fonction d'adaptation de source de couche serveur de VPN adapte les informations caractéristiques de la couche client du VPN Y en informations adaptées dans la couche serveur de VPN et les informations adaptées de couche serveur de VPN sont transmises à travers le chemin de couche serveur de VPN. Au puits de couche serveur de VPN, la fonction d'adaptation adapte les informations adaptées de couche serveur de VPN aux informations caractéristiques de couche client du VPN Y. A titre d'exemple, si la couche client du VPN X est en relais de trames et la couche client du VPN Y est en ATM,

l'extrémité fournisseur de source convertira alors le trafic de relais de trames en trafic ATM (en utilisant par exemple FRF.8) et le trafic de couche client de VPN sera transporté comme ATM sur la couche serveur de VPN.

La Figure 7-11 présente un modèle fonctionnel générique pour l'interfonctionnement de client VPN de niveau homologue où la fonction d'interfonctionnement prend place après la fonction d'adaptation de puits de couche serveur de VPN.

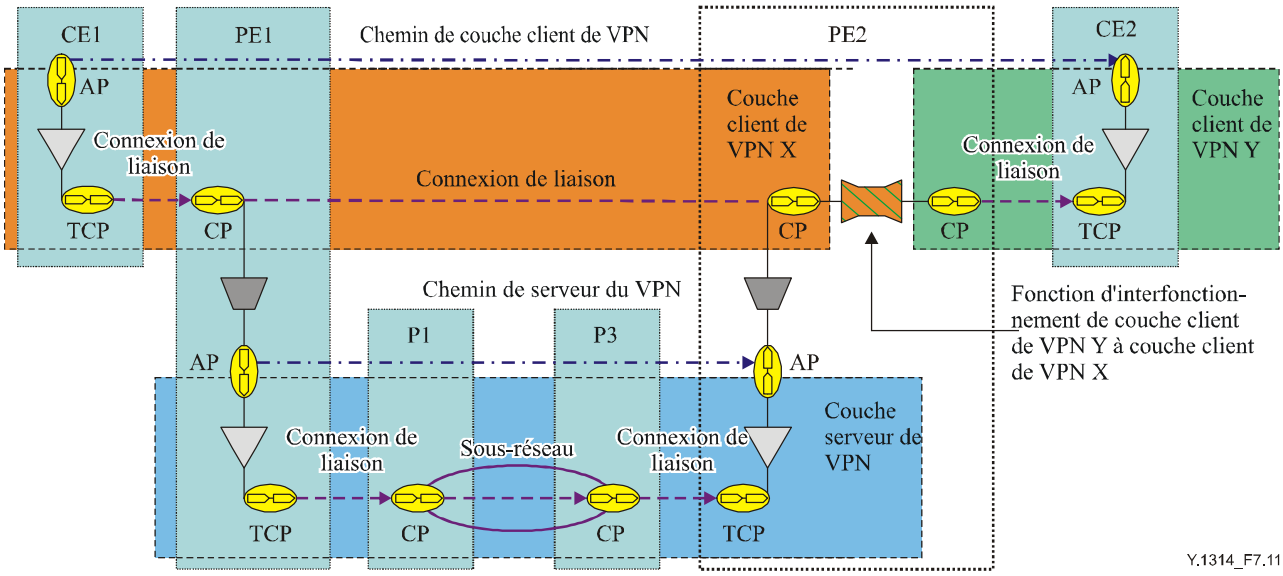


Figure 7-11/Y.1314 – Interfonctionnement de niveau homologue de VPN client (postadaptation de puits de VPN serveur)

La fonction d'adaptation de source de couche serveur de VPN adapte les informations caractéristiques de couche client du VPN X en informations adaptées dans la couche serveur de VPN et les informations adaptées de couche serveur de VPN sont transmises à travers le chemin de couche serveur de VPN. Au puits de couche serveur de VPN, la fonction d'adaptation adapte les informations adaptées de couche serveur de VPN en informations caractéristiques de la couche client du VPN X. La fonction d'interfonctionnement convertit les informations caractéristiques de couche client du VPN X en informations caractéristiques de couche client du VPN Y. Si la couche client du VPN X était en relais de trames et la couche client du VPN Y était en ATM, le trafic de la couche client de VPN serait transporté comme relais de trames sur la couche serveur de VPN et converti en ATM par le puits d'extrémité fournisseur.

7.5 Couches serveur de VPN multiples

Dans les exemples précédents, une seule couche serveur de VPN était utilisée de bout en bout à travers le réseau fournisseur pour prendre en charge la couche client de VPN. Cependant, ceci peut n'être pas toujours le cas; par exemple, un fournisseur peut n'être pas capable de fournir la connectivité de bout en bout en utilisant une seule couche serveur de VPN à cause d'un manque de couverture du réseau, ou une couche client de VPN peut avoir besoin de traverser plusieurs réseaux fournisseurs. Dans de telles circonstances, plusieurs couches serveur de VPN sont nécessaires. En fonction des technologies spécifiques du réseau et des capacités d'interaction des équipements du fournisseur, des couches serveur de VPN séparées peuvent être interconnectées sur la base de niveaux homologues, ou interconnectées avec le VPN client sur une base client/serveur.

Bien qu'il soit possible d'avoir plusieurs couches serveur de VPN, il y a plusieurs facteurs qui doivent être pris en considération lorsqu'on envisage d'utiliser plusieurs couches serveur de VPN en commutation multiprotocolaire par étiquetage (MPLS, *multi-protocol label switching*). Les facteurs

à considérer dépendent du type d'interfonctionnement requis et des technologies de couche serveur de VPN à employer. Des exemples d'interfonctionnement de niveau homologue et de client/serveur de plusieurs couches serveurs avec quelques commentaires pour chacun sont fournis à l'Appendice II.

A noter que l'utilisation de plusieurs couches serveurs en dessous de la couche serveur de VPN ne devrait pas être confondue avec l'utilisation de plusieurs couches serveur de VPN. Par exemple, comme illustré à la Figure 7-12, un fournisseur de services peut utiliser une seule couche serveur de VPN MPLS de bout en bout, mais utiliser une couche serveur MPLS (en utilisant un empilement d'étiquettes MPLS) en dessous de la couche serveur de VPN dans une partie du réseau, et utiliser une couche serveur IP (par exemple, en utilisant une encapsulation GRE) dans une autre partie du réseau.

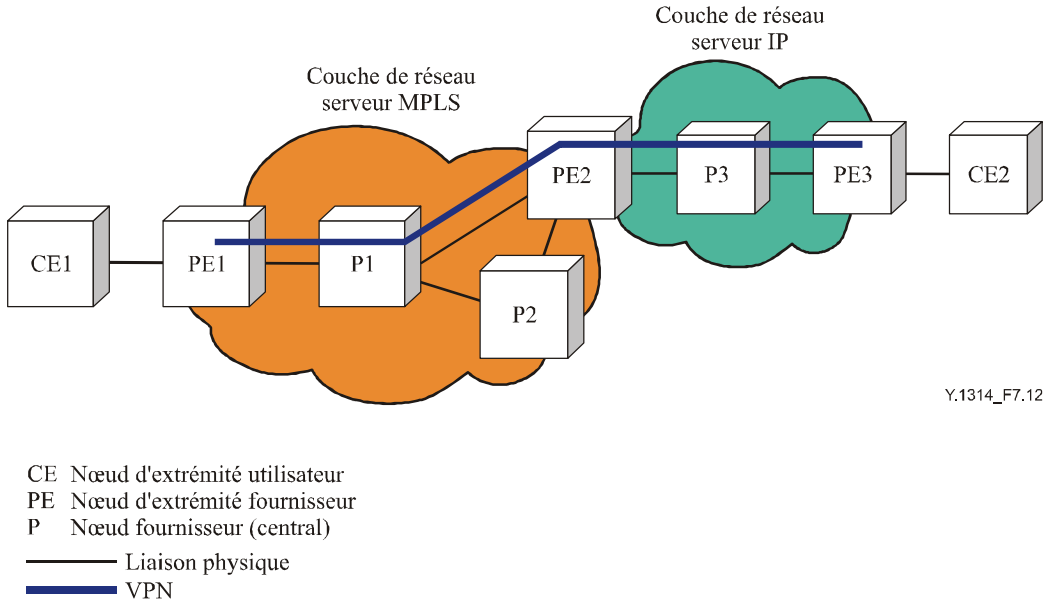


Figure 7-12/Y.1314 – VPN client/serveur avec couches serveur de VPN avec MPLS et IP

Les routeurs d'extrémité fournisseur et fournisseur doivent tous prendre en charge MPLS dans la couche serveur de réseau MPLS, cependant, seuls les routeurs d'extrémité fournisseur dans la couche serveur IP ont besoin de prendre en charge MPLS, et les routeurs fournisseur n'ont pas besoin de prendre en charge MPLS. Le modèle fonctionnel qui se rapporte au réseau illustré à la Figure 7-12 est décrit à la Figure 7-13.

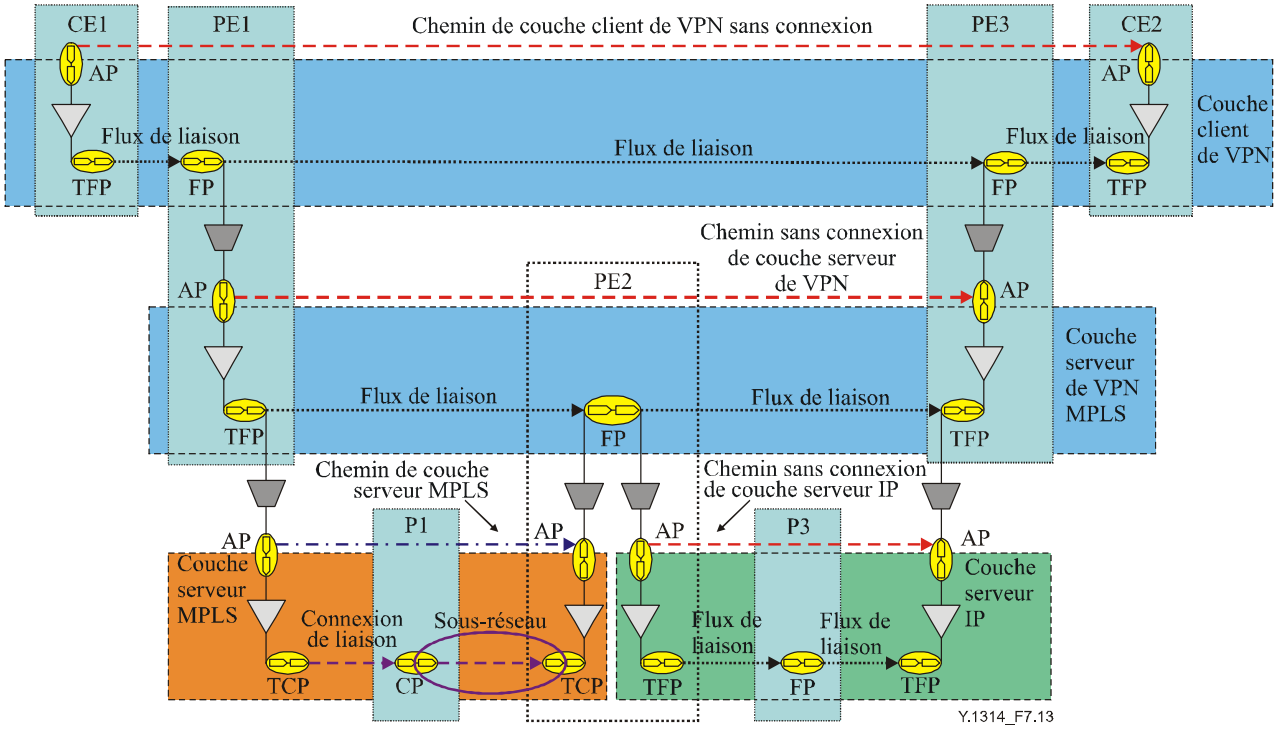


Figure 7-13/Y.1314 – Couche serveur de VPN prise en charge par plusieurs couches serveur

Dans cet exemple la fonction d'adaptation de source de couche serveur MPLS adapte les informations caractéristiques de couche serveur de VPN MPLS (qui est un client de la couche serveur MPLS) en informations adaptées dans la couche serveur MPLS, et la fonction d'adaptation de puits de couche serveur MPLS adapte les informations adaptées de couche serveur MPLS aux informations caractéristiques de couche serveur de VPN MPLS. La fonction d'adaptation de source de couche serveur IP adapte les informations caractéristiques de couche serveur de VPN MPLS en informations adaptées dans la couche serveur IP, et la fonction d'adaptation de puits de couche serveur IP adapte les informations adaptées de couche serveur IP aux informations caractéristiques de couche serveur de VPN MPLS.

7.6 Modélisation VPN utilisant la partition

Le modèle fonctionnel présenté dans les paragraphes précédents a été développé en utilisant une approche en couches. Décomposer les réseaux en un certain nombre de réseaux de couches indépendantes permet de modéliser les relations client/serveur entre des réseaux de couches adjacentes et de décrire les fonctions correspondantes d'adaptation, de terminaison et d'interfonctionnnement.

Une autre approche de la modélisation est la partition, qui est utilisée pour définir la structure du réseau au sein d'un réseau de couche et les frontières administratives/d'acheminement entre les domaines de réseau, par exemple appartenant à des opérateurs différents. La partition permet de décomposer un sous-réseau à un niveau en ses sous-réseaux contenants avec les liaisons entre eux. Cette partition peut se poursuivre jusqu'à la limite de récurrence, qui est un seul sous-réseau au sein d'un élément de réseau. Ceci est connu comme une matrice, décrite dans la Rec. UIT-T G.805. La partition est illustrée à la Figure 7-14.

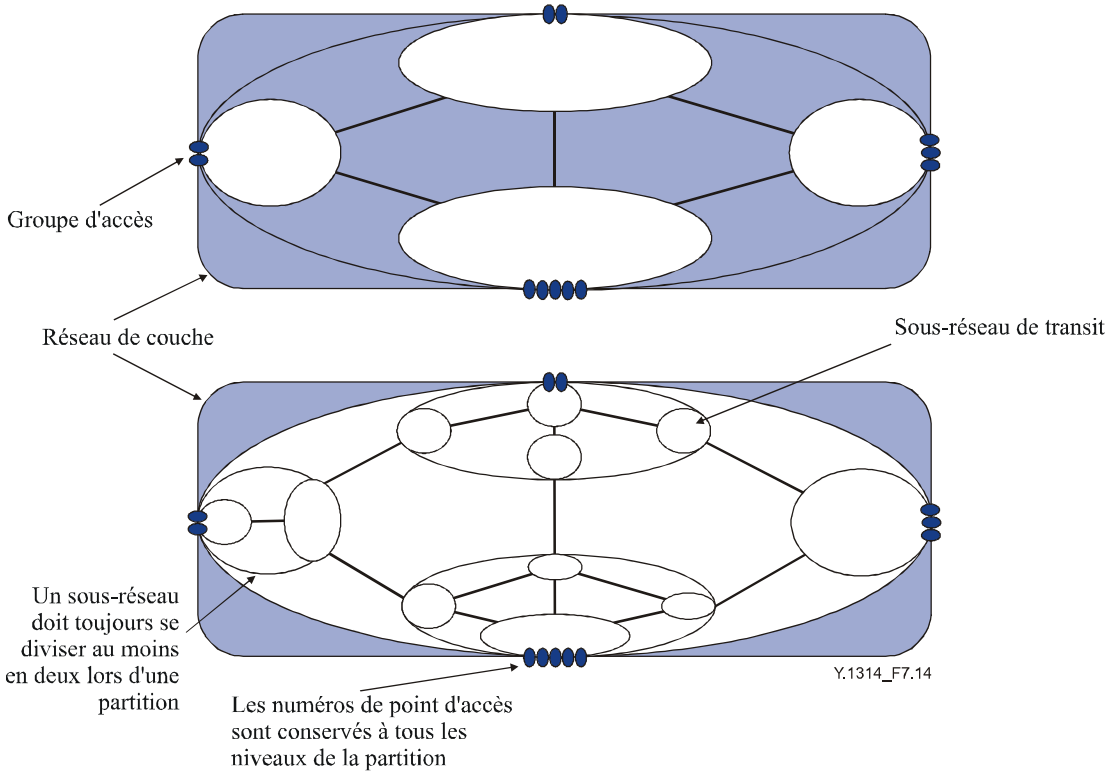


Figure 7-14/Y.1314 – Partition de sous-réseaux au sein d'un réseau de couche

Au titre du processus de partition, le nombre de points de flux/connexion dans le plus grand sous-réseau reste le même pendant la partition, alors que les points de connexion qui lui sont internes au prochain niveau de partition sont révélés. Du point de vue de la connectivité, le sous-réseau (domaine de flux) représente un point de flexibilité entre ses entrées et ses sorties (par exemple points d'accès source/puits ou points de flux/connexion). Cela permet généralement à toute entrée d'être connectée à toute sortie.

Ce modèle est suffisant pour les réseaux publics où les ressources peuvent être supposées disponibles à l'utilisation. Cependant, cela ne convient pas pour les réseaux privés virtuels. La raison en est que la connectivité entre entrées et sorties sur le domaine sous-réseau/flux est limitée aux entrées et sorties qui appartiennent au même VPN. Pour prendre en charge la modélisation d'un VPN utilisant l'approche de partition, des constructions de fragments de domaine de flux (FDFr, *flow domain fragment*) comme décrits dans la Rec. UIT-T G.8010/Y.1306, et des constructions de connexions de sous-réseau (SNC, *subnetwork connection*) sont utilisées. Un FDFr/SNC est fragmenté en divisant ses entrées et ses sorties en différents groupes. La connectivité est limitée aux membres du même groupe. Un tel groupe peut être un VLAN sur un pont Ethernet (un domaine de flux Ethernet) ou un VPN sur un sous-réseau ou domaine de flux. Noter que le fragment n'a pas de points de flux; ceux-ci sont associés à un domaine de flux. Un FDFr/SNC peut être étiqueté par le nom de son réseau de couche associé et le numéro de fragment, ou au moyen d'un groupement de points de flux dans un fragment particulier, par exemple par un identificateur de VLAN. Un exemple de réseau utilisant des VLAN pour fournir l'isolation de VPN est donné à la Figure 7-15.

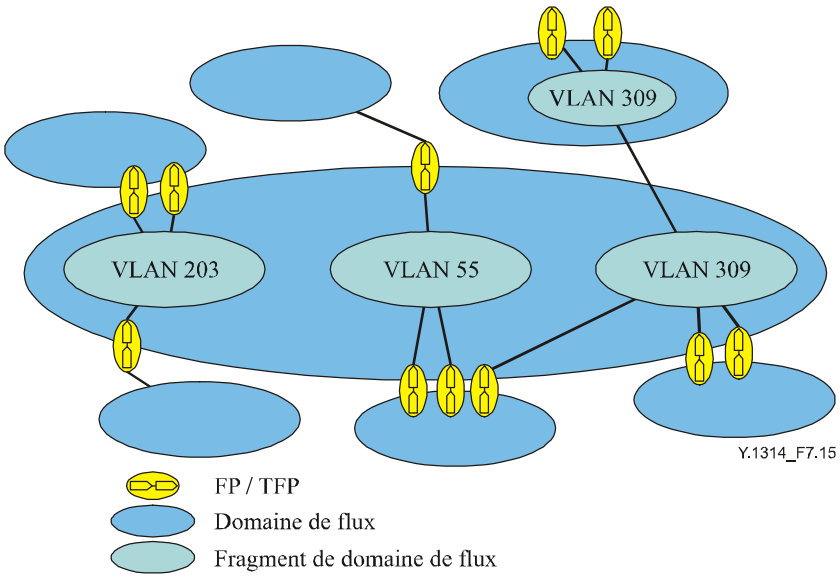


Figure 7-15/Y.1314 – Exemple de modèle fonctionnel de partition de VPN

Un FDFr d'un domaine de flux est associé à un FDFr dans un autre domaine de flux au moyen d'une liaison de composant d'interconnexion. De la même façon, un SNC dans un sous-réseau est associé à un SNC dans un autre sous-réseau via la connexion de liaison d'interconnexion. Ceci permet que la construction soit partitionnée ou agrégée en ligne au modèle de sous-réseau. Comme tel, le modèle est très souple et permet de montrer la structure VPN à tout niveau de partition de sous-réseau.

7.7 Couche homologue de VPN

La Figure 7-16 montre la topologie physique d'un niveau homologue de VPN. Dans cet exemple, le nuage de réseau retrace le domaine du réseau partagé et la ligne bleue représente un VPN point à point. L'isolation de VPN pourrait être réalisée en utilisant n'importe quelle approche définie au § 6, par exemple, un VLAN Ethernet, un tunnel IPsec, etc.

