UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Y.1310

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(03/2000)

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

Aspects relatifs au protocole Internet – Transport

Transport des services IP sur des connexions ATM dans les réseaux publics

Recommandation UIT-T Y.1310

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION ET PROTOCOLE INTERNET

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

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

Recommandation UIT-T Y.1310

Transport des services IP sur des connexions ATM dans les réseaux publics

Résumé

Etant donné la croissance rapide des réseaux et des applications fondés sur des services IP, tant dans les réseaux privés que publics, il est nécessaire d'étudier les dispositions nécessaires pour le transport de services IP sur des connexions ATM dans l'environnement des réseaux publics.

Pour l'environnement des réseaux privés, le Forum ATM a spécifié le multiprotocole sur ATM (MPOA, *multi-protocol over ATM*) [21]. Le groupe de travail IETF (IETF, *Internet engineering task force*) a spécifié le modèle IP sur des connexions ATM classique (C-IPOA, *classical IP over ATM*) [25], le protocole de résolution du prochain saut (NHRP, *next hop resolution protocol*) [26] et la commutation par étiquette multiprotocole (MPLS, *multi-protocol label switching*) [31] [32]. Pour assurer que les réseaux publics interfonctionneront les uns avec les autres en prenant en charge l'ensemble des services définis dans la présente Recommandation UIT-T et pour assurer l'interfonctionnement des réseaux publics et privés, il est nécessaire de recommander la méthode préférée pour le transport des services IP sur des connexions ATM dans les réseaux publics.

La méthode adoptée dans la présente Recommandation UIT-T est d'identifier les prescriptions génériques, les services IP clés et de déterminer la méthode IP sur des connexions ATM préférée pour chaque service. Il est recommandé d'utiliser la même méthode pour tous les services considérés. Cette méthode est recommandée pour tous les services identifiés qui utilisent le transport des services IP sur des connexions ATM dans les réseaux publics.

Source

La Recommandation Y.1310 de l'UIT-T, élaborée par la Commission d'études 13 (1997-2000) de l'UIT-T, a été approuvée le 10 mars 2000 selon la procédure définie dans la Résolution 1 de la CMNT.

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.

La Conférence mondiale de normalisation des télécommunications (CMNT), 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 la CMNT.

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

NOTE

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références	1
2.1	Références normatives	1
2.1.1	UIT-T	1
2.1.2	ISOC/IETF	2
2.2	Références informatives	2
2.2.1	Forum ATM	2
2.2.2	ISOC/IETF	2
3	Termes et définitions	3
4	Abréviations et acronymes	3
5	Prescriptions génériques	5
6	Architecture cadre	6
6.1	Architecture réseau	6
6.1.1	Interfonctionnement de réseaux et de services	8
6.2	Architecture de protocole	8
6.2.1	Description générale du modèle de référence de protocole IPOA	8
6.2.2	Description fonctionnelle du modèle de référence du protocole IPOA	9
7	Services IP	11
7.1	Mappage des classes de QS IP avec l'ATM	11
7.1.1	Introduction	11
7.1.2	Modèle de réseau pour la prise en charge de services IP sensibles à la QS	12
7.1.3	Liste de fonctions de mappage de services	14
7.1.4	Mappages de services intégrés IP avec des services ATM	14
7.1.5	Mappages de services IP différenciés avec des services ATM	15
7.2	Réseaux virtuels privés IP (IP-VPN, *IP virtual private network*)	16
7.2.1	Domaine d'application des réseaux IP-VPN	16
7.2.2	Définitions de services IP-VPN	17
7.2.3	Prescriptions pour les services IP-VPN	17
8	Solution réseau préférée	18
8.1	Méthode recommandée	18
8.1.1	Petits réseaux contre grands réseaux	18
8.1.2	Porteuse ATM contre porteuse non ATM	19
8.1.3	Contrôle statique contre contrôle dynamique	19
8.1.4	Contrôle ATM contre contrôle non ATM dans la méthode IPOA	19
8.1.5	Ingénierie du trafic pour les services IP	19
8.1.6	Utilisation des investissements existants	19

Page

8.1.7 Prise en charge de services VPN 19
8.1.8 Aspects QS 19
8.2 Cadre pour la commutation MPLS sur des connexions ATM dans les réseaux publics 20
8.2.1 Modèle architectural 20
8.2.2 Protocole de contrôle pour la commutation MPLS sur des connexions ATM 20
Appendice I – Méthodes de transport de IP sur des connexions ATM 23
I.1 Méthode IP sur des connexions ATM classique 23
I.1.1 Protocole de résolution du prochain saut (NHRP) 24
I.1.2 Utilisation d'un court-circuit ATM local 24
I.2 Multiprotocole sur des connexions ATM (MPOA) 26
I.3 Commutation multiprotocole avec étiquette (MPLS) 28
Appendice II – Lignes directrices en matière de mappage de services avec des connexions ATM 32
II.1 Mappage de services Intserv avec des connexions ATM 32
II.1.1 Mappages de services garantis (GS) en ATM 32
II.1.2 Mappage de service en charge contrôlée (CLS) en ATM 35
II.2 Mappage de services Diffserv sur des connexions ATM 36
II.3 Service Intserv en MPLS sur des connexions ATM 37
II.4 Service Diffserv en MPLS sur des connexions ATM 37
II.4.1 Procédures d'établissement d'un conduit LSP 38
II.4.2 Procédure de réacheminement par étiquette 38
II.4.3 Mappages entre <PSC, CLP> et PHB 39
II.4.4 Considérations relatives à l'implémentation 40
Appendice III – Scénarios possibles d'évolution de la commutation MPLS pour le transport des services IP sur des connexions ATM dans les réseaux publics 40
III.1 Introduction 40
III.2 Scénarios proposés 40
III.2.1 Exploitant établi offrant tous les services 40
III.2.2 Exploitant téléphonique établi 41
III.2.3 Nouvel exploitant centré sur le protocole IP 41
III.2.4 Nouvel exploitant offrant tous les services 41
III.3 Réseau ATM hybride 41
III.3.1 Techniques pour les réseaux ATM hybrides 42
III.3.2 Réseaux utilisant la technique MPLS sur PVC 44
III.3.3 Réseaux utilisant des jonctions virtuelles 46
III.3.4 Réseaux utilisant la technique VCID 48

Page

Appendice IV – Exemples de méthodes de prise en charge de réseaux IP-VPN dans des réseaux publics MPLS/ATM 50
IV.1 Introduction 50
IV.2 Scénario 1 52
IV.2.1 Configuration de réseau simple 52
IV.2.2 Composants du réseau 52
IV.3 Scénario 2 54
IV.3.1 Aperçu général de l'architecture 54
IV.3.2 Composants du réseau 54
Appendice V – Bibliographie 57

Recommandation UIT-T Y.1310

Transport des services IP sur des connexions ATM dans les réseaux publics

1 Domaine d'application

La présente Recommandation UIT-T traite du transport des services IP sur des connexions ATM. Dans la présente Recommandation UIT-T, les services IP sont définis comme étant des services fournis dans la couche IP. Dans la présente Recommandation UIT-T, les services IP n'incluent pas les services fournis dans la couche application (par exemple les services bancaires en réseau).

La présente Recommandation UIT-T identifie la méthode IP sur des connexions ATM préférée pour les réseaux publics qui adoptent la technologie ATM, y compris les réseaux de fournisseurs de services et les réseaux d'exploitants, mais n'interdit pas la même méthode lorsqu'elle est applicable dans les réseaux d'accès, les réseaux privés et les systèmes terminaux. Les méthodes considérées comprennent les protocoles IPOA classique et MPOA et la commutation MPLS. Ces méthodes sont décrites brièvement dans l'Appendice I.

2 Références

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

2.1 Références normatives

2.1.1 UIT-T

[1] Recommandation CCITT I.321 (1991), *Modèle de référence pour le protocole du RNIS à large bande et son application*.

[2] Recommandation UIT-T I.326 (1995), *Architecture fonctionnelle des réseaux de transport fondés sur le mode ATM*.

[3] Recommandation UIT-T I.361 (1999), *Spécifications de la couche ATM du RNIS à large bande*.

[4] Recommandation UIT-T I.364 (1999*)*, *Prise en charge du service support de données sans connexion à large bande par le RNIS à large bande*.

[5] Recommandations UIT-T I.432.1 (1999), I.432.2 (1999), I.432.3 (1999) et I.432.4 (1999), *Interface usager-réseau du RNIS-LB – Spécification de la couche physique*.

[6] Recommandation UIT-T I.356 (2000), *Caractéristiques du transfert de cellules de la couche ATM du RNIS-LB*.

[7] Recommandation UIT-T I.371 (2000), *Gestion du trafic et des encombrements dans le RNIS-LB*.

[8] 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*.

[9] Recommandation UIT-T Q.2941.2 (1999), *Système de signalisation d'abonné numérique n° 2 – Extensions relatives au transport des identificateurs génériques*.

2.1.2 ISOC/IETF

[10] IETF, RFC 768, *Protocole de données d'utilisateur*.

[11] IETF, RFC 791, *Spécification du protocole Internet, Programme Internet DARPA*.

[12] IETF, RFC 793, *Spécification du protocole de commande de transmission, Programme Internet DARPA*.

[13] IETF, RFC 2211, *Spécification du service d'élément de réseau en charge contrôlée*.

[14] IETF, RFC 2212, *Spécification de la qualité de service garantie*.

[15] IETF, RFC 2460, *Spécification du protocole Internet version 6*.

[16] IETF, RFC 2474, *Définition du champ des services différenciés dans les en-têtes IPv4 et IPv6*.

2.2 Références informatives

2.2.1 Forum ATM

[17] Forum ATM/AF-MPOA-0087.000 (1997), *Multiprotocole sur ATM,* version 1.0.

2.2.2 ISOC/IETF

[18] IETF, RFC 2684, *Encapsulation multiprotocole sur la couche d'adaptation ATM 5*.

[19] IETF, Spécification du protocole LDP, *(draft-ietf-mpls-ldp-06.txt)*, octobre 1999.

[20] IETF, Etablissement de conduit LSP fondé sur des contraintes en utilisant le protocole LDP, *(draft-ietf-mpls-ldp-03.txt)*, septembre 1999.

[21] IETF, Extensions du protocole RSVP pour les tunnels LSP, *(draft-ietf-mpls-rsvp-lsp-tunnel-04.txt)*, septembre 1999.

[22] IETF, Codage de pile d'étiquettes MPLS, *(draft-ietf-mpls-label-encaps-07.txt)*, septembre 1999.

[23] IETF, RFC 2205, *Protocole de réservation de ressources (RSVP) – Spécification fonctionnelle de la version 1*.

[24] IETF, RFC 2208, *Déclarations d'applicabilité de la version 1 du protocole RSVP – Lignes directrices pour la mise en place*.

[25] IETF, RFC 2225, *Modèle IP et ARP sur ATM classique*.

[26] IETF, RFC 2332, *Protocole de résolution du prochain saut NBMA (NHRP)*.

[27] IETF, RFC 2597, *Groupe de comportements PHB avec réacheminement assuré*.

[28] IETF, RFC 2598, *Comportement PHB avec réacheminement exprès*.

[29] IETF, RFC 2547, *Réseau privé virtuel BGP/MPLS*.

[30] IETF, RFC 2475, *Architecture des services différenciés*.

[31] IETF, Architecture de commutation par étiquette multiprotocole, *(draft-ietf-mpls-arch-06.txt)*, septembre 1999.

[32] IETF, Cadre général de la commutation par étiquette multiprotocole, *(draft-ietf-mpls-framework-05.txt)*, septembre 1999.

[33] IETF, Prise en charge par la commutation MPLS de services différenciés, *(draft-ietf-mpls-diff-ext-02.txt)*, octobre 1999.

[34] IETF, Commutation MPLS utilisant le protocole LDP et la commutation de circuit virtuel ATM, *(draft-ietf-mpls-atm-02.txt)*, avril 1999.

[35] IETF, Notification d'identificateur VCID sur liaison ATM, *(draft-ietf-mpls-vcid-atm-04.txt)*, juillet 1999.

3 Termes et définitions

Le présent paragraphe contient la liste, par ordre alphabétique, des acronymes associés aux termes clés utilisés dans la présente Recommandation UIT-T et des références aux documents où ils sont définis. On se reportera au paragraphe 4 en ce qui concerne les acronymes et au paragraphe 2 en ce qui concerne les références:

CR-LDP [20]

DS [30]

DSCP [30]

FEC [31]

LIB [31]

LSR [32]

MPLS [32]

PHB [30]

RSVP [23]

VPN [29]

4 Abréviations et acronymes

La présente Recommandation UIT-T utilise les abréviations suivantes:

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

ABR débit disponible (*available bit rate*)

ABT transfert de bloc ATM (*ATM block transfer*)

AESA adresse de système d'extrémité ATM (*ATM endsystem address*)

ARP protocole de résolution d'adresse (*address resolution protocol*)

ATC capacité de transfert ATM (*ATM transfer capability*)

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

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

BUS diffusion et serveur inconnu (*broadcast and unknown server*)

CE bord client (*customer edge)*

CE équipement du client *(customer equipment*)

C-IPOA modèle IP sur ATM classique (*classical IP over ATM*)

CLP priorité de pertes de cellules (*cell loss priority*)

CLS service en charge contrôlée (*controlled load service*)

CoF	fonction de coordination (*coordination function*)
CR-LDP	protocole LDP avec étiquette d'acheminement basé sur les contraintes (*constraint-based routing LDP*)
DBR	débit déterministe (*deterministic bit rate*)
DS	services différenciés (*differentiated services*)
DSCP	point de code de service différencié (*differentiated service code point*)
ER	route explicite (*explicit routing*)
ES	système terminal (*end system*)
FEC	classe d'équivalence de réacheminement (*forwarding equivalence class*)
FIB	base de données de réacheminement (*forwarding information base*)
GFR	débit de trame garanti (*guaranteed frame rate*)
GS	service garanti (*guaranteed service*)
IP	protocole Internet (*Internet protocol*)
IPOA	services IP sur connexions ATM (*IP over ATM*)
IPSF	fonctions de service IP (*IP service functions*)
IP-SSCS	service de convergence propre au service IP (*IP-service specific convergence service*)
IS	service intégré (*integrated service*)
ISP	fournisseur de services IP (*IP service provider*)
LANE	émulation de réseau local (*local area network emulation*)
LDP	protocole de distribution d'étiquettes (*label distribution protocol*)
LEC	client LANE (*LANE client*)
LECS	serveur de configuration LANE (*LANE configuration server*)
LER	routeur de bord utilisant des étiquettes (*label edge router*)
LES	serveur LANE (*LANE server*)
LIB	base de données d'étiquettes (*label information base*)
LIS	sous-réseau Internet logique (*logical Internet subnet*)
LLC	commande de liaison logique (*logical link control*)
LSP	conduit commuté avec étiquette (*label switched path*)
LSR	routeur avec commutation par étiquette (*label switching router*)
MAC	commande d'accès au support (*medium access control*)
MBS	taille maximale des rafales (*maximum burst size*)
MCR	débit cellulaire minimal (*minimum cell rate*)
MPC	client MPOA (*MPOA client*)
MPLS	commutation multiprotocole avec étiquette (*multi-protocol label switch*)
MPOA	multiprotocole sur ATM (*multi-protocol over ATM*)
MPS	serveur MPOA (*MPOA server*)
NAT	traduction d'adresse de réseau (*network address translation*)

NHC client NHRP (*NHRP client*)

NHRP protocole de résolution du prochain saut (*next hop resolution protocol*)

NHS serveur NHRP (*NHRP server*)

NNI interface réseau-réseau (*network to network interface*)

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

PCI information de commande de protocole (*protocol control information*)

PCR débit cellulaire crête (*peak cell rate*)

PDR débit de données de crête (*peak data rate*)

PE bord fournisseur (*provider edge*)

PHB comportement par saut (*per hop behaviour*)

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

PPP protocole point à point

PSC programmation par saut (*per hop scheduling*)

QS qualité de service

RGT Réseau de gestion des télécommunications

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

SBR débit statistique (*statistical bit rate*)

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

SNAP point de rattachement au sous-réseau (*subnet attachment point*)

SSCS service de commande propre au service (*service specific control service*)

TCP protocole de commande de transmission (*transmission control protocol*)

UDP protocole des données d'utilisateur (*user data protocol*)

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

VPN réseau privé virtuel (*virtual private network*)

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

xDSL boucle d'abonné numérique x (*x-digital subscriber loop*)

5 Prescriptions génériques

La présente Recommandation UIT-T impose un certain nombre de prescriptions génériques aux méthodes IP sur des connexions ATM. De telles prescriptions sont applicables à tous les services IP identifiés. Les prescriptions génériques obligatoires sont les suivantes:

- La méthode recommandée doit être indépendante de la version du protocole IP prise en charge.
- La méthode recommandée doit présenter une évolutivité suffisante pour pouvoir prendre en charge de grands réseaux. Des éléments à prendre en considération en matière d'évolutivité comprennent:
  - l'utilisation de valeurs d'identificateurs VCI et VPI;
  - la complexité du calcul de routage dans la couche 2 et la couche 3;
  - la complexité du mécanisme de résolution d'adresse;

– la charge de messagerie de contrôle (par exemple la fréquence d'établissement et de libération des connexions ATM, la fréquence des messages de signalisation IP);

– la complexité du mécanisme de classification des paquets nécessaire à la prise en charge de la classe de QS. Moins la granularité de la classe de QS est importante (par exemple par flux IP, par agrégation de flux IP, par service, telle que pour les services Diffserv), plus le mécanisme de classification de paquet est simple.

• La méthode recommandée doit être en mesure de proposer des solutions efficaces et évolutives pour prendre en charge la multidiffusion IP dans les réseaux ATM.

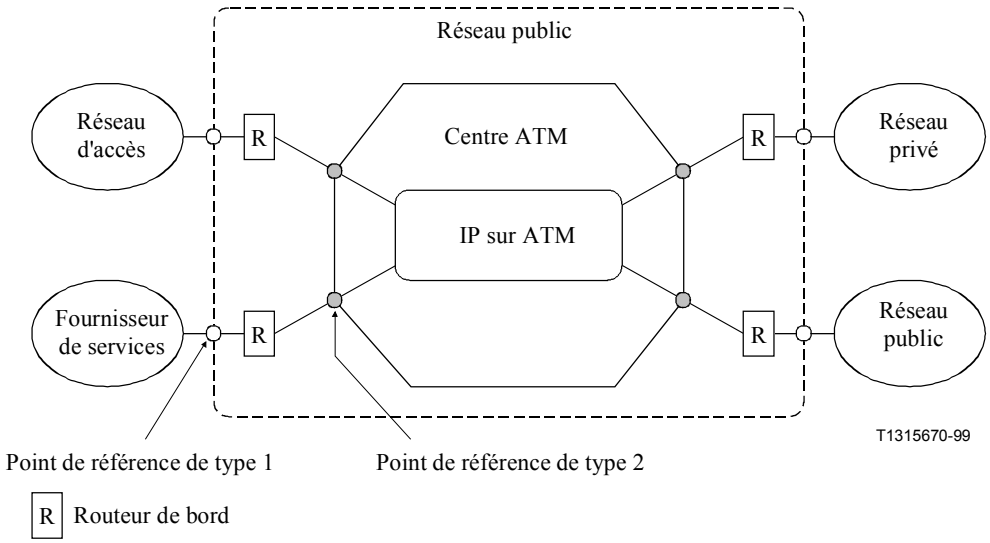
• La méthode recommandée doit être suffisamment robuste pour pouvoir prendre en charge de grands réseaux. Des éléments à prendre en considération comprennent:

– la capacité de prendre en charge des systèmes de récupération.

6 Architecture cadre

L'architecture cadre nécessaire pour prendre en charge les services de couche IP sur des connexions ATM est définie comme comprenant l'architecture réseau et l'architecture de protocole nécessaires pour prendre en charge les services IP nécessaires.

6.1 Architecture réseau



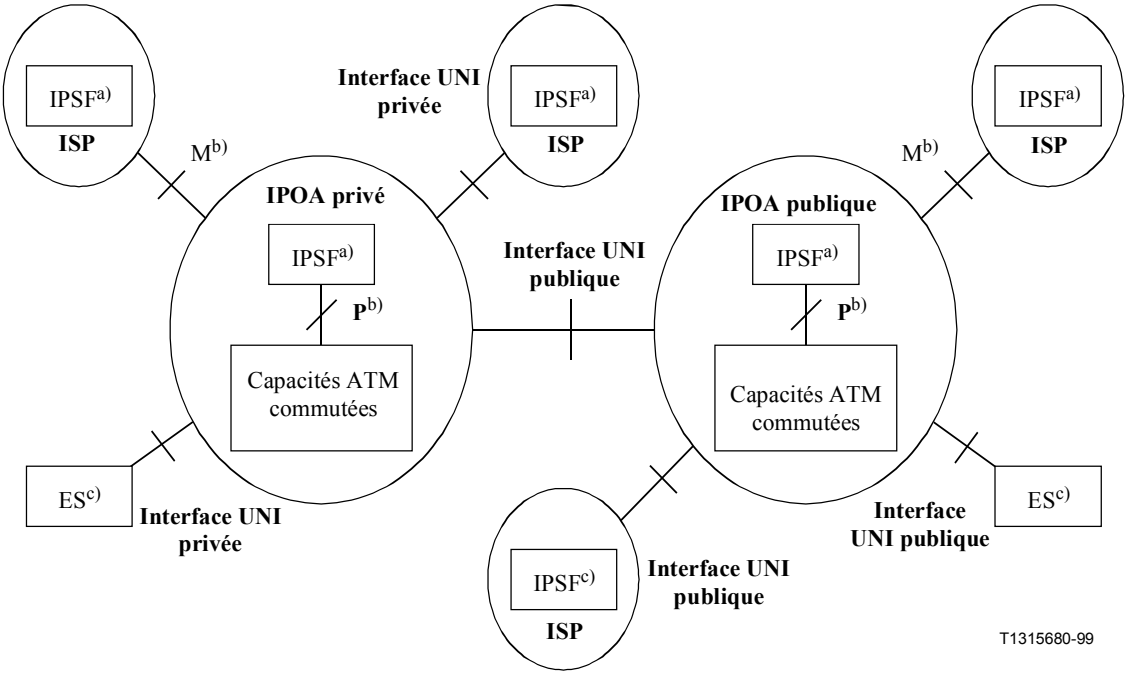
NOTE 1 – Les fournisseurs de services Internet peuvent également fournir le centre ATM.
NOTE 2 – Les points de référence de types 1 et 2 peuvent être des points de référence normalisés tels qu'une interface RNIS S, T ou une interface non normalisée.

Figure 6-1/Y.1310 – Architecture réseau de référence pour IP sur ATM

L'architecture réseau de référence pour IP sur des connexions ATM est illustrée à la Figure 6-1. Cette configuration illustre les scénarios possibles pour prendre en charge les services IP sur ATM identifiés dans la présente Recommandation UIT-T. Le rectangle en pointillés indique un réseau public sur lequel le présent document se concentre. Il est à noter que le réseau public dans la présente Recommandation UIT-T est limité aux réseaux qui ont un centre ATM. Les cases situées à l'intérieur du rectangle en pointillés décrivent les dispositions génériques dans le réseau public: un centre ATM, un réseau IP sur ATM et des routeurs de bord. Un certain nombre de différents types de réseaux sont décrits à l'extérieur du rectangle en pointillés, chacun identifiant un scénario dans lequel

le réseau public fournit un service IP identifié donné à un certain type de réseau. Du point de vue du réseau public, ces réseaux sont considérés comme des réseaux d'abonnés.

Deux points de référence distincts sont décrits dans cette figure. Le point de référence 1 est la limite entre le réseau public et les réseaux d'abonnés et le point de référence 2 est l'interface vers le réseau IP sur des connexions ATM à l'intérieur du réseau public. L'emplacement du point de référence 1 peut dépendre des installations des réseaux d'abonnés et de la définition des services IP assurés. Des fonctions d'interfonctionnement ou des fonctions d'adaptation peuvent être nécessaires dans les routeurs de bord. La présente Recommandation UIT-T se concentre principalement sur le point de référence 2 et sur la méthode adoptée dans le réseau public.



a) IPSF: fonctions de service IP.

b) P ou M: sur la base de la Recommandation UIT-T I.364.

c) ES: le système terminal a une pile de protocole IPOA complète.

Figure 6-2/Y.1310 – Configuration de référence pour services IP sur des connexions ATM

La Figure 6-2 présente la configuration de référence pour les services IP dans des réseaux ATM publics et privés. Dans les réseaux IPOA privés et publics, les services IP sont assurés au moyen de capacités ATM commutées et de fonctions de service IP (IPSF). Dans ce cas, les interfaces entre la capacité ATM commutée et la fonction IPSF doivent être définies aux points de référence P ou M [4]. Les fonctions de service IP (IPSF) sont les fonctions nécessaires pour permettre le transport de IP sur ATM. Un exemple typique de fonction IPSF est le service de résolution d'adresse. En tant que système terminal, la fonction IPSF est essentiellement un routeur avec une interface ATM.

La fonction IPSF peut être mise en œuvre dans le même équipement que les capacités ATM commutées. Dans ce cas, il n'est pas nécessaire de définir l'interface au point de référence P. La fonction IPSF et les capacités ATM commutées peuvent également être mises en œuvre dans des équipements séparés. Dans ce cas, les interfaces doivent être définies aux points de référence M ou P selon que la fonction IPSF se trouve à l'extérieur ou à l'intérieur du réseau central ATM.

Les ISP et les systèmes terminaux (ES) à l'extérieur des réseaux ATM peuvent être connectés aux réseaux ATM privés ou publics. Chaque système terminal a une pile de protocole IPOA complète et est connecté au moyen d'une interface UNI privée pour l'IPOA privé ou d'une interface UNI publique pour l'IPOA public.

6.1.1 Interfonctionnement de réseaux et de services

Dans le scénario d'interfonctionnement de réseaux, l'information de commande de protocole IP (PCI) et la charge utile sont transférées de manière transparente à travers le réseau ATM vers un autre réseau IP au moyen d'une fonction d'interfonctionnement (IWF, *interworking function*) entre les deux réseaux. Généralement, la fonction IWF encapsule simplement le paquet IP au moyen d'une fonction d'adaptation et le transfère de manière transparente vers la fonction IWF distante. Pour l'interfonctionnement courant IP et ATM, l'interfonctionnement de réseaux est le cas typique, l'ATM étant utilisé dans le réseau fédérateur ou central pour le transport du protocole Internet. Dans ce scénario, le réseau ATM peut être considéré comme une sous-couche de transport pour les protocoles de la couche 3 (et supérieurs).

Dans le cas d'interfonctionnement de services, la fonction IWF met fin au protocole IP et traduit les informations PCI en informations PCI de réseau ATM pour les fonctions de transfert, de contrôle et de gestion. Puisqu'il n'est généralement pas possible de prendre en charge toutes les fonctions dans tous les réseaux, le scénario d'interfonctionnement de services est seulement en mesure d'assurer "la meilleure conversion possible" entre deux différentes technologies. Il ne convient toutefois pas que cette conversion entraîne une perte de données d'utilisateur puisque ces données ne sont pas affectées par la conversion des informations PCI dans la fonction IWF d'interfonctionnement de services.

Les Figures 6-1 et 6-2 présentent l'interfonctionnement de réseaux pour services IP sur des connexions ATM.

6.2 Architecture de protocole

6.2.1 Description générale du modèle de référence de protocole IPOA

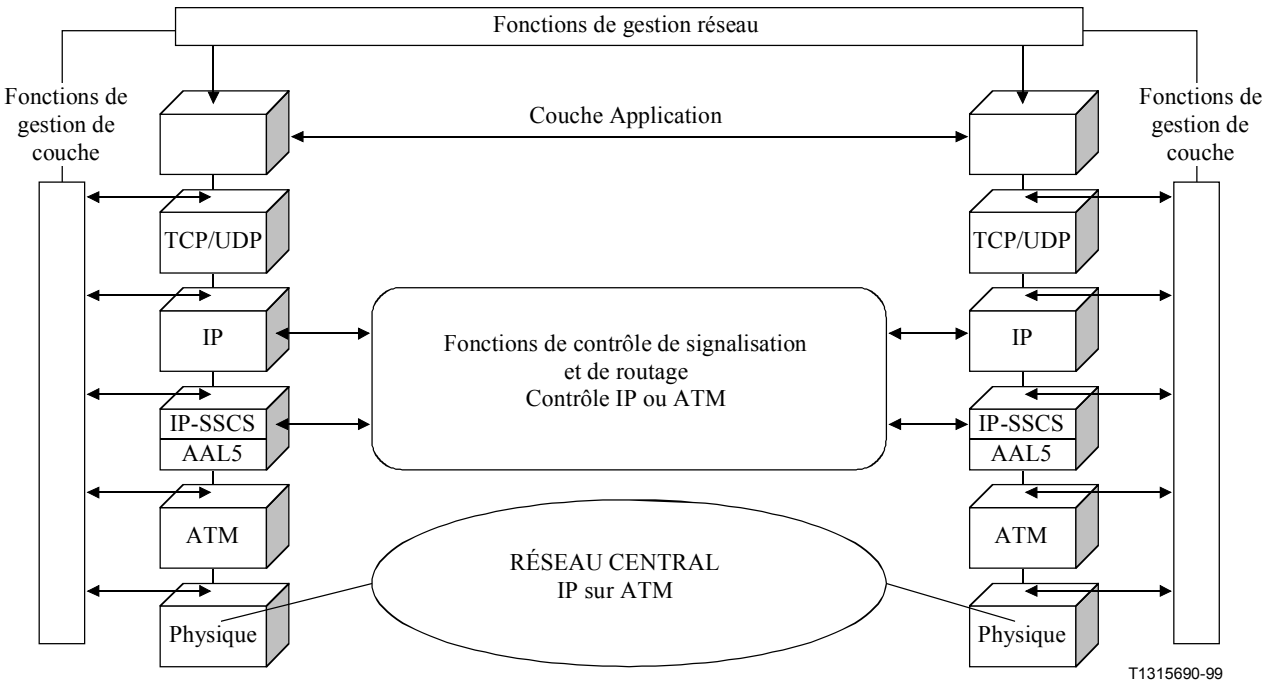


Figure 6-3/Y.1310 – Modèle de référence de protocole pour IP sur des connexions ATM

La Figure 6-3 généralise le modèle de référence de protocole pour le transport de IP sur des connexions ATM dans des réseaux publics. Il peut être noté que les concepts sous-jacents de modèle de référence de protocole gestion de couche, gestion de réseau et contrôle de signalisation et de routage sont étendus pour inclure la couche 3 et les blocs fonctionnels supérieurs. Il convient également de noter que les blocs illustrés à la Figure 6-3 correspondent aux représentations logiques des fonctions et ne signifient ou n'impliquent, par conséquent, pas une mise en œuvre réseau particulière.

Les interfaces entre les blocs fonctionnels peuvent être une communication interne non normalisée entre les sous-couches ou des protocoles externes normalisés. Chaque couche dans le modèle général a son bloc fonctionnel associé de gestion de couche. Les blocs de gestion de couche sont uniquement chargés de traiter la gestion et les informations de commande de protocole (PCI) de cette couche. La communication d'informations entre les couches peut uniquement avoir lieu par la fonction de gestion réseau. Ceci est assuré par la fonction de coordination (CoF) de la gestion réseau.

Il n'est pas nécessaire que tous les blocs fonctionnels soient présents dans toutes les applications réseau du protocole IPOA. Les blocs peuvent ainsi être considérés comme des "modules" fondamentaux permettant toute application réseau de protocole IPOA. Les relations de base et l'ordonnancement entre les différents blocs doivent toutefois être maintenus pour assurer un interfonctionnement cohérent.

6.2.2 Description fonctionnelle du modèle de référence du protocole IPOA

Le présent sous-paragraphe décrit uniquement les blocs fonctionnels relatifs au protocole IPOA puisque les fonctions de couche Physique, ATM et de contrôle ATM sont traitées dans d'autres Recommandations UIT-T [1], [2], [3], [5] et [8]. Le bloc de couche d'application est hors du domaine d'application de la présente Recommandation UIT-T.

6.2.2.1 Fonctions IP-SSCS/AAL5

L'IP-SSCS/AAL5 comprend les fonctions de transfert nécessaires pour mapper le paquet IP avec l'AAL5. Le bloc fonctionnel IP-SSCS/AAL5 assure les fonctions d'encapsulage et de multiplexage multiprotocole définies par le protocole de contrôle de la couche de liaison/du point de rattachement au sous-réseau (LLC/SNAP, *link layer control/subnetwork attachment point*) fondé sur l'IEEE 802.2 tel qu'adopté par l'IETF dans la référence [18].

6.2.2.2 Fonctions de couche IP

Les fonctions de couche IP assurent le réacheminement IP (acheminement de datagrammes IP) d'une source vers une destination par un système interconnecté. Le réacheminement IP est le processus consistant à recevoir un paquet et à utiliser un processus de décision à très faible en-tête pour déterminer comment traiter le paquet. Le paquet peut soit être acheminé localement, soit réacheminé en externe. Pour le trafic qui est réacheminé en externe, le processus de réacheminement IP détermine également l'interface par laquelle il convient d'envoyer le paquet et enlève, le cas échéant, une encapsulation de couche de support pour la remplacer par une autre ou modifie certains champs de l'encapsulation de la couche de support.

L'architecture du protocole IPOA doit être indépendante de la version IP. Il existe actuellement deux versions, IPv4 (IP version 4) et IPv6 (IP version 6). Les fonctions de couche IP sont identiques à celles définies par l'IETF dans les références [11] et [15] conformément à l'IPv4 et l'IPv6 respectivement.

Les fonctions de couche IP ne constituent pas de fonctions de communication fiables. Il n'y a pas d'accusé de réception, que ce soit de bout en bout ou de saut en saut.

Il est à noter qu'il ne faut pas changer les fonctions de couche IP pour utiliser des fonctions IP-SSCS/AAL5 sur ATM.

6.2.2.3 Fonctions de gestion de couche IP

La fonction de gestion de couche IP a deux fonctions de base: l'adressage et la fragmentation. Les fonctions de couche IP utilisent les adresses acheminées dans l'en-tête IP pour transmettre les datagrammes IP vers leurs destinations. Le choix du conduit pour la transmission est résolu en utilisant le bloc de fonctions de signalisation et de routage. Les fonctions de couche IP utilisent des champs dans l'en-tête IP pour fragmenter et réassembler les datagrammes IP lorsque cela est nécessaire pour la transmission.

Le protocole IPv4 utilise quatre mécanismes clés fondamentaux pour assurer son service: le type de service, la durée de vie, les options et la somme de contrôle d'en-tête. Le protocole IPv6 est une nouvelle version de protocole Internet destinée à succéder au protocole IPv4. Les changements entre le protocole IPv4 et le protocole IPv6 appartiennent principalement aux catégories suivantes: les capacités d'adressage étendues, la simplification du format d'en-tête, la prise en charge améliorée des extensions et options, la capacité d'étiquetage de flux et les capacités d'authentification et de confidentialité. La fonction de gestion de couche IP n'assure pas un contrôle d'erreur pour les données, uniquement une somme de contrôle de l'en-tête. Il n'y a pas de retransmissions. Il n'y a pas de contrôle du flux.

6.2.2.4 Fonctions de la couche Transport

La couche Transport comprend des fonctions TCP en mode connexion et des fonctions UDP sans connexion. Celles-ci dépendent du type de programme d'application.

Les fonctions TCP assurent un service de connexion fiable entre processus homologues. Les fonctions TCP sont identiques à celles définies par l'IETF dans la référence [12]. Les fonctions TCP comprennent les caractéristiques suivantes: le transfert de données standard, la fiabilité, le contrôle de flux, le multiplexage, la connexion, la préséance et la sécurité.

Les fonctions UDP assurent le transfert de datagrammes. Les fonctions UDP sont identiques à celles définies par l'IETF dans la référence [10]. Le protocole UDP est orienté transaction, l'acheminement et la double protection ne sont pas garantis.

Il est à noter qu'il ne faut pas changer les fonctions de couche Transport pour utiliser des fonctions de couche IP sur des connexions ATM.

6.2.2.5 Fonctions de couche Application

La couche Application et ses blocs fonctionnels de gestion de couche comprennent des applications propres à l'utilisateur ou au réseau telles que HTTP, FTP, TELNET, etc. La description des fonctions de la couche Application est hors du domaine d'application de la présente Recommandation UIT-T.

Il est à noter que dans l'architecture de protocole TCP/IP, on considère généralement que la fonction de couche Application comprend les fonctions de couche Session et Présentation.

6.2.2.6 Fonctions de gestion du réseau

Les fonctions de gestion du réseau dépendent de l'application réseau spécifique pour l'IPOA. Elles comprennent généralement les fonctions RGT (réseau de gestion des télécommunications) associées à: la gestion des dérangements, la gestion de la qualité de fonctionnement, la gestion de configuration, la gestion de sécurité, etc.

6.2.2.7 Fonctions de contrôle de signalisation et de routage

Ceci comprend les blocs fonctionnels de signalisation et de routage dans le contrôle IP ou ATM. Le contrôle et la signalisation IP englobent différents aspects du contrôle IP, y compris le routage. Le contrôle ATM inclut la signalisation et le routage ATM.

7 Services IP

Une gamme de services IP est incluse dans la présente Recommandation UIT-T afin de déterminer la méthode IP sur des connexions ATM préférée dans les réseaux publics. En premier lieu, le mappage des classes de QS IP avec les services ATM et VPN est traité. Les services additionnels appellent un complément d'étude.

7.1 Mappage des classes de QS IP avec l'ATM

7.1.1 Introduction

Le groupe IETF a explicité deux méthodes principales pour la prise en charge de la différenciation des classes de QS au niveau IP: le paradigme Intserv destiné à prendre en charge la différenciation de classe de QS par flux IP et le paradigme Diffserv destiné à prendre en charge une différenciation "grossière" de classe de QS pour l'agrégation des flux IP.

7.1.1.1 Le paradigme IP Intserv

Le paradigme Intserv repose sur des demandes explicites de QS par flux IP acheminées par le protocole RSVP et sur des contrôles d'admission de flux au niveau des routeurs compatibles RSVP le long du trajet du flux. Deux services sont définis dans le paradigme Intserv: le service garanti – GS [14] et le service en charge contrôlée – CLS [13]. Dans le service GS, la durée maximale de mise en file d'attente est contrôlée pour le flux. Pour calculer le retard maximal qu'un datagramme subira, l'attente du conduit doit être déterminée et additionnée à la durée maximale de mise en file d'attente [14]. Le service CLS ne donne pas de garantie stricte de durée, mais le service offert au flux doit être comparable au service dont le flux profiterait dans un réseau légèrement chargé, même si ce n'est pas le cas [13]. En pratique, le service CLS nécessite une largeur de bande disponible à long terme.

Les deux services requièrent que les caractéristiques du flux soient spécifiées au moyen d'une case à jetons [23] et que l'excès de trafic soit traité au mieux.

7.1.1.2 Le paradigme IP Diffserv

Le modèle IETF Diffserv est fondé sur le concept de comportements par saut (PHB, *per hop behaviour*) [16] et [30]. Les comportements PHB Diffserv sont définis par un ensemble de comportements de réacheminement que chaque routeur local le long du trajet adopte. Jusqu'à présent, le groupe IETF a identifié deux comportements PHB:

- Comportement PHB avec réacheminement exprès (EF, *expedited forwarding*) [28]:

  Le comportement EF-PHB est caractérisé par une quantité configurable de largeur de bande qui ne subit pas l'incidence des autres trafics qui partagent la liaison. Le comportement peut être utilisé pour établir un service de bout en bout qui requiert de faibles taux de perte, de faibles temps de propagation et de faibles variations de délai dans les domaines Diffserv.

- Groupe de comportements PHB avec réacheminement assuré (AF, *assured forwarding*) [27]:

  Le groupe de comportements AF-PHB est caractérisé par quatre classes de AF et chaque classe se voit attribuer une certaine quantité de ressources de réacheminement telles que de la mémoire-tampon et de la largeur de bande dans un nœud Diffserv. Dans chaque classe AF, les paquets IP sont marqués avec une valeur de préséance de suppression possible parmi trois valeurs. En cas d'encombrement, la préséance de suppression d'un paquet détermine l'importance relative du paquet dans la classe AF. Il n'existe toutefois aucune relation normalisée entre les qualités de fonctionnement relatives des quatre classes AF. Le groupe de comportements AF-PHB peut être utilisé pour assurer que le débit d'information souscrit d'un service est garanti avec une probabilité élevée.

7.1.2 Modèle de réseau pour la prise en charge de services IP sensibles à la QS

Le présent sous-paragraphe décrit un modèle de réseau pour prendre en charge des services IP sensibles à la QS dans des réseaux IPOA. Dans le cadre IETF, la QS de bout en bout est fournie en couplant des régions Intserv au bord du réseau avec des régions Diffserv dans le centre du réseau. Le modèle de réseau proposé ici offre toutefois des possibilités supplémentaires. La couche de liaison est en outre toujours supposée être ATM.

7.1.2.1 Description du modèle

Les modèles de réseau envisageables pour prendre en charge les services IP sensibles à la QS sont illustrés aux Figures 7-1, 7-2 et 7-3. Dans chaque cas, la zone grisée indique la fonction active utilisée.

Cas 1 Intserv dans des réseaux ATM

Dans ce modèle, la communication entre deux tronçons de réseau Intserv est prise en charge par des réseaux centraux IPOA. Les dispositifs IPOA dans les réseaux centraux peuvent assurer des capacités tant Intserv que Diffserv. Seule la fonctionnalité Intserv des dispositifs IPOA sera toutefois activée pour prendre en charge les services intégrés de bout en bout. Les deux accords au niveau service (SLA 1 et SLA 2) nécessitent que les prescriptions du service Intserv soient satisfaites.

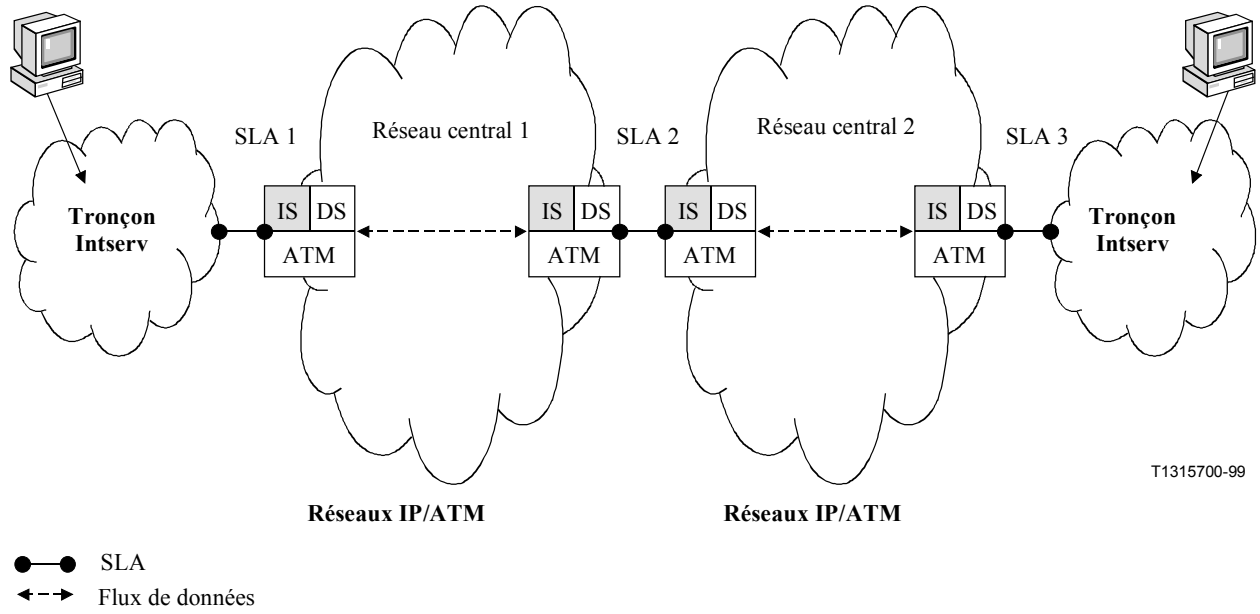


Figure 7-1/Y.1310 – Modèle de réseau pour la prise en charge de Intserv sur des connexions ATM

Cas 2 Diffserv dans des réseaux ATM

Dans ce modèle, la communication entre deux tronçons de réseau Diffserv est prise en charge par des réseaux centraux IPOA. Les dispositifs IPOA dans les réseaux centraux peuvent assurer des capacités tant Intserv que Diffserv. Seule la fonctionnalité Diffserv des dispositifs IPOA sera toutefois activée pour prendre en charge les services différenciés de bout en bout. Les deux accords au niveau service (SLA 1 et SLA 2) nécessitent que les prescriptions du service Diffserv soient satisfaites.