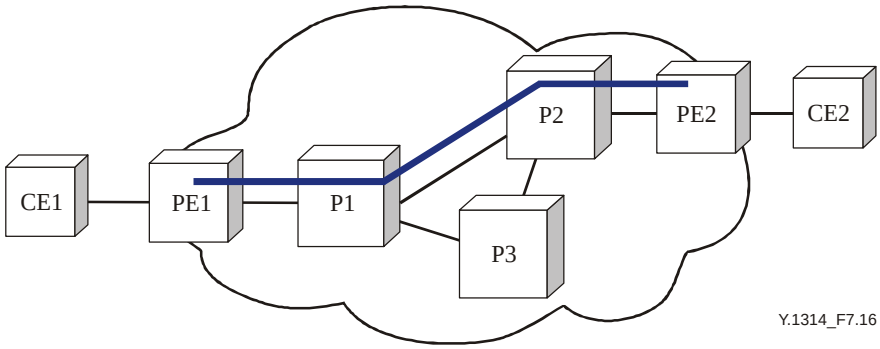


Figure 7-16/Y.1314 – Exemple de topologie physique de niveau homologue de VPN

La Figure 7-17 décrit la topologie VPN de la Figure 7-1 d'un point de vue fonctionnel qui montre la couche VPN et une seule couche serveur sous-jacente entre les extrémités fournisseur. Dans cet exemple la couche serveur est orientée connexion, mais pourrait également être sans connexion.

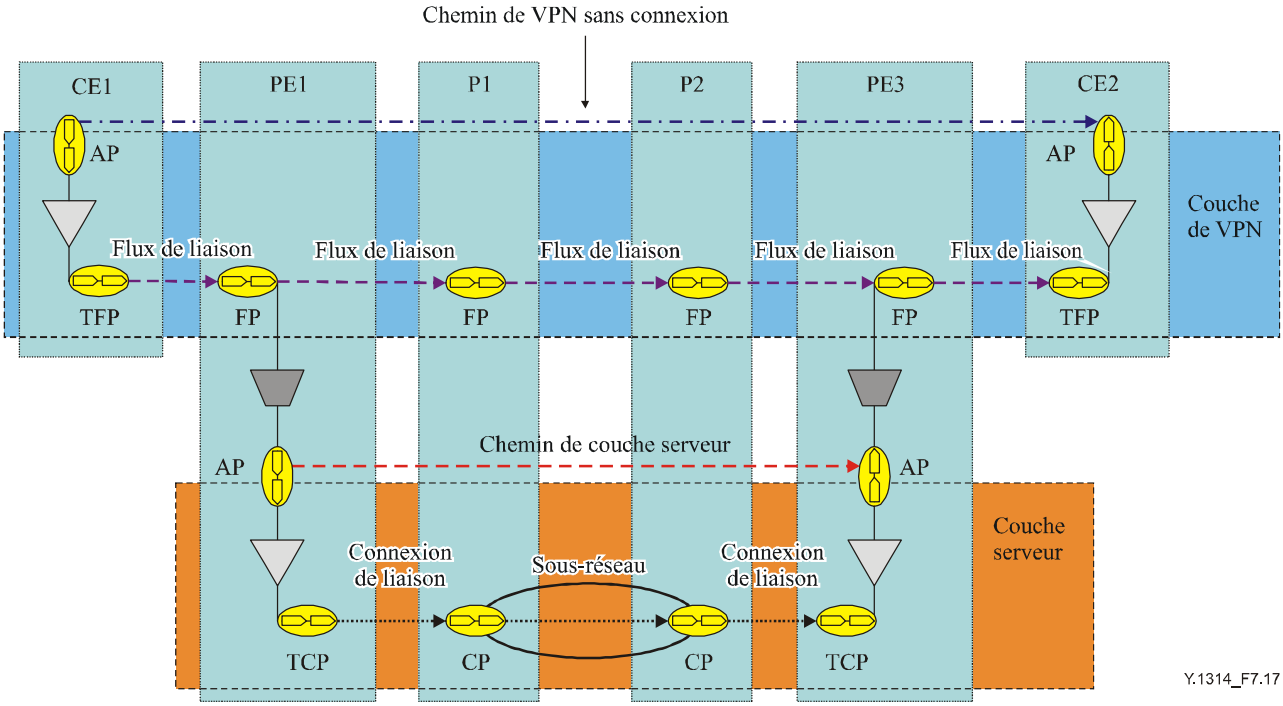


Figure 7-17/Y.1314 – Modèle en couche d'une seule couche VPN

Comme le montre la Figure 7-17, tous les nœuds dans le réseau (y compris les nœuds fournisseur) appartiennent à la couche VPN et ils doivent donc être capables de transmettre les paquets à la destination correcte en utilisant les informations dans les en-têtes de paquets de couche VPN. Du fait de l'architecture VPN à couche unique, le modèle en couche ne fournit pas autant d'informations qu'il le fait lorsqu'il est utilisé dans le cas de VPN client/serveur. En particulier, le format de présentation de la Figure 7-17 ne fournit aucune information sur où commence et où finit le VPN. Une façon d'incorporer ces informations est de s'étendre sur les fonctions d'adaptation de VPN/couche serveur. La Figure 7-18 montre deux exemples différents de fonctions d'adaptation de VPN/couche serveur, une qui utilise IPsec et une qui utilise des étiquettes VLAN Ethernet.

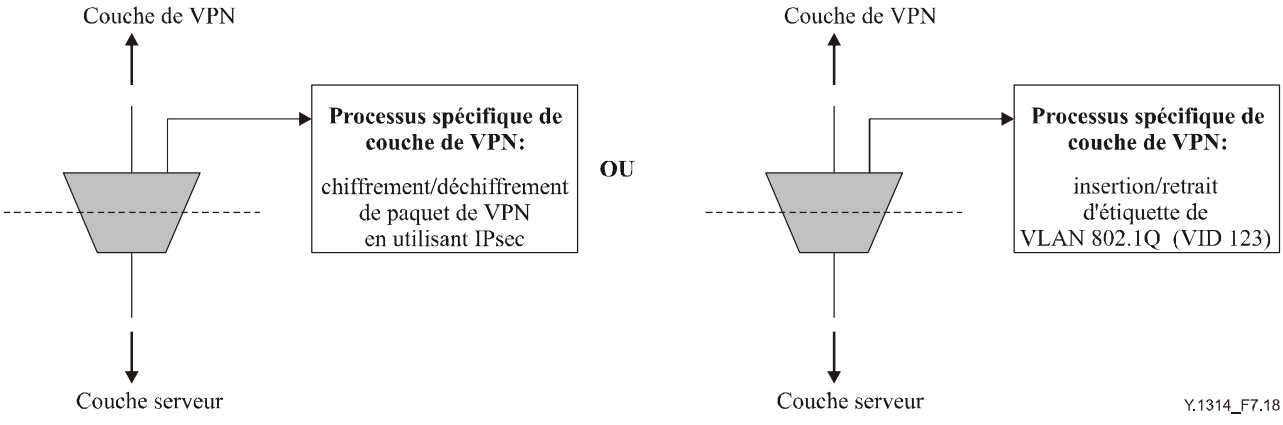


Figure 7-18/Y.1314 – Expansion des fonctions d'adaptation de VPN/couche serveur

Une autre façon de décrire un niveau homologue de VPN est d'utiliser le concept de partition introduit au paragraphe précédent. Un exemple de la façon dont la partition peut être utilisée pour cela est donné à la Figure 7-19.

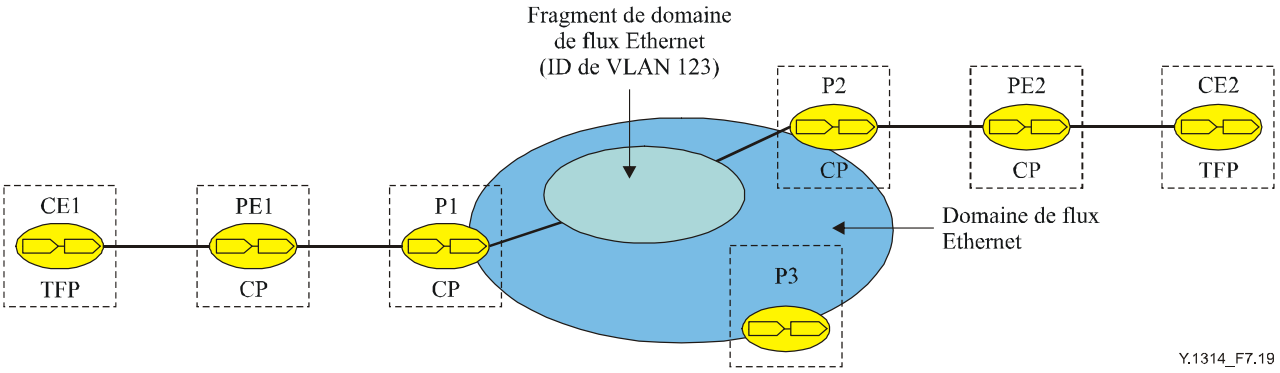


Figure 7-19/Y.1314 – Niveau homologue de VPN modélisé en utilisant la partition

La Figure 7-19 décrit la topologie de niveau homologue de VPN, et montre aussi le VLAN correspondant (123), mais ne donne pas d'information sur où commence et finit le VPN, c'est-à-dire où les étiquettes IEEE 802.1Q de VLAN sont insérées/retirées. Il est facile de voir à partir du modèle de la Figure 7-19 que les nœuds P1 et P2 font partie du VLAN 123, mais bien que PE1 et PE2 soient les points de début/fin du VPN, le modèle ne donne pas cette information. Ceci dit, incorporer les fonctions d'adaptation de VPN/couche serveur dans le modèle de partition et développer les processus spécifiques de couche VPN pourraient fournir ces informations (comme le montre la Figure 7-18).

8 Prise en charge de la topologie VPN

Le terme "topologie VPN" utilisé dans la présente Recommandation se réfère à la topologie de réseau du point de vue de l'utilisateur VPN, c'est-à-dire la topologie entre les sites VPN qui peuvent être des nœuds d'extrémité client ou des systèmes d'extrémité. La connectivité entre les sites VPN ne peut être fournie que si les chemins de couche serveur ou couche homologue de VPN ont été établis entre eux. En général, la topologie à la couche n dépend de la topologie fournie par les chemins de couche serveur à la couche n–1. Une fois que les chemins de couche serveur ou homologue VPN ont été établis, si la technologie de couche client ou couche homologue VPN est par commutation de paquets, il est alors possible de faire des coupures dans la topologie VPN en restreignant la connectivité entre certains sites au sein du VPN. Une méthode pour restreindre la connectivité entre des membres du VPN est de contrôler la distribution de l'acheminement à la couche client de VPN (les sites VPN ne peuvent pas communiquer s'ils n'ont pas de routes pour s'atteindre les uns les autres). Une autre méthode qui peut être utilisée pour restreindre la connectivité est l'utilisation du filtrage de paquet (par exemple sur la base des adresses de source/destination de couche client ou de couche homologue VPN). Les trois topologies VPN de base sont le maillage complet, le maillage partiel, et le réseau en étoile (*hub and spoke*) et sont décrits dans les paragraphes 8.1, 8.2 et 8.3.

8.1 Topologies VPN à maillage complet

Dans une topologie VPN à maillage complet, chaque site VPN a une route/connexion vers chaque autre site VPN comme le décrit la Figure 8-1.

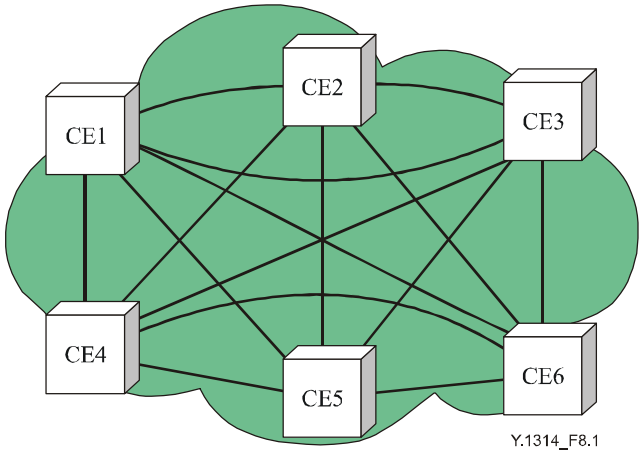


Figure 8-1/Y.1314 – Exemple de topologie VPN à maillage complet

Une topologie à maillage complet fournit une redondance complète et peut aussi fournir une utilisation et des performances de réseau efficaces car les sites VPN peuvent utiliser le chemin/route le plus court/le meilleur pour s'atteindre les uns les autres. Un désavantage de l'approche à maillage complet est que son implémentation peut être coûteuse, bien que cela dépende du mode et des technologies de réseau VPN employées (par exemple, un réseau VPN constitué d'un maillage complet de voies virtuelles en ATM coûtera vraisemblablement plus cher qu'un VPN Ethernet qui prend en charge une connectivité de tous vers tous). Un autre désavantage est que lorsque le nombre de sites dans un maillage complet augmente le nombre de connexions/routes, l'adjacence des plans de contrôle augmente proportionnellement (le nombre de connexions dans un maillage complet est de n(n–1)/2, où n est le nombre de sites VPN). La prise en charge d'un grand nombre de connexions/routes et de plans de contrôles adjacents introduit des problèmes d'échelle dus à l'augmentation de la quantité de bande passante et de ressources de CPU nécessaires.

8.2 Topologies VPN à maillage partiel

Dans une topologie à maillage partiel, les sites VPN ont des routes/connexions avec certains sites VPN, mais pas avec tous. Un exemple de topologie à maillage partiel est donné à la Figure 8-2.

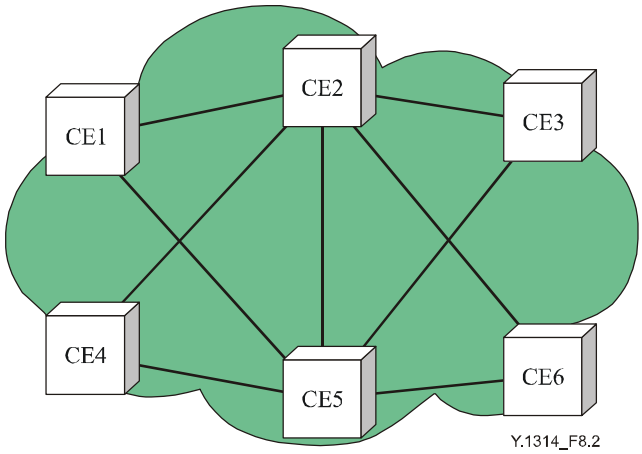


Figure 8-2/Y.1314 – Exemple de topologie VPN à maillage partiel

Dans certains cas, les sites VPN peuvent être capables d'atteindre des sites VPN pour lesquels ils n'ont pas de routes/connexions directes via des sites VPN de transit. Cependant, dans d'autres cas, si les sites VPN n'ont pas de routes/connexions directes pour s'atteindre les uns les autres, la communication entre eux peut alors n'être pas possible. La capacité à instaurer la communication entre les nœuds qui n'ont pas de routes ou connexions directes pour s'atteindre les uns les autres dépend de l'existence de chemins de couche serveur ou de couche homologue de VPN et de toutes les restrictions de connectivité de la topologie (par exemple, les politiques d'acheminement ou de filtre de paquet). Les topologies à maillage partiel sont plus échelonnables que les topologies à maillage complet parce que la bande passante et les ressources en CPU nécessaires sont réduites, bien que cela soit aux dépends de l'optimisation de l'acheminement et de l'utilisation efficace du réseau (si certaines extrémités client sont utilisées comme nœuds de transit). La redondance du réseau est aussi réduite, bien que les réseaux à maillage partiel soient habituellement conçus de telle sorte que des routes/connexions redondantes soient utilisées où elles sont les plus nécessaires. Par exemple, à la Figure 8-2, les nœuds d'extrémité client CE2 et CE5 pourraient être des nœuds centraux et les autres nœuds d'extrémité client pourraient être des nœuds périphériques. Auquel cas, dans cette topologie, les nœuds périphériques ont des connexions/routes redondantes pour atteindre le cœur. Les utilisateurs sont souvent forcés d'utiliser des topologies à maillage partiel en raison de facteurs tels que le coût (c'est-à-dire que les réseaux à maillage complet sont plus coûteux) et en raison de contraintes géographiques.

8.3 Topologies VPN à réseau en étoile

Dans une topologie de réseau en étoile (*hub and spoke*), un site VPN peut être soit un noyau soit un rayon pour un VPN particulier (quoique si un site VPN appartient à plusieurs VPN, il puisse être un noyau pour certains VPN et un rayon pour d'autres). Tous les rayons dans une topologie de réseau en étoile ont des routes/connexions directes pour atteindre le noyau, mais n'ont pas de routes/connexions directes pour s'atteindre les uns les autres. La Figure 8-3 donne un exemple de topologie de réseau en étoile dans laquelle CE2 est le noyau et tous les autres nœuds d'extrémité client sont des rayons.

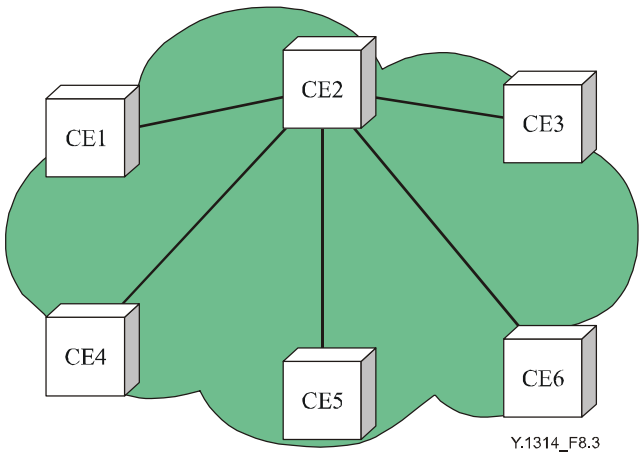


Figure 8-3/Y.1314 – Exemple de topologie de réseau VPN en étoile

Dans certains cas, le noyau peut être configuré comme un nœud de transit de sorte que les rayons puissent communiquer les uns avec les autres via le noyau. Cependant, dans d'autres cas, la connectivité entre les nœuds rayons peut n'être pas permise. Une utilisation courante de la topologie de réseau en étoile sert à connecter des bureaux (les rayons) à un siège social (le noyau). Utiliser une topologie de réseau en étoile permet d'avoir des ressources de réseau centralisées (par exemple pour l'accès à l'Internet, pour les pare-feu, et les serveurs de messagerie électronique), qui peuvent conduire à une réduction des coûts par rapport à une approche de ressources de réseau distribuées.

9 Considérations de qualité de service sur VPN

Il y a un grand nombre de sources d'information sur la qualité de service (QS), qui contiennent différentes définitions de ce que signifie réellement la qualité de service. La Rec. UIT-T E.800 définit la qualité de service comme l'effet collectif des performances de service, qui détermine le degré de satisfaction d'un utilisateur du service. La Rec. UIT-T G.1000 fournit un cadre de travail et des définitions pour la qualité de service des communications, et la Rec. UIT-T G.1010 définit un modèle pour les catégories de qualité de service multimédia du point de vue d'un utilisateur final. Les fonctions requises pour satisfaire aux exigences de qualité de service définies dans ces Recommandations et ailleurs dépendent du mode de fonctionnement du réseau. Toutefois, les exigences de qualité de service peuvent avoir un impact sur le choix par un fournisseur de services VPN de la technologie de couche serveur de VPN et des technologies de couches client de VPN qui peuvent être prises en charge.

9.1 Réseaux de couche à commutation de circuit

Dans les réseaux de couche à commutation de circuit orientée connexion, un chemin fondé sur une liaison physique, une longueur d'onde optique, un circuit virtuel SDH/SONET, ou un intervalle de temps TDM est établi et dédié à une seule connexion entre les points d'accès dans le réseau pour la durée de la connexion. Lorsqu'une nouvelle connexion est nécessaire, le réseau doit décider d'accepter ou non la connexion; et s'il l'accepte, comment l'acheminer à travers le réseau et quelles ressources réserver à la connexion. Les mécanismes de contrôle d'admission de connexion (CAC, *connection admission control*) sont utilisés pour accepter une connexion si la bande passante est disponible ou pour la rejeter lorsque la bande passante d'une connexion demandée excède la bande passante disponible.

Les données sont transmises à un débit binaire constant exactement dans le même ordre que celui selon lequel elles ont été envoyées. Les connexions peuvent être établies manuellement en utilisant un approvisionnement statique, ou de façon dynamique en utilisant des mécanismes de signalisation ou des outils d'approvisionnement automatique. La capacité à établir de nouvelles connexions dépend des capacités de réserve dans le réseau. Si une connexion est établie, la livraison des données à travers la connexion est garantie.