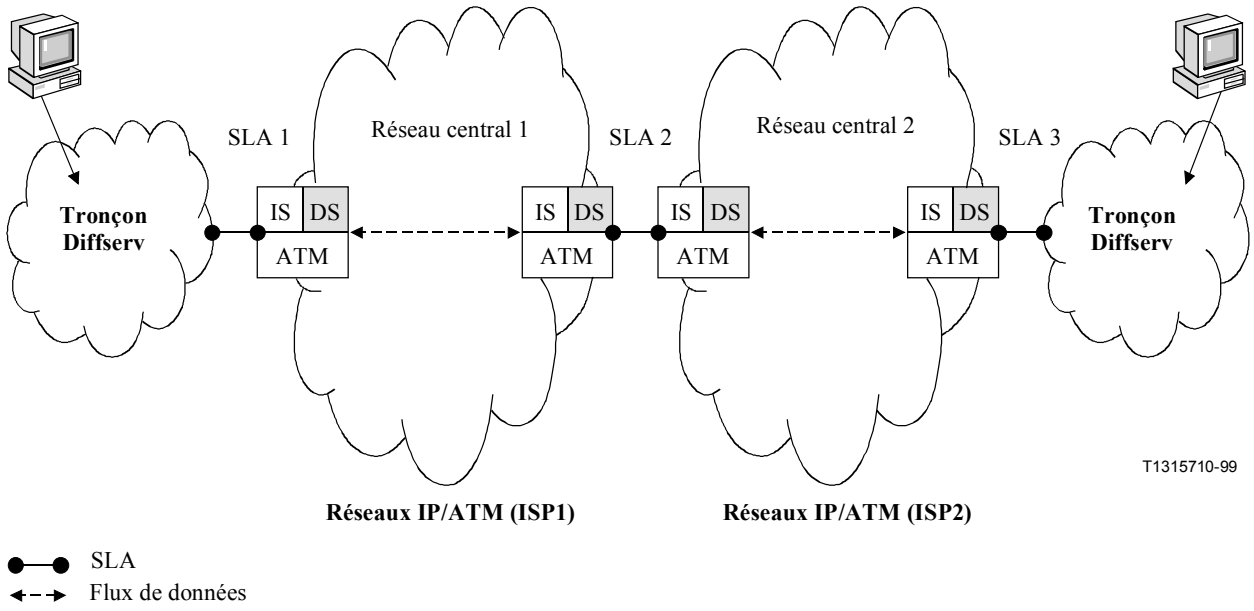


Figure 7-2/Y.1310 – Modèle de réseau pour la prise en charge de Diffserv sur des connexions ATM

Cas 3 Intserv par des domaines Diffserv dans des réseaux ATM

Dans ce modèle, la communication entre deux tronçons de réseau Intserv est prise en charge par des réseaux centraux IPOA. Dans les réseaux centraux IPOA, certains domaines peuvent seulement assurer des capacités Diffserv alors que d'autres peuvent assurer des capacités Intserv et Diffserv. Dans ce cas, la capacité Intserv peut être transportée de manière transparente par des domaines Diffserv seulement. Dans ce cas, il y a deux types d'accord au niveau service.

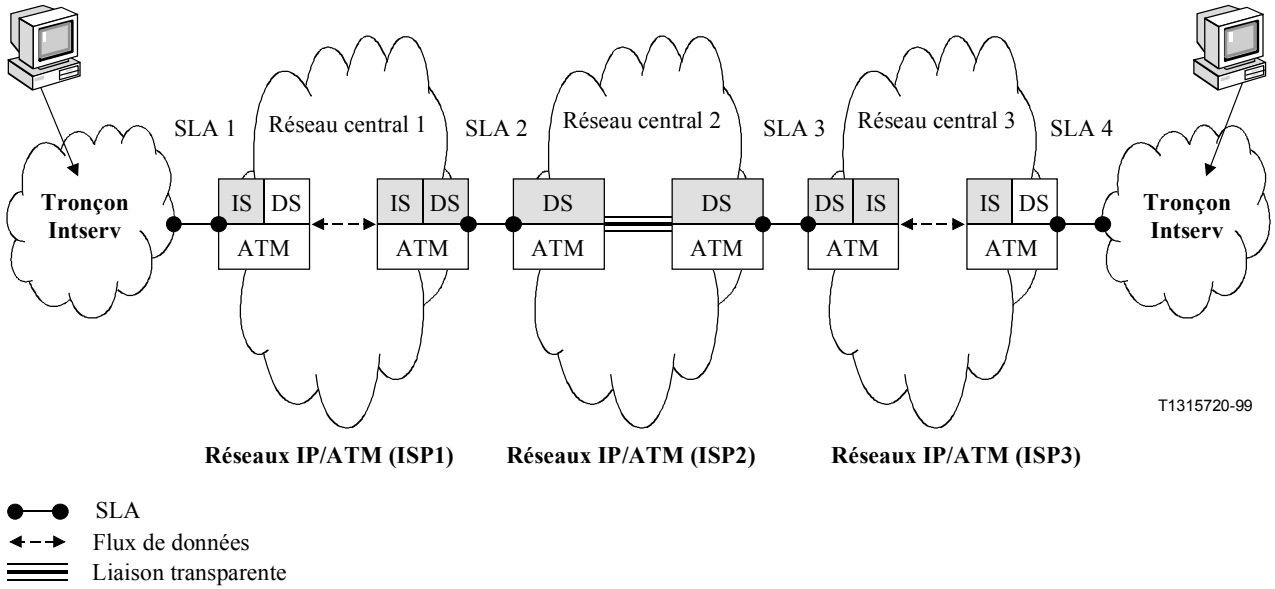


Figure 7-3/Y.1310 – Modèle de réseau pour la prise en charge de Intserv par des domaines Diffserv sur des connexions ATM

7.1.3 Liste de fonctions de mappage de services

Les fonctions de mappage de services ne dépendent pas de l'architecture du réseau environnant mais uniquement de la manière dont la QS IP et ATM est prise en charge des deux côtés de l'interface lorsque le mappage est nécessaire. La Figure 7-4 présente ainsi l'ensemble nécessaire de mappages possibles de services IP en services ATM de l'architecture cadre considérée (voir le paragraphe 6).

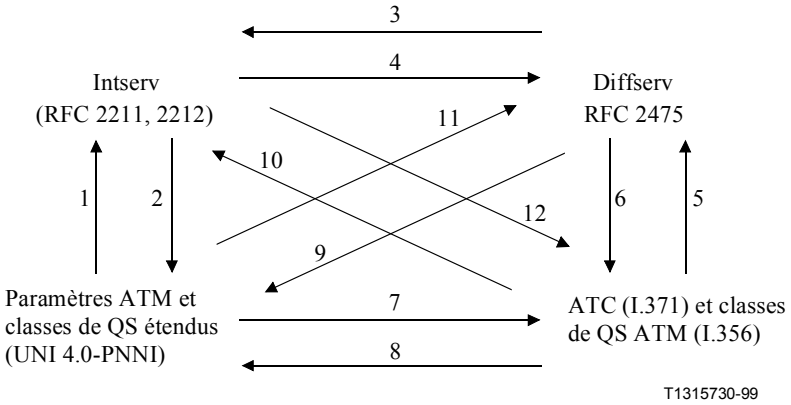


Figure 7-4/Y.1310 – Liste de fonctions de mappage de services

Parmi tous ces mappages, seuls les mappages 6 et 12 sont traités dans la présente Recommandation UIT-T. Il est à noter que dans ce cas, aucune fonction de mappage de type 5 ou 10 n'est nécessaire à la sortie de la portion ATM puisque la prise en charge de la QS dans le réseau IP de destination est entièrement fondée sur les informations de niveau IP qui sont acheminées de manière transparente par la portion ATM. Les mappages 5 et 10 peuvent être nécessaires dans le cas d'un trafic natif ATM qui doit franchir ou atteindre un réseau entièrement IP et appellent un complément d'étude.

Les mappages 3 et 4 appartiennent uniquement au domaine IP et font partie de l'activité du groupe IETF, alors que tous les mappages en provenance/se terminant dans les paramètres ATM étendus et classes de QS (pris en charge dans les réseaux ATM privés) font partie du travail du forum ATM.

7.1.4 Mappages de services intégrés IP avec des services ATM

La question du mappage de Intserv avec ATM est soulevée chaque fois qu'un flux IP nécessitant des services garantis (GS) [14] ou des services en charge contrôlée (CLS) [13] doivent être pris en charge par une connexion ATM reliant deux routeurs compatibles Intserv et est indépendante de la méthode spécifique de prise en charge des services IP sur des connexions ATM.

Deux différents types de mappage sont prévus: le mappage de un à un et le mappage de plusieurs à un.

7.1.4.1 Mappage de un à un

Le mappage de un à un est observé lorsqu'une seule connexion ATM est entièrement dédiée à la prise en charge d'un flux IP unique. Le processus de mappage consiste notamment dans le choix d'un service ATM (en d'autres termes la capacité ATC et la classe de QS associée) qui peut satisfaire les engagements en matière de QS pour le service IP (GS ou CLS). Dans cette optique, plusieurs mappages peuvent être envisagés. De manière plus générale, il est toutefois également possible de considérer le processus de mappage comme une manière de communiquer, au niveau ATM, des informations supplémentaires concernant les caractéristiques du flux acheminé pour que le réseau ATM situé en aval puisse les utiliser et acheminer la connexion de manière efficace (par exemple en la multiplexant avec d'autres). De ce point de vue, il est possible de classer tous les mappages envisageables et certains mappages sont meilleurs que d'autres.

7.1.4.2 Mappage de plusieurs à un

Le mappage de plusieurs à un est observé lorsqu'une seule connexion ATM peut acheminer plusieurs flux IP. Dans ce cas, le processus de mappage est constitué du choix d'un service ATM qui satisfait à tous les engagements en matière de QS d'un ensemble de flux IP. Puisque les flux IP commencent et se terminent généralement de manière asynchrone, ce mappage peut être considéré comme un processus d'agrégation qui, sur la base des caractéristiques de niveau IP du flux (par exemple QS de case à jetons ou demandée), décide de la possibilité d'acheminer le flux avec d'autres sur une connexion ATM existante (tout en respectant les contraintes de QS du flux IP) ou de la nécessité de renégocier les paramètres de connexion.

Les règles de prise de décision sont hors du domaine d'application de la présente Recommandation UIT-T.

7.1.4.3 Mappages de services garantis (GS) en ATM

L'ATM ne nécessite pas d'extensions pour réaliser ces mappages. Il convient toutefois que le schéma de mappage satisfasse les prescriptions suivantes:

- la capacité ATC choisie doit être en mesure de prendre en charge les prescriptions de temps de propagation;
- la capacité ATC choisie doit être en mesure de réserver une certaine quantité de largeur de bande pour le flux.

L'Appendice II fournit des suggestions et des conseils sur la mise en œuvre de ces mappages.

7.1.4.4 Mappage de service en charge contrôlée (CLS) en ATM

L'ATM ne nécessite pas d'extensions pour réaliser ces mappages. L'Appendice II fournit des suggestions et des conseils sur la mise en œuvre de ces mappages. Il convient toutefois que le schéma de mappage satisfasse les prescriptions suivantes:

- la capacité ATC choisie doit être en mesure de réserver une certaine quantité de largeur de bande pour le flux.

7.1.4.5 Incidence sur la gestion de trafic ATM

Ce point appelle un complément d'étude.

7.1.4.6 Incidence sur la signalisation ATM

Ce point appelle un complément d'étude.

7.1.4.7 Incidence sur le routage ATM

Ce point appelle un complément d'étude.

7.1.5 Mappages de services IP différenciés avec des services ATM

Le modèle de services IP différenciés (Diffserv) se sert du concept de comportement par saut (PHB, *per hop behaviour*) [16] et [30] pour permettre des services IP fondés sur la QS.

Les comportements PHB peuvent être utilisés comme un facteur important pour définir un service IP dans le domaine Diffserv. Le comportement PHB n'est toutefois pas lui-même associé aux services IP de QS de bout en bout. Il convient par conséquent de fonder le mappage entre Diffserv et ATM sur des services IP et des services ATM. Les services IP peuvent notamment être définis par une combinaison de mises en œuvre de comportement PHB avec des caractéristiques de trafic aux extrémités des domaines Diffserv et les services ATM peuvent être définis par une combinaison de capacités de transfert ATM [7] avec des classes de QS [6].

7.1.5.1 Mappage de services

Pour fournir des services aux abonnés, les fournisseurs de Diffserv doivent combiner des mises en œuvre de comportement PHB avec des conditionneurs de trafic et des stratégies de fourniture de service. Le concept de comportement PHB n'est pas traité en ATM. Le mappage de comportements PHB avec les capacités de transfert ATM ne semble, par conséquent pas approprié. Le mappage d'un service différencié particulier avec un service ATM peut en revanche être envisagé. Le mappage de services de Diffserv avec ATM est clairement assuré par la négociation entre deux fournisseurs de réseau, sur la base de la définition des services IP considérés.

Le mappage de services dépend par conséquent de la politique des fournisseurs de services et peut varier fortement entre différents fournisseurs de services. Des exemples de mappages de services envisageables sont fournis dans l'Appendice II.

Les prescriptions suivantes s'appliquent au mappage de services:

- il n'est pas nécessaire d'associer un débit minimum à la prise en charge de certains comportements PHB Diffserv sur des connexions ATM.

Il est également nécessaire de considérer le service qualitatif ou relatif. Des solutions appellent un complément d'étude.

7.1.5.2 Incidence sur la gestion de trafic ATM

Ce point appelle un complément d'étude.

7.1.5.3 Incidence sur la signalisation ATM

Ce point appelle un complément d'étude.

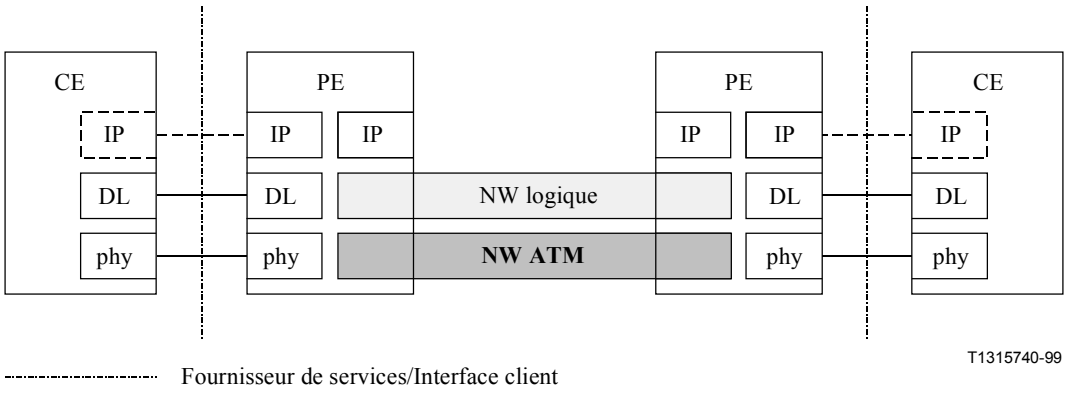
7.1.5.4 Incidence sur le routage ATM

Ce point appelle un complément d'étude.

7.2 Réseaux virtuels privés IP (IP-VPN, *IP virtual private network*)

7.2.1 Domaine d'application des réseaux IP-VPN

Dans la présente Recommandation UIT-T, le réseau IP-VPN est défini comme une émulation d'installations de réseau privé étendu IP fournie sur un réseau de transport ATM à échelle d'un exploitant. La Figure 7-5 présente les dispositions du réseau IP-VPN dans la présente Recommandation UIT-T. Un exemple de méthode pour démontrer la prise en charge d'un réseau IP-VPN dans un réseau public MPLS/ATM est fourni dans l'Appendice IV.



CE Equipement d'abonné (*customer equipment*)
PE Routeur de bord de fournisseur (*provider edge number*)

Figure 7-5/Y.1310 – Modèle de réseau pour réseau IP-VPN

Un site d'abonné est connecté au réseau du fournisseur de services par un équipement d'abonné (CE). Il peut s'agir d'un hôte isolé, d'un commutateur ou d'un routeur IP. D'autre part, le réseau du fournisseur de services se connecte au site de l'abonné avec un routeur de bord de fournisseur (PE). Lorsque l'équipement CE est un routeur, il est possible de le configurer de manière à ce qu'il soit un homologue de routage du routeur PE, mais il n'est pas un homologue de routage de l'équipement CE de l'autre site. Les routeurs des différents sites n'échangent pas directement des informations de routage les uns avec les autres. Cette disposition permet facilement de prendre en charge de très grands réseaux VPN, alors que la stratégie de routage de chaque site individuel est fortement simplifiée. Cette capacité est considérée être importante pour les fournisseurs de services à l'échelle d'un exploitant qui fournissent le service IP-VPN externalisé.

7.2.2 Définitions de services IP-VPN

Le service IP-VPN permet aux sites abonnés de former des groupes: vers et en provenance desquels l'accès IP est limité. Ce groupe est appelé IP-VPN. Un site spécifique peut être membre d'un ou de plusieurs IP-VPN. Les sites membres d'un IP-VPN spécifique peuvent communiquer entre eux en utilisant le protocole IP. Des sites spécifiques peuvent disposer de capacités supplémentaires leur permettant d'accéder à des sites en dehors du groupe ou inversement.

7.2.3 Prescriptions pour les services IP-VPN

7.2.3.1 Prescriptions dans le plan de l'utilisateur

7.2.3.1.1 Prise en charge du transport de paquet opaque

Le transport de paquet opaque permet aux abonnés d'un réseau IP-VPN d'utiliser des adresses IP indépendantes au sein de leur réseau. Les réseaux de fournisseurs de services doivent avoir la capacité de router des paquets IP en fonction de l'appartenance VPN, même s'ils utilisent des espaces d'adresse chevauchants. Les fonctions pour identifier un VPN (par exemple l'utilisation d'un identificateur VPN-ID) ou la fonction pour différencier le réacheminement par paquet VPN peut être nécessaire.

7.2.3.1.2 Prise en charge de la sécurité des données

La sécurité des données assure aux abonnés IP-VPN un certain niveau de communication sécurisée entre les sites membres d'un IP-VPN. Il est nécessaire que les réseaux des fournisseurs de services s'assurent contre l'espionnage de données, l'acheminement erroné ou l'insertion erronée de paquets. Des fonctions de filtrage, de chiffrage et d'autorisation peuvent être nécessaires.

7.2.3.1.3 Prise en charge de QS

La QS permet aux abonnés IP-VPN de souscrire à un certain niveau d'assurance de qualité de communication entre les sites membres d'un IP-VPN. Il est nécessaire que les réseaux des fournisseurs de services aient la capacité de prendre en charge n'importe quelle catégorie de service QS de la même manière que pour fournir des services IP généraux. Le sous-paragraphe 7.1 décrit ces capacités en détail.

7.2.3.2 Prescriptions dans le plan de commande

7.2.3.2.1 Prise en charge de la signalisation des ressources de réseau logique

Il convient que les fournisseurs de services aient la capacité de signaler les ressources de leur réseau pour prendre en charge le transport de paquets IP pour des abonnés IP-VPN.

7.2.3.2.2 Prise en charge du transport d'identificateurs VPN-ID

Ce point appelle un complément d'étude.

7.2.3.2.3 Prise en charge de routage par VPN

Ce point appelle un complément d'étude.

7.2.3.3 Prescriptions dans le plan de gestion

7.2.3.3.1 Identificateurs VPN-ID interopérables

Si un réseau IP-VPN couvre plusieurs fournisseurs de services, il peut être nécessaire que le réseau de chaque fournisseur distingue correctement le trafic IP-VPN. Dans ce cas, la définition généralement acceptée d'identificateur VPN-ID est nécessaire pour réduire le traitement de routeurs de bord.

7.2.3.3.2 Prise en charge de la gestion des membres de IP-VPN

Il convient que les fournisseurs de services aient la capacité de gérer les informations d'appartenance VPN, par exemple quel site abonné appartient à quel IP-VPN. Il convient que cette capacité assure une interopérabilité suffisante pour prendre en charge les réseaux IP-VPN qui couvrent plusieurs fournisseurs de services.

7.2.3.3.3 Prise en charge de la configuration de ressources de réseau logique

Il convient que les réseaux des fournisseurs de services aient la capacité de configurer les ressources de leur réseau pour prendre en charge le transport de paquets IP pour des abonnés IP-VPN. Il convient que cette capacité assure une interopérabilité suffisante pour prendre en charge les réseaux IP-VPN qui couvrent plusieurs réseaux.

8 Solution réseau préférée

8.1 Méthode recommandée

En tenant compte des prescriptions génériques décrites au paragraphe 5 ainsi que des services décrits au paragraphe 7, il est recommandé d'adopter la commutation MPLS [31] et [32] comme la seule méthode préférée sur les réseaux publics. La commutation MPLS prend en charge tous les services identifiés. Il est reconnu que la commutation MPLS ne présente pas d'avantages sensibles par rapport à une méthode IP sur des connexions ATM classique bien conçue (telle que décrite au I.1.2) pour la prise en charge des services Intserv. La commutation MPLS n'offre toutefois pas moins que la méthode IPOA classique pour la prise en charge d'Intserv alors qu'elle assure également la prise en charge de tous les autres services.

D'autres arguments pour le choix de la commutation MPLS comme la seule méthode préférée comprennent:

8.1.1 Petits réseaux contre grands réseaux

Il est bien connu que le protocole MPOA est très bien adapté aux petits réseaux mais qu'il est limité quand il s'agit de l'appliquer à de grands réseaux. La présente Recommandation UIT-T est destinée aux fournisseurs de services et vise par conséquent des grands réseaux. La commutation MPLS a été conçue pour satisfaire les prescriptions de grands réseaux en termes de souplesse, d'évolutivité et de facilité de gestion.

8.1.2 Porteuse ATM contre porteuse non ATM

Alors que l'objectif de la présente Recommandation UIT-T est le transport de IP sur des connexions ATM, il est important de garder à l'esprit que de grands réseaux peuvent avoir plusieurs technologies de porteuses distinctes, y compris de type ATM. Dans un domaine d'application plus large, il est important de choisir une technologie qui est optimale pour le transport des services IP sur des connexions ATM mais qui est en même temps optimale pour le transport des services IP sur d'autres technologies de couche de liaison. La commutation MPLS est probablement la seule technologie envisageable qui couvre ce domaine d'application étendu.

8.1.3 Contrôle statique contre contrôle dynamique

Du point de vue du routage, l'architecture MPLS offre la possibilité d'avoir, et en même temps de choisir entre, le routage attribué et le routage dynamique. L'exploitant de réseau est libre de choisir la méthode.

8.1.4 Contrôle ATM contre contrôle non ATM dans la méthode IPOA

Il est préférable de disposer d'un contrôle générique qui est indépendant de la couche de liaison. Le contrôle ATM peut en outre toujours être utilisé dans les mêmes commutateurs en mode SIN [32].

8.1.5 Ingénierie du trafic pour les services IP

L'ATM dispose de l'ensemble le plus complet de fonctionnalités d'ingénierie du trafic connu actuellement. La superposition des modèles IP sur des connexions ATM peut toutefois ne pas utiliser toutes les capacités ATM de manière efficace et avoir tendance à limiter l'évolutivité en raison du problème bien connu de la "puissance n" lorsqu'un réseau complet de connexions PVC est fourni. La commutation MPLS emprunte certaines capacités de technologie ATM en termes de QS, de routage, de gestion des ressources et d'autres aspects et y ajoute la notion de routage explicite pour faciliter le mappage des demandes de trafic avec les topologies du réseau. L'utilisation de la commutation MPLS offre ainsi des caractéristiques de gestion du trafic nouvelles en en plus grand nombre qu'avant.

8.1.6 Utilisation des investissements existants

Vu les investissements existants dans les technologies ATM et autres, il est manifestement nécessaire d'acheminer le trafic IP sur des connexions ATM et autres protocoles de couche de liaison, une technologie de commutation unitaire est par conséquent nécessaire. Dans les réseaux actuels d'exploitant, le matériel ATM est utilisé en mode attribué pour acheminer le trafic IP, la commutation MPLS est considérée être l'évolution logique du protocole C-IPOA dans un proche avenir puisque le routage explicite peut être développé sur la base des connexions PVC fournies et que l'architecture est suffisamment souple pour accepter des évolutions potentielles du réseau.

8.1.7 Prise en charge de services VPN

Le principal avantage de la commutation MPLS est son aptitude à fournir des services en mode connexion par un routage sans connexion ou explicite, ce qui la rend idéale pour la tunnelisation dynamique. Il n'existe aucun moyen unique de fournir des réseaux VPN de type MPLS, ce qui rend la comparaison plus difficile que pour d'autres technologies IPOA.

8.1.8 Aspects QS

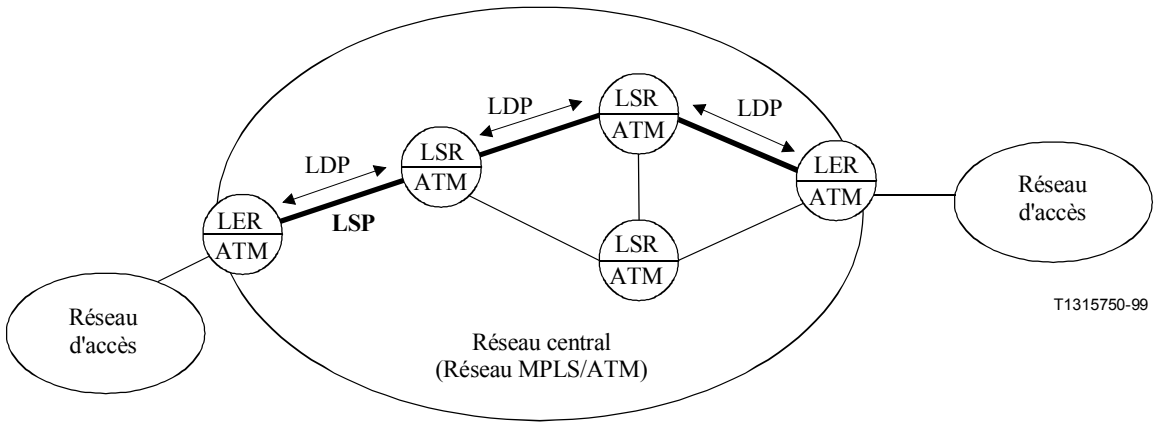
Il existe une synergie évidente entre les services IP différenciés et la commutation MPLS, puisque les deux évoluent avec les prescriptions du fournisseur de services intégrées de manière intrinsèque dans leur conception. L'étiquette, avec sa sémantique étendue, peut acheminer des informations relatives au service Diffserv et des conduits LSP de bout en bout peuvent garantir la cohérence des mécanismes de QS dans un domaine MPLS spécifique par des mécanismes de réservation de ressources appropriés.

8.2 Cadre pour la commutation MPLS sur des connexions ATM dans les réseaux publics

8.2.1 Modèle architectural

La Figure 8-1 illustre le modèle général d'un réseau central MPLS/ATM. Le réseau public est mis en œuvre en tant que réseaux MPLS avec ATM composés de routeurs de bord utilisant des étiquettes (LER, *label edge router*) et de routeurs avec commutation par étiquette (LSR, *label switching router*). Le routeur LER est situé au bord du réseau MPLS en tant que routeur d'entrée/de sortie compatible MPLS. Le bord du réseau MPLS ne coïncide pas nécessairement avec le bord du réseau ATM central. Le routeur LER assure toutes les fonctions de la couche 3 et de rattachement d'étiquette fondées sur la base de données d'étiquette (LIB, *label information base*) générée par le protocole LDP en cours. Le routeur LER est connecté à des routeurs LSR internes. Le routeur LSR réalise l'échange d'étiquettes fondé sur la base LIB. Le conduit LSP (*label switched path*) entre les routeurs LER ou le routeur LER et le routeur LSR est établi en utilisant le protocole LDP [19] et [22].

Sur la base de ce modèle simple, différents services IP tels que la QS IP (Intserv et Diffserv) et IP-VPN peuvent être fournis de manière efficace et souple à l'abonné IP par différents réseaux d'accès (par exemple ATM pur, relais de trames, xDSL, IP pur, etc., y compris des domaines non MPLS).



LDP Protocole de distribution d'étiquette
LER Routeur de bord utilisant des étiquettes
LSP Conduit commuté avec étiquette
LSR Routeur avec commutation par étiquette

Figure 8-1/Y.1310 – Modèle d'un réseau central MPLS/ATM

8.2.2 Protocole de contrôle pour la commutation MPLS sur des connexions ATM

- *Mode d'annonce d'étiquette*

  Dans les réseaux MPLS sur des connexions ATM, les identificateurs VCI et VPI ATM sont utilisés en tant qu'étiquette. L'étiquette peut être annoncée dans les réseaux de deux différentes manières:

  – un protocole de distribution d'étiquettes explicite tel que le protocole LDP;

  – le passage en double avec d'autres messages de contrôle tels que les protocoles RSVP, BGP, etc.

  Tant la distribution d'étiquettes explicite que le passage en double peuvent être utilisés dans le réseau. Dans la présente Recommandation UIT-T toutefois, le protocole LDP est recommandé pour la distribution d'étiquette saut par saut.

- *Mode d'attribution d'étiquette*

  L'étiquette peut être attribuée à un routeur LSR du réseau des deux manières suivantes:

  – le mode spontané dans le sens descendant;

  – le mode sur demande dans le sens descendant.

  Dans la présente Recommandation UIT-T, le mode sur demande dans le sens descendant est recommandé comme mode d'annonce de l'étiquette dans les réseaux MPLS sur des connexions ATM pour les raisons suivantes:

  – dans le mode sur demande dans le sens descendant, les valeurs des identificateurs VPI/VCI ne sont consommées que lorsqu'elles sont demandées;

  – le mode sur demande dans le sens descendant ressemble plus à la signalisation conventionnelle telle que la signalisation ATM et il peut par conséquent interopérer avec des réseaux publics existants.

- *Mode de contrôle d'un conduit commuté avec étiquette (LSP*)

  Les étiquettes d'un conduit LSP sont contrôlées des deux manières suivantes:

  – le mode de contrôle ordonné de conduit LSP, où un routeur LSR ne rattache une étiquette à une classe FEC donnée que s'il est le routeur LSR de sortie pour cette classe FEC ou s'il a déjà reçu une étiquette de rattachement pour cette classe FEC en provenance du saut suivant pour cette classe FEC;

  – le mode de contrôle indépendant de conduit LSP, où chaque routeur LSR décide de façon indépendante, dès qu'il reconnaît une classe FEC donnée, de rattacher une étiquette à cette classe FEC et de distribuer ce rattachement à ses homologues distribuant des étiquettes.

  Dans la présente Recommandation UIT-T, le mode de contrôle ordonné est recommandé pour les raisons suivantes:

  – dans le mode de contrôle indépendant, il est possible, puisque chaque routeur LSR attribue de manière indépendante les étiquettes pour les classes d'équivalence de réacheminement IP, que différents routeurs LSR prennent des décisions incohérentes. Le mode de contrôle ordonné n'est pas concerné par ce problème;

  – par rapport au mode de contrôle indépendant, les ressources telles que les identificateurs VCI/VPI peuvent être utilisées de manière plus efficace dans le mode de contrôle ordonné.

Deux méthodes de signalisation sont envisageables pour satisfaire aux prescriptions d'ingénierie du trafic du fournisseur de services:

1) MPLS/LDP avec CR-LDP.

2) MPLS/LDP avec extension RSVP-TE.

Pour les raisons suivantes, il est recommandé que les fournisseurs de services sélectionnent une seule des deux méthodes:

- bien que les caractéristiques de protocole diffèrent, le protocole CR-LDP et l'extension RSVP offrent des fonctions clés semblables et permettent d'atteindre les mêmes objectifs. Il convient par conséquent que les réseaux publics n'en choisissent qu'un seul;
- il est plus facile, dans un environnement multi-fournisseurs de services et multi-vendeurs, d'atteindre l'interopérabilité en prenant en charge un protocole de signalisation commun;
- la gestion de deux protocoles engendre des frais et une complexité supplémentaires.

Pour les raisons suivantes, il est recommandé que le protocole CR-LDP soit le seul protocole de signalisation pour les réseaux de type MPLS:

- **simplicité du réseau (les protocoles CR-LDP et LDP constituent un seul protocole)**: le protocole CR-LDP [20] est une extension du protocole LDP [19] et utilise les mêmes messages et mécanismes que le protocole LDP pour la détection d'homologues, l'établissement et le maintien de session, la distribution d'étiquettes et le traitement d'erreur. Les protocoles LDP et CR-LDP offrent ainsi un système unifié et commun de protocole de signalisation qui fournit aux exploitants de réseau tous les modes de distribution d'étiquettes et d'établissement de conduit nécessaires pour la commutation MPLS. Les extensions de RSVP et MPLS/LDP sont en revanche deux protocoles différents avec différents ensembles de messages et différentes procédures de protocole. Ils imposent à un réseau MPLS de déployer un protocole supplémentaire (RSVP). L'adoption d'extensions RSVP dans un réseau MPLS serait à l'origine d'une complexité et de coûts inutiles;
- **fiabilité de protocole (CR-LDP fonctionne sur TCP)**: le protocole CR-LDP fonctionne sur le transport TCP fiable. En cas de défaillance, une procédure simple d'indication d'erreur est utilisée, protégée par la couche de transport fiable pour assurer une réponse et un rétablissement rapides. Le protocole RSVP fonctionne en revanche sur le transport IP de base. Toutefois, en raison du manque d'infrastructure de transport fiable, le protocole RSVP ne peut pas garantir une notification rapide des défaillances. Le protocole RSVP dispose d'un mécanisme de contrôle explicite, mais il n'est pas envoyé de manière fiable. Il peut en résulter que les points d'extrémité ne commencent pas à rerouter le trafic avant l'expiration de l'intervalle d'acquittement;
- **évolutivité (le protocole CR-LDP est facilement évolutif)**: dans un réseau de grande échelle, où le nombre de micro-flux est important, deux questions principales d'évolutivité se posent. Premièrement, les prescriptions de ressources, en termes de traitement et de mémoire, augmentent proportionnellement avec le nombre de micro flux [24]. Deuxièmement, des mises à jour périodiques de protocole RSVP sont prescrites pour maintenir des états souples de routeur dans des grands réseaux fédérateurs d'exploitant. Cette évolutivité est plus importante dans les grands réseaux d'exploitant, lorsque les messages tels que les confirmations sont acheminés sur un protocole IP non fiable;
- **aptitude à l'emploi pour l'ATM (le protocole CR-LDP est plus proche de l'ATM)**: du point de vue architectural, le protocole CR-LDP ressemble au mode ATM: Interfonctionnement: le mappage des messages entre la signalisation CR-LDP et la signalisation ATM est relativement aisé en raison des ressemblances inhérentes entre les protocoles Q.2931 et CR-LDP. Tant le contrôle d'appel ATM que le protocole CR-LDP sont déclenchés par la source;
- **services différenciés (le protocole CR-LDP vise le Diffserv)**: le protocole CR-LDP fournit les modules pour la prise en charge et le mappage des services différenciés IP. Son architecture permet au fournisseur de services de mapper le service Diffserv avec les paramètres de trafic tels que signalés par le protocole CR-LDP. Le protocole RSVP vise la prise en charge des services intégrés IP. Il est généralement reconnu que le service Diffserv est mieux adapté aux réseaux fédérateurs d'exploitant alors que Intserv est destiné aux réseaux d'entreprise.

Il est à noter que les protocoles d'établissement pour la prise en charge complète de la mise en œuvre de la qualité de service de bout en bout ne sont pas encore disponibles.

APPENDICE I

Méthodes de transport de IP sur des connexions ATM

I.1 Méthode IP sur des connexions ATM classique

La méthode IP et ARP sur des connexions ATM classique (C-IPOA, *classical IP and ARP over ATM*) est défini dans la référence [25]. La Figure I.1 fournit une description fonctionnelle de la méthode IP sur des connexions ATM classique.

La méthode C-IPOA définit un mécanisme pour le transport dans des réseaux ATM de différents types de protocoles, y compris le transport de IP sur des connexions ATM en utilisant une couche AAL5. Dans cette méthode, il est possible de choisir entre deux types d'encapsulation lorsqu'une voie de type VC ATM (PVC ou SVC) est établie. Il s'agit de l'encapsulation IEEE 802.2 Contrôle de couche de liaison/Point de rattachement au sous-réseau (LLC/SNAP, *link layer control/subnet attachment point*) ou du multiplexage de type VC. L'encapsulation LLC/SNAP est le format de paquet par défaut pour les datagrammes IP. Dans le multiplexage LLC/SNAP, la distinction entre les protocoles est assurée par l'utilisation d'un identificateur de protocole LLC/SNAP dans chaque message de couche 3, IP dans le cas présent. Il est possible d'utiliser le mécanisme de multiplexage de type VC pour réduire l'en-tête d'encapsulation. Le protocole à utiliser sur une voie VC est défini pendant le temps d'établissement de la voie VC et est maintenu tout au long du temps de connexion de la voie VC. Ce mécanisme ne permet toutefois pas de bénéficier de l'encapsulation multiprotocole disponible dans l'encapsulation LLC/SNAP.

L'encapsulation multiprotocole seule, bien qu'elle soit nécessaire, ne suffit pas à assurer le routage et le réacheminement des datagrammes IP sur des connexions ATM. La résolution d'adresses IP en adresses natives ATM est requise. Le document [25] définit un modèle IP sur des connexions ATM classique. La Figure I.1 présente les blocs fonctionnels pour construire les plans de signalisation, de gestion et d'utilisateur et les flux de messages entre un hôte IP et un serveur de ATMARP. Un réseau ATM est découpé en domaines administratifs et fonctionnels discrets appelés sous-réseaux IP logiques (LIS, *logical IP subnet*). Chaque sous-réseau LIS fonctionne indépendamment des autres LIS. Tous les membres (hôtes et routeurs) au sein d'un sous-réseau LIS ont le même préfixe d'adresse et les mêmes masques d'adresse de réseau/sous-réseau IP. Dans ce modèle, le déploiement du mode ATM est utilisé en tant que remplacement direct des réseaux étendus prenant en charge le protocole IP. Ainsi, un serveur de type protocole de résolution d'adresse (ARP, *address resolution protocol*), appelé ATMARP, est nécessaire pour la résolution des adresses IP cibles en adresses ATM cibles au sein d'un sous-réseau LIS donné. Les adresses ATM peuvent être des adresses E.164 ou des adresses ATM de système terminal (AESA). Les fonctions ATMARP restent dans un sous-réseau LIS donné.

Dans le modèle classique, les hôtes communiquent entre eux en mode ATM au sein d'un même sous-réseau LIS en utilisant le service ATMARP pour la résolution d'adresse cible. La communication en dehors du sous-réseau LIS local est assurée par un routeur IP. L'utilisation du protocole de résolution du prochain saut (NHRP, *next hop resolution protocol*) pour communiquer entre les sous-réseaux LIS est une extension du modèle classique (voir la Figure I.1 et le § I.1.1). Le protocole ATMARP est un protocole client-serveur demande-réponse. Les clients ATMARP (hôtes ATM) doivent être configurés avec les adresses ATM du serveur ATMARP ou doivent en être informés par l'ILMI avant que l'opération demande-réponse soit possible. Avant toute opération demande-réponse ATMARP, un client ATMARP doit établir une connexion SVC ou utiliser une connexion PVC préconfigurée pour s'enregistrer auprès du serveur ATMARP (étape 1 de la Figure I.1). Pendant l'opération ATMARP, le client envoie un message de demande ATMARP au serveur par cette connexion VCC. Les adresses IP et ATM source sont incluses dans le message de demande avec l'adresse IP cible. Il est prévu que le serveur réponde avec l'adresse ATM cible correspondante dans un message de réponse ATMARP s'il est possible de résoudre l'adresse IP. Dans le cas contraire, un message ATMARP-NAK est retourné (étapes 2 á 6 de la Figure I.1). Une fois l'adresse ATM cible

résolue, la communication peut commencer entre deux hôtes en établissant une connexion VCC ATM et en réalisant le transfert de données (étapes 7 et 8 de la Figure I.1). Chaque client ATMARP conserve un tableau qui contient les enregistrements des entrées d'adresses résolues. Un client doit mettre à jour ce tableau par rapport à son serveur au cours de la période de péremption en utilisant la procédure d'enregistrement. Un processus de résolution d'adresse inverse (In ATMARP) est également fourni dans le modèle classique et sert à résoudre l'adresse IP cible en fonction de l'adresse ATM cible d'un membre de sous-réseau LIS.

I.1.1 Protocole de résolution du prochain saut (NHRP)

Le protocole NHRP, spécifié dans la référence [26], étend le modèle classique en permettant la communication entre plusieurs sous-réseaux LIS. Dans le protocole NHRP, une station source (hôte ou routeur), connue comme client source de prochain saut (NHC, *source next hop client*), qui tente de communiquer avec une station cible connue sous la désignation de NHC cible (hôte ou routeur), utilise le protocole de demande et réponse NHRP pour obtenir l'adresse ATM de la station cible. Une demande NHRP traverse une série de serveurs NHRP (NHS) le long du conduit défini par le protocole de routage en cours d'utilisation jusqu'à ce qu'elle atteigne le NHS qui dessert la station cible, puis une réponse NHRP est renvoyée à la station source. Un conduit "court-circuit" est alors établi entre les stations sources et cibles par le biais d'un circuit virtuel ATM direct. Si la station cible se trouve au sein du réseau ATM desservi par un serveur NHS, elle sera atteinte directement par ce court-circuit. Un routeur de sortie "le plus proche" de la cible sera connecté par le biais du serveur NHS si elle se trouve en dehors de ce réseau ou pour une quelconque contrainte politique. Si l'hôte cible n'est desservi par aucun serveur NHS, une réponse NHRP négative sera renvoyée et le routage vers la cible suivra le protocole de routage normal.

I.1.2 Utilisation d'un court-circuit ATM local

Le protocole NHRP se révèle particulièrement utile lorsque des flux IP exigeant une certaine QS (par exemple des flux Intserv GS ou CLS) doivent être pris en charge, puisqu'il élimine les sauts IP à chaque limite de sous-réseau LIS. Il nécessite toutefois l'introduction dans le réseau de serveurs dédiés et ajoute la complexité d'un autre protocole de demande-réponse. Le retard d'établissement de la connexion de court-circuit prenant en charge le flux peut en outre être important.

Une autre manière d'éviter les multiples sauts IP sans qu'il soit nécessaire de réaliser des ajouts sur le modèle classique est de réaliser des courts-circuits ATM locaux à chaque limite de sous-réseau LIS [54]. Pour cela, il est nécessaire que les routeurs de bord de sous-réseau LIS soient des dispositifs IP/ATM hybrides, en d'autres termes pas uniquement des routeurs avec des interfaces ATM mais des commutateurs IP/ATM intégrés capables de partager des informations entre les deux couches.

Les fonctions de base qu'il convient notamment que ces dispositifs hybrides réalisent sont:

- l'établissement et la tenue à jour d'un tableau d'association entre les flux IP et les connexions ATM qui les prennent en charge, dans le sens entrant et sortant;
- le court-circuit ATM local sur la base de ce tableau d'association.

L'effort d'établir un tel tableau d'association ne vaut toutefois que la peine d'être fourni pour les flux IP exigeant une certaine QS et ayant une longue durée. Les flux Intserv GS ou CLS exigeant une certaine QS par signalisation RSVP sont les exemples les plus directs.

Il est à noter que si le dispositif hybride est chargé d'établir des connexions ATM en réponse à la réception de messages de signalisation RSVP, l'établissement du tableau d'association dans le sens sortant est direct et ne nécessite pas l'utilisation d'un mécanisme normalisé particulier: une communication interne entre les composants IP et ATM du dispositif suffit. Pour le sens entrant, en revanche, le dispositif hybride doit exploiter certaines informations qui peuvent être acheminées dans les messages de signalisation ATM. La nouvelle Recommandation UIT-T Q.2941.2 [9] définit notamment la capacité de signalisation DSS2 pour acheminer, entre autres, des identificateurs relatifs à Internet (par exemple un identificateur de session Ipv4 ou Ipv6 identifiant un flux IP). Ces

informations sont évidemment disponibles si des dispositifs hybrides analogues situés en amont se chargent de remplir les champs susmentionnés dans les messages de signalisation ATM.

Le tableau ci-dessous énumère si et comment le dispositif hybride peut exploiter le tableau d'association et réaliser des court-circuits ATM locaux, en fonction du type d'association entre les flux IP et les connexions ATM (un flux IP par connexion ATM ou de nombreux flux IP sur une seule connexion ATM).

Dans le cas 1, le maximum d'avantages est obtenu: le flux IP est pris en charge dans plusieurs sous-réseaux LIS par concaténation de connexions ATM, mais bénéficie, grâce à la possibilité du réacheminement à la volée, d'une QS identique à celle dont elle profiterait dans le cas d'une connexion ATM directe.

Dans le cas 3 (fusion de voies VC), le seul avantage est d'éviter le traitement au niveau IP mais le réacheminement à la volée est impossible. Dans les deux autres cas, le traitement IP reste nécessaire et aucun gain de qualité de fonctionnement n'est possible sur ce saut.

	Association entrante	**Association sortante**	**Traitement IP nécessaire**	**Réacheminement à la volée autorisé**
1	Un à un	Un à un	Non	Oui
2	Plusieurs à un	Un à un	Oui	Non
3	Un à un	Plusieurs à un	Non	Non
4	Plusieurs à un	Plusieurs à un	Oui	Non

Dans un tel scénario, chaque dispositif hybride est responsable de l'association dans le sens sortant, en fonction d'une politique donnée. Il peut par exemple décider de toujours établir une connexion ATM séparée pour chaque flux IP GS et, ainsi, avoir une association de un à un et de toujours fusionner les flux CLS sur une seule connexion ATM pour économiser des identificateurs VCI. Un choix coordonné de politiques pour les dispositifs hybrides d'un même domaine administratif est évidemment souhaitable.