Dans les réseaux à commutation de circuit orientée connexion (CO-CS) tels qu'un RTPC, le délai est principalement une fonction de la distance de transmission. Les délais de commutation dans les nœuds de réseaux CO-CS sont relativement petits par rapport au délai de transmission (propagation), particulièrement lorsque les appels traversent des artères longue distance.

9.2 Réseaux de couche à commutation de paquets

Dans les réseaux à commutation de paquets, les paquets sont transmis sur la base des informations de l'en-tête du paquet. La commutation de paquets fournit la connectivité tout en faisant un usage efficace des ressources du réseau en les partageant entre de nombreux utilisateurs (en se fondant sur l'hypothèse que tous les utilisateurs n'ont pas besoin des ressources tout le temps). Le comportement de transmission des paquets pour les flux ou connexions peut être décrit par un ensemble de paramètres appelés descripteurs de trafic. Des exemples de descripteurs de trafic incluent le débit moyen de bit/paquet, la taille maximale de longueur de rafale/paquet, et la probabilité de l'arrivée d'un paquet dans un intervalle de temps donné. Les exigences de qualité pour l'utilisateur sont souvent exprimées en termes de perte de paquet, délais et gigue acceptables.

Des mécanismes de formatage du trafic peuvent être utilisés pour réguler la quantité de trafic admise sur le réseau, généralement sur la base de la file d'attente/flux, par connexion, ou par interface. L'encombrement peut survenir dans les réseaux par paquets si le volume de trafic excède les capacités de transmission d'une entité du réseau (NE) ou la capacité disponible du réseau. Lorsque le réseau devient encombré, les paquets peuvent être mis en mémoire tampon, ce qui introduit un retard, ou ils peuvent être abandonnés.

Dans les réseaux à commutation de paquets, le délai dépend de la distance de transmission associée à la couche Physique serveuse sous-jacente, plus un certain nombre d'autres facteurs à la couche de commutation de paquets. Les facteurs qui introduisent des délais à la couche de commutation de paquet incluent la taille de paquet, la vitesse de la liaison, le délai de transmission par bond (qui peut être détérioré par la mise en paquets, la compression/décompression, la commutation/acheminement et les délais de mise en mémoire tampon) et le nombre de bonds. Un contrôle de priorité est nécessaire dans le réseau de paquets afin de garantir différents niveaux de gamme de qualité. Généralement, les contrôles de priorité sont implémentés en utilisant des files d'attentes séparées, par connexion, par flux, ou par classe de qualité de service à chaque interface, et en contrôlant la priorité de chaque queue. Les mécanismes de programmation de paquet sont utilisés pour allouer les paquets à une file d'attente particulière conformément à des politiques spécifiques.

9.2.1 Commutation de paquets orientée connexion

Dans les réseaux de couche à commutation de paquets orientée connexion, les connexions sont établies et maintenues jusqu'à ce que la connectivité ne soit plus requise (que des données aient été transmises ou non). Comme avec les réseaux de couche à commutation de circuit orientée connexion, les connexions peuvent être établies via un approvisionnement manuel, un système de gestion, ou par un protocole de signalisation. L'état en cours du réseau peut être déterminé en surveillant l'utilisation des ressources du réseau et/ou en caractérisant le comportement des connexions déjà admises. Les mécanismes de contrôle d'admission de connexion (CAC) peuvent être utilisés pour réserver la bande passante de crête de la connexion requise pour les sources de trafic à débit binaire constant (CBR, *constant bit rate*). Autrement, on peut utiliser des schémas de multiplexage statistique avec les mécanismes de CAC pour allouer moins que la bande passante de crête requise afin d'augmenter l'efficacité du réseau. Cependant, il peut être difficile de caractériser la bande passante d'une connexion demandée car la bande passante requise peut varier dans le temps de façon significative.

Dans un réseau CO-PS (par exemple, un réseau ATM), si les services CBR sont pris en charge (sans supplément d'abonnement) le délai de transmission par bond reste constant et donc le délai/gigue peut être calculé/garanti. Si cependant, les services font l'objet de surréservation pour accroître l'utilisation du réseau (ce qui se passe habituellement), des retards/pertes vont alors être introduits aux nœuds encombrés du fait de la mise en mémoire tampon ou de l'abandon de trafic contractuel. Bien que le délai de transmission par bond devienne variable, les autres facteurs tels que la vitesse des liaisons, la distance/nombre de bonds (et la taille de paquet dans le cas de l'ATM) restent constants.

9.2.2 Commutation de paquets sans connexion

Dans les réseaux à commutation de paquets sans connexion, une fois que les données sont envoyées, la connexion est rompue jusqu'à ce que d'autres informations soient envoyées ou reçues (un paquet peut être vu comme une connexion qui existe pour la durée pendant laquelle le paquet est émis et reçu). Aucun état de connexion n'est mémorisé et donc les paquets successifs ne suivent pas nécessairement le même chemin ni n'arrivent dans l'ordre dans lequel ils ont été envoyés. Le trafic est envoyé à des débits binaires variables et les ressources sont normalement allouées au fur et à mesure, sur la base du premier arrivé, premier servi.

Dans les réseaux CL-PS, (par exemple, les réseaux IP), les facteurs qui déterminent le retard tels que la taille de paquet, la vitesse de la liaison, le nombre de bonds, et le délai de transmission par bond sont variables, particulièrement lorsque des techniques sont utilisées pour fournir un équilibrage de charge. La limitation de débit et le formatage du trafic peuvent être implémentés en bordure pour limiter la quantité de trafic entrant dans un réseau, mais du fait de la nature de tous à tous du trafic CL-PS (qui est accru par le réseautage d'homologue à homologue), il est difficile de prédire l'utilisation de bande passante par liaison à travers un réseau CL-PS. La surveillance du trafic ainsi que les techniques de modélisation peuvent être utilisées pour développer une matrice de

trafic, et la métrique du protocole IGP peut être infléchie pour fournir une utilisation accrue des liaisons, mais du fait de la nature en salve et imprévisible du trafic CL-PS, la façon la plus simple/sûre d'assurer que les garanties de service seront satisfaites est de surprovisionner le réseau.

Cependant, même avec le surprovisionnement, du fait de la nature non déterministe du trafic sans connexion, les nœuds/liaisons dans un réseau CL-PS peuvent subir l'encombrement, particulièrement lors d'une défaillance de liaison/nœud ou d'attaque de déni de service (DoS). Aussi, l'impact d'une défaillance de liaison/nœud n'est pas limité au trafic qui traverse la liaison/nœud défaillant, le réacheminement peut causer l'encombrement ailleurs dans le réseau. Une approche courante pour protéger le trafic prioritaire de l'encombrement du réseau est d'utiliser la priorité fondée sur la mise en file d'attente (par exemple, sur la base de l'architecture de services différenciés pour IP de la RFC 2475) pour contrôler le comportement de transmission selon la classe, c'est-à-dire qu'une priorité de trafic supérieure reçoit un traitement préférentiel par rapport au trafic de priorité inférieure. Cela permet à un fournisseur d'offrir au consommateur plusieurs niveaux de service (par exemple, super, temps réel, au mieux) et de tarifer les services en conséquence. L'inconvénient de l'approche des Services différentiés (Diffserv) est que la bande passante ne peut être réservée que sur une base agrégée et donc la livraison de flux individuels ne peut être garantie dans un agrégat.

Une autre approche (ou complémentaire) est d'utiliser une Architecture de services intégrés (fondée sur la RFC 1633) dans laquelle le protocole de réservation de ressources (RSVP, RFC 2205) est utilisé pour réserver de la capacité le long d'un chemin de bout en bout en signalant les exigences d'un flux avant d'envoyer des paquets. Du fait que la bande passante peut être réservée flux par flux, il est possible de fournir une livraison garantie pour les flux individuels. Cela imite le modèle CAC utilisé dans les réseaux orientés connexion dans lesquels le trafic n'est pas envoyé tant que le CAC n'a pas été effectué pour s'assurer qu'il y a une capacité suffisante dans le réseau. Les inconvénients majeurs de cette approche sont qu'elle fait peser une charge de traitement significative (RSVP) sur les routeurs centraux, qui augmente proportionnellement avec le nombre de flux de paquets qui requièrent la réservation de ressources. Une autre approche qui prend en charge la réservation de ressources flux par flux est l'utilisation de routeurs sur la base du flux. Les routeurs fondés sur le flux maintiennent un état par flux et n'acceptent de nouveaux flux que s'il y a des ressources disponibles suffisantes. Comme avec RSVP, le défi de cette approche est que la charge de traitement augmente avec le nombre de flux. Cependant, il y a aujourd'hui des routeurs disponibles qui prennent en charge l'acheminement par flux pour un grand nombre de flux.

10 Fonctions requises pour l'établissement de VPN client/serveur

Un strict ordonnancement des événements qui doivent survenir doit être respecté dans l'établissement d'un VPN client/serveur. Les flux/connexions de couche client de VPN ne peuvent pas être établis tant que les flux/connexions de couche serveur de VPN n'ont pas été établis. De même, les flux/connexions de couche serveur de VPN ne peuvent pas être établis tant que les connexions/flux de couche serveur (pour lesquels la couche serveur de VPN est un client) n'ont pas été établis. Cet ordonnancement de l'établissement de flux/connexion est dû au fait qu'une topologie de couche client est déterminée par la topologie de la couche serveur sous-jacente, qui est récurrente jusqu'à la canalisation.

10.1 Etablissement de couche serveur de VPN

En supposant que la topologie de la couche serveur sous-jacente a été établie et que les TCP/TFP et CP/FP de la couche serveur de VPN ont été configurés avec des adresses, il y a trois étapes principales qui sont impliquées dans l'établissement de la connectivité d'une couche serveur de VPN entre les membres d'une couche client de VPN:

Etape 1: découvrir les membres du VPN et mémoriser les informations d'adhésion au VPN.

Etape 2: calculer les routes entre les membres du VPN à la couche serveur de VPN.

Etape 3: établir les connexions/tunnels/VLAN entre les membres du VPN à la couche serveur de VPN.

Chacune des fonctions nécessaires à la prise en charge de l'établissement et la maintenance de la couche serveur de VPN ainsi que les entités fonctionnelles individuelles sont décrites plus en détail dans le Tableau 10-1.

Tableau 10-1/Y.1314 – Fonctions de couche serveur de VPN

Fonction	Entités fonctionnelles	Eléments de réseau	Mode de couche serveur de VPN
Découverte des membres du VPN	Découverte des membres du VPN (CP/FP de couche client de VPN appartenant au même VPN)	PE	Tous
	Distribution/collecte des informations sur les membres du VPN (y compris adhésions, départs, disponibilité)	PE	Tous
	Information maintenance des membres du VPN	PE	Tous
	Mappage des CP/FP de la couche client de VPN aux AP de la couche serveur de VPN	PE	Tous
Acheminement de couche serveur de VPN	Distribution/collection des informations d'accessibilité/topologie/ressources de couche serveur de VPN	PE, P	Tous
	Maintenance des informations d'accessibilité/topologie/ressources de couche serveur de VPN	PE, P	Tous
	Calcul de la ou des meilleures routes entre AP de couche serveur de VPN	PE, P	Tous
Etablissement de tunnel/connexion de couche serveur de VPN	Contrôle d'admission de connexion (CAC)	PE, P	Tous
	Notification de succès/échec de demande de connexion/tunnel	PE, P	Tous
	Allocation et configuration de champs de démultiplexage de couche serveur de VPN	PE, P	Tous
	Distribution d'informations de connexion/tunnel, par exemple de qualité de service, de champs de démultiplexage, de bande passante, etc.	PE, P	Tous

10.1.1 Découverte des membres du VPN

Pour établir une topologie de couche serveur de VPN entre les extrémités fournisseur, il est nécessaire tout d'abord de déterminer quelles extrémités fournisseur sont connectées aux extrémités client qui sont membres du VPN client/serveur particulier. Cette fonction peut être effectuée manuellement par un opérateur humain sur la base de la topologie de réseau connue. Autrement, cette fonction peut être effectuée de façon dynamique via un serveur/système centralisé ou un protocole distribué afin d'automatiser/simplifier le processus d'approvisionnement. Pour prendre en charge la découverte dynamique, les extrémités fournisseur doivent être configurées avec des identificateurs de VPN pour indiquer qu'elles sont connectées à une ou plusieurs extrémités client qui appartiennent à un VPN particulier. Un exemple de serveur/système centralisé pour la découverte est l'utilisation d'un serveur d'authentification (par exemple RADIUS) pour distribuer les informations sur les membres d'un VPN au titre du processus d'authentification du client. Un exemple de protocole distribué est l'utilisation de BGP pour les réseaux virtuels privés de la

RFC 2547, qui utilisent les cibles d'acheminement comme identificateurs de VPN pour s'assurer que seules les extrémités fournisseur reçoivent les informations sur les VPN dont ils sont membres.

10.1.2 Acheminement de couche serveur de VPN

Si la couche serveur sous-jacente (la couche en dessous de la couche serveur de VPN) entre les points de terminaison de source/puits de couche serveur de VPN est une connexion ou un flux point à point à un seul bond, aucun acheminement n'est alors nécessaire car il n'y a qu'une seule route/chemin disponible. D'un autre côté, s'il y a des chemins/routes de remplacement à travers des nœuds intermédiaires pour la même destination, ou si la couche serveur sous-jacente fournit une topologie de point à multipoint[4], l'acheminement doit alors être effectué à la couche serveur de VPN afin de découvrir la topologie et/ou de calculer la ou les meilleures routes jusqu'à la destination.

10.1.2.1 Besoin d'acheminement

Dans le cas de réseau de couches orientées connexion, la signalisation ne peut pas avoir lieu tant qu'une route/chemin n'a pas été calculé à la couche concernée. Dans le cas de réseau de couche sans connexion, un paquet ne peut pas être transmis tant qu'une route pour la destination n'a pas été calculée/configurée. Ceci ne veut pas dire que chaque nœud dans le réseau doit avoir une route explicite pour chaque autre nœud dans le réseau. Le résumé d'adresse réseau est communément utilisé en conjonction avec la hiérarchie de domaine d'acheminement pour améliorer l'échelonnement. La forme ultime de résumé d'adresse est l'utilisation de routes par défaut, qui peuvent être utilisées comme mécanisme "attrape-tout" pour transmettre un paquet sans considération de son adresse de destination.

Une exception à la règle qu'un paquet sans connexion ne peut être transmis tant qu'une route n'a pas été calculée (ou une route par défaut configurée) est lorsque la technologie sans connexion prend en charge la diffusion. La diffusion se réfère à la réplication et transmission de paquets avec des adresses de destination inconnues à travers tout chemin de couche serveur dans la topologie (excepté le chemin sur lequel le paquet a été reçu). Un exemple de technologie qui prend en charge cette fonctionnalité est Ethernet. Une autre exception à la règle est la façon dont fonctionnent les réseaux à anneaux de jetons. Dans les réseaux de couches en anneau à jetons, lorsqu'un nœud reçoit un paquet, il retransmet le paquet en l'envoyant au prochain nœud de l'anneau jusqu'à ce qu'il revienne au nœud source où il est retiré. Le nœud de destination retient une copie de la trame et indique qu'il a reçu la trame en mettant les bits de réponse dans la trame. Bien qu'il y ait des technologies qui ne requièrent pas d'acheminement, il faut noter que ces technologies ne sont pas idéales comme technologies de couche serveur de VPN. Pour les réseaux de couches à étalonner avec un grand nombre de nœuds sur une grande zone géographique, l'acheminement et des structures d'adresse hiérarchisées sont des exigences fondamentales. Des mécanismes tels que la diffusion et le passage de jetons sont non sûrs par nature du point de vue d'un VPN et sont très inefficaces pour la transmission de trafic en monodiffusion (point à point).

10.1.2.2 Exemple de topologies de réseau requérant un acheminement

La Figure 10-1 donne un exemple d'un réseau où il y a deux routes/chemins (A et B) possibles pour la même destination.

---

[4] La référence à point à multipoint renvoie ici à la topologie de couche serveur sortante du point de vue d'une seule source d'extrémité fournisseur. La topologie globale réelle de réseau de couche pourrait être tous à tous fondée sur un maillage complet/partiel de connexions/flux bidirectionnels entre extrémités fournisseur.

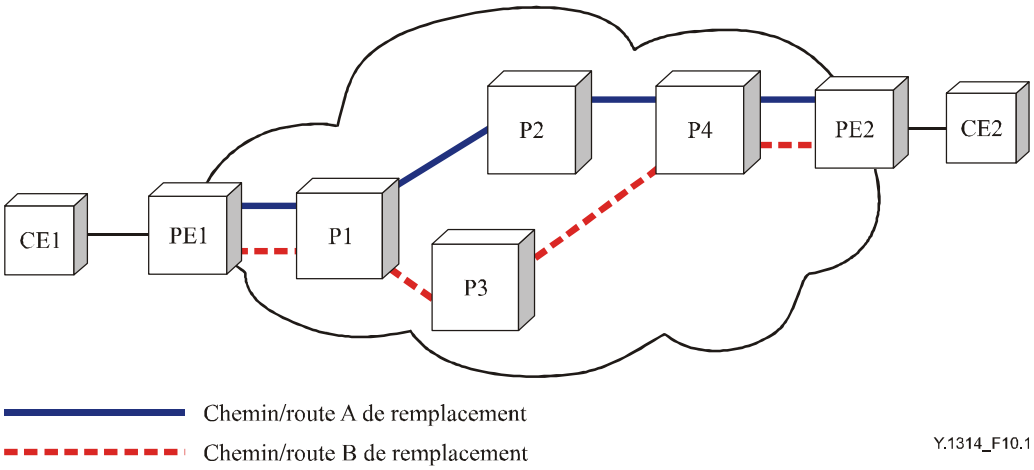


Figure 10-1/Y.1314 – Multiples routes/chemins pour la même destination

Comme l'indique la Figure 10-1, la route A du CE1 au CE2 passe à travers PE1, P1, P2, P4 et PE2, tandis que la route B passe à travers PE1, P1, P3, P4 et PE2. Ces informations sont décrites en utilisant le modèle fonctionnel de la Figure 10-2.

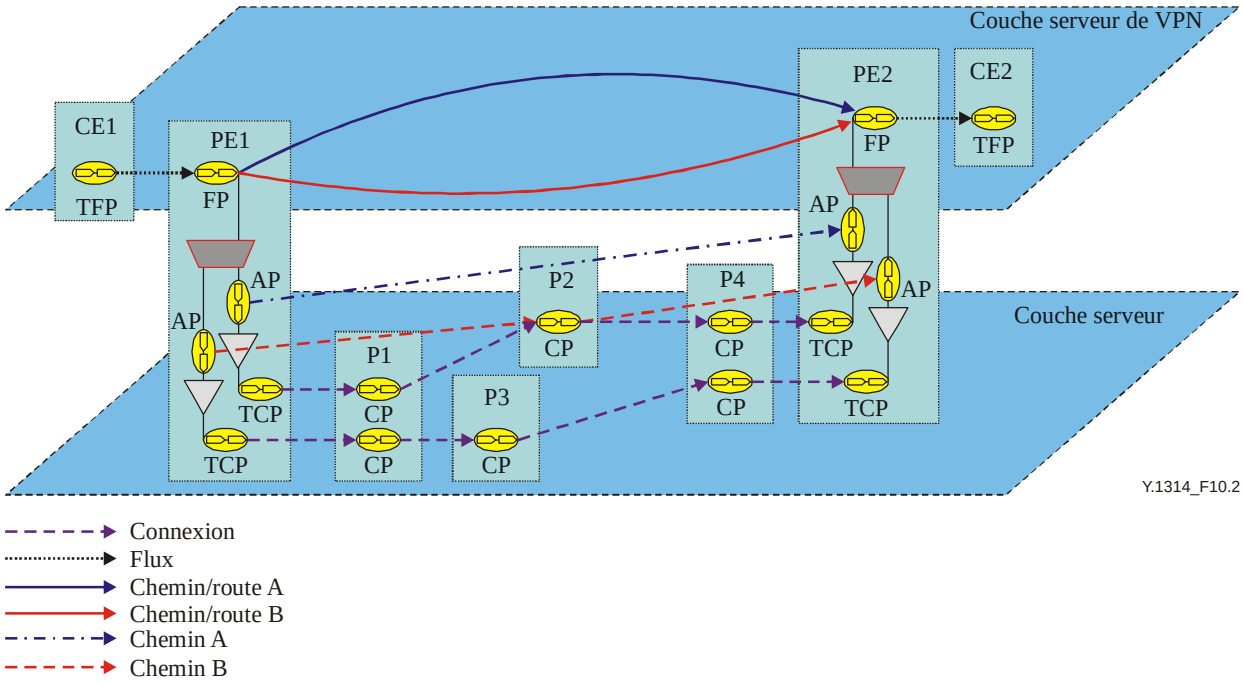


Figure 10-2/Y.1314 – Modèle fonctionnel pour chemins/routes multiples

La Figure 10-2 montre un choix de deux chemins de couche serveur (A et B) qui peuvent être utilisés par la couche serveur de VPN. Sur la base de la route calculée via la fonction d'acheminement à la couche serveur de VPN, un des chemins de couche serveur sera choisi (ou les deux si l'équilibrage de charge est nécessaire) afin de transmettre le ou les flux de couche serveur de VPN entre le point de flux de terminaison de source de couche serveur de VPN situé en CE1 et le TFP puits situé en CE2.

La Figure 10-3 montre le cas où une couche serveur fournit la connectivité de point à multipoint de CE1 (la source) à CE2, CE3, et CE4 (les puits de branche dans la topologie de point à multipoint).

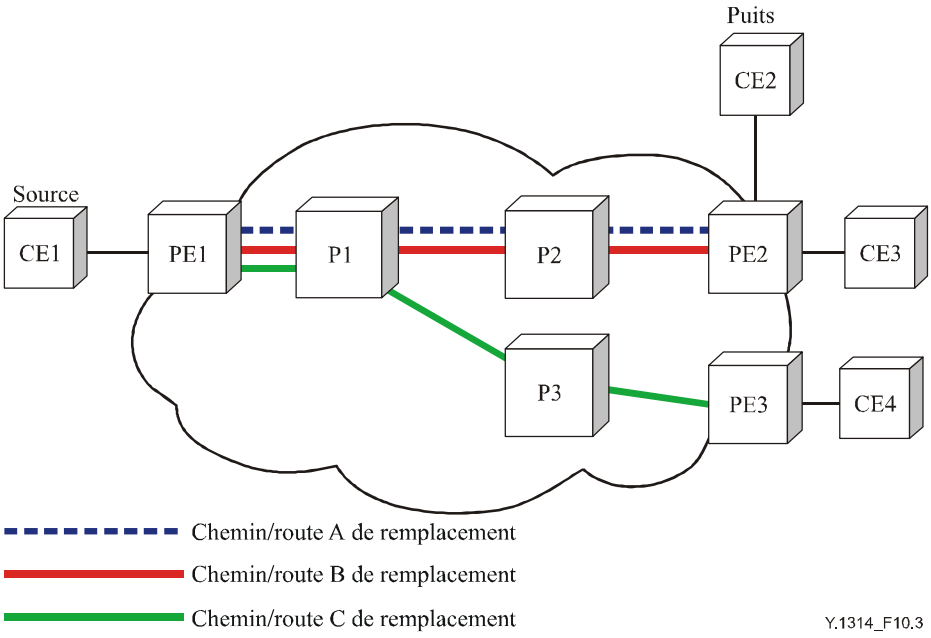


Figure 10-3/Y.1314 – Topologie de couche serveur en point à multipoint

Le réseau est montré à la Figure 10-3 comme un modèle fonctionnel de la Figure 10-4.

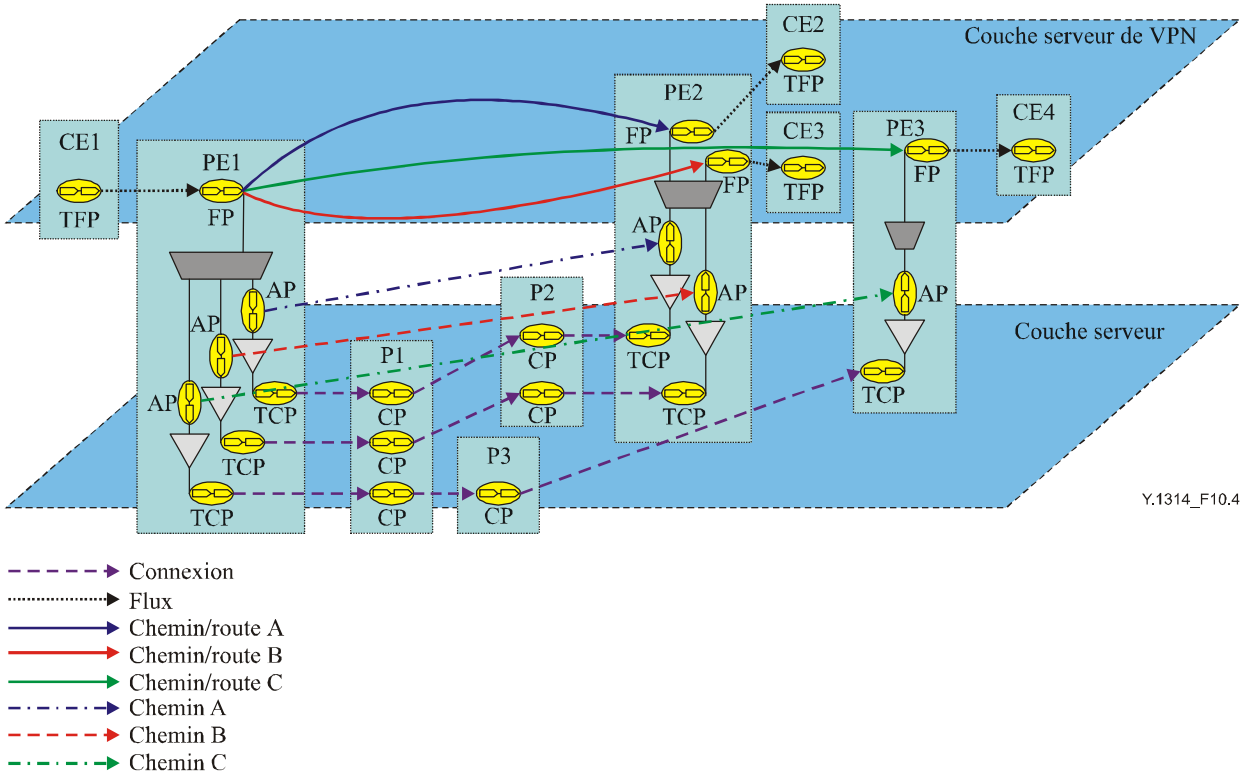


Figure 10-4/Y.1314 – Modèle fonctionnel de topologie de couche serveur en point à multipoint

Si CE1 est la source et CE2 le puits pour un flux de couche serveur de VPN particulier, CE1 a alors besoin de savoir quelle est la route pour atteindre CE2. Cependant, les routes/chemins à la couche serveur de VPN montrés à la Figure 10-4 sont fournis par des chemins de point à point dans la couche serveur sous-jacente, c'est-à-dire qu'il existe seulement une route depuis le point de terminaison de flux de source jusqu'à chaque TFP puits de branche dans la topologie de point à multipoint. Cela signifie que la fonction d'acheminement a seulement besoin de découvrir la topologie, elle n'a pas besoin d'effectuer les calculs de routage (puisqu'il n'existe qu'une seule route pour chaque puits). A la suite de la découverte de la topologie, les flux provenant de CE1 et destinés à CE2 utiliseront la route/le chemin A, fourni par le chemin de couche serveur A.

10.1.2.3 Autres approches d'acheminement

Lorsque l'acheminement est nécessaire, un opérateur humain peut effectuer la fonction d'acheminement, auquel cas il calcule les routes à travers le réseau sur la base de la topologie de réseau connue et des informations sur l'utilisation des ressources. Un exemple d'acheminement effectué manuellement est celui de la configuration de nœuds d'extrémité client à rattachement dual lorsque la couche client de VPN est fondée sur IP. Dans cet exemple, il peut valoir la peine d'utiliser des routes statiques (c'est-à-dire une route primaire et une route par défaut flottante) car il n'existe d'alternative qu'entre deux routes.

Si on utilise un système de gestion de réseau (NMS, *network management system*) pour effectuer la fonction d'acheminement, le système de gestion doit alors découvrir la topologie du réseau en demandant ou en collectant les informations d'accessibilité/topologie/ressources, et utiliser ensuite ces informations pour calculer les routes et distribuer les informations d'acheminement aux nœuds du réseau. Un exemple d'acheminement effectué par un NMS est l'établissement de connexions point à point à travers une couche de réseau fondée sur SDH. Avant que les connexions ne puissent être établies, le NMS doit d'abord calculer la ou les meilleures routes à travers le réseau.

Si on utilise un protocole d'acheminement dynamique pour effectuer la fonction d'acheminement, les informations d'accessibilité/topologie/ressources sont distribuées à travers le réseau via le protocole d'acheminement à chaque nœud et utilisées pour calculer le meilleur chemin/route pour atteindre chaque destination. Un exemple de protocole d'acheminement dynamique est le composant d'acheminement d'interface réseau privé à réseau public (PNNI) utilisé pour une couche de réseau ATM (bien qu'elle puisse aussi être utilisée avec d'autres technologies de réseau) pour découvrir la topologie du réseau et calculer les routes pour les connexions dynamiques. Un autre exemple est l'anneau de paquet résilient (RPR), qui utilise les messages de topologie pour découvrir la topologie d'anneau. Lorsqu'un nœud reçoit un message de topologie, il y ajoute son adresse MAC et le passe au nœud suivant sur l'anneau, et à la fin le paquet retourne à sa source avec une carte topologique (liste des adresses) de l'anneau.

Une solution de remplacement à l'utilisation d'un protocole d'acheminement dynamique dans le plan de contrôle est d'utiliser l'acquisition d'adresse dans le plan des données. Ethernet est un exemple de technologie de réseau qui utilise ce mode de fonctionnement. Ethernet utilise un arbre d'expansion (en élaguant la topologie du réseau pour éviter des boucles) et le pontage transparent (fondé sur l'acquisition d'adresse source) dans le plan des données pour transmettre les paquets à la destination correcte sans avoir à les diffuser à tous les nœuds/stations terminales. Cependant, si l'acquisition d'adresse dans le plan des donnés est utilisée, la technologie de réseau doit alors aussi prendre en charge la diffusion pour transmettre les paquets avec des adresses de destination qui n'ont pas encore été acquises. Du fait que les routes ne sont pas connues tant que les paquets avec les adresses correspondantes n'ont pas été reçus, l'acquisition d'adresse dans le plan des données ne peut pas être utilisée pour effectuer les fonctions d'acheminement pour les réseaux de couches orientées connexion, elle ne convient que pour les réseaux de couches sans connexion.

10.1.3 Signalisation de couche serveur de VPN

Pour les besoins de la présente Recommandation, la signalisation se réfère à l'échange d'informations nécessaires pour l'établissement de tunnels sans connexion (par exemple des tunnels du protocole de création de tunnel de couche 2) et de connexions orientées connexion (par exemple, des identificateurs de canal et de conduit virtuel ATM). Les informations nécessaires incluent des paramètres tels que les champs de multiplexage/démultiplexage, de qualité de service (par exemple, délai, gigue), de bande passante, de clés de chiffrement, et de résilience (par exemple, protection 1+1).

Une des différences-clés entre tunnels et connexions est que les connexions exigent toujours de la signalisation (ou un approvisionnement manuel) pour établir les connexions avant l'envoi de toutes données d'utilisateur. Bien que certaines techniques de tunnelage (par exemple, les tunnels L2TP, les tunnels GRE explicitement configurés) exigent aussi la signalisation des paramètres de tunnel avant l'envoi des données d'utilisateur, d'autres n'exigent aucune signalisation comme les tunnels GRE doux/dynamiques et dans IP. Ces techniques de tunnelage incorporent simplement un paquet de couche client de VPN dans un en-tête de paquet de couche serveur de VPN sur la base des informations de politique/acheminement local. Les nœuds (fournisseur) intermédiaires rencontrés entre les points de terminaison de source/puits de tunnel regardent seulement l'en-tête de paquet de couche serveur de VPN pour déterminer s'il faut transmettre le paquet vers le puits de couche serveur de VPN (extrémité fournisseur de destination) et comment le faire. Les en-têtes de couche client de VPN ne sont utilisés qu'une fois que le paquet atteint l'extrémité fournisseur de destination où est situé le puits de couche serveur de VPN. Noter aussi que souvent les nœuds intermédiaires ne seraient pas capables de donner un sens (par exemple être capables d'acheminer) aux en-têtes internes de couche client de VPN.

Le contrôle d'admission de connexion (CAC) est effectué au moment de l'établissement de la connexion pour déterminer si une bande passante suffisante est disponible dans la couche serveur sous-jacente pour soutenir les exigences de qualité de service de la couche client. Les descripteurs de trafic (par exemple, le débit de crête de cellule (PCR, *peak cell rate*) et le débit de cellules soutenu (SCR, *sustained cell rate*) utilisés en ATM) sont utilisés durant la signalisation de couche client pour demander les ressources appropriées de la part de la couche serveur sous-jacente. La capacité à déterminer quelle quantité de bande passante est disponible à la couche serveur sur la base d'une demande de la part d'une couche client signifie que la fonction CAC doit regarder dans le plan de contrôle par rapport à la fois aux couches serveur et client.

Dans le cas de couches serveur CO-CS, le CAC est fondé sur la quantité de bande passante physique disponible au réseau de couche auquel il est demandé (par exemple des intervalles de temps TDM disponibles ou des longueurs d'onde WDM). Dans le cas de réseau serveur CO-PS, le CAC se fonde sur la quantité de bande passante disponible qui n'est pas utilisée par les connexions existantes. Ces informations sont rendues disponibles en entretenant des informations sur l'état (par exemple montant/descendant, quantité de ressources utilisées) de chacune des connexions à chaque nœud pour ce réseau de couche particulier. A la différence des réseaux de couches CO-CS dans lesquelles la bande passante disponible est limitée par la bande passante physique disponible, dans les réseaux CO-PS, la politique de connexion doit être effectuée (particulièrement si on suppose un multiplexage statistique) à chaque nœud dans le réseau pour s'assurer que chaque connexion n'émet(ne reçoit) que la quantité de trafic acceptée pendant l'établissement de la connexion.

Dans le cas de réseaux de couche serveur CL-PS, le CAC peut être effectué sur la base de la bande passante disponible à l'interface physique/logique, ou d'une file d'attente/flux/classe de niveau de service. Comme avec les réseaux de couche CO-PS, la politique doit être effectuée à chaque nœud dans le réseau sur la base de la bande passante demandée. Cependant, à la différence du cas CO-PS où l'état est maintenu pour chaque connexion, les informations équivalentes (c'est-à-dire par flux)

ne sont pas normalement maintenues dans les réseaux de couche sans connexion[5]. Ceci, combiné avec la nature tous à tous non déterministe du trafic sans connexion, signifie que le CAC, dans les réseaux de couche sans connexion, repose sur l'utilisation d'une surveillance et d'une modélisation extensives du trafic pour développer une matrice de trafic, conjointement avec le surprovisionnement du réseau pour s'assurer que la bande passante est disponible, particulièrement dans des conditions de défaillance. Si un contrôle d'admission de connexion dur et des accords de niveau de service élevés sont demandés pour le VPN, on devrait alors utiliser un réseau de couche serveur orienté connexion plutôt qu'un réseau de couche serveur sans connexion.

10.2 Authentification/configuration de couche client de VPN

Les fonctions nécessaires pour établir la connectivité entre les nœuds d'extrémité client et fournisseur à la couche client de VPN peuvent être effectuées en utilisant l'approvisionnement statique ou en utilisant des protocoles dynamiques. L'approvisionnement statique peut être effectué via une configuration manuelle ou via des systèmes de gestion de réseau automatisés. Les entités fonctionnelles impliquées dans l'établissement de la connectivité de couche client de VPN sont indiquées au Tableau 10-2.

Tableau 10-2/Y.1314 – Fonctions d'authentification et de configuration de couche client de VPN

Fonction	Entités fonctionnelles	Eléments de réseau	Mode de couche client de VPN
Authentification, autorisation, et comptabilité (AAA) de CE/utilisateur	Authentification: identification du CE/utilisateur fondée sur les paramètres d'authentification, par exemple, un nom d'utilisateur et un mot de passe valides	CE, PE	Tous
	Autorisation: alloue ou refuse l'accès aux ressources/services de couche client de VPN	CE, PE	Tous
	Comptabilité: mesure des ressources/services utilisés	CE, PE	Tous
Configuration d'élément de couche client de VPN	Allocation et configuration des adresses de couche client de VPN à travers les CP/FP et TCP/TFP de couche client de VPN	CE, PE	Tous
	Allocation et configuration des identificateurs de VPN à travers les CP/FP de couche client de VPN appartenant au même VPN	PE	Tous
	Configuration des profils et politiques par VPN	CE, PE	CO-PS, CL-PS

10.2.1 AAA de CE/utilisateur

La fonction AAA de CE/utilisateur contrôle l'accès à la couche client de VPN, met en application les politiques, prend en charge les audits d'utilisation, et fournit les informations nécessaires à la facturation des services de VPN. Les fonctions AAA peuvent être effectuées par l'appareil d'extrémité fournisseur auquel se connecte l'extrémité client, par un appareil séparé, ou par un mélange des deux.

Dans certains cas, un serveur d'authentification centralisé sera vraisemblablement nécessaire pour l'authentification de CE/utilisateur, et dans d'autres, seules les extrémités client et fournisseur seront impliquées dans le processus d'authentification. Un exemple du premier cas est lorsque

[5] Les exceptions incluent l'utilisation de RSVP de la RFC 2205 (solution fondée sur la signalisation de bout en bout) et l'acheminement d'état de flux (solution bond par bond), où l'état de chaque flux est maintenu et les nouveaux flux sont rejetés s'il n'y a pas assez de bande passante disponible.

IEEE 802.1X est utilisé pour l'authentification d'un appareil d'extrémité client Ethernet. Dans cet exemple, l'extrémité fournisseur serait l'authentifiant et un serveur d'authentification centralisé servirait à exécuter l'authentification. Un exemple du second cas est l'authentification des messages de contrôle (par exemple des messages BGP) envoyés par une extrémité client pour authentifier la source du message et se protéger contre les usurpations.

10.2.2 Configuration d'élément de réseau de couche client de VPN

Durant l'approvisionnement de couche client de VPN, les éléments de réseau à la bordure du consommateur et du réseau fournisseur doivent être configurés avec les paramètres suivants: adresses de réseau de couche VPN client, champs de démultiplexage de réseau de couche client, identificateurs de VPN, et politiques/profils par VPN. La configuration pourrait être effectuée durant le processus d'authentification/autorisation ou de façon indépendante. Un exemple du premier cas est après une authentification réussie, une extrémité client pourrait automatiquement être configurée avec une allocation de bande passante spécifique et un profil de marquage de paquet fondé sur les informations reçues d'un serveur d'authentification. Un exemple du second cas est l'utilisation d'une configuration manuelle ou du protocole de configuration de serveur dynamique (DHCP, *dynamic host configuration protocol*) pour allouer une adresse IP à une extrémité client.

Les adresses de couche client de VPN à configurer aux points de connexion/points de flux d'extrémité fournisseur et aux TCP/TFP ou CP/FP d'extrémité client sont les adresses appartenant à la couche client de VPN (par exemple adresses IP pour une cliente VPN IP ou adresses E.164/NSAP pour une cliente VPN en ATM).

Les champs de démultiplexage de réseau de couche client n'ont besoin d'être configurés que si plusieurs clients VPN sont transportés sur la même liaison d'extrémité client à extrémité fournisseur, ou si la technologie de couche client de VPN employée porte toujours un champ démultiplexage. Un exemple du premier cas est celui d'une couche client de VPN Ethernet, qui a seulement besoin d'utiliser des étiquettes de VLAN lorsqu'elle doit prendre en charge plusieurs VPN. Un exemple du second cas est celui de l'ATM, qui utilise toujours des valeurs d'identificateur VPI/VCI dans les en-têtes d'unités de trafic (cellules). Dans certains cas, la configuration du champ de démultiplexage dépendra de la configuration physique plutôt que de la configuration d'une valeur dans un en-tête de paquet (par exemple, rattacher une fibre à l'interface d'entrée correcte à l'extrémité fournisseur correspondant à la longueur d'onde DWDM de sortie correcte).

Bien qu'un identificateur VPN soit un nom utilisé pour identifier un VPN particulier et n'ait seulement besoin d'être alloué/configuré que si la prise en charge de la découverte et de la signalisation dynamique d'appartenance au VPN est exigée, il peut aussi être utile d'un point de vue opérationnel (par exemple, pour aider au dépannage, à la facturation). Un exemple d'identificateur VPN utilisé pour la découverte et la signalisation dynamique est l'attribut route cible utilisé pour les VPN de la RFC 2547. Un identificateur de VPN peut être configuré statiquement ou manuellement sur une extrémité fournisseur via un approvisionnement manuel/OSS, ou de façon dynamique (par exemple, au titre du processus d'authentification en utilisant RADIUS). Si l'identificateur de VPN est utilisé pour la découverte/signalisation, il devrait alors être unique au moins dans un seul domaine d'acheminement/signalisation (et dans l'idéal unique au monde si la prise en charge de VPN inter-AS/fournisseur est exigée).