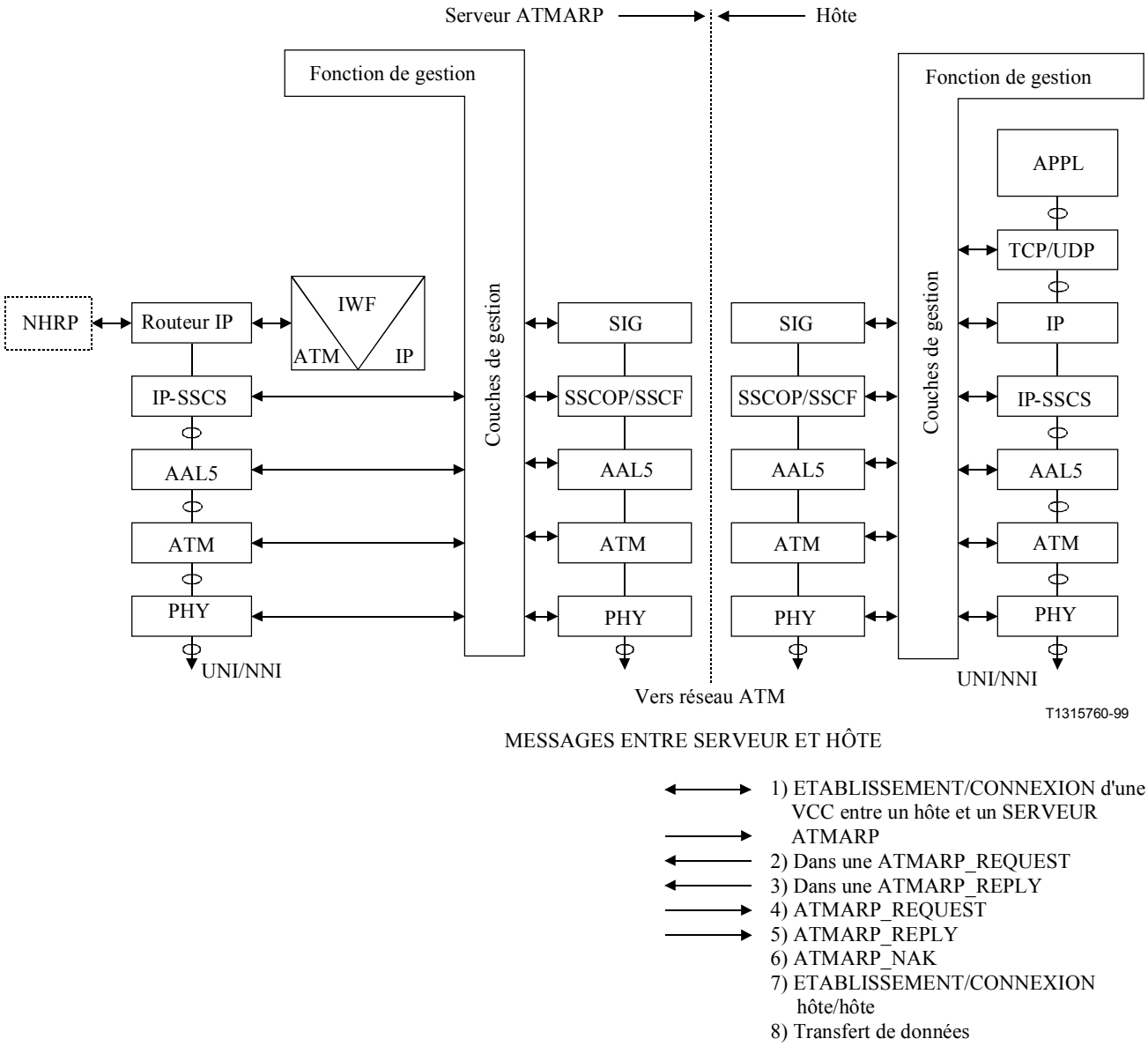


Figure I.1/Y.1310 – Description fonctionnelle de la méthode IP et ARP sur des connexions ATM classique

I.2 Multiprotocole sur des connexions ATM (MPOA)

La référence [17] spécifie un environnement générique de pontage et de routage pour le transport de multiprotocole (par exemple paquets IP) sur des connexions VCC ATM directes. La technologie combine la technologie d'émulation de réseau local (LANE, *local area network emulation*) avec la technologie de protocole de résolution du prochain saut (NHRP, *next hop resolution protocol*) pour assurer un paradigme de court-circuit ATM. La Figure I.2 illustre les blocs fonctionnels du MPOA, présentant la relation entre les plans de commande, de gestion et de données. Les composants MPOA dans cette figure sont: NHS, NHC, MPC, MPS et LANE. Leurs fonctions sont expliquées ci-dessous.

L'émulation LANE fait partie intégrante du protocole MPOA. L'émulation LANE découpe un grand réseau ATM en plusieurs domaines dont chacun peut être émulé comme un segment de réseau LAN. L'émulation LANE spécifie un ensemble de protocoles pour les utilisateurs de LAN pour communiquer entre eux au sein d'un environnement ATM. Ces utilisateurs d'émulation LANE peuvent être des systèmes terminaux connectés ATM ou des utilisateurs connectés à un réseau LAN. Les services IP sont pris en charge dans cet environnement LAN. Le protocole d'émulation LANE

fonctionne entre les couches ATM AAL5 et le réseau et les couches LLC. L'émulation LANE a quatre composants LANE principaux: le client LANE (LEC), le serveur LANE (LES), le serveur de diffusion et inconnu (BUS) et le serveur de configuration LANE (LECS). Un client LEC (par exemple une station de LAN) obtient des informations de configuration en provenance d'un serveur LECS et s'enregistre auprès de celui-ci. Un serveur LES résout les adresses MAC des clients d'émulation LANE en leurs adresses ATM correspondantes. Le protocole de résolution d'adresse (LE_ARP) fonctionne de manière semblable à celui utilisé par IP ARP. Dans un état stable, les voies de données directes VC ATM sont utilisées pour le raccordement de ces clients pour le transfert de données. Le serveur BUS distribue les données-client avant l'achèvement de la résolution d'adresse et l'établissement des conduits de données ou lorsque le client ne sait pas quelle voie de données VC il doit utiliser. Les paquets IP sont acheminés par encapsulation LLC/SNAP ou par multiplexage VC tel que décrit plus haut.

L'autre partie intégrante du MPOA est le protocole NHRP, qui est décrit au I.1. Le modèle IP sur des connexions ATM classique est soumis à la contrainte de desservir un seul sous-réseau LIS. Le protocole NHRP étend cette capacité en permettant des "courts-circuits" dans plusieurs sous-réseaux LIS au sein d'un réseau ATM.

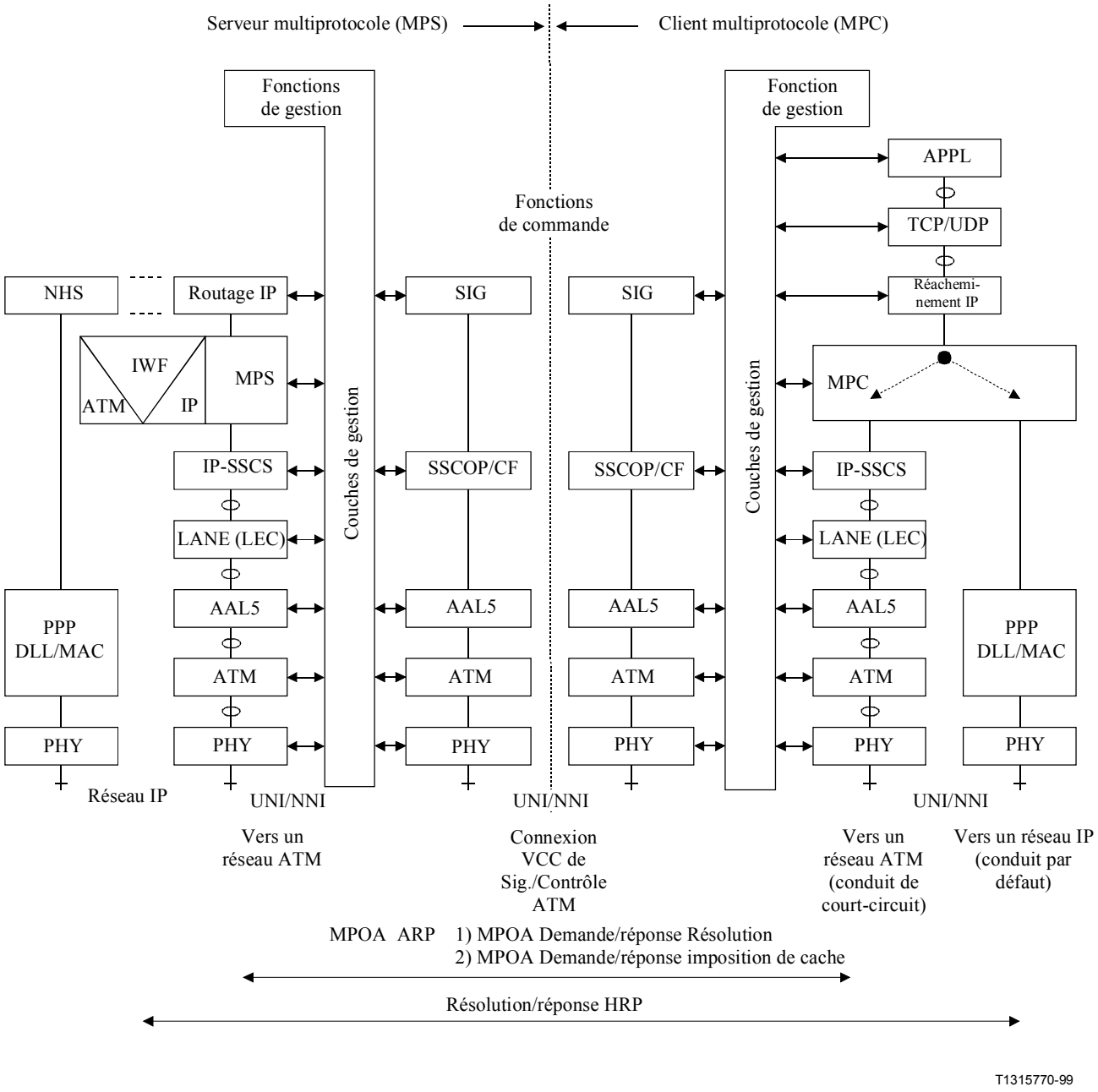


Figure I.2/Y.1310 – Description fonctionnelle de MPOA

I.3 Commutation multiprotocole avec étiquette (MPLS)

La commutation MPLS a été développée pour permettre un réacheminement rapide et efficace de données pour les routeurs Internet [31]. Bien qu'elle vise, d'un point de vue architectural, des applications multiprotocole, la commutation MPLS est principalement utilisée pour le protocole IP. Dans un environnement IP sans connexion, les routeurs IP réalisent conventionnellement le réacheminement IP de chaque datagramme le long du conduit désigné vers la destination sur la base de décisions de routage saut par saut. Cette décision du prochain saut implique l'examen de l'en-tête du paquet IP par le routeur pour attribuer le paquet à une classe d'équivalence de réacheminement (FEC, *forwarding equivalence class*) et le mappage de la classe FEC avec le prochain saut pour déterminer la direction du conduit de routage. Ce processus peut être simplifié et rendu plus efficace

par un processus de commutation MPLS. Avec la commutation MPLS, l'attribution d'un paquet IP à une classe FEC est réalisée une seule fois par le routeur avec commutation par étiquette d'entrée (LSR, *ingress label switching router*) et la classe FEC est représentée et codée par une étiquette de longueur fixe. Cette étiquette est attachée à l'en-tête du paquet IP. L'en-tête n'est plus utilisé par les routeurs subséquents pour le réacheminement du paquet. Les routeurs LSR, le long des conduits commutés avec étiquette (LSP, *label switching path*), utilisent l'étiquette pour indexer un tableau qui spécifie le prochain saut et une nouvelle étiquette. Les anciennes étiquettes sont remplacées par des nouvelles au fur et à mesure que les paquets franchissent les routeurs LSR le long du conduit LSP vers la destination. Les étiquettes ont une portée locale et leur codage est spécifié dans la référence [32]. Les étiquettes représentent le comportement de réacheminement global d'un paquet. Il en découle un comportement saut par saut qui inclut le choix du prochain saut pour le paquet et l'opération à réaliser sur l'étiquette, telle que la suppression ou le remplacement. Dans une situation normale, le conduit LSP suit le même conduit que celui déterminé par les protocoles de routage IP normaux tels que l'OSPF. La commutation MPLS peut fonctionner sur tout transport de couche de liaison tel que ATM, le relais de trames ou le protocole de point-à-point (PPP). La Figure I.3 décrit la structure de protocole d'une commutation MPLS fonctionnant sur des connexions ATM. Les éléments principaux de protocole MPLS dans cette figure sont le conduit LDP et les bases LIB et FIB. Le conduit LDP est décrit dans le paragraphe suivant. La base de données d'étiquette (LIB) et la base de données de réacheminement (FIB) sont des bases de données qui contiennent des informations sur le rattachement des étiquettes et des informations de réacheminement concernant les étiquettes [31], [32] et [19].

Un protocole de signalisation MPLS est nécessaire pour fournir une définition sensée et une compréhension commune des étiquettes MPLS au sein d'un domaine MPLS. Celui-ci peut être réalisé en utilisant le protocole de distribution d'étiquettes (LDP) [19] qui fournit un mécanisme de signalisation MPLS normalisé pour l'attribution et la distribution d'étiquettes. Comme cela est décrit à la Figure I.3, la commutation MPLS utilise le protocole LDP pour créer une base de données LIB dérivée du protocole de routage en cours d'utilisation et établit également une connexion LSP entre les points d'extrémité LSR d'entrée et de sortie. Le protocole LDP fonctionne principalement sur des connexions TCP fiables (sauf pour le processus de détection précisé ci-dessous, qui utilise le protocole UDP). Le protocole LDP fonctionne en quatre phases:

- détection: annonce et maintient la présence de routeurs LSR dans le réseau;
- session: établit et maintient des sessions entre homologues LDP;
- annonce: réalise l'attribution et la distribution d'étiquettes;
- notification: rapport sur les erreurs.

Lors de la distribution d'étiquettes, il est possible de choisir entre certains mécanismes et modes. Un mécanisme, par exemple, est la distribution d'étiquettes sur demande dans le sens descendant, où les étiquettes sont distribuées par un routeur LSR en aval en réponse à une demande explicite d'un routeur LSR en amont. D'autres mécanismes et modes de distribution sont présentés en détail dans la référence [19]. Des protocoles IP pré-configurés ou existants autres que le protocole LDP, tels que les protocoles RSVP et BGP, peuvent être étendus pour traiter la distribution d'étiquettes [31] et [32].

Le routage de type par contrainte (CR, *constraint-based routing*) est un mécanisme qui sert à distribuer des caractéristiques de capacité en termes d'ingénierie du trafic (TE, *traffic engineering*) et de performance en matière de QS au sein d'un réseau. Ces prescriptions peuvent être satisfaites par extension du protocole LDP "conventionnel" ou du protocole de réservation de ressource (RSVP) [21] pour prendre en charge des conduits avec commutation par étiquette à routage de type contrainte (CR-LSP, *constraint-based routed label switched path*) [20]. Le protocole LDP amélioré (maintenant CR-LDP) contient des paramètres de signalisation supplémentaires pour assurer les capacités CR suivantes:

- *routage explicite (ER)*: un routage explicite peut être défini comme une liste de nœuds et établi par une signalisation CR-LDP. Ce routage peut s'écarter des conduits LSP

conventionnels fondés sur le routage IP. Les routages ER stricts et souples sont pris en charge;

- *caractérisation du trafic*: le protocole CR-LDP peut définir les caractéristiques de trafic d'un conduit CR-LSP en termes de débit de crête, de débit garanti et de taille de rafale en excès;
- *priorité de conduit*: lors de l'établissement du conduit, la signalisation CR-LDP confère, si nécessaire, à ce nouveau conduit la capacité d'être prioritaire sur des conduits CR-LSP existants. La possibilité qu'a le nouveau conduit d'être prioritaire par rapport à un conduit existant dépend de la priorité d'établissement du nouveau conduit et de la priorité de maintien du conduit existant. Cette capacité permet à l'exploitant de réseau de respecter la politique du réseau et les prescriptions en termes d'ingénierie dans les limites des ressources disponibles;
- *épinglage de routage*: cette option permet à un segment d'un routage ER souple d'être fixé;
- *classes de ressource*: les ressources réseau peuvent être catégorisées par un exploitant de réseau en "classes de réseau". La signalisation CR-LDP spécifie la classe de ressource qu'un conduit CR-LSP peut déduire d'un temps d'établissement.

L'extension RSVP assure des nouvelles capacités de routage CR en introduisant de nouveaux paramètres dans les messages RSVP définis dans la référence [23]. Ces nouveaux paramètres permettent au protocole RSVP d'exécuter les fonctions LDP de base, telles que l'attribution et la distribution d'étiquettes, et d'assurer les capacités de routage de type contrainte suivantes: le routage explicite, la priorité de conduit et la caractérisation de trafic.

Les commutateurs ATM peuvent servir de nœuds avec commutation par étiquette. Lorsqu'un commutateur ATM sert de nœud ou de routeur avec commutation par étiquette (appelé ATM-LSR), l'étiquette sur la base de laquelle les décisions de réacheminement sont prises est transportée dans le champ d'identificateur VCI/VPI de l'en-tête de la cellule ATM. Pour prendre en charge la commutation par étiquette, un routeur ATM-LSR doit prendre en charge le protocole de contrôle et de signalisation pour la commutation par étiquette tel que le protocole LDP et participer à un protocole de routage de couche Réseau tel que le protocole OSPF. Le routage et l'adressage spécifiques ATM ne sont pas nécessaires. Une connexion virtuelle ATM dédiée (VPI/VCI dédiés) doit être établie entre routeurs ATM-LSR homologues pour la signalisation de contrôle LDP. Comme pour les routeurs LSR conventionnels, il est possible d'utiliser d'autres méthodes telles que OSPF, RSVP, PIM pour la distribution d'étiquettes. Un routeur ATM-LSR peut réaliser la commutation par étiquette sur un champ VPI, VCI, ou VPI/VCI suivant si la fusion de voie VC ou de conduit VP est utilisée pour l'agrégation de flux. Des routeurs ATM-LSR homologues peuvent être connectés directement sur une liaison ATM ou à distance par un nuage ATM sur une connexion virtuelle ATM. Dans ce dernier cas, la signalisation ATM devra acheminer les informations de rattachement.

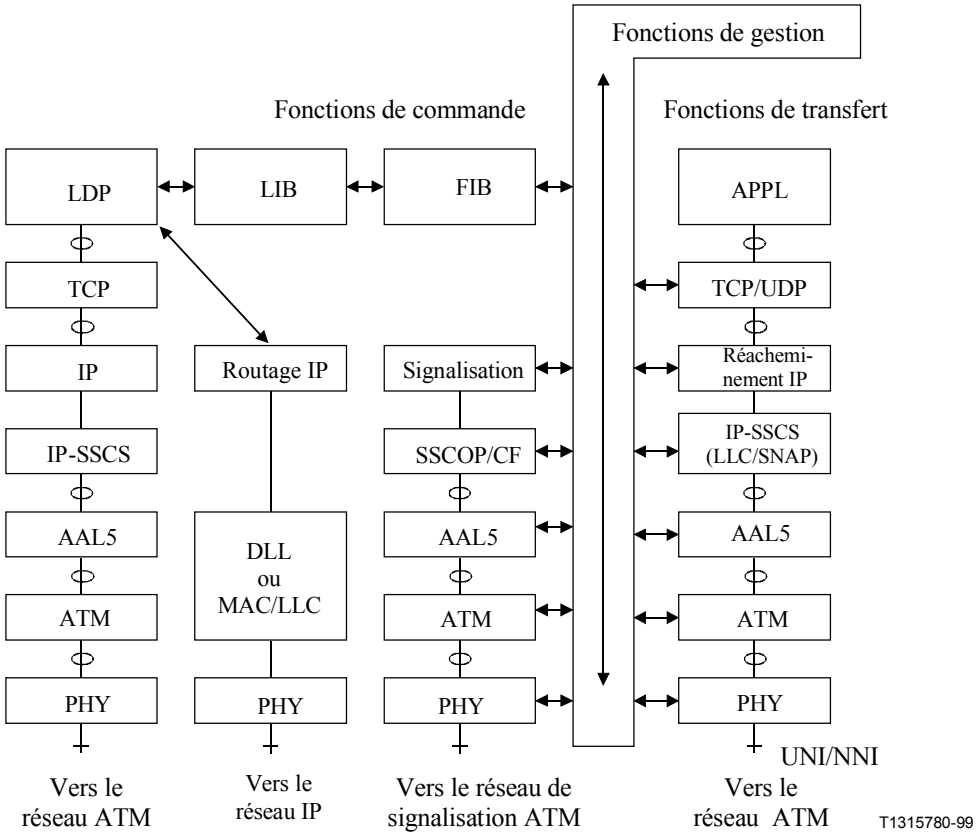
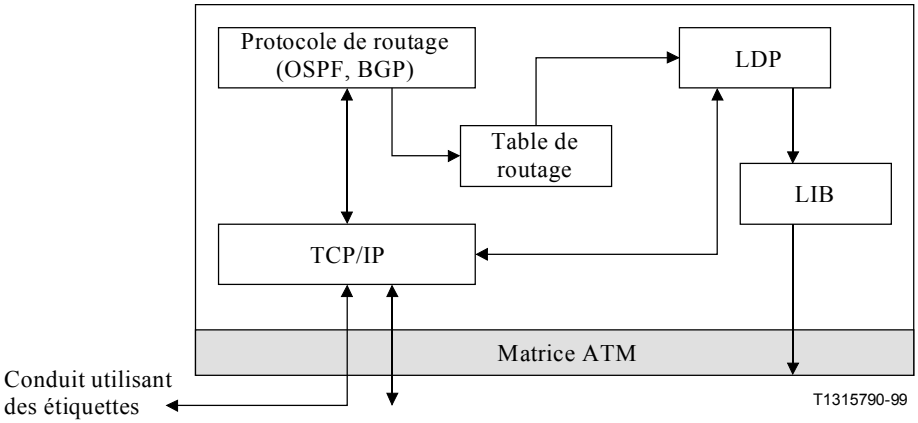


Figure I.3/Y.1310 – Description fonctionnelle de la commutation MPLS

NOTE – L'utilisation de la signalisation ATM est uniquement nécessaire pour l'interfonctionnement entre MPLS et RNIS-LB.

La Figure I.4 présente une structure de protocole d'une architecture MPLS de type ATM. L'architecture MPLS/ATM est constituée de deux parties: le module de routage MPLS et le module de réacheminement ATM. Le module de routage MPLS comprend le bloc fonctionnel de protocole de routage IP qui prend en charge OSPF et BGP, la pile de protocole TCP/IP et le protocole LDP et son résultat courant, la base LIB utilisée pour la distribution et l'attribution d'étiquettes. Le module de réacheminement ATM est la matrice ATM.



LDP Protocole de distribution d'étiquettes
LIB Base de données d'étiquette

Figure I.4/Y.1310 – Exemple de mise en œuvre de la commutation MPLS

APPENDICE II

Lignes directrices en matière de mappage de services avec des connexions ATM

II.1 Mappage de services Intserv avec des connexions ATM

II.1.1 Mappages de services garantis (GS) en ATM

II.1.1.1 Modèle de réseau pour les GS

Le modèle de réseau supposé dans le document [14] est représenté à la Figure II.1.

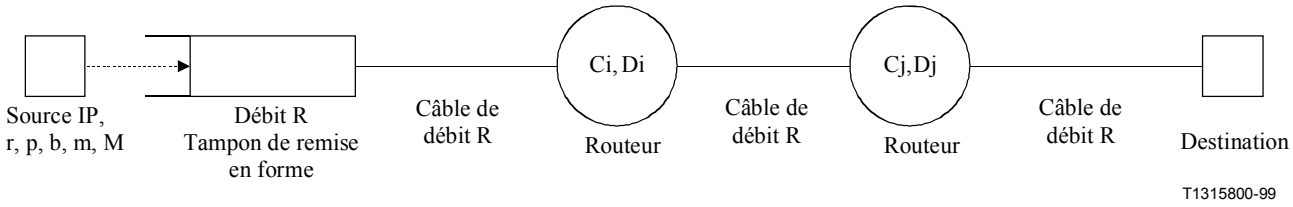


Figure II.1/Y.1310 – Modèle de réseau pour services GS

La source du flux IP qui demande des services GS émet du trafic conformément à sa spécification de case à jetons (r, p, b, m, M). Après une phase de transition pendant laquelle le trafic peut être acheminé "au mieux", des ressources sont attribuées de sorte à pouvoir modéliser le réseau comme une séquence de "câbles" de débit R. Immédiatement avant le premier câble, tout le trafic qui dépasse instantanément le débit R (même s'il est conforme à la spécification de case à jetons) est mis en tampon et remis en forme au débit R. En supposant cette remise en forme d'entrée au débit R, le modèle de réseau considère la situation la plus défavorable en matière de variation du temps de transfert. Les câbles sont reliés par des dispositifs (routeurs) qui introduisent une "distorsion" par rapport au modèle fluide idéal (un seul câble au débit R). La distorsion introduite par chaque routeur est prise en compte par deux termes désignés par C (dépendant du débit) et D (indépendant du débit). Les messages RSVP acheminent vers le récepteur la somme de toutes les valeurs Ci et Di de manière à ce qu'il puisse calculer la limite supérieure de la partie variable du temps de transfert. Si le débit des câbles est R, cette limite supérieure est:

$$[(b\text{-}M)/R][(p\text{-}R)/(p\text{-}r)] + (M+C_{tot})/R + D_{tot} \qquad \text{pour } r \le R < p^1 \qquad \text{(II-1)}$$

$$(M+C_{tot})/R + D_{tot} \qquad \text{pour } r \le p \le R \qquad \text{(II-2)}$$

Le récepteur demande donc que la largeur de bande réservée sur les câbles soit R (en envoyant un message RSVP RESV en amont) afin de maintenir (II-1) ou (II-2) inférieur à une valeur cible. Il est à noter que le retard dans la mémoire-tampon de remise en forme (voir Figure II.1) est pris en considération dans le premier terme de (II-1), mais que si R > p [comme dans (II-2)], le trafic ne sera jamais retardé dans la mémoire-tampon de remise en forme.