La configuration de profils et politiques selon le VPN pour les clientes VPN fondées sur le paquet peut être nécessaire dans l'appareil d'extrémité client, dans l'appareil d'extrémité fournisseur, ou dans les deux. Parmi les exemples de profils et politiques de VPN qui peuvent avoir besoin d'être configurés en fonction du service VPN figurent la limitation de débit/le formatage du trafic, le marquage/la classification de paquet, et le choix de route/connexion pour les sites multirattachement (c'est-à-dire une primaire, une de secours).

10.3 Acheminement et signalisation de couche client de VPN

Comme avec la couche serveur de VPN, l'acheminement de couche client de VPN est nécessaire lorsqu'il existe plusieurs routes/chemins entre TCP/TFP source et puits, ou si les chemins de couche serveur de VPN créent une topologie de point à multipoint à la couche client de VPN. Si la couche client de VPN est orientée connexion et si l'approvisionnement dynamique doit être pris en charge à la couche client de VPN, la signalisation est alors aussi nécessaire.

Un point important à noter ici est que les chemins de couche serveur de VPN doivent être établis avant que ne puisse avoir lieu l'acheminement/signalisation de couche client de VPN. La topologie de plan de données de couche client de VPN est fondée sur la topologie des chemins de la couche serveur de VPN sous-jacente, et donc, il n'est pas possible d'effectuer de calcul de route ou de signaler des connexions/tunnels tant que les chemins de couche serveur de VPN n'ont pas été établis.

Les fonctions d'acheminement et de signalisation de couche client de VPN ainsi que les entités fonctionnelles individuelles sont décrites dans le Tableau 10-3.

Tableau 10-3/Y.1314 – Fonctions d'acheminement et signalisation de couche client de VPN

Fonction	Entité fonctionnelle	Eléments de réseau	Mode de couche client de VPN
Acheminement de couche client de VPN	Distribution/collecte d'informations d'accessibilité/topologie/ressource de couche client de VPN	CE, PE	Tous
	Maintenance d'informations d'accessibilité/topologie/ressource de couche client de VPN	CE, PE	Tous
	Calcul de la ou des meilleures routes entre points d'accès de couche client de VPN	CE, PE	Tous
Signalisation de tunnel/connexion de couche client de VPN	Contrôle d'admission de connexion (CAC)	PE, P	CO-CS, CO-PS
	Notification de réussite/échec de demande de connexion/tunnel	PE, P	Tous
	Allocation et configuration des champs de démultiplexage de couche client de VPN	PE, P	Tous
	Distribution des informations de connexion/tunnel de couche client de VPN, par exemple QS, champs de démultiplexage, bande passante, etc.	PE, P	Tous

10.3.1 Connectivité de tous à tous de couche client de VPN CL-PS

Si le chemin de couche serveur de VPN fournit une topologie de tous à tous à maillage complet/partiel pour une couche client de VPN CL-PS avec plusieurs sites, les nœuds contenant les TFP/FP de couche client de VPN (c'est-à-dire les nœuds d'extrémité fournisseur/client, mais pas les nœuds fournisseur) doivent prendre des décisions de transmission en ce qui concerne l'endroit où transmettre un paquet sur la base des informations d'adresse de couche client de VPN. Cela signifie que les nœuds d'extrémité client et fournisseur doivent échanger des informations d'acheminement de couche client de VPN en utilisant des protocoles dynamiques d'acheminement via le plan de contrôle, ou des routes statiques doivent être configurées en utilisant un approvisionnement manuel ou par le système d'assistance à l'exploitation. Une solution de remplacement à l'utilisation de protocoles d'acheminement dynamique ou de l'acheminement statique est d'utiliser l'acquisition d'adresse dans le plan de données, comme c'est le cas avec Ethernet qui utilise l'acquisition d'adresse fondée sur la source pour envoyer du trafic en monodiffusion à la destination correcte.

Les informations d'acheminement pour chaque VPN doivent être isolées des informations d'acheminement provenant des autres VPN. Ceci pour fournir la séparation de transmission des VPN (c'est-à-dire de s'assurer que les paquets ne sont pas acheminés aux nœuds appartenant à un VPN différent) et pour permettre d'utiliser des espaces d'adresse de couche serveur de VPN en recouvrement. Cela peut être obtenu en utilisant des extrémités fournisseurs séparées physiquement pour chaque VPN, ou des extrémités fournisseur communes avec des bases de données d'information d'acheminement logiquement/virtuellement séparées. Une autre solution serait d'utiliser des appareils d'extrémité fournisseur et des tableaux d'acheminement communs mais d'allouer des espaces d'adresse séparés pour chaque client du VPN[6]. Un exemple de solution VPN qui prend en charge l'acheminement à la couche serveur de VPN est celui de la RFC 2547. La RFC 2547 utilise l'acheminement dynamique ou statique d'extrémité client à extrémité fournisseur conjointement aux protocoles MP-BGP pour distribuer les informations d'acheminement de couche client de VPN entre les extrémités fournisseur et des tableaux séparés d'acheminement virtuel pour effectuer l'isolation de route de couche client de VPN.

10.3.2 Etablissement/suppression à la demande de connexion dynamique de couche client de VPN

Dans la plupart des cas, les connexions de couche client de VPN CO-CS et CO-PS seront configurées statiquement via l'approvisionnement manuel ou du système d'assistance à l'exploitation. Cependant, si l'établissement de connexion dynamique à la demande est nécessaire, il faut alors qu'ait lieu un examen attentif de l'appariement de plan de contrôle (acheminement et signalisation) à la couche client de VPN entre tous les points de connexion et points de connexion de terminaison (c'est-à-dire entre les nœuds d'extrémité fournisseur et les nœuds d'extrémité client). Le CAC doit aussi être effectué au moment de l'établissement de la connexion pour déterminer si une bande passante suffisante est disponible à la couche serveur de VPN pour la connexion de couche client de VPN. Cela signifie que la fonction CAC doit scruter à la fois les plans de contrôle de couche serveur de VPN et de couche client de VPN. Si les technologies de couche serveur et de couche client de VPN sont différentes, l'interaction de plan de contrôle d'homologue doit avoir lieu entre les couches VPN client et serveur.

10.3.3 Connexions à la demande contrôlées par le consommateur

Les connexions dynamiques à la demande sous le contrôle du consommateur se réfèrent au cas où celui-ci a un certain contrôle (ou un contrôle total) sur le nœud d'extrémité client, ce qui leur permet d'établir de nouvelles connexions de couche client de VPN. L'avantage de cette capacité du point de vue du consommateur est que cela lui donne la souplesse d'établir de façon dynamique les VPN comme et quand ils sont nécessaires, et d'être facturé en conséquence pour leur utilisation. Par exemple, un consommateur peut souhaiter établir une connexion à la demande pour une brève période pour télécharger un gros fichier (par exemple, un fichier d'application ou de vidéo) ou établir une connexion fiable pour une visioconférence. Un exemple d'utilisation d'établissement de connexion dynamique à la demande de couche client de VPN est l'utilisation de PNNI pour établir/supprimer des SPVC à travers des chemins de couche serveur de VPN fournis en utilisant des chemins virtuels.

Un facteur important à prendre en considération lorsqu'on envisage d'ajouter la prise en charge des connexions dynamiques à la demande de couche client de VPN est la distribution des informations d'adresse/topologie. Un fournisseur de services ne veut vraisemblablement pas dévoiler sa topologie de réseau ou l'adressage interne de réseau aux consommateurs, pour des raisons de sécurité. Il est

---

[6] Il y a plusieurs désavantages majeurs à cette approche: elle nécessite une gestion soigneuse de l'espace d'adresse par le fournisseur de service, l'accord du consommateur pour l'utilisation des adresses allouées par le fournisseur de service (le consommateur peut vouloir utiliser ses propres adresses), et le filtrage de paquet pour garantir l'isolation entre VPN, qui est une tâche fastidieuse et propice aux erreurs.

donc souhaitable que la fonction d'acheminement à l'extrémité fournisseur ne distribue les informations d'accessibilité qu'aux extrémités client. Une autre considération importante porte sur la décision des actions à entreprendre au moment de l'établissement de la connexion si la bande passante n'est pas disponible. La capacité à établir une nouvelle connexion de couche client de VPN dépend de la disponibilité des chemins de couche serveur entre les points de terminaison source et puits. S'il n'existe pas de chemin ou s'il n'y a pas assez de bande passante en réserve, la connexion doit être rejetée, ou une nouvelle connexion/tunnel de couche serveur de VPN doit être établie (ou la bande passante augmentée pour les connexions/tunnels existants). Pour établir de nouvelles connexions/tunnels de couche serveur de VPN ou augmenter la bande passante de connexions/tunnels existants, le CAC doit être effectué pour s'assurer que la bande passante est disponible dans la couche serveur sous-jacente.

Si la couche serveur est sans connexion, il n'est alors pas possible d'effectuer un CAC dur, et donc le réseau doit être surprovisionné pour permettre d'établir de nouveaux tunnels de couche serveur de VPN. Le désavantage de cette approche est qu'elle exige une planification et un contrôle/politique soigneux du réseau pour s'assurer que les tunnels de couche serveur de VPN existants n'en sont affectés d'aucune façon. Si la couche serveur sous-jacente est orientée connexion, on peut faire un CAC dur pour s'assurer que la bande passante est disponible pour établir de nouvelles connexions/tunnels de couche serveur de VPN. Cependant, chaque demande de connexion à la couche n a un impact sur la bande passante disponible à la couche n–1, et ceci est récurant jusqu'au conduit. Au fur et à mesure qu'on se rapproche du conduit, la granularité de la bande passante et les temps d'approvisionnement/garde augmentent pour les connexions. En général, s'il y a une insuffisance de capacité dans une couche serveur sous-jacente pour prendre en charge une nouvelle connexion, celle-ci devrait être rejetée. La capacité de couche serveur devrait être fournie comme résultat des activités de planification de capacités, y compris la modélisation du réseau et l'analyse/prévision de l'utilisation.

10.3.4 Connexions à la demande sous le contrôle du fournisseur de services

Les connexions dynamiques à la demande sous le contrôle du fournisseur de services se réfèrent au scénario dans lequel le fournisseur de services gère le nœud d'extrémité client et utilise l'acheminement/signalisation pour établir de façon dynamique des nouvelles connexions de couche serveur de VPN. L'avantage de cette capacité du point de vue des fournisseurs de services est qu'elle leur permet d'établir de façon dynamique des connexions de couche client de VPN de bout en bout plutôt que d'avoir à utiliser la configuration statique (c'est-à-dire manuelle ou par approvisionnement d'OSS). Un exemple de scénario où un établissement dynamique de couche client de VPN peut être utile est lorsque deux réseaux d'accès ATM ou plus sont interconnectés via un cœur MPLS. Dans cet exemple, PNNI pourrait être utilisé pour établir/supprimer les SPVC à la couche client de VPN à travers les chemins de couche serveur de VPN MPLS. Comme les technologies de couche client et serveur VPN sont différentes, l'interfonctionnement de niveau homologue dans le plan de contrôle doit avoir lieu.

Dans le cas de connexions dynamiques à la demande sous le contrôle du fournisseur de services, même si le fournisseur gère le nœud d'extrémité client au nom du consommateur, la distribution des informations d'adressage interne et de topologie aux extrémités client comporte un risque, par exemple, l'extrémité client est localisée dans les locaux du consommateur plutôt que chez le fournisseur. Une façon d'éviter ce risque pour la sécurité serait d'utiliser un approvisionnement statique/manuel entre l'appareil d'extrémité client et le nœud intermédiaire adjacent dans le réseau du fournisseur, et d'utiliser l'acheminement/signalisation dynamique depuis ce nœud jusqu'au retour à l'extrémité fournisseur. Par exemple, si la couche serveur de VPN est en ATM, le canal virtuel serait alors approvisionné manuellement entre l'extrémité client et le commutateur ATM du fournisseur auquel il est connecté, et ensuite, PNNI serait utilisé de bout en bout entre les commutateurs ATM. En ce qui concerne le contrôle de l'établissement de connexion/tunnel à des couches différentes dans la hiérarchie des réseaux de couches, comme le fournisseur contrôle les

connexions à la demande, le fournisseur a plus de contrôle sur ce qui se passe dans le réseau. Cependant, une planification soigneuse du réseau et la surveillance par le système de gestion du réseau des connexions à chaque couche doivent encore avoir lieu, particulièrement si le département responsable dans la compagnie de la gestion de couche client de VPN est différent du département responsable de la gestion de couche serveur de VPN (et des couches serveurs en dessous).

11 Fonctions nécessaires à l'établissement de VPN de niveau homologue

En supposant que la topologie de la couche serveur sous-jacente ait été établie et que les TFP et FP de couche VPN homologue aient été configurés avec les adresses, trois étapes principales sont impliquées dans l'établissement de la connectivité de couche VPN homologue entre membres du VPN:

Etape 1: découvrir et authentifier les membres du VPN et mémoriser les informations d'adhésion au VPN.

Etape 2: calculer les routes entre les membres du VPN à la couche VPN homologue.

Etape 3: configurer les éléments de réseau de couche VPN homologue pour fournir l'isolation du VPN.

Chacune des fonctions requises pour prendre en charge l'établissement et la maintenance de couche VPN homologue ainsi que des entités fonctionnelles individuelles est décrite plus en détail au Tableau 11-1.

Tableau 11-1/Y.1314 – Fonctions de couche serveur de VPN

Fonction	Entités fonctionnelles	Eléments de réseau
Découverte des membres du VPN	Découverte des membres du VPN	CE/PE
	Distribution/collecte des informations d'adhésion au VPN (y compris adhésions, départs, disponibilité)	CE/PE
	Maintenance des informations d'adhésion au VPN	CE/PE
Authentification, autorisation, et comptabilité (AAA) d'extrémité client/utilisateur	Authentification: identification de CE/utilisateur sur la base des paramètres d'authentification, par exemple, un nom d'utilisateur et un mot de passe valides	CE, PE
	Autorisation: accorder ou refuser l'accès aux ressources/services de couche serveur de VPN	CE, PE
	Comptabilité: mesurer les ressources/services utilisés	CE, PE
Acheminement de couche VPN homologue	Distribution/collecte des informations d'accessibilité/topologie/ressources de couche VPN homologue	CE, PE, P
	Maintenance des informations d'accessibilité/topologie/ressources de couche VPN homologue	CE, PE, P
	Calcul de la ou des meilleures routes entre les points d'accès de couche VPN homologue	CE, PE, P
Configuration d'élément de réseau de couche VPN homologue	Configuration des filtres de paquet par VPN	PE
	Configuration des filtres d'acheminement par VPN	PE
	Configuration et échange des clés de chiffrement par VPN/CE	ES, CE, PE
	Allocation et configuration des identificateurs de VLAN	CE, PE, P

11.1 Découverte des membres du VPN

Dans les scénarios de VPN de niveau homologue approvisionné par le consommateur où le VPN est transparent pour le fournisseur (par exemple, un VPN IPsec sur l'Internet), il est nécessaire avant d'établir le VPN de déterminer d'abord toutes les extrémités client qui appartiennent au VPN. Dans les scénarios de VPN approvisionné par le fournisseur (par exemple, des VPN fondés sur des VLAN Ethernet), le fournisseur doit découvrir quelles extrémités fournisseur sont connectées à des extrémités client qui sont membres du VPN. La découverte peut être effectuée manuellement par un opérateur humain sur la base de la topologie de réseau connue, ou peut être effectuée de façon dynamique via un serveur/système centralisé ou un protocole distribué.

11.2 Authentification, autorisation, et comptabilité (AAA) de CE/utilisateur

Une fonction AAA d'extrémité client/utilisateur est utilisée dans les scénarios de VPN approvisionné par le fournisseur pour contrôler l'accès aux ressources de couche VPN homologue. AAA est aussi utilisée pour mettre en application les politiques, pendre en charge les audits d'utilisation, et pour fournir les informations nécessaires à la facturation des services de VPN au consommateur. La fonction AAA peut être effectuée par une extrémité fournisseur, par un appareil séparé, ou en utilisant un mélange des deux. Par exemple, si IEEE 802.1X est utilisé pour authentifier une extrémité client pour un VPN fondé sur un VLAN Ethernet, l'extrémité fournisseur serait un authentifiant et un serveur d'authentification centralisé pourrait être utilisé pour mener à bien l'authentification.

11.3 Acheminement de couche VPN homologue

Lorsqu'il existe des chemins/routes de remplacement entre des membres du VPN, l'acheminement doit être effectué à la couche VPN homologue afin de découvrir la topologie et/ou calculer la ou les meilleures routes entre les membres du VPN. Comme les nœuds d'extrémité client, d'extrémité fournisseur et de fournisseur appartiennent tous à la couche VPN homologue, les trois types de nœud sont impliqués dans tout calcul de route/chemin. La fonction d'acheminement peut être effectuée manuellement par un opérateur humain, ou peut être effectuée de façon dynamique via un serveur/système centralisé ou un protocole d'acheminement distribué. Pour les besoins de la présente Recommandation, l'acheminement inclut le pontage transparent fondé sur l'acquisition d'adresse de source dans le plan des données.

11.4 Configuration d'élément de réseau de couche de VPN homologue

Il y a un grand nombre de fonctions de remplacement pour fournir l'isolation de VPN. Une option est de configurer des filtres de paquet par VPN sur des nœuds d'extrémité fournisseur partagés pour s'assurer d'une pleine accessibilité entre les sites d'un même utilisateur, et de l'isolation entre utilisateurs. Une autre option est d'utiliser des nœuds d'extrémité fournisseur dédiés et de configurer des filtres de route de telle sorte que bien que les nœuds fournisseurs contiennent toutes les routes des utilisateurs, les nœuds d'extrémité fournisseur ne contiennent que les routes d'un seul utilisateur. Le filtrage de paquet/route n'est applicable qu'aux scénarios de VPN approvisionné par le fournisseur et donc ils doivent être menés à bien par les nœuds d'extrémité fournisseur.

En remplacement de l'utilisation du filtrage de route/paquet lorsque la connectivité existe entre les utilisateurs (par exemple à travers l'Internet) on peut utiliser le chiffrement de paquet. L'utilisation du chiffrement de paquet assure que si les utilisateurs reçoivent des paquets d'un VPN auquel ils n'appartiennent pas, ils ne peuvent obtenir les données contenues dans le paquet. Le chiffrement de paquet est effectué par les nœuds d'extrémité fournisseur pour les VPN approvisionnés par le fournisseur et par les nœuds d'extrémité client ou par des systèmes terminaux pour les VPN approvisionnés par l'utilisateur.

Les types courants de cryptographie utilisés pour prendre en charge le chiffrement/déchiffrement incluent la cryptographie à clé secrète et la cryptographie à clé publique. La cryptographie à clé

secrète est la plus convenable pour des groupes fermés d'utilisateurs où les clés secrètes peuvent être conservées et distribuées de façon sécurisée par une autorité unique, par exemple dans un environnement de VPN d'entreprise. L'avantage de la cryptographie à clé publique est qu'elle permet aux utilisateurs de communiquer en toute sécurité sans avoir accès préalablement à une clé secrète partagée. Cette approche utilise deux clés, une clé privée qui est gardée secrète et une clé publique qui doit être distribuée à tous les membres du VPN. Les clés publiques et privées sont en relation mathématique et quiconque ne possède pas une clé privée spécifique ne peut décrypter les informations dans le paquet chiffré. Un usage courant de la cryptographie à clé publique est l'échange des clés secrètes à utiliser pour la cryptographie à clé secrète.

Lorsque Ethernet est utilisé comme technologie de couche VPN homologue, l'isolation de VPN peut être réalisée en allouant et configurant les VLAN. Les VLAN sont normalement alloués et configurés manuellement ou via l'OSS, bien que des protocoles dynamiques puissent aussi être utilisés. Pour fournir la connectivité de bout en bout entre les extrémités client, les VLAN doivent être configurés correctement sur les nœuds d'extrémité client, d'extrémité fournisseur et de fournisseur.

12 Fonctions OAM de VPN

Les outils et fonctions OAM sont essentiels pour maintenir l'efficacité du fonctionnement dans les réseaux à grande échelle. Des exemples de caractéristiques importantes de connexion/flux de réseau porté via les fonctions OAM incluent la qualité, l'intégrité et la validité. Si un réseau de couche ne prend pas en charge l'OAM ou a des fonctionnalités OAM manquantes, ce réseau de couche particulier est fonctionnellement déficient par rapport à cette fonctionnalité OAM. Des fonctions/outils OAM de couche supérieure/inférieure ne peuvent pas être utilisés en remplacement/substitut pour fournir la même fonctionnalité, en particulier lorsqu'il s'agit de localisation de faute. Ceci ne signifie pas qu'il est impossible de fournir des services VPN en utilisant des technologies de réseau auxquelles manqueraient des fonctions OAM. Cependant, une fonctionnalité OAM manquante va vraisemblablement accroître de façon significative les coûts et la complexité du fonctionnement.

Le Tableau 12-1 présente certaines des fonctions-clés d'OAM et identifie les éléments de réseau qui devraient prendre en charge les fonctions associées.

Tableau 12-1/Y.1314 – Fonctions OAM client/serveur

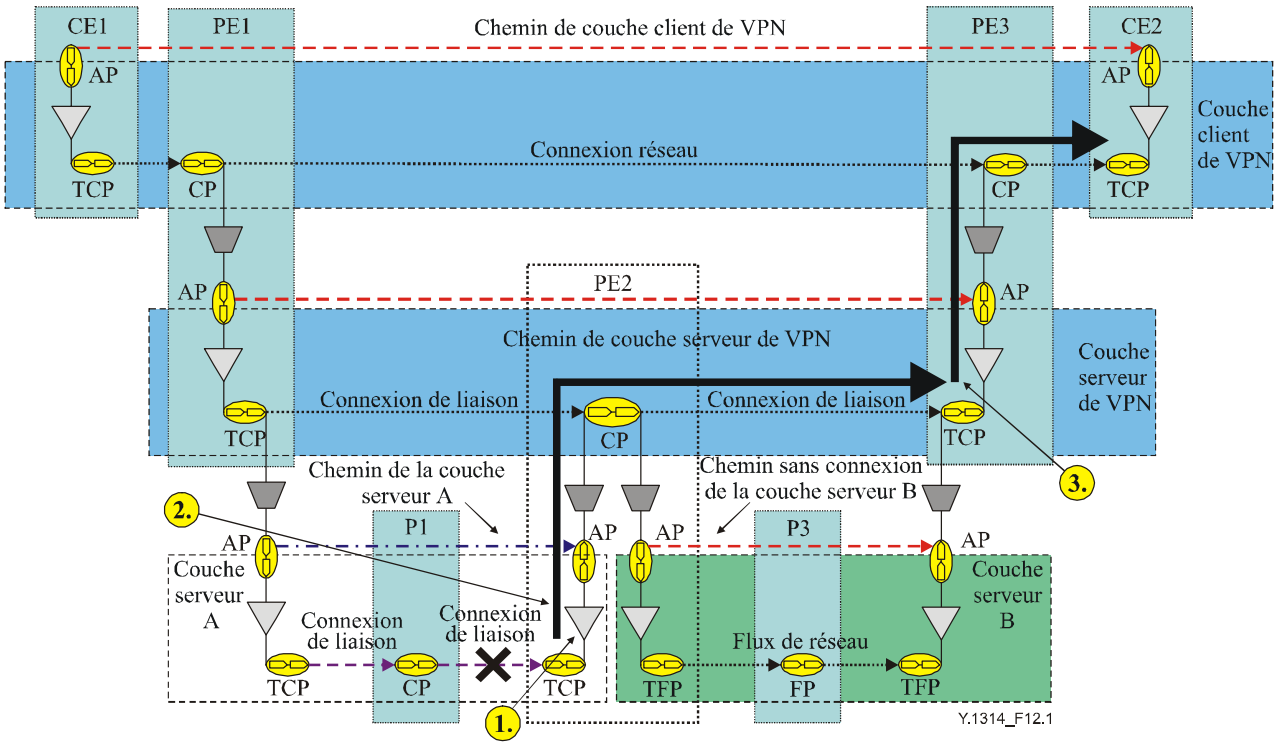
Fonction	Entités fonctionnelles	Eléments de réseau
OAM de couche client de VPN	Détection/gestion de faute de couche client de VPN	CE et PE
	Surveillance des performances de couche client de VPN	CE et PE
	Activation et désactivation d'OAM de couche client de VPN	CE et PE
OAM de couche serveur de VPN	Détection/gestion de faute de couche serveur de VPN	PE et P
	Surveillance des performances de couche serveur de VPN	PE et P
	Activation et désactivation d'OAM de couche serveur de VPN	PE et P
OAM de couche homologue de VPN	Détection/gestion de faute de couche homologue de VPN	CE, PE, P (tous)
	Surveillance des performances de couche homologue de VPN	CE, PE, P (tous)
	Activation et désactivation d'OAM de couche homologue de VPN	CE, PE, P (tous)

12.1 Gestion des fautes

La gestion des fautes inclut la détection, la localisation, la correction des fautes et les essais diagnostiques à la demande. Les défauts doivent être détectés et traités au point de terminaison puits de connexion/flux dans le réseau de couche dans lequel ils surviennent. Si tel n'est pas le cas, il en résultera des indications de faute ambiguës, ce qui augmente de façon significative la complexité de fonctionnement et le temps mis à résoudre une faute. Dès la détection d'une défaillance, outre la génération et l'envoi d'alarmes au système de gestion de réseau (NMS), pour empêcher des tempêtes d'alarmes dans les réseaux de couches client, un signal d'indication de défaut vers l'avant (FDI, *forward defect indication*) ou un signal d'indication d'alarme (AIS, *alarm indication signal*) devrait être passé au ou aux réseaux de couche client en utilisant la syntaxe appropriée de l'OAM utilisé par la technologie particulière (s'il en existe une) de couche client affectée.

Le mécanisme de détection de faute le plus important est l'utilisation de la vérification de connectivité (CV, *connectivity verification*), qui est une exigence commune aux trois modes de réseautage. Dit simplement, cela demande à la source d'un flux de trafic de s'identifier de façon déterministe (de quelque façon que ce soit) auprès du puits. La façon de le réaliser dépend du mode de réseautage et est expliquée dans les paragraphes suivants. La localisation de faute est une autre exigence clé commune aux trois modes de réseautage afin de déterminer la cause fondamentale d'une défaillance. En plus des informations sur la défaillance initiale, des outils d'essai diagnostique à la demande peuvent être utilisés pour localiser la faute.

Un exemple de scénario de défaillance dans une couche serveur de VPN est décrit du point de vue fonctionnel à la Figure 12-1.



1. *La couche serveur A détecte une perte de continuité sur la base de la non-réception de paquets de vérification de connexion*
2. *La couche serveur A transmet une FDI à la couche serveur du VPN*
3. *La couche serveur de VPN reçoit une FDI et la propage jusqu'à la couche client de VPN*

Figure 12-1/Y.1314 – Propagation d'indication FDI de couche client/serveur

Dans cet exemple, la détection d'une défaillance de liaison par la fonction de terminaison de puits dans la couche serveur A cause la production d'une indication FDI/AIS qui est passée à la couche

serveur de VPN. La FDI est passée à la fonction de terminaison de puits de couche serveur de VPN qui à son tour envoie une FDI à la couche client. Ce comportement est récursif jusqu'au réseau de couche qui n'accepte pas de FDI, donc, bien que ce ne soit pas montré ici, à réception d'une indication FDI, la couche serveur de VPN peut envoyer une FDI à la couche supérieure en fonction de ce qu'est la technologie de la couche supérieure (par exemple ATM, Ethernet, IP, etc.).

Le seul endroit où une alarme devrait être déclenchée est au point de terminaison de chemin du réseau de couche où la faute originelle est détectée. En particulier, il ne devrait pas y avoir de déclenchement d'alarme dans une des couches client affectées (c'est principalement dans ce but qu'une indication FDI leur est envoyée). De plus, si la surveillance mono terminaison des deux directions est nécessaire, une indication de défaut vers l'arrière (BDI, *backward defect indicator*) peut être envoyée dans l'autre direction. Des détails complémentaires sur la façon dont fonctionnent les indicateurs/alarmes de défauts (y compris des précisions sur les critères d'entrée et de sortie de défaut et d'indisponibilité et les actions qui en découlent) pourront y être trouvés dans les Recommandations qui traitent de l'OAM pour les technologies spécifiques de réseau de couche, par exemple la Rec. UIT-T Y.1711 pour l'OAM MPLS.

La correction de faute est chargée de la réparation d'une faute et du contrôle des procédures qui utilisent des ressources redondantes pour remplacer les équipement ou dispositifs défaillants. Par exemple, dans le cas de coupure de fibre ou de défaillance d'un nœud, la commutation de protection ou le réacheminement de connexion peuvent être utilisés pour restaurer/maintenir le service.

Les outils d'essai diagnostique à la demande sont généralement utilisés pour localiser la faute, mais peuvent aussi être utilisés pour vérifier que la connectivité/configuration d'une connexion/tunnel sont correctes avant de les mettre en service. Le bouclage arrière est un exemple d'essai diagnostique durant lequel une boucle sur une connexion réseau depuis la source revient à la source via une connexion ou un point de terminaison de connexion point, isolant ainsi cette section de la connexion.

12.2 Gestion des performances

La surveillance de performances (PM, *performance monitoring*) est le processus de collecte, d'analyse et de rapport, des données de performances. Ces données servent à faire l'estimation et la maintenance du réseau ainsi qu'à documenter la qualité de service vis-à-vis des utilisateurs. Si plusieurs niveaux de classe de service sont pris en charge (par exemple, sur la base de l'architecture Diffserv) la surveillance des performances devrait alors être effectuée sur la base de la classe de service. La surveillance des performances inclut entre autres choses la détection de la dégradation du signal, la surveillance du délai de latence/gigue, et le comptage des paquets perdus. Il y a un certain nombre d'objectifs différents pour la surveillance des performances parmi lesquels la maintenance de l'accord de niveau de service, la prise en charge de l'ingénierie du trafic, la comptabilité de l'utilisateur, et la restauration de service/commutation de protection (par exemple due à la dégradation du signal).

Il est important d'obtenir la relation entre les défauts, la disponibilité et la surveillance des performances. Il y a un ordonnancement particulier qui peut être résumé comme suit:

1) le mode de réseau définit les défauts qui sont pertinents (qui sont différents pour chaque mode) et la nature de l'OAM nécessaire;

2) tous les défauts devraient être définis en termes de critères d'entrée/sortie normalisés et des actions qui en découlent;

3) on entre dans l'état d'indisponibilité lorsqu'un défaut ou une dégradation inacceptable des performances a persisté pendant un certain nombre de secondes consécutives. En SDH l'état d'indisponibilité commence à la suite de 10 secondes consécutives gravement erronées (SES)[7] et se termine par 10 secondes consécutives non SES. Pour assurer l'harmonisation, la période d'indisponibilité devrait être la même à travers tous les réseaux de couches, c'est-à-dire 10 secondes;

4) la surveillance des performances pour les besoins d'un accord de niveau de service n'est valide qu'en état de disponibilité, et donc, la surveillance des performances pour les besoins d'un accord de niveau de service doit être suspendue lorsqu'on entre dans l'état d'indisponibilité.

En état disponible, la surveillance des performances pour les besoins d'un accord de niveau de service est une mesure unidirectionnelle. Cependant, comme la plupart des applications exigent que les deux directions (amont et aval) fonctionnent, si une des directions a une défaillance, les deux sont réputées être défaillantes du point de vue d'une application. Cela signifie que l'indisponibilité est une fonction "OU" de chaque direction et donc si une des directions passe en état indisponible, la surveillance des performances pour les besoins d'un accord de niveau de service devrait être suspendue dans les deux directions.

12.3 Activation/désactivation d'OAM

Pour les modes CO-CS et CO-PS, les mécanismes d'OAM de détection/traitement de défaut de base devraient être activés/désactivés en synchronisation avec l'établissement/suppression de chemin, ce qui pourrait être via l'approvisionnement NMS/OSS ou via la signalisation. Par exemple, la génération vérification de connexion devrait être activée à la source avant d'activer la détection de vérification de connexion au puits afin d'éviter les alarmes sans signification. La méthode d'approvisionnement ou de signalisation utilisée pour établir le chemin devrait aussi être capable de dire au point de puits de chemin quel identificateur de source (par exemple, TTSI dans la Rec. UIT-T Y.1711) attendre dans le plan des données pour un chemin particulier afin de déterminer à quel chemin appartiennent les paquets d'OAM qu'il reçoit.

12.4 Défauts pertinents pour chaque mode de réseau

Les défauts de transport potentiels qui peuvent survenir dans un réseau de couche client ou serveur VPN dépendent du mode de réseau auquel appartient la technologie de réseau de couche. Un résumé des défauts potentiels dépendants du mode est donné ci-dessous:

– **CL-PS**: seulement les coupures;

– **CO-PS**: coupures, échanges, et fusions;

– **CO-CS**: coupures, échanges (mais seulement entre entités semblables).

Dans les paragraphes qui suivent, chacun des modes de réseau est décrit plus en détail pour expliquer ce que les exigences et considérations clé d'OAM sont pour ce mode particulier. Il convient de noter que cela n'est pas conçu comme une liste détaillée des exigences d'OAM pour chaque mode. Seules les différences fonctionnelles fondamentales sont soulignées afin de montrer comment le mode de réseau auquel appartiennent les couches client et serveur de VPN impacte les fonctions/outils OAM nécessaires.

12.4.1 Réseaux de couche CL-PS

Dans l'hypothèse d'informations d'acheminement cohérentes et valides (ce qui en réalité s'applique à tous les modes) les défauts de mauvaise connectivité (c'est-à-dire échanges ou fusions) ne peuvent

---

[7] Période d'une seconde avec un taux d'erreur binaire égal ou supérieur à 1E-3, ou durant laquelle une LOS ou une AIS est détectée.

pas survenir dans des réseaux de couche CL-PS. Chaque paquet contient à la fois une adresse de source (c'est la fonction de vérification de connexion) et une adresse de destination qui contient toutes les informations nécessaires pour l'acheminement correct du paquet à chaque nœud du réseau. Donc, le seul défaut possible dans un réseau de couche CL-PS est le cas où il y a une rupture (par exemple due à une défaillance d'acheminement, de liaison ou de nœud). Dans les réseaux de couche CL-PS, la fonction de vérification de connexion fait partie intégrante de l'en-tête de paquet car chaque paquet contient une adresse de source/destination unique pour le réseau. Dans les réseaux CL-PS, les données de contrôle et d'utilisateur partagent habituellement le même chemin de données, et donc, s'il y a une défaillance dans le plan de contrôle (par exemple, la rupture d'une adjacence d'acheminement) on peut alors supposer que cela implique que la connectivité a été perdue et que les données d'utilisateur ne peuvent pas non plus être envoyées. C'est généralement ainsi que les fautes sont détectées et corrigées dans les réseaux de couche CL-PS, par exemple, la non-réception des accusés de réception d'acheminement dans le plan de contrôle indique qu'il y a une faute dans le plan des données et donc qu'il faut entreprendre une action corrective (par exemple le choix d'une route de remplacement). Un cas où cela n'est cependant pas vrai est celui de l'utilisation de l'équilibrage de charge dans des réseaux de couche IP. Dans ce cas, il existe plusieurs routes pour la même destination, donc si une route devient indisponible, cela peut n'être pas détecté par le plan de contrôle car le trafic de contrôle peut simplement utiliser une des autres routes disponibles. Pour détecter des défaillances lorsque l'équilibrage de charge est employé, un mécanisme OAM doit être utilisé pour tester la connectivité sur toutes les routes disponibles.

12.4.2 Réseaux de couche CO-PS

Dans le cas de CO-PS, seuls les points d'accès de réseau de couche connaissent les adresses uniques pour le réseau utilisées par la fonction d'acheminement pour calculer la meilleure route/chemin à travers le réseau pour la connexion. Une fois que la route/chemin a été calculé, la signalisation (ou l'approvisionnement manuel) est utilisé pour allouer et configurer localement les champs significatifs de multiplexage/démultiplexage d'entrée/sortie (ou les identificateurs de connexion), qui sont utilisés dans le plan des données pour commuter le paquet sur la destination correcte. Comme les champs de multiplexage/démultiplexage n'ont qu'une signification locale, les mêmes valeurs peuvent être réutilisées par les nœuds amont/aval pour la même connexion, ou pour des connexions différentes. La réutilisation des champs de multiplexage/démultiplexage combinée au manque d'adressage unique de réseau dans le plan des données signifie que dans les réseaux de couche CO-PS, en plus des ruptures, on peut rencontrer les défauts d'échange et de fusion. Comme les paquets CO-PS sont transmis en asynchrone et ne contiennent pas d'adresse de source/destination unique pour le réseau, la fonction de vérification de connexion doit être ajoutée d'une façon déterministe, normalement en transmettant des paquets de vérification de connexion à un débit spécifique. Le débit auquel les paquets de vérification de connexion sont envoyés doit être soigneusement étudié pour s'assurer de ne pas entreprendre d'actions inutiles dans le cas de rafales d'erreurs transitoires.

12.4.3 Réseaux de couche CO-CS

Les réseaux de couche CO-CS ne souffrent pas de fusions car les champs de multiplexage/démultiplexage sont fondés sur des identificateurs de connexion de liaison physique de temps/espace/fréquence avec un débit binaire constant. Les défauts qui peuvent survenir dans un réseau de couche CO-CS incluent les coupures et les connexions échangées, cependant le défaut d'échange de connexion ne peut survenir qu'entre des chemins exactement semblables, par exemple des échanges ne peuvent survenir entre un VC12 et un VC4 en SDH. Dans le cas de réseaux de couche CO-CS, comme avec les réseaux de couche CO-PS, la fonction de vérification de connexion doit être ajoutée de façon déterministe. Comme une trame CO-CS est transmise à un débit binaire constant (qu'il y ait ou non des données à envoyer), les informations de vérification de connexion peuvent être transportées dans chaque trame en utilisant le débit d'émission de trame comme débit d'émission de vérification de connexion, par exemple le message de trace J0 dans une trame VC4 en

SDH a un débit d'insertion de base de 125 µs. Dans le cas CO-CS, le trafic de contrôle est toujours transporté hors bande et donc les fonctions OAM doivent être fournies connexion par connexion pour les plans de données d'utilisateur et de contrôle.

12.4.4 Séparation de plan de données de contrôle et d'utilisateur

Les données de contrôle et les données d'utilisateur dans les réseaux CO-PS peuvent être transmises en utilisant différents plans de données (souvent dénommés contrôle hors bande (OOB, *out of band*)). Et comme noté dans les paragraphes précédents, en mode CO-CS, c'est un comportement obligé dans tous les cas. Cette séparation des plans de données de contrôle et d'utilisateur est avantageuse pour de nombreuses raisons, et particulièrement du point de vue de la sécurité et de la stabilité du réseau car elle protège le plan de contrôle des attaques du plan d'utilisateur et des problèmes de surcharge/encombrement causés par le trafic du plan d'utilisateur. Lorsque les plans de données d'utilisateur et de contrôle sont séparés, on peut clairement ne pas supposer qu'une défaillance dans le plan de contrôle indique une défaillance dans le plan de données d'utilisateur (ou bien sûr, vice versa). Donc les mécanismes d'OAM, dans les réseaux de couche CO-PS où on utilise le contrôle hors bande, doivent être utilisés sur la base du plan de données (c'est-à-dire par connexion). C'est aussi le cas lorsque le trafic de contrôle peut utiliser le même plan de données qu'une partie du trafic d'utilisateur, mais pas la totalité (par exemple, en MPLS, l'ingénierie de trafic peut être utilisée pour fournir un acheminement explicite pour certains types de trafic et donc le trafic de données d'utilisateur n'a pas besoin de suivre le même chemin que les paquets de contrôle utilisés pour établir les tunnels d'ingénierie du trafic).

L'échec à utiliser le plan des données sur la base des mécanismes d'OAM peut conduire à un scénario dans lequel une connexion transportant des paquets de données peut rencontrer une faute, mais comme le trafic de contrôle est transmis en utilisant une connexion distincte, les informations de contrôle continuent à s'écouler et donc la faute n'est pas détectée par le plan de contrôle. Sans mécanisme OAM de détection de plan des données, la source de connexion va continuer à envoyer des données d'utilisateur et créer un trou noir de trafic, ou pire, compromettant la sécurité des données du consommateur en envoyant le trafic à une localisation erronée.

Afin de déterminer de façon non ambiguë dans quelle direction une faute est survenue, et pour prendre en charge un traitement de faute correct aussi bien pour les connexions en point à point qu'en point à multipoint, l'OAM devrait fonctionner de façon unidirectionnelle. Aussi, la surveillance de fautes à extrémité unique dans les deux directions devrait-elle être prise en charge si possible. Ceci est particulièrement important lorsqu'un utilisateur ou un fournisseur a le contrôle d'une seule extrémité d'une connexion/tunnel mais pas de l'autre extrémité, par exemple, dans un scénario de VPN interfournisseurs où chaque extrémité d'une connexion de couche serveur de VPN point à point est située dans un réseau d'un fournisseur de services différent.