II.1.1.2 Choix du service ATM

Le problème du mappage se pose lorsque les câbles doivent être remplacés par des connexions ATM. Si le modèle de câble doit être respecté strictement, aucun choix n'est possible puisque les connexions ATM introduisent toujours une variation CDV qui est reflétée par une variation du temps

[1] Cette formule reste inchangée même si la remise en forme n'a pas lieu à l'entrée mais au niveau d'un ou de plusieurs des routeurs franchis.

de transfert pour les paquets, ce qui n'est pas le cas des câbles. Il convient en pratique de limiter le choix aux capacités ATC qui peuvent être associées à une classe de QS qui assure une variation CDV limitée (par exemple la classe de QS 1 [6] ou la classe de QS 4 [voir Note ci-dessous]). Cette variation CDV peut alors être prise en compte dans le terme D de (II-1) ou de (II-2).

Il est possible d'associer les débits DBR [7] et SBR1 [7] de la capacité ATC à la classe de QS 1 [6]. Les débits SBR2 [7] et SBR3 [7] peuvent être associés à la classe de QS 4 (voir Note). Quel critère faut-il alors utiliser pour choisir le service ATM? Un premier critère peut être d'étudier si un flux IP est bien remis en forme au niveau IP à un débit R avant d'être envoyé au niveau ATM comme le suppose le modèle. Dans ce cas, le choix le plus naturel est d'adopter une connexion ATM de débit DBR avec une classe de QS 1 avec un débit PCR = (équivalent ATM de R)[2]. Le choix d'une connexion SBR avec un débit SCR = (équivalent ATM de R) nécessiterait de manière inutile plus de ressources que le débit DBR, sauf dans le cas de PCR = SCR = (équivalent ATM de R) et MBS = 0, c'est-à-dire lorsqu'on se retrouve à nouveau dans le cas DBR.

Dans le cas contraire, si le point de départ de la connexion ATM est insensible à une quelconque remise en forme de paquet au niveau IP, le meilleur mappage serait avec une connexion SBR avec le débit SCR = (équivalent ATM de R), PCR = (équivalent ATM de p), MBS = [équivalent ATM de bp/(p-r)]. Un débit DBR nécessiterait de plus importantes ressources pour accepter des rafales conformes de trafic jusqu'au débit p et nécessiterait par conséquent un débit PCR = (équivalent ATM de P) ou MCR = (équivalent ATM de P).

Parmi les trois versions de débit SBR, celle qui correspond le mieux au modèle d'un service GS est le débit SBR3 qui permet le marquage du trafic non conforme. Ceci permet de reléguer au niveau ATM toute la complexité du traitement au mieux du trafic en excès, conformément aux prescriptions de la référence [14]. La classe de QS associée est la classe 4 (voir Note).

Tableau II.1/Y.1310 – Mappage préféré de GS à ATM

	Le niveau ATM est sensible à la remise en forme des paquets au niveau IP au débit R immédiatement avant le point de départ de la connexion	Le niveau ATM est insensible à une quelconque remise en forme des paquets au niveau IP au débit R immédiatement avant le point de départ de la connexion
Classe de QS et capacité ATC préférée	DBR classe 1	SBR3 classe 4
Mappage entre les descripteurs de trafic ATM et les paramètres de case à jetons	PCR = (équivalent ATM de R)	Note (*) Note (&) PCR = (équivalent ATM de p) SCR = (équivalent ATM de R) MBS = (équivalent ATM de bp/(p-r))

[2] Voir II.1.1.3.

Tableau II.1/Y.1310 – Mappage préféré de GS à ATM *(fin)*

NOTE (*) – Le mappage de paramètre vers SBR est toujours valide lorsque $R \leq p$. Toutefois, dans le service GS, le paramètre *R* peut être mis comme supérieur à *p* [voir (II-2)]. Puisque le débit PCR ne peut pas être mis inférieur à *R*, il en résulte PCR = SCR = *R* > *p* et il n'existe aucune raison d'avoir un MBS > 0. Dans le cas de R > p, le mappage préféré est donc le DBR avec classe de QS 1, avec PCR = (équivalent ATM de R).

NOTE (&) – Dans l'utilisation de SBR, le schéma de mappage souffre d'une inefficacité intrinsèque puisque le modèle de réseau du service GS considère des "câbles" au débit R alors que les connexions SBR sont bien "meilleures" que des câbles au débit R, dans le sens qu'elles peuvent absorber des rafales instantanées de trafic jusqu'à un débit p, sans être obligées de mettre en mémoire-tampon le trafic qui dépasse R. Cette inefficacité est reflétée par une surattribution de R, due au premier terme de (II-1) qui est supposé par le modèle de service GS mais qui peut être absent ou sensiblement moins important dans le réseau réel.

NOTE – La classe de QS 4 est une nouvelle classe de QS en cours de définition. Il est possible qu'elle soit incluse dans une future version révisée de la Recommandation UIT-T I.356 [6].

II.1.1.3 Equivalents ATM des paramètres de case à jetons

Il convient de garder à l'esprit lors de la traduction des paramètres de case à jetons en descripteurs de trafic ATM que les premiers sont exprimés en octets ou en octets/s alors que les deuxièmes sont exprimés en cellules ou en cellules/s. Il faut de plus tenir compte des en-têtes ATM et AAL.

Une limite supérieure au nombre de cellules nécessaires pour acheminer un paquet IP de B octets est donnée par:

$$C(B) = (H+B+T+47)/48 \qquad \text{(II-3)}$$

où H et T sont les longueurs d'en-tête et de postambule d'unité PDU AAL et où "47" tient compte de la dernière cellule qui ne peut être remplie que partiellement.

Les équivalents ATM pour les termes figurant dans le Tableau II.1 sont énumérés dans le Tableau II.2. Il est supposé que la spécification de case à jetons est (r, b, p, m, M).

Tableau II.2/Y.1310 – Equivalents ATM pour le mappage de services GS en ATM

Mappage avec débit DBR classe 1	Mappage avec débit SBR3 classe 4
$\text{PCR} = \left\lfloor \frac{R}{m} \right\rfloor C(m)$	$\text{PCR} = \left\lfloor \frac{p}{m} \right\rfloor C(m)$ $\text{SCR} = \left\lfloor \frac{R}{m} \right\rfloor C(m)$ Note (%) $\text{MBS} = \left\lfloor \frac{bp}{m(p-r)} \right\rfloor C(m)$
NOTE (%) – Pendant combien de temps une source conforme à la spécification de case à jetons peut-elle envoyer des "octets" au débit de crête p[octets/s]? Pendant T = b/(p–r) secondes. Combien d'octets peut-elle envoyer au débit de crête p avant de devenir "non conforme"? bp/(p–r). Combien de paquets, au maximum? bp/[m(p–r)]. Il convient par conséquent qu'une connexion SBR ATM qui achemine ce trafic transmette cette quantité de paquets de manière "transparente" (en d'autre termes à leur débit crête), et il convient par conséquent qu'elle ait la taille MBS indiquée (en cellules).	

Ces équivalences sont le cas le plus défavorable; elles sont en d'autres termes calculées en supposant que tous les paquets ont la longueur minimale déclarée, en considérant par conséquent l'incidence

d'en-tête maximale. Une évaluation plus réaliste est possible en remplaçant *m* dans les formules ci-dessus par une valeur dans la gamme [*m, M*], mais ceci nécessite une connaissance détaillée de la distribution de tailles de paquet de l'application source.

II.1.1.4 Prise en compte de la variation CDV

Une fois la segmentation en paquets réalisée, les cellules qui appartiennent à un paquet sont prêtes simultanément pour la transmission et peuvent être envoyées au débit de ligne si aucune remise en forme au niveau de la cellule n'est réalisée. Lorsqu'il est supposé qu'aucune fonction de remise en forme au niveau des cellules n'existe pour absorber les rafales dues à la segmentation en paquet, il est nécessaire de tenir compte de ce comportement de rafale en ajoutant une valeur appropriée à la tolérance CDVT sur le paramètre PCR de la connexion DBR ou SBR. Cette valeur peut être évaluée à:

$$[C(M)-1][(1/PCR)-(1/LCR)] \qquad \text{(II-4)}$$

II.1.2 Mappage de service en charge contrôlée (CLS) en ATM

Pour le service CLS le modèle de réseau considéré dans la référence [13] est également constitué d'une source dont le trafic est décrit par une spécification de case à jetons (r, p, b, m, M) et d'une séquence de routeurs reliés par des "câbles" (voir Figure II.1), mais il n'existe aucune garantie explicite en matière de temps de transfert et il n'existe aucune formule spécifique telle que (II-1) ou (II-2). Lorsque les câbles doivent être remplacés par des connexions ATM, le choix n'est plus limité à des capacités ATC qui peuvent avoir une variation CDV limitée. Puisque la prescription des services CLS est simplement d'avoir de la largeur de bande disponible "à long terme"[3] et de faibles pertes, des services ATM appropriés peuvent être:

- DBR avec la classe 2;
- ABT avec la classe 2;
- ABR avec la classe 3;
- SBR1 avec la classe 2;
- SBR2 avec la classe 3;
- SBR3 avec la classe 3;
- GFR1;
- GFR2.

NOTE – Ces GFR font référence aux GFR spécifiés dans le TM4.1 du Forum ATM.

Le mappage du débit DBR avec la classe 2 signifierait de déterminer le débit PCR comme s'inscrivant quelque part entre (l'équivalent ATM de r et p)[4], en d'autres termes de trouver une largeur de bande équivalente pour le flux unique, mais serait en plus spécifique à l'application, ce qui risque également d'être inefficace. La classe 2 ne permet en outre pas à la couche ATM de s'occuper au mieux du traitement du trafic excédant la spécification de case à jetons comme cela est prescrit dans la référence [13].

---

[3] "A long terme" signifie sur une échelle temporelle sensiblement plus importante que b/r, où b et r font partie du paramètre de case à jetons de la source.

[4] Voir aussi le II.1.1.3.

Le mappage avec le transfert ABT avec transmission différée avec la classe 2, même s'il est potentiellement attrayant, a le désavantage de l'en-tête de renégociation au niveau de la rafale qui est probablement inacceptable. Avec des renégociations à plus longs termes, les mêmes désavantages que ceux précisés pour le débit DBR s'appliquent.

Le mappage avec le débit ABR avec la classe 3 serait possible en mettant MCR = (l'équivalent ATM de r), mais présente le désavantage que tout le trafic qui dépasse instantanément r est traité au mieux. La détermination de MCR comme s'inscrivant quelque part entre (l'équivalent ATM de r et p) présente les mêmes désavantages que ceux présentés pour le débit DBR sans toutefois pouvoir garantir que la couche ATM est en mesure de distinguer exactement le trafic conforme et non conforme à la spécification de case à jetons.

Le mappage avec SBR1 avec la classe 2 ou SBR2 avec la classe 3 permet au niveau ATM de connaître la quantité maximale d'informations pour réaliser un multiplexage statistique efficace, mais pour ce qui concerne la partie non conforme du trafic il ne satisfait pas aux attentes, c'est-à-dire le meilleur traitement possible.

Les trois derniers mappages satisfont tous à l'objectif de refléter le plus exactement possible au niveau ATM les caractéristiques de trafic spécifiées par la spécification de case à jetons en assurant le meilleur traitement possible de la quantité exacte de trafic qui les dépasse. Les équivalents ATM détaillés sont présentés dans le Tableau II.3.

Tableau II.3/Y.1310 – Equivalents ATM pour le mappage de services CLS en ATM

Mappage en SBR3	Mappage en GFR 1 ou en GFR 2
$\text{PCR} = \left\lfloor \frac{p}{m} \right\rfloor C(m)$ $\text{SCR} = \left\lfloor \frac{r}{m} \right\rfloor C(m)$ $\text{MBS} = \left\lfloor \frac{bp}{m(p-r)} \right\rfloor C(m)$	$\text{PCR} = \left\lfloor \frac{p}{m} \right\rfloor C(m)$ $\text{MCR} = \left\lfloor \frac{r}{m} \right\rfloor C(m)$ $\text{MFS} = C(M)$ $\text{MBS} = \max\left(\left\lfloor \frac{bp}{m(p-r)} \right\rfloor C(m), MFS \right)$

Les remarques sur la nécessité de remplacer m par une valeur comprise entre [*m*, *M*] et sur la valeur à ajouter à la tolérance CDVT exprimées à la fin du II.1.1.4 s'appliquent.

II.2 Mappage de services Diffserv sur des connexions ATM

Le présent sous-paragraphe décrit à titre d'information quelques exemples envisageables de mappage de services différenciés avec des services ATM. Le groupe IETF a uniquement décrit les services d'application qui peuvent être pris en charge par chaque comportement PHB ou groupe de comportements PHB [27] et [28].

- *Service d'émulation de ligne louée*

  Egalement appelé "service de prime". Ce service peut être mis en œuvre en utilisant le comportement EF-PHB. Ce type de service requiert généralement des garanties strictes en matière de faible taux de perte et de temps de transfert. Ce service est également caractérisé par son débit crête. Il est par conséquent possible de mapper ce service avec la capacité ATC en DBR utilisant la classe de QS 1 pour satisfaire de telles prescriptions de perte et de temps de transfert. Le débit crête peut être mappé directement avec le paramètre PCR de la capacité ATC en débit DBR.

- *Service assuré en termes de quantité*

  Egalement appelé le "service à débit assuré". Ce service peut être mis en œuvre en utilisant l'une des quatre classes de comportement AF-PHB. Ce service est caractérisé par un débit minimal garanti sur une base statistique. Ce service offre des garanties plus souples que le service d'émulation de ligne louée, mais il est tout de même considéré comme un service quantitatif. Il promet notamment de distribuer le trafic avec un degré élevé de fiabilité et avec des temps d'attente limités, jusqu'à un débit négocié. Il semble par conséquent parfaitement approprié de mapper ce service avec une capacité ATC en débit ABR en utilisant la classe de QS 3. Dans ce cas, le débit MCR peut être mis égal au débit minimal de service.

II.3 Service Intserv en MPLS sur des connexions ATM

Les paramètres de trafic de services Intserv y compris *p, r, b* et *R* sont définis dans les objets RSVP tels que *Tspec* et *Rspec*. Il est possible d'utiliser le protocole CR-LDP pour prendre en charge le protocole RSVP/service Intserv dans les réseaux MPLS sur ATM. Dans ce cas, les prescriptions suivantes doivent être prises en considération:

– lorsque le flux RSVP/Intserv, y compris les services garantis et les services en charge contrôlée, pénètre dans un routeur LSR d'entrée de réseaux MPLS, les paramètres RSVP *Tspec* tels que *p, r* et *b* doivent être reflétés dans les paramètres de trafic dans le message de demande d'étiquette du protocole CR-LDP;

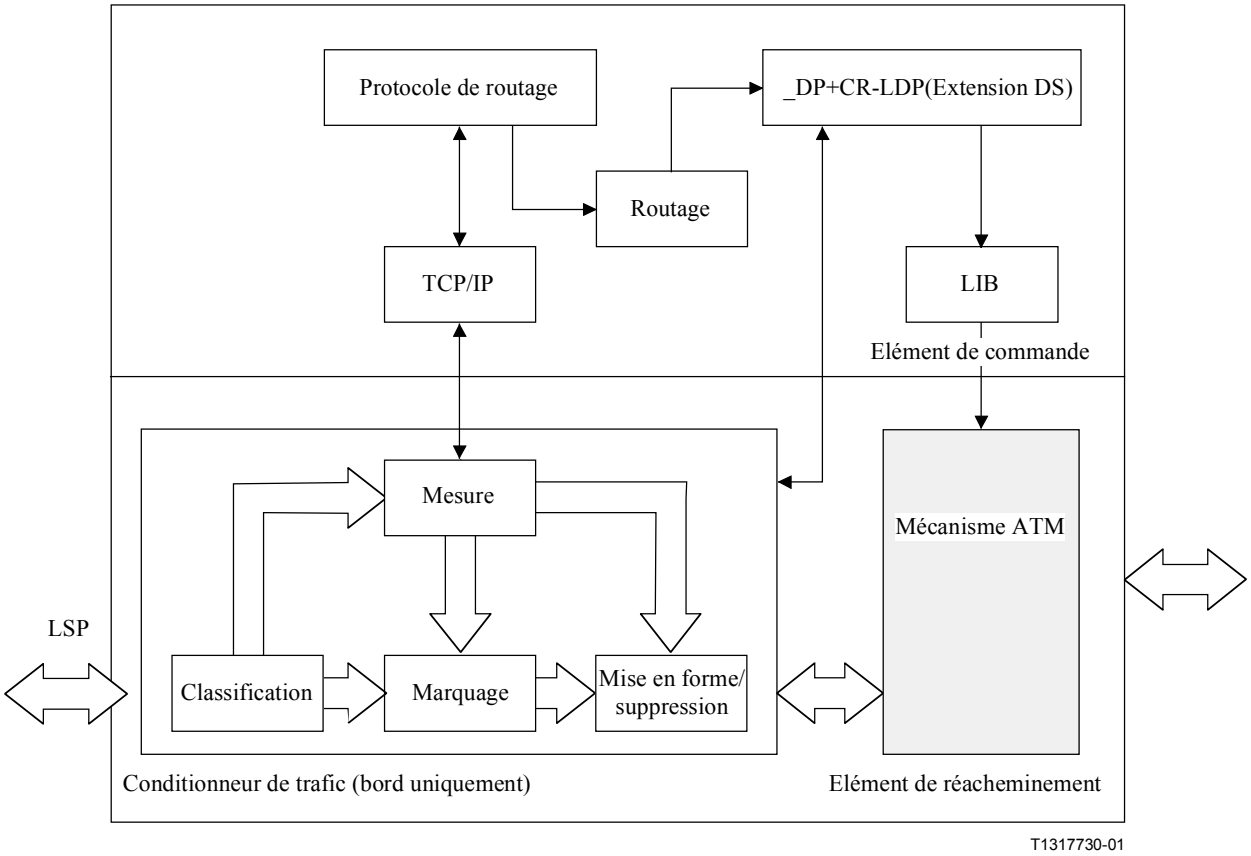
– pour prendre en charge le service garanti, les paramètres RSVP *Rspec* tels que *R* et *S* doivent être reflétés dans les paramètres de trafic dans le message de mappage d'étiquette du protocole CR-LDP.

Le mappage de paramètre de trafic d'Intserv avec le protocole CR-LDP dépend de la politique de conditionnement du trafic au niveau du routeur LSR d'entrée.

II.4 Service Diffserv en MPLS sur des connexions ATM

Le présent sous-paragraphe décrit une méthode de prise en charge du service Diffserv dans un réseau MPLS ATM. Un routeur ATM-LSR compatible Diffserv doit avoir la structure logique spécifiée sur la Figure II.2. Il est à noter qu'un routeur ATM-LSR de transit n'aura en général pas besoin de l'élément de conditionnement de trafic, mais qu'un routeur ATM-LSR de bord devra avoir cet élément pour assurer les fonctions de classification, de marquage, de mesure et de mise en forme/suppression de paquet requises par l'architecture Diffserv [30].

Le présent sous-paragraphe porte principalement sur la solution CR-LDP. Ainsi, l'élément de commande de la Figure II.2 utilise les protocoles LDP et CR-LDP (avec l'extension Diffserv) comme système de signalisation. Toutefois, si cela est nécessaire, cette partie peut en outre utiliser l'extension RSVP comme système de signalisation. Pour plus de détails sur le conditionneur de trafic, voir la référence [30].



LIB Base de données d'étiquette

Figure II.2/Y.1310 – Architecture logique d'un routeur ATM-LSR compatible Diffserv

II.4.1 Procédures d'établissement d'un conduit LSP

La procédure de base d'établissement d'un conduit LSP Diffserv MPLS ATM comprendra les actions suivantes:

- au bord du domaine Diffserv MPLS ATM, les routeurs ATM-LER traiteront les demandes de service et procéderont à la classification du service. Les routeurs LER détermineront alors le comportement par saut (PHB) qui sera utilisé par le service. Le routeur ATM-LER doit ensuite mapper le comportement PHB sur des couples <PSC, CLP> (programmation par saut, priorité de pertes de cellules). Les relations de mappage sont spécifiées dans le Tableau II.4;
- conformément aux prescriptions de Diffserv, en utilisant le système de signalisation MPLS (on peut par exemple utiliser le protocole CR-LDP avec l'extension Diffserv [33] comme système de signalisation), il faut procéder à la fourniture du service [30] et établir un conduit LSP sensible à la qualité de service pour le service. A ce stade, les tables de réacheminement au niveau des routeurs LSR le long du conduit LSP auront une nouvelle colonne pour les programmations PSC entrantes.

II.4.2 Procédure de réacheminement par étiquette

L'opération de base du réacheminement par étiquette du schéma Diffserv MPLS ATM comprendra les actions suivantes:

- à l'entrée du domaine Diffserv MPLS ATM, les routeurs LER déterminent le comportement PHB et la classe FEC pour un paquet en vérifiant l'adresse IP et la valeur du point DSCP (point de code de service différencié) figurant dans le paquet IP;

- le routeur ATM-LSR d'entrée procède alors au conditionnement du trafic et détermine la priorité CLP de sortie pour le paquet. Lorsqu'un conduit L-LSP ATM a été établi, seul le champ CLP peut être réécrit;
- le routeur ATM-LSR d'entrée détermine ensuite l'identificateur VCI de sortie et le numéro de l'interface de sortie, procède à la programmation PSC de sortie pour le paquet, encapsule le paquet IP dans un paquet ATM et l'envoie à l'interface de sortie;
- dans le domaine Diffserv MPLS, le routeur LSR de transit vérifie l'identificateur VCI et le champ CLP de l'en-tête du paquet ATM. Au moyen de la table de réacheminement, il détermine la programmation PSC requise par le paquet;
- au moyen de la table de mappage montrée dans le Tableau II.4, le routeur LSR de transit détermine alors le comportement PHB requis par le paquet. En général, le routeur LSR de transit ne procédera pas à un conditionnement du trafic, il ne fera qu'implémenter le comportement PHB pour le paquet et utiliser la table de réacheminement pour transmettre le paquet au routeur LSR en aval. Si le routeur LSR de transit a besoin de procéder à un conditionnement du trafic, il utilise les résultats des procédures de conditionnement du trafic pour modifier la priorité CLP de sortie pour un paquet ATM;
- à la sortie du domaine Diffserv MPLS ATM, le routeur ATM-LSR de sortie vérifie l'identificateur VCI et le champ CLP de l'en-tête du paquet ATM. Au moyen de la table de réacheminement, il détermine la programmation PSC requise par le paquet. Au moyen de la table de mappage montrée dans le Tableau II.4, le routeur LSR de transit détermine alors le comportement PHB requis par le paquet. Il exécute ensuite les procédures de conditionnement du trafic et utilise les résultats combinés avec le comportement PHB d'entrée pour déterminer le comportement PHB de sortie et la valeur du point DSCP de sortie pour le paquet;
- la sortie ATM reconvertira alors le paquet ATM en paquet IP, qui contient l'adresse IP et le champ DSCP (ce champ doit avoir la valeur obtenue par l'opération précitée).

II.4.3 Mappages entre <PSC, CLP> et PHB

Les comportements PHB suivants ont été définis:

II.4.3.1 DF (comportement PHB par défaut): ce comportement PHB est utilisé pour les paquets à traiter au mieux ou les paquets ayant une valeur de point DSCP inconnue.

II.4.3.2 CS (comportement PHB avec sélecteur de classe): ce comportement PHB est utilisé pour la compatibilité amont avec le système existant de préséance IP à 8 niveaux.

II.4.3.3 EF (comportement PHB avec réacheminement exprès): ce comportement PHB est utilisé pour les services qui nécessitent un faible taux de perte de paquet, une faible attente, une faible gigue et une garantie de largeur de bande. Un paquet avec ce comportement PHB sera associé au rang de priorité de service le plus élevé et au service de prime dans le domaine.

II.4.3.4 AF (comportement PHB avec réacheminement assuré): ce comportement PHB est utilisé pour classer les paquets appartenant à la même connexion avec une préséance de suppression différente. L'IETF a défini quatre classes de comportement AF et, dans chacune d'elles, il y a trois comportements PHB avec des préséances de suppression différentes, ce qui fait 12 comportements PHB AF au total. Un exemple d'application de ce comportement PHB est lorsque le trafic dépasse un certain débit de transmission, auquel cas on assignera aux paquets excédentaires un comportement PHB avec une préséance de suppression supérieure. Une autre caractéristique importante de ce comportement PHB est que les paquets appartenant à une même connexion et à la même classe de comportement PHB ne peuvent pas être réordonnés.

Le Tableau II.4 montre le mappage entre les comportements PHB et les couples <PSC, CLP>. Ces mappages doivent être cohérents au niveau de chaque routeur LSR dans un domaine Diffserv ATM et doivent être reconfigurables.

Tableau II.4/Y.1310 – Mappage entre les comportements PHB Diffserv et les couples <PSC, CLP> ATM

Comportement PHB Diffserv	Programmation PSC	Priorité CLP ATM
DF	DF	0
CSn	CSn (Note 1)	0
AFi1 (Note 2)	AFCi	0
AFi2	AFCi	1
AFi3	AFCi	1
EF	EF	0
NOTE 1 – "n" ($1 \leq n \leq 8$) désigne le numéro de préséance IP. NOTE 2 – "i" ($1 \leq i \leq 4$) désigne la classe de comportement PHB AF; par exemple, lorsque i = 1, AFi1 représentera AF11, qui appartient à la classe de comportement PHB AF 1 et a la préséance de suppression 1.		

II.4.4 Considérations relatives à l'implémentation

Les routeurs LSR MPLS ATM doivent prendre en charge les comportements PHB et les règles de conditionnement de trafic des services IP. Toutefois, les règles détaillées relatives au traitement des paquets et au conditionnement du trafic au niveau des routeurs LSR MPLS ATM sont fonction de l'implémentation.

APPENDICE III

Scénarios possibles d'évolution de la commutation MPLS pour le transport des services IP sur des connexions ATM dans les réseaux publics

III.1 Introduction

Quelles sont les routes potentielles pour la commutation MPLS dans l'infrastructure de réseau actuelle? Cela dépend de l'état actuel ainsi que des services qui seront offerts par un exploitant donné.

Dans la présente Recommandation UIT-T, on suppose que la commutation MPLS sera mise en œuvre dans les réseaux fédérateurs ATM existants. Dans le cadre de l'étude des solutions d'évolution de la commutation MPLS, les exploitants sont classés selon qu'il s'agit de nouveaux exploitants ou d'exploitants établis et selon qu'il s'agit d'exploitants offrant tous les services (données, parole, vidéo, lignes louées) ou d'exploitants centrés sur le protocole IP. Il ne s'agit pas d'un classement universel; il s'agit plutôt d'une manière pratique de classer les fournisseurs de services en fonction de l'état actuel de leur réseau et de leur offre de services prévisible.

Dans le présent appendice, on considère plusieurs types d'infrastructure existante et on envisage des stratégies générales de mise en œuvre de la commutation MPLS dans ces types de réseau. On examine ensuite diverses techniques pour l'utilisation de la commutation MPLS sur des équipements ATM incompatibles MPLS et on fait des recommandations sur l'utilisation de ces techniques.

III.2 Scénarios proposés

Plusieurs scénarios sont présentés et étudiés de la manière suivante:

III.2.1 Exploitant établi offrant tous les services

Supposons un exploitant établi qui dispose d'un réseau téléphonique et qui transporte le trafic de données sur le réseau TDM ou sur un réseau distinct. Supposons également que cet exploitant est en train de fusionner son réseau de données et son réseau téléphonique dans une même infrastructure.

L'exploitant existant dispose probablement d'une infrastructure ATM qui est utilisée pour le trafic de données (IP ou relais de trames) et qui peut être utilisée pour le trafic de parole et de vidéo ou pour tout autre service ATM natif. Dans ce cas, le mode ATM est utilisé comme une technique de commutation multiservice.

Le transport actuel de trafic IP dans le réseau d'exploitant relève probablement de l'un des trois cas suivants:

– utilisation de connexions PVC ATM de point à point avec encapsulation RFC 2684 [18];

– utilisation de la méthode IP sur des connexions ATM classique;

– utilisation du protocole MPOA.

Dans tous les cas, il sera nécessaire de mettre en œuvre la commutation MPLS dans un réseau qui utilise alors uniquement des PVC, SPVC, SVC, PVP et SPVP et pas de circuits virtuels avec commande MPLS. Les circuits virtuels MPLS peuvent être désignés par "circuits virtuels étiquetés (LVC, *label VC*)" afin de les distinguer des circuits SVC avec PNNI ou commande analogue.

III.2.2 Exploitant téléphonique établi

Supposons un exploitant qui dispose uniquement d'un réseau téléphonique traditionnel SS7/TDM sans investissements ATM substantiels et qui souhaite acheminer la parole et des données dans l'avenir en utilisant une infrastructure de commutation MPLS cellulaire. Quelle est la meilleure évolution?

L'exploitant téléphonique décidera probablement en premier lieu de conserver son contrôle SS7 et de transférer son trafic téléphonique d'un réseau TDM vers un réseau en mode paquet. En supposant la probabilité du choix d'une commutation MPLS cellulaire, le trafic de données ainsi que le trafic téléphonique seront transportés sur ce réseau de type MPLS. Le fournisseur de services peut choisir de conserver les deux réseaux séparés ou de travailler vers une intégration progressive.

III.2.3 Nouvel exploitant centré sur le protocole IP

La question dans ce cas est de savoir si un déploiement du mode ATM est sensé. Si l'exploitant choisit de déployer une commutation MPLS cellulaire, il fait un petit pas dans la direction d'un contrôle ATM dans le réseau. L'élément principal serait la réutilisation des capacités de commutation ATM uniquement.

III.2.4 Nouvel exploitant offrant tous les services

Le nouvel exploitant offrant tous les services proposera des services de parole, de vidéo et de lignes louées ainsi que des services centrés sur le protocole IP. En raison de ces différents types de trafic, il peut être supposé que l'exploitant choisira de déployer une infrastructure ATM pour intégrer son offre de service sur un seul réseau.

Des routeurs pourront être déployés aux bords du réseau pour prendre en charge les services IP, mais le centre commuté sera en mode ATM. La commutation MPLS cellulaire sera déployée au centre. Le fonctionnement en mode "Ships-in-the-Night" avec le mode ATM peut être nécessaire pour intégrer la commutation MPLS et les services en mode ATM. Une commutation MPLS avec routage explicite sera nécessaire pour l'ingénierie du trafic, une commutation MPLS saut par saut serait nécessaire pour traiter le trafic qui n'est pas acheminé dans des conduits LSP avec routage explicite.

III.3 Réseau ATM hybride

Le présent sous-paragraphe traite de trois moyens possibles d'intégration d'équipements MPLS avec des équipements non MPLS dans un réseau ATM. Dans le présent sous-paragraphe, on suppose que la commutation ATM est prise en charge dans un réseau existant. En revanche, on ne traite pas de la prise en charge des protocoles MPOA et C-IPOA; toutefois, les techniques examinées ici peuvent s'appliquer.

III.3.1 Techniques pour les réseaux ATM hybrides

Pendant la mise en œuvre de la commutation MPLS ATM dans un réseau ATM existant, il sera parfois nécessaire de raccorder des routeurs LSR sur des équipements ATM classiques, d'où la création d'un réseau "hybride". Dans des réseaux hybrides, certains commutateurs ou routeurs possèdent la capacité MPLS et d'autres pas. Le présent sous-paragraphe traite des moyens possibles d'implémentation de réseaux ATM hybrides – MPLS sur PVC, jonctions virtuelles et notification d'identificateur de connexion virtuelle pour LDP (VCID, *virtual connection identifier notification*) – illustrés sur la Figure III.1.

III.3.1.1 MPLS sur PVC

La technique MPLS sur PVC est illustrée sur la Figure III.1 a). Elle ne peut être utilisée que pour raccorder des routeurs LSR utilisant des paquets. Elle ne peut pas être utilisée pour raccorder des routeurs avec commutation par étiquette ATM (ATM-LSR, *ATM label switch router*) entre eux. La technique MPLS sur PVC permet de raccorder des routeurs avec commutation par étiquette (LSR) utilisant des paquets au moyen de connexions par circuit virtuel permanent (PVC, *permanent virtual circuit connection*) sur un réseau ATM classique. Il est également possible d'utiliser des connexions par circuit virtuel permanent commutable (SPVC, *soft permanent virtual circuit connection*). (Toute mention d'un circuit "PVC" en ce qui concerne la technique MPLS sur PVC dans le présent appendice renvoie aussi à un circuit SPVC.) Les routeurs s'envoient des paquets MPLS les uns aux autres, des étiquettes étant explicitement encapsulées avec le paquet IP. C'est ce qu'on appelle "l'étiquetage fondé sur des paquets", car l'étiquette MPLS est appliquée à un paquet entier et non à des cellules individuelles. Lorsque l'étiquetage fondé sur des paquets est utilisé sur des circuits PVC, des paquets ayant de nombreuses étiquettes différentes sont envoyés dans le même circuit PVC. Cela diffère de la commutation MPLS ATM, pour laquelle chaque étiquette différente est représentée par un circuit virtuel différent, appelé "circuit virtuel étiqueté" (LVC). L'étiquetage fondé sur des paquets utilisé sur des circuits PVC est virtuellement identique au cas où des routeurs avec commutation par étiquette (LSR) MPLS sont raccordés par des liaisons telles que les liaisons paquet sur SONET, paquet sur SDH, ou toute autre liaison point à point. Il est à noter que la technique MPLS sur PVC n'utilise pas la commutation MPLS ATM au niveau des commutateurs ATM prenant en charge les circuits PVC. Autrement dit, les fournisseurs de services doivent continuer à fournir et gérer les circuits PVC à une échelle identique au cas de la méthode IP sur ATM classique.

La technique MPLS sur PVC utilise l'encapsulation générique décrite dans la référence [22]. Les encapsulations possibles de la couche Liaison pour le circuit PVC comprennent l'encapsulation Null et l'encapsulation LLC/SNAP. Si les circuits PVC ne transportent que des paquets MPLS, l'encapsulation Null est recommandée. Autrement, il convient d'utiliser l'encapsulation LLC/SNAP, avec un en-tête SNAP contenant les autres types spécifiés pour la commutation MPLS sur support LAN [22].

III.3.1.2 Jonctions virtuelles

Une méthode différente d'implémentation de réseaux ATM hybrides consiste à utiliser des jonctions virtuelles. Les jonctions virtuelles sont fondées sur des connexions par conduit virtuel (VP, *virtual path*). Pour la commutation MPLS ATM, on procède normalement à un étiquetage des paquets IP en les mettant dans différents circuits virtuels dans la même jonction ATM. Les différents circuits virtuels de la jonction représentent des valeurs d'étiquette différentes. Les routeurs ATM-LSR traitent les jonctions virtuelles presque de la même façon que les jonctions physiques: les différents circuits virtuels du conduit virtuel représentent des valeurs d'étiquette différentes. La différence est que la jonction virtuelle n'est pas une jonction physique reliant deux routeurs LSR adjacents. La jonction virtuelle est une connexion par conduit virtuel permanent (PVP, *permanent virtual path connection*) ou une connexion par conduit virtuel permanent commutable (SPVP, *soft permanent virtual path connection*) qui raccorde des routeurs ATM-LSR au moyen de commutateurs ATM classiques. Les jonctions virtuelles peuvent aussi raccorder des routeurs LSR de bord ATM à des

routeurs ATM-LSR, ou raccorder des routeurs de bord ATM entre eux. L'utilisation de jonctions virtuelles est illustrée sur la Figure III.1 b). L'utilisation de la commutation MPLS ATM avec des jonctions virtuelles et des étiquettes fondées sur des identificateurs VCI, qui est décrite dans la référence [34], est, à bien des égards, identique à l'utilisation de la commutation MPLS sur des jonctions physiques avec des étiquettes fondées sur des identificateurs VPI/VCI. Un circuit virtuel doit être assigné pour transporter le trafic de commande LDP et ce circuit virtuel doit utiliser l'encapsulation LLC/SNAP.

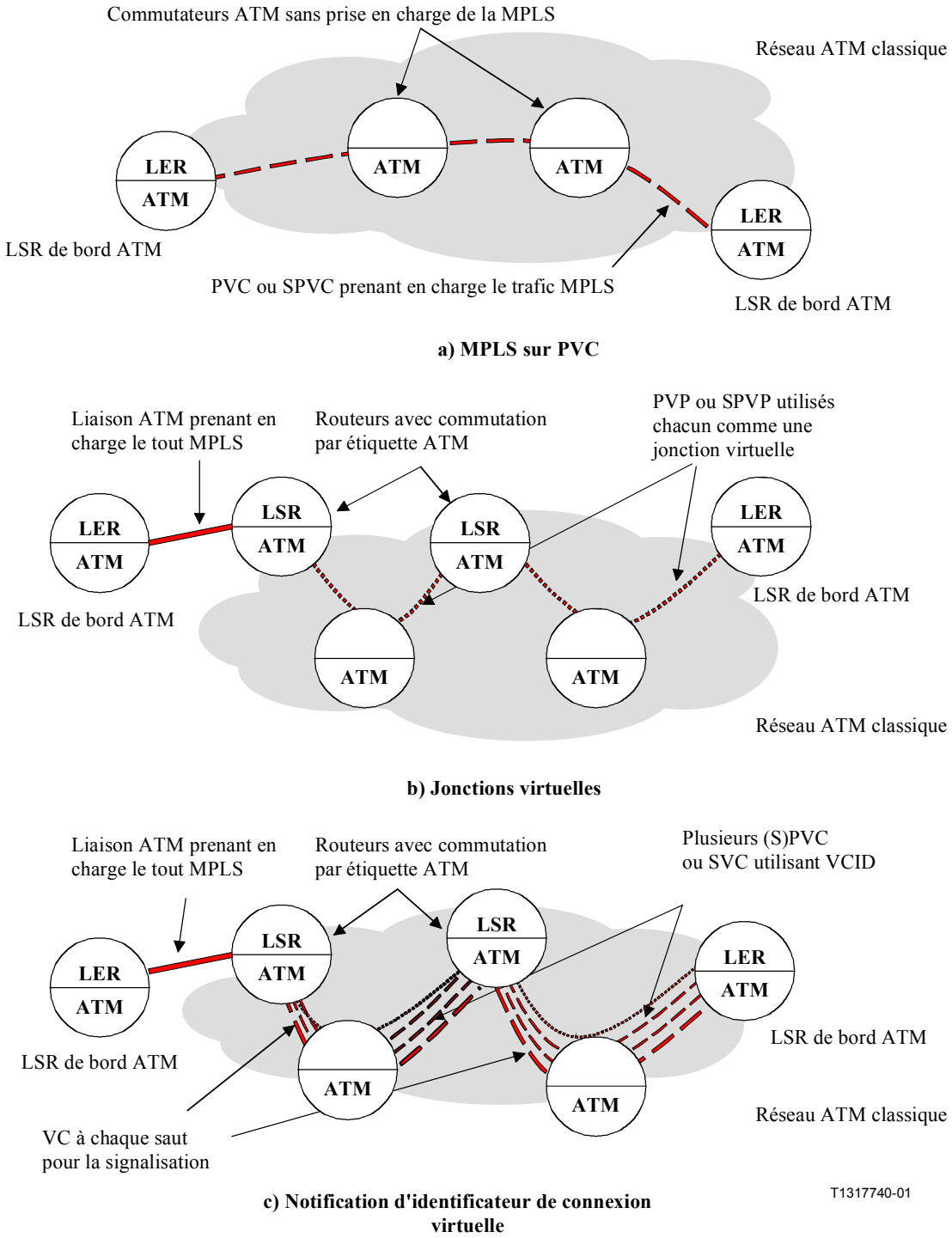


Figure III.1/Y.1310 – Techniques pour les réseaux hybrides

III.3.1.3 Notification d'identificateur de connexion virtuelle pour LDP (VCID)

La technique VCID permet d'utiliser des PVC, SPVC et des connexions par circuit virtuel commuté (SVC, *switched virtual circuit connection*) pour la commutation MPLS ATM [35]. (Ici, "SVC" désigne spécifiquement un circuit virtuel (VC) établi dynamiquement dans un réseau ATM classique. Les circuits virtuels utilisés directement pour la commutation MPLS ATM sont désignés ici par "circuits virtuels étiquetés" ou "LVC".) En revanche, la technique MPLS sur PVC utilise la commutation MPLS fondée sur des paquets et pas la commutation MPLS ATM et la technique des jonctions virtuelles utilise des connexions par conduit PVP ou SPVP et pas des PVC, SPVC ou SVC. La technique VCID prend en charge l'utilisation de PVC, SPVC et SVC dans des configurations de réseau analogues au cas des jonctions virtuelles, comme illustré sur la Figure III.1 c). Lorsqu'on emploie la technique VCID, un certain nombre de PVC, SPVC ou SVC sont utilisés pour transporter des paquets étiquetés entre les dispositifs MPLS ATM, avec un seul circuit virtuel par étiquette. Comme il y a un circuit virtuel distinct pour chaque étiquette, on peut utiliser le réacheminement de paquet MPLS ATM au niveau des dispositifs MPLS ATM en utilisant la technique VCID.

Il faut qu'un circuit virtuel par défaut soit préétabli sur chaque "saut" LSR-LSR, pour le routage IP et le protocole LDP. Ce circuit virtuel vient s'ajouter aux circuits virtuels utilisés par la technique VCID pour la correspondance avec les étiquettes.

III.3.2 Réseaux utilisant la technique MPLS sur PVC

III.3.2.1 Utilisation de la technique MPLS sur PVC

La structure de réseau la plus simple en cas d'utilisation de la technique MPLS sur PVC est la structure entièrement maillée illustrée sur la Figure III.2 a). La mise en œuvre de protocoles de routage IP dans un réseau MPLS présentant cette structure conduit aux mêmes problèmes d'évolutivité que dans le cas de réseaux IP sur ATM classiques présentant une structure analogue. Une solution consiste à utiliser une structure maillée partielle entre les routeurs, mais elle se traduirait par l'utilisation de routes multi-sauts inefficaces. Une autre solution consiste à ajouter des routeurs LSR de bord ATM supplémentaires, comme indiqué sur la Figure III.2 b), ou éventuellement un couple redondant de tels routeurs. Les routeurs LSR de bord ATM supplémentaires permettent de réduire la taille des structures maillées. Il est à noter que la qualité de fonctionnement requise sur les routeurs LSR supplémentaires sera relativement élevée, car ces routeurs transporteront une grande partie du trafic de réseau. Il n'existe pas de moyen direct permettant d'utiliser des routeurs ATM-LSR dans un réseau utilisant la technique MPLS sur PVC.