13 Convergence fonctionnelle et scénarios de service

Le mappage des exigences de service VPN dans les fonctions décrites dans la présente Recommandation permet aux opérateurs de réseau de choisir les technologies et mécanismes de réseau les plus appropriés nécessaires pour fournir les services de VPN qu'ils souhaitent offrir. Le choix des meilleurs mécanismes/protocoles d'alimentation pour chaque fonction permet que les composants fonctionnels individuels évoluent de façon indépendante. Cette approche prend aussi en charge la réutilisation des mécanismes/protocoles communs à travers les technologies de réseau VPN différentes (en tant que de besoin) pour réduire les coûts et la complexité.

13.1 Scénarios de services VPN client/serveur

Les fonctions (et donc les mécanismes/protocoles) nécessaires pour prendre en charge les VPN client/serveur dépendent du mode de réseau client/serveur ainsi que des services de VPN réels qui sont offerts. Par exemple, certains consommateurs peuvent vouloir être capables d'établir des

circuits virtuels commutés à la demande entre plusieurs sites, comme et quand c'est nécessaire, alors que d'autres consommateurs peuvent vouloir juste des connexions permanentes sur la base d'une topologie statique connue. Dans un autre exemple, certains consommateurs peuvent vouloir utiliser l'authentification par utilisateur/extrémité client pour accroître la sécurité alors que d'autres consommateurs peuvent penser que restreindre l'accès physique à l'infrastructure de réseau est adéquat. Les Tableaux III.1 et III.2 fournissent quelques exemples de différents scénarios de service et identifient des exemples de mécanismes/protocoles qui peuvent être utilisés pour fournir les fonctions exigées.

13.2 Scénarios de VPN de niveau homologue

Les fonctions nécessaires pour la prise en charge des VPN de niveau homologue dépendent de la technologie de réseau de couche homologue et du type de service VPN qui est offert. Par exemple, l'authentification est obligatoire dans le cas de VPN fondé sur le chiffrement afin d'utiliser les clés correctes tandis que dans le cas de VPN fondé sur un VLAN Ethernet, l'authentification (par exemple, en utilisant IEEE 802.1X) fournit une sécurité supplémentaire mais n'est pas essentielle. Le Tableau III.3 fournit quelques exemples de différents scénarios de service et identifie quelques exemples de mécanismes/protocoles qui peuvent être utilisés pour fournir les fonctions demandées.

14 Considérations sur la sécurité chez les VPN

La présente Recommandation n'introduit aucune nouvelle question de sécurité. Cependant, la sécurité est un facteur fondamental à prendre en compte lors de la conception/développement de réseaux VPN afin de choisir les technologies et composants fonctionnels des réseaux qui satisfont les exigences de sécurité du consommateur. Il y a des risques pour la sécurité inhérents à toutes les technologies de VPN qui sont dus au fait qu'une infrastructure partagée est utilisée pour transporter du trafic pour plusieurs consommateurs.

La sécurité des réseaux est un vaste domaine en lui-même et n'est donc pas examinée en détail dans la présente Recommandation. En regardant la sécurité avec un certain recul, on voit que l'infrastructure physique de réseau VPN doit être protégée contre les accès non autorisés ou les attaques malveillantes (par exemple, en interdisant l'accès aux bâtiments qui contiennent les équipements de réseau). De plus, l'accès non autorisé à distance, depuis l'extérieur de l'infrastructure du réseau VPN doit aussi être empêché (par exemple en utilisant des pare-feu pour protéger contre les attaques nées de l'Internet).

Comme décrit au § 5.1, dans le cas de VPN client/serveur, un réseau de couche VPN serveur doit prendre en charge le multiplexage/démultiplexage pour fournir une séparation du plan des données entre plusieurs couches client de VPN. Cette séparation du trafic doit être combinée avec un contrôle d'accès effectif au VPN à la bordure du réseau sur la base des politiques de VPN utilisateur par utilisateur.

Dans le cas de VPN de niveau homologue, comme décrit au § 6, pour prendre en charge les VPN à travers un domaine partagé, la technologie de réseau utilisée doit avoir des moyens de fournir l'isolation de VPN. Les extrémités client doivent seulement être capables de communiquer avec les autres extrémités client qui appartiennent au même VPN, ou être capables de déchiffrer seulement les paquets provenant des extrémités client qui appartiennent au même VPN.

On peut augmenter la sécurité à la fois pour les VPN client/serveur et les VPN de niveau homologue en utilisant le chiffrement pour crypter les unités de trafic d'utilisateur/de contrôle et l'authentification peut être utilisée pour authentifier les utilisateurs et les nœuds du réseau. L'authentification pour les VPN client/serveur et les VPN de niveau homologue est respectivement décrite plus en détail aux § 10.2.1 et 11.2. Le chiffrement est décrit plus précisément aux § 6.2 et 11.4.

Appendice I

Localisation des TCP/TFP de couche client de VPN

La Figure I.1 donne un exemple d'un réseau VPN client/serveur. Elle montre la topologie physique du réseau dans laquelle la ligne noire représente la couche serveur de VPN et les lignes grises représentent les liaisons physiques entre les nœuds.

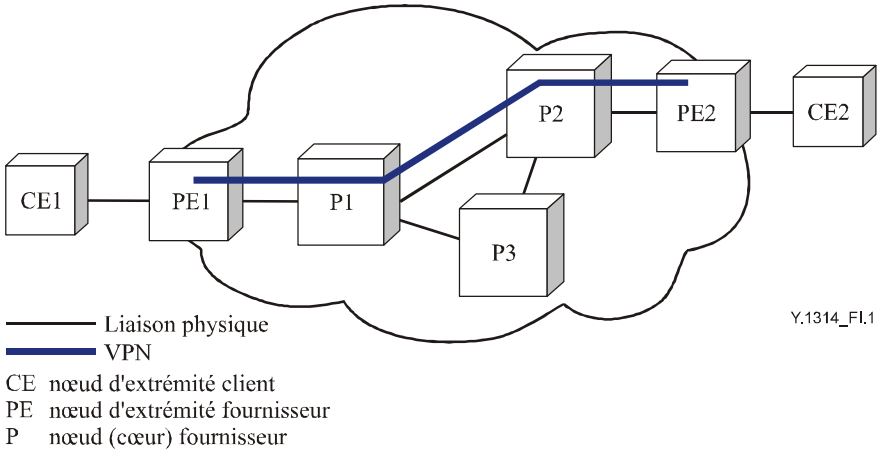


Figure I.1/Y.1314 – Topologie physique de VPN client/serveur – Exemple 1

Bien que la Figure I.1 montre la topologie physique et la couche serveur de VPN, elle ne montre pas les topologies séparées de couche client et de couche serveur de VPN ou la localisation des TCP/TFP. La Figure I.2 montre un modèle fonctionnel fondé sur la topologie physique de la Figure I.1 dans laquelle les TFP sont localisés dans les nœuds d'extrémité client. Dans cet exemple la couche serveur de VPN est orientée connexion (par exemple ATM) tandis que la couche client de VPN est sans connexion (par exemple Ethernet), bien que toute combinaison de paires CO ou CL soit possible.

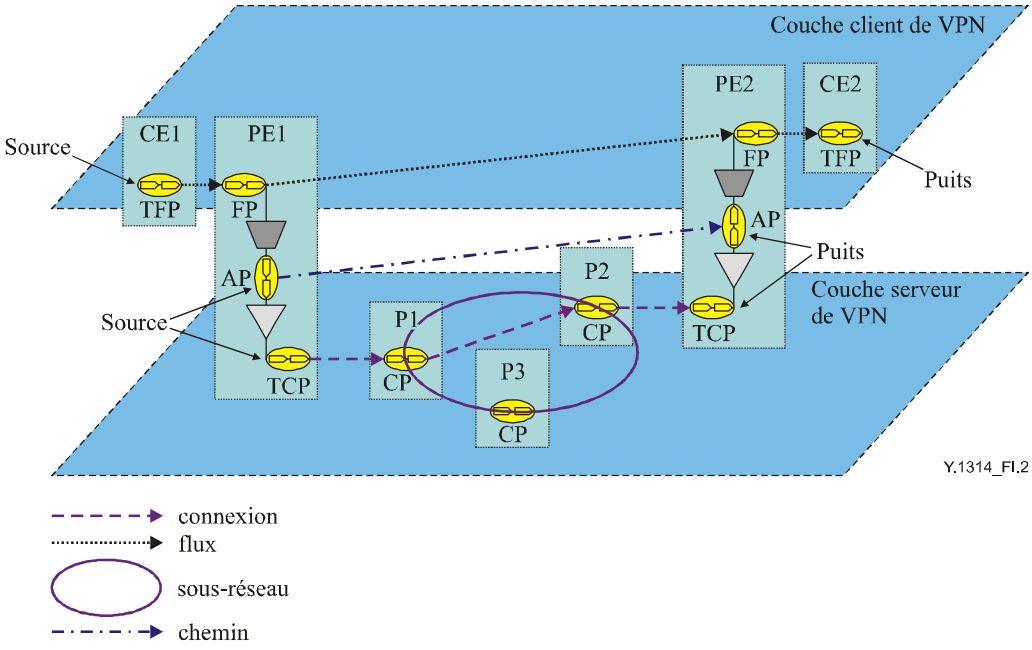


Figure I.2/Y.1314 – TFP de couche client de VPN localisés dans les nœuds CE

Les nœuds d'extrémité client et de fournisseur appartiennent respectivement aux couches client et serveur VPN, tandis que les nœuds d'extrémité fournisseur appartiennent aux deux couches. Les TFP dans la couche client de VPN identifient où commence (sa source) la couche serveur de VPN en point à point (dans ce cas, quel nœud d'extrémité client) et où elle se termine (son puits), et les points de flux identifient quels nœuds d'extrémité fournisseur sont traversés par le flux point à point. De même, les TFP dans la couche serveur de VPN identifient la source et le puits pour la connexion de couche serveur de VPN, et les points de flux identifient à travers quels nœuds fournisseur passe le flux. Les points d'accès dans la couche serveur de VPN identifient la source/puits pour le chemin de couche serveur de VPN.

Dans l'exemple précédent, les TFP de couche client de VPN étaient situés dans les nœuds d'extrémité client (CE1 et CE2), ce n'est cependant pas le cas pour toutes les relations client/serveur de VPN. Par exemple, la couche client de VPN peut être une couche de réseau Ethernet ou IP où les TFP sont situés dans les hôtes/systèmes terminaux.

La Figure I.3 montre la topologie physique d'un réseau VPN client/serveur. Si la couche client de VPN est en Ethernet, les nœuds client sont alors des commutateurs Ethernet, et les systèmes terminaux/hôtes sont des ordinateurs/serveurs avec des interfaces Ethernet.

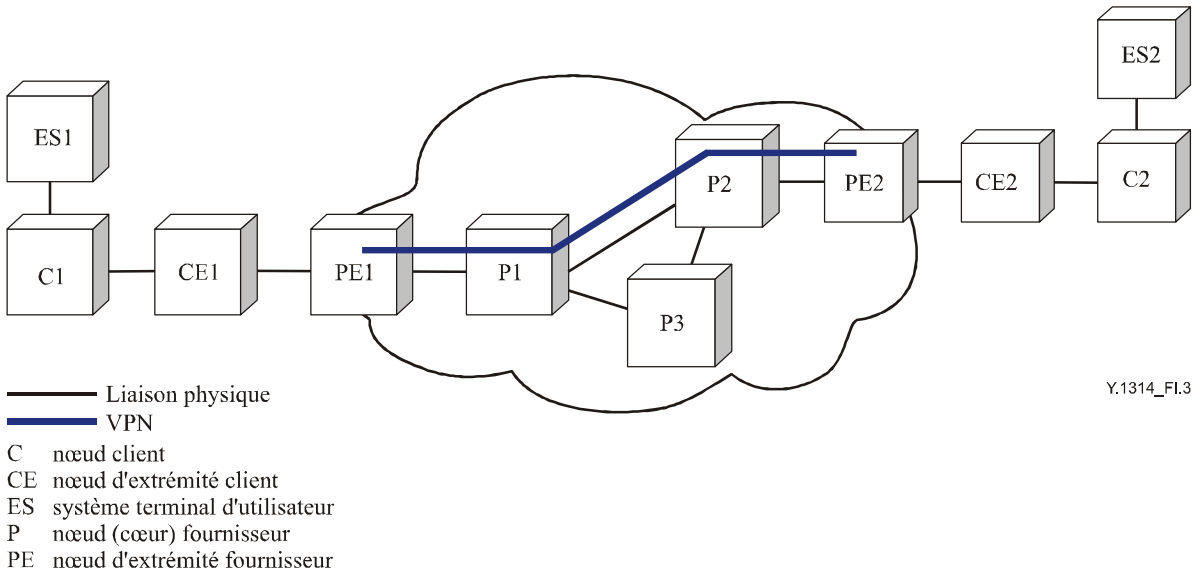


Figure I.3/Y.1314 – Topologie physique de VPN client/serveur – Exemple 2

Un modèle fonctionnel fondé sur le réseau physique décrit à la Figure I.3 est présenté à la Figure I.4, où les TFP/TCP de couche client de VPN sont situés dans les systèmes terminaux/hôtes plutôt que dans les extrémités client.

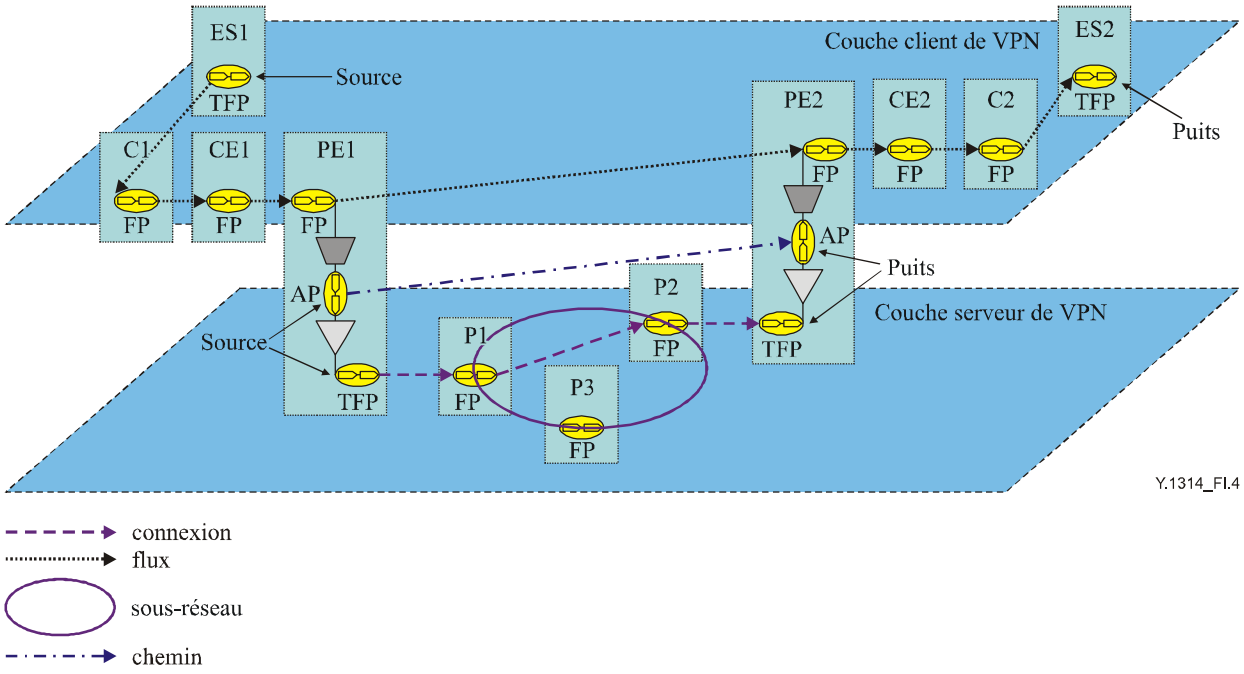


Figure I.4/Y.1314 – TFP de couche client de VPN situés dans les systèmes terminaux/hôtes

Les nœuds client et d'extrémité client ainsi que les systèmes terminaux appartiennent à la couche client de VPN. Les nœuds d'extrémité fournisseur appartiennent à la couche serveur et à la couche client de VPN tandis que les nœuds fournisseur n'appartiennent qu'à la couche serveur de VPN. Dans la couche client de VPN, les TFP identifient la source et le puits (c'est-à-dire respectivement ES1 et ES2) pour le flux de couche client de VPN, et les points de flux identifient quels nœuds client, d'extrémité client et d'extrémité fournisseur sont traversés par le flux.

Bien que ce ne soit pas illustré par les exemples précédents, il est aussi possible qu'un côté du TFP/TCP source ou puits du VPN soit situé dans l'extrémité client, tandis qu'à l'autre bout, le TFP n'est pas situé dans l'extrémité client, c'est-à-dire qu'un point de connexion/point de flux est situé dans l'extrémité client et le TFP/TCP est situé dans un nœud client ou un système terminal.

Appendice II

VPN client/serveur avec plusieurs couches serveurs de VPN

La Figure II.1 montre la topologie physique d'un réseau VPN client/serveur qui utilise deux différentes couches serveurs de VPN, X et Y. Les nœuds PE1, P1 et P2 appartiennent à la couche serveur de VPN X, tandis que les nœuds P3 et PE3 appartiennent à la couche serveur de VPN Y. Le nœud PE2 appartient aux deux couches serveurs et agit comme une passerelle entre les deux.

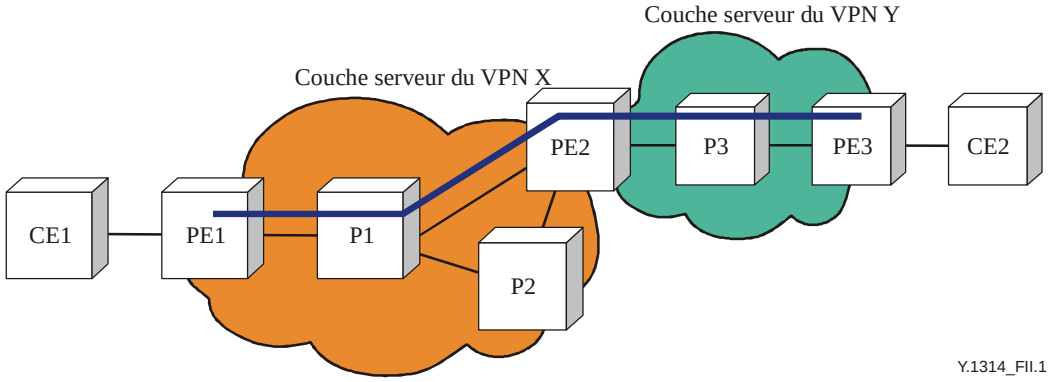


Figure II.1/Y.1314 – Topologie physique d'interfonctionnement de couches serveurs de VPN

Une méthode d'interfonctionnement entre couches serveurs des VPN X et Y serait d'utiliser l'interfonctionnement client/serveur tel qu'illustré à la Figure II.2. Dans ce modèle, le nœud PE2 appartient à la couche serveur des VPN X et Y et les trois nœuds d'extrémité fournisseur appartiennent tous à la couche serveur de VPN.

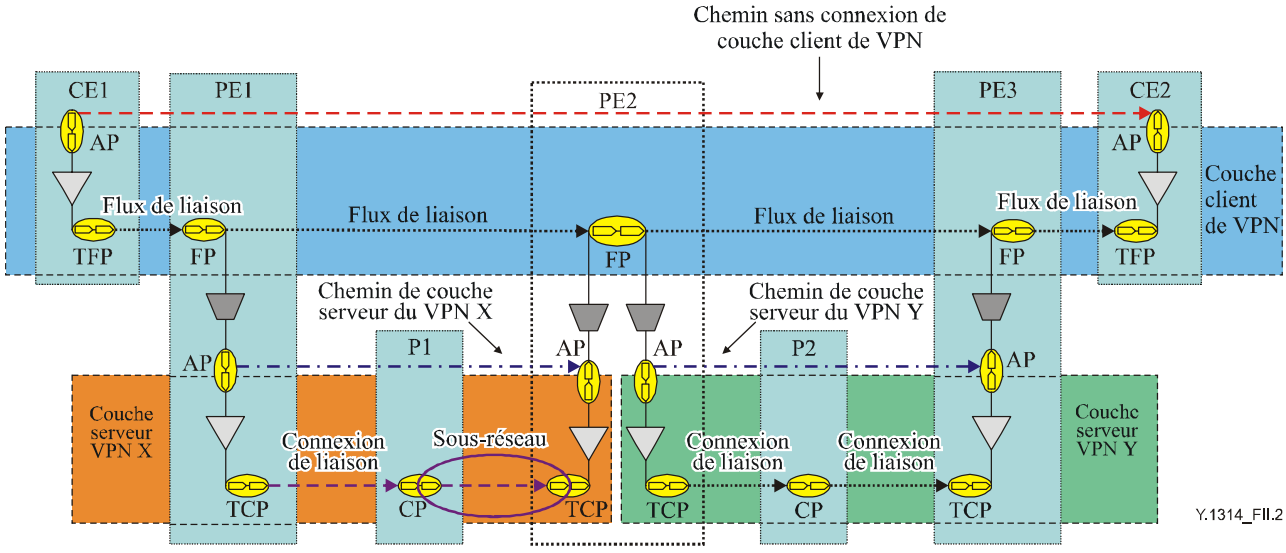


Figure II.2/Y.1314 – Interfonctionnement client/serveur de couche serveur de VPN

La fonction d'adaptation de source de la couche serveur de VPN X adapte les informations caractéristiques de couche client de VPN en informations adaptées dans la couche serveur de VPN X, et la fonction d'adaptation de puits adapte les informations adaptées de la couche serveur de VPN X en informations caractéristiques de couche client de VPN. De façon similaire, la fonction d'adaptation de source de la couche serveur de VPN Y adapte les informations caractéristiques de la couche client de VPN en informations adaptées dans la couche serveur de VPN Y, et la fonction d'adaptation de puits adapte les informations adaptées de la couche serveur de VPN Y en informations caractéristiques de la couche client de VPN.

Les éléments de réseau dans lesquels a lieu l'adaptation client/serveur contiennent des points de flux ou des points de connexion appartenant à la couche client de VPN, qui doivent être identifiés en utilisant les adresses de couche client de VPN. Ainsi, par exemple, si la couche client de VPN est IP, PE1, PE2, et PE3 auraient besoin des adresses IP appartenant à la couche client de VPN.

Utiliser plusieurs couches serveurs de VPN avec l'adaptation client/serveur pour les couches client de VPN orientées connexion signifie qu'une route/chemin doit être calculé de façon dynamique/manuelle à travers les points de connexion et qu'au moins deux connexions de liaison soient établies de bout en bout à la couche client de VPN au sein du réseau du fournisseur. Utiliser plusieurs couches serveurs de VPN avec l'adaptation client/serveur pour des couches client de VPN sans connexion signifie qu'une route/chemin doit être calculé de façon dynamique/manuelle à travers les points de flux, et que les unités de trafic sans connexion (c'est-à-dire les paquets) doivent être transmis sur la base des informations d'adresse à la couche client de VPN. Ceci est différent du cas où une seule couche serveur de VPN a été établie de bout en bout à travers le réseau fournisseur entre deux points de connexion/points de flux à la couche client de VPN. Dans ce cas, c'est une seule connexion/flux de liaison qui est nécessaire au sein du réseau fournisseur entre la source et le puits de chemin de couche serveur de VPN, et donc une route/chemin n'a pas besoin d'être calculé à travers le réseau fournisseur à la couche client de VPN.

La méthode de remplacement de l'interfonctionnement entre les couches serveurs des VPN X et Y de la Figure II.2 serait d'utiliser l'interfonctionnement de niveau homologue comme illustré à la Figure II.3. Dans ce modèle, le nœud PE2 appartient à la couche serveur de VPN X et Y mais n'appartient pas à la couche client de VPN. PE1 et PE3 appartiennent respectivement à la couche serveur des VPN X et Y, et appartiennent aussi à la couche client de VPN.

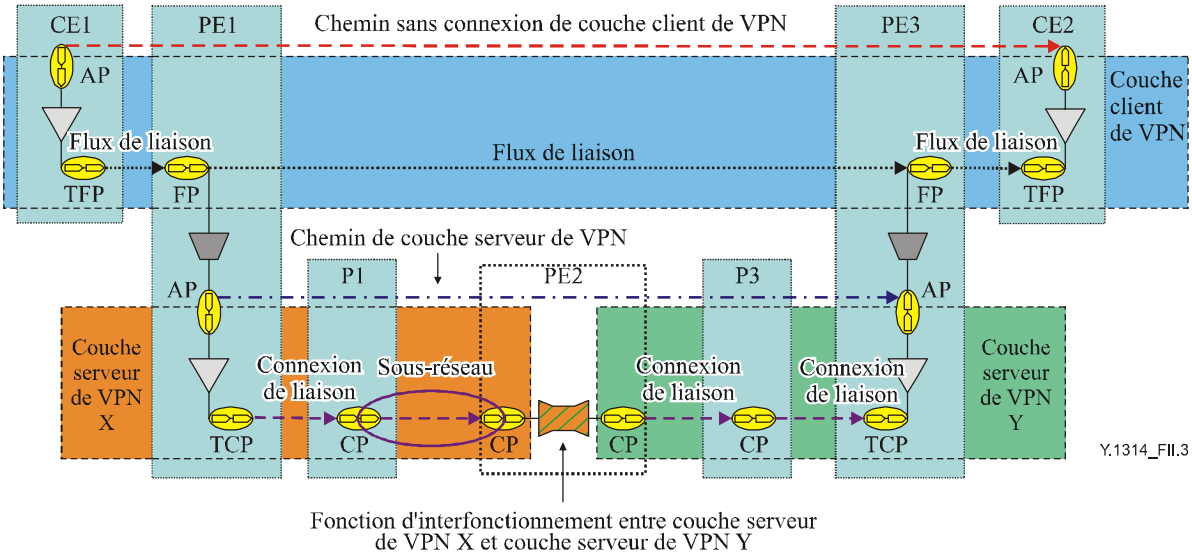


Figure II.3/Y.1314 – Interfonctionnement de niveau homologue de couche serveur de VPN

La fonction d'adaptation de source de couche serveur de VPN X adapte les informations caractéristiques de la couche client de VPN en informations adaptées dans la couche serveur de VPN X. La fonction d'interfonctionnement de la couche serveur de VPN X à la couche serveur de VPN Y adapte les informations adaptées de la couche serveur de VPN X aux informations adaptées de la couche serveur de VPN Y. La fonction d'adaptation de puits de la couche serveur de VPN Y adapte les informations adaptées de la couche serveur de VPN Y aux informations caractéristiques de la couche client de VPN.

Le principal facteur à prendre en considération lorsqu'on envisage l'interfonctionnement de niveau homologue est que seulement certaines technologies de réseau peuvent interagir sur la base d'un niveau homologue, par exemple, les réseaux en ATM et en relais de trames peuvent interagir sur une base de niveau homologue (en utilisant FRF.8), mais les réseaux IP et TDM ne le peuvent pas. L'interfonctionnement de niveau homologue exige l'interfonctionnement non seulement dans le plan des données mais aussi dans le plan de contrôle pour des fonctions telles que l'acheminement, la signalisation, et l'OAM.

Appendice III

Exemples de scénarios de service de VPN client/serveur et de niveau homologue

Les tableaux ci-dessous donnent quelques exemples de différents scénarios de service de VPN et identifient quelques exemples de mécanismes/protocoles qui peuvent être utilisés pour fournir les fonctions demandées.

NOTE – Des références supplémentaires se rapportant aux tableaux du présent appendice sont fournies dans la bibliographie.

Tableau III.1/Y.1314 – Scénarios 1 de service client/serveur de VPN

	Service de relais de trames de couche 2 sur MPLS	**Service VPWS Ethernet de couche 2 sur IP/L2TPv3**	**Service de VPN IP de couche 3 de la RFC 2547**
Couche client de VPN	Relais de trames	Ethernet	IP
Couche serveur de VPN	Pseudo circuit MPLS	IP/L2TPv3	MPLS
Découverte des membres du VPN	RADIUS, BGP, manuel, NMS	RADIUS, BGP, LDP, RSVP-TE, manuel, NMS	BGP
Acheminement de couche serveur de VPN	IGP, BGP, manuel, NMS	IGP, BGP, manuel, NMS	BGP
Etablissement de tunnel/connexion de couche serveur de VPN	LDP, BGP, manuel, NMS	Signalisation L2TPv3	BGP
Authentification, autorisation, et comptabilité (AAA) de CE/usager	RADIUS, IEEE 802.1X, RMON, SNMP, NMS	RADIUS, IEEE 802.1X, RMON, SNMP, NMS	Protocole d'acheminement CE-PE (par exemple, EBGP avec MD5), RMON, SNMP, NMS
Configuration d'élément de réseau de couche client de VPN	NMS, manuel	NMS, manuel, E-LMI	DHCP, NMS, manuel
Acheminement de couche client de VPN	NMS, manuel	Acquisition d'adresse MAC	EBGP, OSPF, manuel/statique
Signalisation de tunnel/connexion de couche client de VPN	NMS, manuel	Non requis car le client est CL-PS	Non requis car le client est CL-PS
OAM de couche client de VPN	LMI en relais de trames	IEEE 802.1ag, E-LMI, IEEE 802.3ah, Y.1731	Ping/traceroute IP
OAM de couche serveur de VPN	Rec. UIT-T Y.1711, Rec. UIT-T Y.1713, ping MPLS, VCCV, BFD/LSP	ping/traceroute IP	Y.1711, Y.1713, ping/traceroute LSP

Tableau III.2/Y.1314 – Scénarios 2 de service client/serveur de VPN

	Service de couche 1 de VPN en SDH sur OTN	**Service de couche 1 de VPN en TDM sur MPLS**	**Service de couche 2 de VPN en ATM sur SDH**
Couche client de VPN	SDH (par exemple, STM-16)	TDM (par exemple, E1)	ATM
Couche serveur de VPN	chemin léger/canal optique (OCh)	Pseudo circuit MPLS	SDH (par exemple, VC4)
Découverte des membres du VPN	Rec. UIT-T G.7714.1/Y.1705.1, manuel, NMS	RADIUS, BGP, LDP, manuel, NMS	Manuel, NMS
Acheminement de couche serveur de VPN	Protocoles d'acheminement GMPLS/ASON, manuel, NMS	IGP, BGP, manuel, NMS	Protocoles d'acheminement GMPLS/ASON, manuel, NMS
Etablissement de tunnel/connexion de couche serveur de VPN	Protocoles d'acheminement GMPLS/ASON, manuel, NMS	LDP, BGP, manuel, NMS	Protocoles d'acheminement GMPLS/ASON, manuel, NMS
Authentification, autorisation, et comptabilité (AAA) de CE/utilisateur	Protocoles GMPLS/ASON, SNMP, NMS	RMON, SNMP, NMS	ATM, PNNI/UNI sécurité, RMON, SNMP, NMS
Configuration d'élément de réseau de couche client de VPN	NMS, manuel	NMS, manuel	ATM UNI, manuel, NMS
Acheminement de couche client de VPN	Protocoles d'acheminement GMPLS/ASON, manuel, NMS	Manuel, NMS	Manuel/statique, NMS, PNNI
Signalisation de tunnel/connexion de couche client de VPN	Protocoles d'acheminement GMPLS/ASON, manuel, NMS	Manuel, NMS	Manuel, NMS, PNNI
OAM de couche client de VPN	Redondance SDH (par exemple, octets de trace J0/J1/J2, octet d'état de chemin G1)	AIS/LOS de la Rec. UIT-T G.775	Gestion de faute F4 et F5, bouclage, et vérification de continuité (CC)
OAM de couche serveur de VPN	Redondance OCh (par exemple, identificateur de trace de chemin (TTI) utilisé dans la surveillance de chemin/section (PM/SM))	Rec. UIT-T Y.1711, Rec. UIT-T Y.1713, ping MPLS, VCCV, BFD/LSP	Redondance SDH (par exemple, octets de trace J0/J1/J2, octet d'état de chemin G1)

Tableau III.3/Y.1314 – Scénarios de service de niveau homologue de VPN

	VPN IPsec sur l'Internet	**VPN VLAN Ethernet**
Couche homologue de VPN	IP	Ethernet
Découverte des membres du VPN	Manuel, NMS	Manuel, NMS, RADIUS
Authentification, autorisation, et comptabilité (AAA) de CE/utilisateur	Authentification IKE primaire (sur la base de clés prépartagées ou de signatures numériques), RMON, SNMP, NMS	IEEE 802.1x, RADIUS, RMON, SNMP, NMS
Acheminement de couche homologue de VPN	Protocoles d'acheminement IGP (par exemple ISIS, OSPF, RIP), BGP, manuel, NMS	Elagage de topologie STP et acquisition d'adresse du plan de données (pontage transparent)
Configuration d'élément de réseau de couche homologue de VPN	Configure les clés partagées, ou demande un certificat provenant de l'autorité de certification	Configure les VLAN en utilisant la configuration manuelle, NMS, ou des protocoles dynamiques
OAM de couche homologue de VPN	Ping IP, traceroute	IEEE 802.1ag, E-LMI, IEEE 802.3ah, Y.1731

BIBLIOGRAPHIE

Les références indiquées sont susceptibles d'être révisées. Les utilisateurs de la présente Recommandation sont invités à rechercher l'édition/projet le plus récent de ces références.

ATM UNI: ATM Forum UNI 4.1 (2002), "*ATM User Network Interface (UNI) Signalling Specification version 4.1*", *(Spécification de la signalisation de l'interface usager-réseau (UNI) en ATM, version 4)*, af-sig-0061.001.

ATM Forum PNNI 1.1 (2002), *Private Network-Network Interface Specification v.1.1, (Spécification de l'interface réseau privé-réseau)*, af-pnni-0055.001.

IEEE 802.1ad (2005, Draft 6.0), *Virtual Bridged Local Area Networks – Amendment 4: Provider Bridges (Ponts de fournisseur)*.

IEEE 802.1ag (2005, Draft 4.1), *Virtual Bridged Local Area Networks – Amendment 5: Connectivity Fault Management, (Gestion des fautes de connectivité)*, état: PAR approuvé, tour du groupe de travail en cours.

IEEE 802.1ah (2005, Draft 1.2), *Virtual Bridged Local Area Networks – Amendment 6: (Ponts de réseau dorsal de fournisseur)*, état: PAR approuvé, tour du groupe de travail en cours.

IEEE 802.1Q (2005), *Virtual Bridged Local Area Networks, (Réseaux de zone locale virtuels pontés)*, état: publié.

IEEE 802.1X (2004), *Port-Based Network Access Control, (Contrôle d'accès au réseau fondé sur le port)*, état: publié.

IEEE 802.17 (2004), *Specific requirements – Part 17: Resilient packet ring (RPR) access method and physical layer specifications, (Spécifications de la méthode d'accès par anneau de paquet résilient (RPR) et de la couche physique)*, état: publié.

IEEE 802.3ah (2004), *Specific requirements – Part 3: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications (Amendement: Paramètres de contrôle d'accès au support, couches physiques, et paramètres de gestion pour les réseaux d'accès d'abonnés)*, Ethernet in the First Mile amendment à IEEE Std 802.3.

IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: an Overview (Généralités sur les services intégrés dans l'architecture de l'internet)*.

IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification (Protocole de réservation de ressources (RSVP) – Spécification fonctionnelle version 1)*.

IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol (Architecture de sécurité pour le protocole Internet)*.

IETF RFC 2409 (1998), *The Internet Key Exchange (IKE) (L'échange de clés internet)*.

IETF RFC 2475 (1998), *An Architecture for Differentiated Services (Architecture pour les services différenciés)*.

IETF RFC 2547 (1999), *BGP/MPLS VPNs*.

IETF RFC 3036 (2001), *LDP Specification*.

IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels (RSVP-TE: extensions à RSVP pour les tunnels LSP)*.

IETF draft-ietf-bfd-base-03.txt (2005), *Bidirectional Forwarding Detection, (Détection de la transmission bidirectionnelle)*, travail en cours.

IETF draft-ietf-bfd-mpls-02.txt (2005), *BFD For MPLS LSPs*, travail en cours.

IETF draft-ietf-l2tpext-l2vpn-05.txt (2005), *L2VPN Extensions for L2TP, (Extension L2VPN pour L2TP)*, travail en cours.

IETF draft-ietf-l2vpn-radius-pe-discovery-01.txt (2005), *Using RADIUS for PE-Based VPN Discovery, (Utilisation de Radius pour la découverte de VPN fondés sur l'extrémité fournisseur)*, travail en cours.

IETF draft-ietf-l3vpn-bgpvpn-auto-06.txt (2005), *Using BGP as an Auto-Discovery Mechanism for Network-based VPNs, (Utilisation de BGP comme mécanisme d'autodécouverte pour les VPN fondés sur le réseau)*, travail en cours.

IETF draft-ietf-l3vpn-rfc2547bis-03.txt (2004), *BGP/MPLS VPNs*, travail en cours.

IETF draft-ietf-mpls-lsp-ping-09.txt (2005), *Detecting MPLS Data Plane Failures, (Détection des défaillances de plan de données en MPLS)*, travail en cours.

IETF draft-ietf-pwe3-control-protocol-17.txt (2005), *Pseudowire Setup and Maintenance using the Label Distribution Protocol, (Etablissement et maintenance de pseudocâblage avec le protocole de distribution d'étiquettes)*, travail en cours.

IETF draft-ietf-pwe3-frame-relay-05.txt (2005), *Encapsulation Methods for Transport of Frame Relay Over MPLS Networks, (Méthodes d'encapsulation pour le transport de relais de trame sur des réseaux MPLS)*, travail en cours.

IETF draft-ietf-pwe3-vccv-06.txt (2005), *Pseudo Wire Virtual Circuit Connectivity Verification (VCCV), (Vérification de la connectivité de circuit virtuel en pseudocâblage)*, travail en cours.

Recommandation UIT-T E.164 (2005), *Plan de numérotage des télécommunications publiques internationales*.

Recommandation UIT-T E.800 (1994), *Termes et définitions relatifs à la qualité de service et à la qualité de fonctionnement du réseau, y compris la sûreté de fonctionnement*.

Recommandation UIT-T G.775 (1998), *Critères de détection et d'annulation des défauts de perte de signal, de signal d'indication d'alarme et d'indication de défaut distant en hiérarchie numérique plésiochrone*.

Recommandation UIT-T G.826 (2002), *Paramètres et objectifs relatifs aux caractéristiques d'erreur de bout en bout pour les connexions et conduits numériques internationaux à débit constant*.

Recommandation UIT-T G.827 (2003), *Paramètres et objectifs de disponibilité pour les conduits numériques internationaux de bout en bout à débit constant*.

Recommandation UIT-T G.1000 (2001), *Qualité de service des communications: cadre et définitions*.

Recommandation UIT-T G.1010 (2001), *Catégories de qualité de service multimédia pour l'utilisateur final*.

Recommandation UIT-T G.7714.1/Y.1705.1 (2003), *Protocole d'exploration automatique dans les réseaux à hiérarchie numérique synchrone et les réseaux de transport optiques*.

Recommandation UIT-T I.610 (1999), *Principes et fonctions d'exploitation et de maintenance du RNIS à large bande*.

Recommandation UIT-T Q.933 (2003), *Système de signalisation d'abonné numérique n° 1 du RNIS – Spécification de la signalisation pour la commande et la surveillance de l'état des connexions virtuelles commutées et permanentes en mode trame*.

Recommandation UIT-T Q.2931 (1995), *Système de signalisation d'abonné numérique n° 2 – Spécification de la couche 3 de l'interface utilisateur-réseau pour la commande de connexion/appel de base*.

Recommandation UIT-T X.200 (1994), *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: le modèle de référence de base*.

Recommandation UIT-T Y.1413 (2004), *Interfonctionnement des réseaux TDM et MPLS – Interfonctionnement dans le plan utilisateur*.

Recommandation UIT-T Y.1415 (2005), *Interfonctionnement des réseaux Ethernet-MPLS – Interfonctionnement dans le plan utilisateur*.

Recommandation UIT-T Y.1711 (2004), *Mécanisme d'exploitation et de maintenance pour les réseaux MPLS*.

Recommandation UIT-T Y.1713 (2004), *Détection de mauvais branchement dans les réseaux MPLS*.

Recommandation UIT-T Y.1731 (2006), *Fonctions et mécanismes d'exploitation et de maintenance pour les réseaux fondés sur Ethernet*.

MEF ETH OAM (2003), *Ethernet Services OAM*, Draft.

Frame Relay Forum FRF.8 (1995), *Frame Relay/ATM PVC Service Interworking Implementation Agreement (Accord de mise en œuvre de l'interfonctionnement de service PVC relais de trame/ATM)*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
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	Gestion des télécommunications y compris le RGT et maintenance des réseaux
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, communication entre systèmes ouverts et sécurité
Série Y	**Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération**
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2007