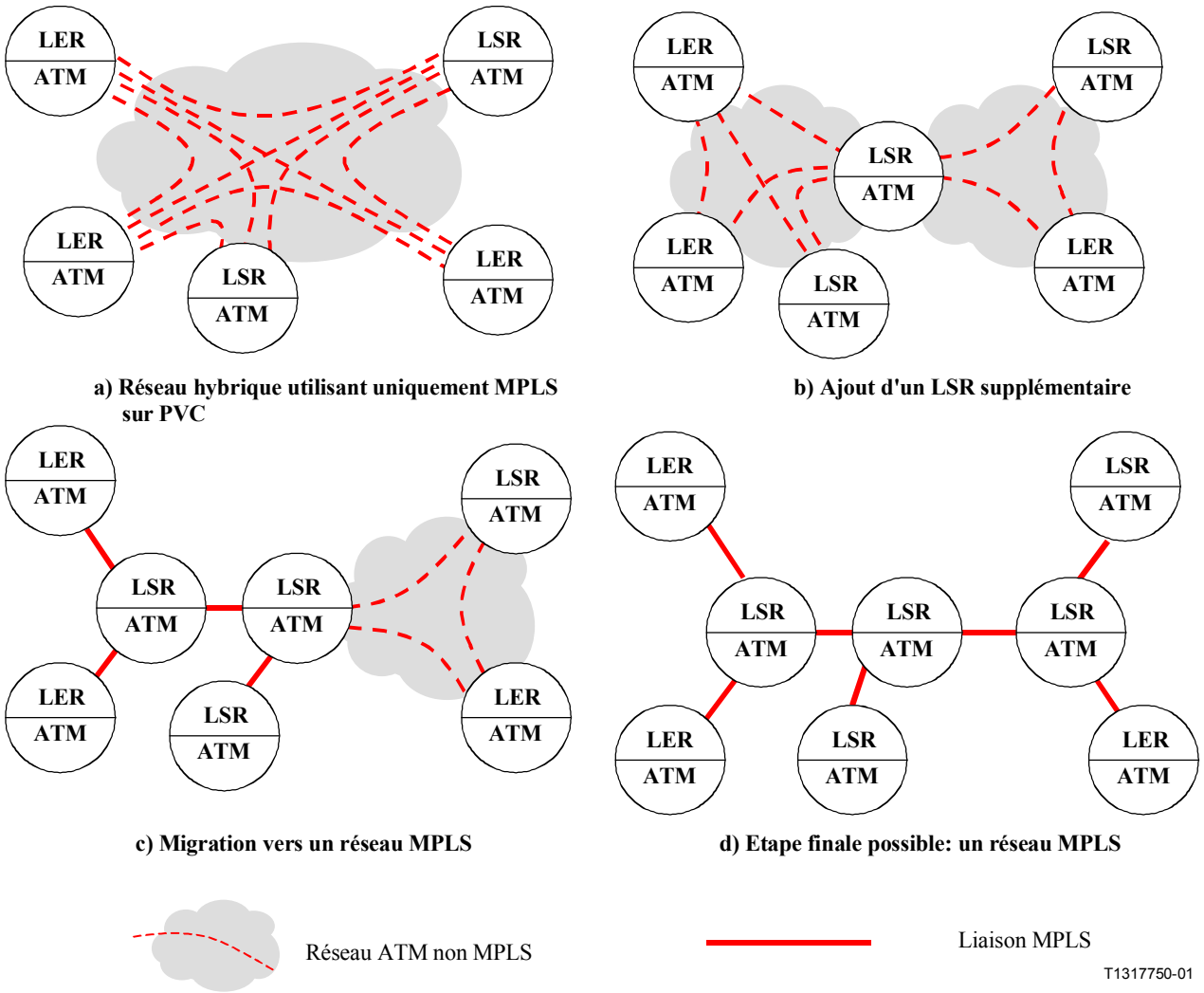


Figure III.2/Y.1310 – Réseaux MPLS ATM utilisant la technique MPLS sur PVC

Certains exploitants préféreront peut-être construire une infrastructure pour leur trafic MPLS qui soit distincte de leur réseau ATM classique. Ce réseau MPLS pourrait utiliser la technique MPLS ATM, ou bien il pourrait utiliser la commutation MPLS fondée sur des paquets, avec des routeurs LSR utilisant des paquets et des liaisons telles que les liaisons PPP sur SDH. Un tel réseau MPLS en mode paquet pourrait utiliser la technique MPLS sur PVC dans une phase transitoire, ce qui permettrait d'utiliser un réseau ATM classique pour transporter le trafic MPLS dans les premières étapes de la mise en place du réseau MPLS en mode paquet. Au fur et à mesure de la croissance de ce réseau, on pourrait remplacer les liaisons MPLS sur PVC par des liaisons physiques. Cette possible migration future est illustrée sur les Figures III.2 c) et d).

III.3.2.2 Equipements pour la technique MPLS sur PVC

Le centre d'un réseau MPLS sur PVC est un réseau ATM classique qui n'a besoin de prendre en charge que des PVC ou des SPVC. On peut utiliser pratiquement n'importe quel réseau ATM. Les routeurs LSR de bord ATM doivent prendre en charge ce qui suit:

- une ou plusieurs cartes d'interface de réseau ATM;
- l'encapsulation MPLS utilisant des paquets sur des PVC ou SPVC;
- la mise en forme du trafic en fonction des paramètres des PVC ou SPVC.

III.3.3 Réseaux utilisant des jonctions virtuelles

- *Utilisation de jonctions virtuelles*

  Un moyen simple d'utiliser des jonctions virtuelles consiste à en utiliser pour raccorder des routeurs LSR de bord ATM sans utiliser de routeurs ATM-LSR dans le réseau, comme illustré sur la Figure III.3 a). Autrement dit, tous les paquets MPLS sont transportés sur des jonctions virtuelles et il ne se produit pas de commutation par étiquette dans le réseau. La partie ATM du réseau est entièrement constituée de commutateurs ATM classiques. Plus généralement, certains commutateurs dans le réseau ATM prendront en charge la pile de protocoles MPLS et d'autres pas. On peut utiliser des jonctions virtuelles pour raccorder des routeurs ATM-LSR entre eux, ou pour raccorder des routeurs LSR de bord ATM à des routeurs ATM-LSR, ainsi que pour raccorder des routeurs LSR de bord ATM entre eux. Voir la Figure III.3 b).

- *Migration vers le tout MPLS*

  Les Figures III.3 a), b) et c) montrent un processus de migration possible pour la mise en œuvre de la commutation MPLS dans un réseau ATM classique.

  Des routeurs LSR de bord ATM sont ajoutés au bord d'un réseau ATM classique; une autre solution consiste à ajouter la fonction MPLS à des routeurs existants. Cela permet d'avoir des VPN MPLS et de conduire aux étapes suivantes.

  Ensuite, la fonction MPLS est ajoutée à certains commutateurs ATM, ou bien des commutateurs ATM-LSR supplémentaires sont ajoutés au réseau. Cela permet de réduire le nombre de jonctions virtuelles nécessaires et de commencer à régler certains problèmes d'évolutivité des réseaux hybrides.

  D'autres routeurs ATM-LSR sont ajoutés, ce qui permet de réduire encore le nombre de jonctions virtuelles et de commencer à mettre en place des liaisons MPLS ATM natives [voir la Figure III.3 c)]. On arrive alors naturellement à l'étape finale.

  Enfin, tous les commutateurs ATM sont des routeurs ATM-LSR et plus aucune jonction virtuelle n'est utilisée. L'ensemble du réseau fonctionne avec la commutation MPLS ATM et ne présente aucun des inconvénients des réseaux hybrides. Voir la Figure III.3 d).

- *Variantes*

  Les routeurs LSR et les commutateurs ATM classiques peuvent être combinés de nombreuses façons différentes. La Figure III.4 illustre d'autres structures de réseau hybride qu'il est possible de rencontrer. De nombreuses autres structures de réseau hybride sont possibles. Un réseau MPLS ATM doit inclure des routeurs LSR de bord, mais il peut utiliser pratiquement n'importe quelle combinaison comportant zéro, un ou plusieurs routeurs ATM-LSR et zéro, un ou plusieurs commutateurs ATM classiques avec des jonctions virtuelles.

- *Conditions pour la prise en charge de jonctions virtuelles*

  Les jonctions virtuelles sont implémentées au moyen de conduits virtuels permanents (PVP) ou de conduits virtuels permanents commutables (SPVP, *soft permanent virtual path*).

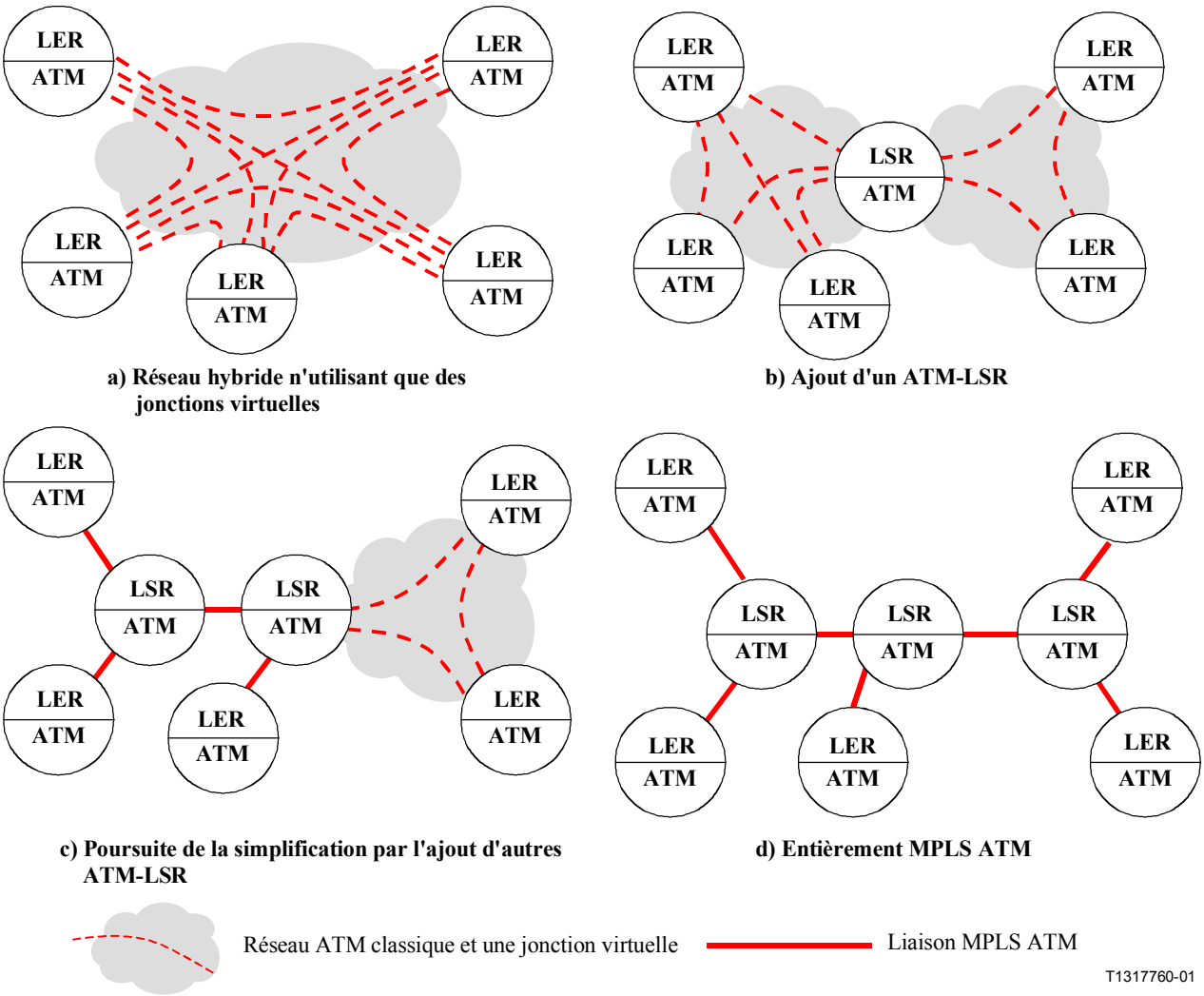


Figure III.3/Y.1310 – Réseaux MPLS ATM utilisant des jonctions virtuelles

III.3.3.1 Prise en charge de jonctions virtuelles au niveau de commutateurs ATM classiques

Les commutateurs situés dans les réseaux ATM classiques doivent prendre en charge des connexions par conduit PVP ou SPVP avec gestion du trafic de type Forum ATM ou UIT qui correspondent à celles utilisées au niveau des routeurs LSR de bord. Ces commutateurs ne sont pas tenus de prendre en charge la commutation MPLS.

III.3.3.2 Prise en charge de jonctions virtuelles au niveau de routeurs LSR de bord

Les routeurs LSR de bord ATM doivent satisfaire aux conditions suivantes pour pouvoir prendre en charge des jonctions virtuelles:

- ils doivent prendre en charge une ou plusieurs cartes d'interface de réseau ATM;
- si une jonction virtuelle donnée utilise un identificateur VPI x au niveau du routeur LSR de bord, le circuit virtuel de signalisation LDP pour la jonction virtuelle doit être associé à x. Il peut avoir VPI = x, VCI = 32, au lieu des valeurs normales par défaut VPI = 0, VCI = 32 pour la signalisation LDP [34]. Toutefois, d'autres valeurs de VCI peuvent être configurées par le biais d'accords bilatéraux mutuels.

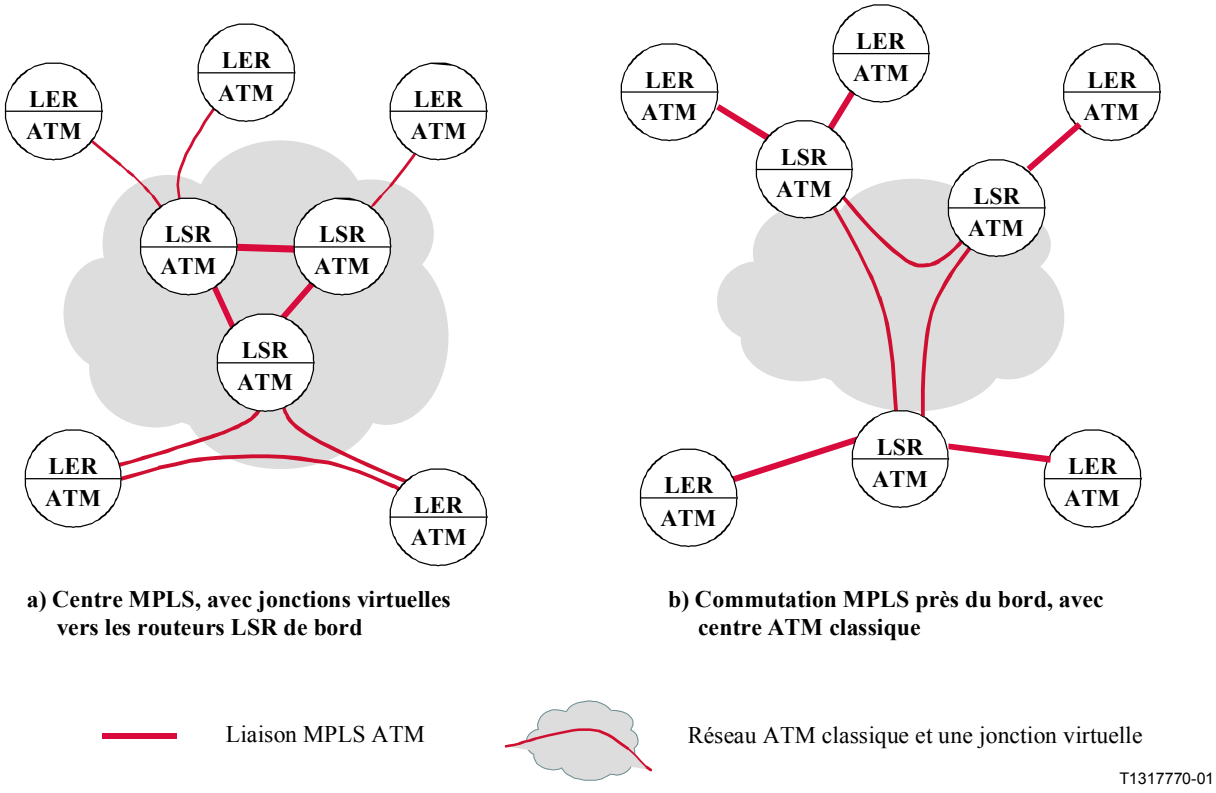


Figure III.4/Y.1310 – Autres exemples de réseau hybride utilisant des jonctions virtuelles au niveau de routeurs ATM-LSR

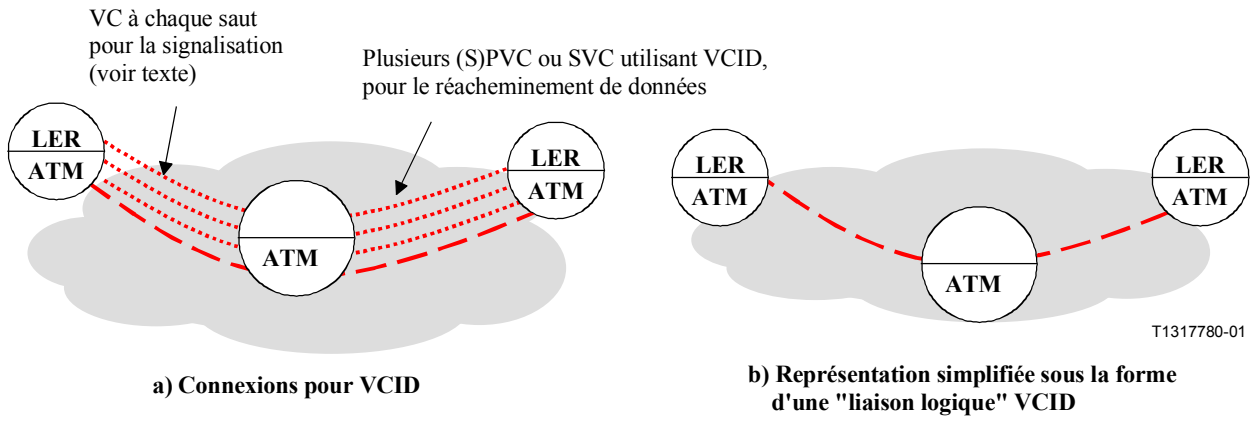
Pour pouvoir prendre en charge des jonctions virtuelles, les routeurs ATM-LSR doivent satisfaire aux mêmes conditions que les routeurs LSR de bord ATM:

- si une jonction virtuelle donnée utilise un identificateur VPI x au niveau du routeur ATM-LSR, le circuit virtuel de signalisation LDP pour la jonction virtuelle doit être associé à x. Il peut avoir VPI = x, VCI = 32, au lieu des valeurs normales par défaut VPI = 0, VCI = 32. Toutefois, d'autres valeurs de VCI peuvent être configurées par le biais d'accords bilatéraux mutuels.

III.3.4 Réseaux utilisant la technique VCID

III.3.4.1 Concept de "liaison logique"

Dans la technique VCID, on utilise plusieurs PVC, SPVC ou SVC pour raccorder chaque couple de dispositifs MPLS ATM dans un réseau classique [35]. Malgré les différences entre la technique VCID et celle des jonctions virtuelles, on peut utiliser la technique VCID dans des configurations de réseau analogues au cas des jonctions virtuelles. Voir la Figure III.1. La Figure III.5 illustre un concept permettant de comparer directement la technique VCID à celle des jonctions virtuelles.



a) Connexions pour VCID

b) Représentation simplifiée sous la forme d'une "liaison logique" VCID

Figure III.5/Y.1310 – Représentation des connexions VCID sous la forme de "liaisons logiques"

Lorsqu'on raccorde deux dispositifs MPLS ATM (routeurs ATM-LSR ou routeurs LSR de bord ATM) avec la technique VCID, de nombreux PVC, SPVC ou SVC sont nécessaires: un pour la signalisation et un grand nombre pour les étiquettes MPLS. Toutefois, le groupe de PVC, SPVC ou SVC utilisés par la technique VCID entre deux dispositifs MPLS ATM joue le rôle d'une seule liaison ATM dans un réseau MPLS ATM. Par conséquent, il est utile de considérer ce groupe de PVC, SPVC ou SVC comme étant une seule "liaison logique".

La Figure III.3 montre comment il est possible d'utiliser des jonctions virtuelles lors de la mise en œuvre de la commutation MPLS dans un réseau ATM classique. Les "liaisons logiques" VCID peuvent être utilisées d'une façon entièrement analogue, comme montré sur la Figure III.6. Les autres structures de réseau possibles montrées sur la Figure III.4 s'appliquent tout aussi bien au cas de la technique VCID.

III.3.4.2 Prise en charge de la technique VCID au niveau de commutateurs ATM classiques

Les commutateurs situés dans les réseaux ATM classiques doivent prendre en charge des connexions PVC, SPVC ou SVC avec gestion du trafic de type Forum ATM ou UIT-T qui correspondent à celles utilisées au niveau des routeurs LSR de bord. Ces commutateurs ne sont pas tenus de prendre en charge la signalisation VCID ou une quelconque fonction MPLS.

III.3.4.3 Prise en charge de la technique VCID au niveau de routeurs LSR de bord ATM

Les routeurs LSR de bord ATM doivent satisfaire aux conditions suivantes:

- ils doivent prendre en charge une ou plusieurs cartes d'interface de réseau ATM;
- ils doivent prendre en charge la technique VCID en plus des protocoles MPLS ATM.

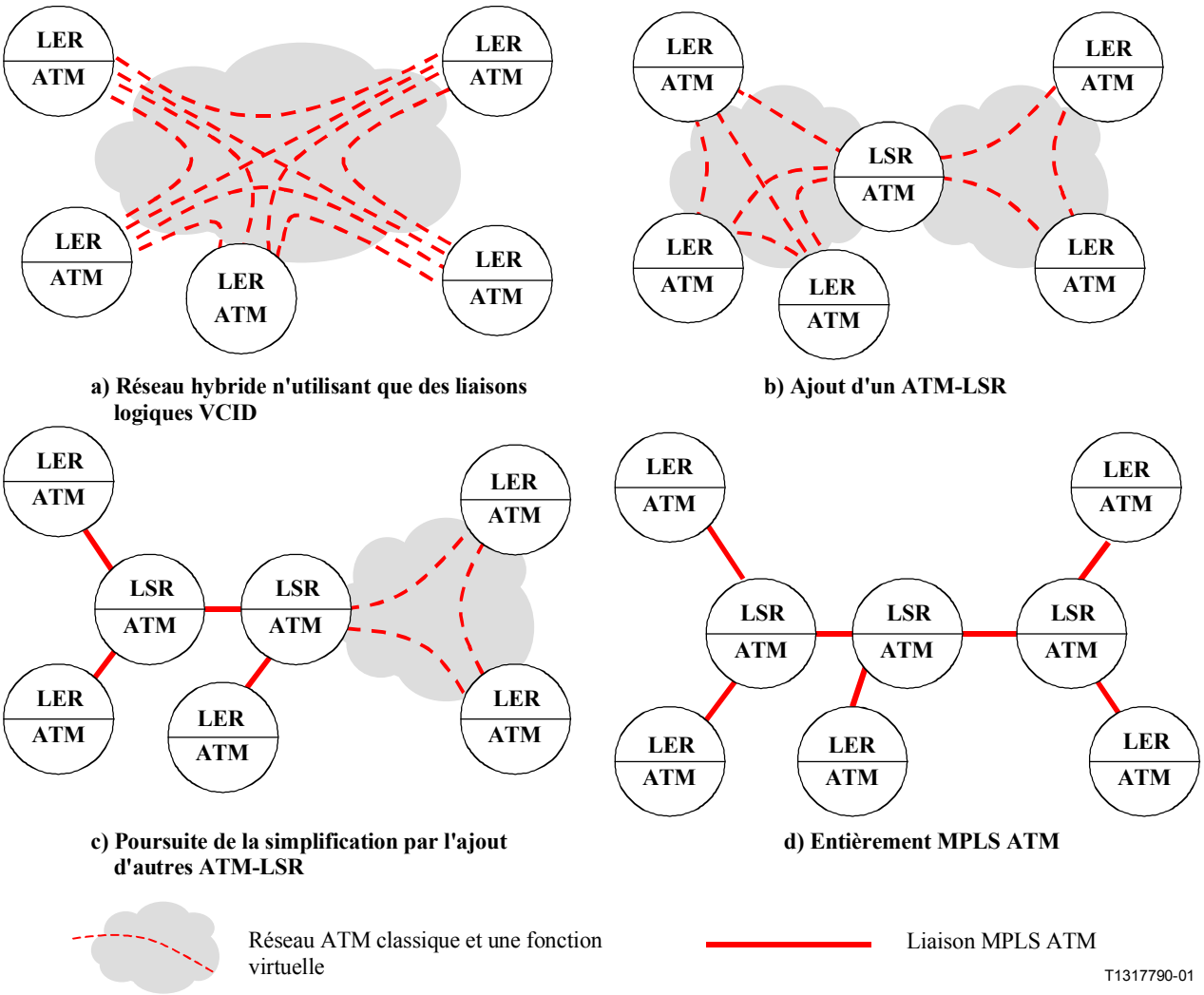


Figure III.6/Y.1310 – Réseaux MPLS ATM utilisant des "liaisons logiques" VCID

APPENDICE IV

Exemples de méthodes de prise en charge de réseaux IP-VPN dans des réseaux publics MPLS/ATM

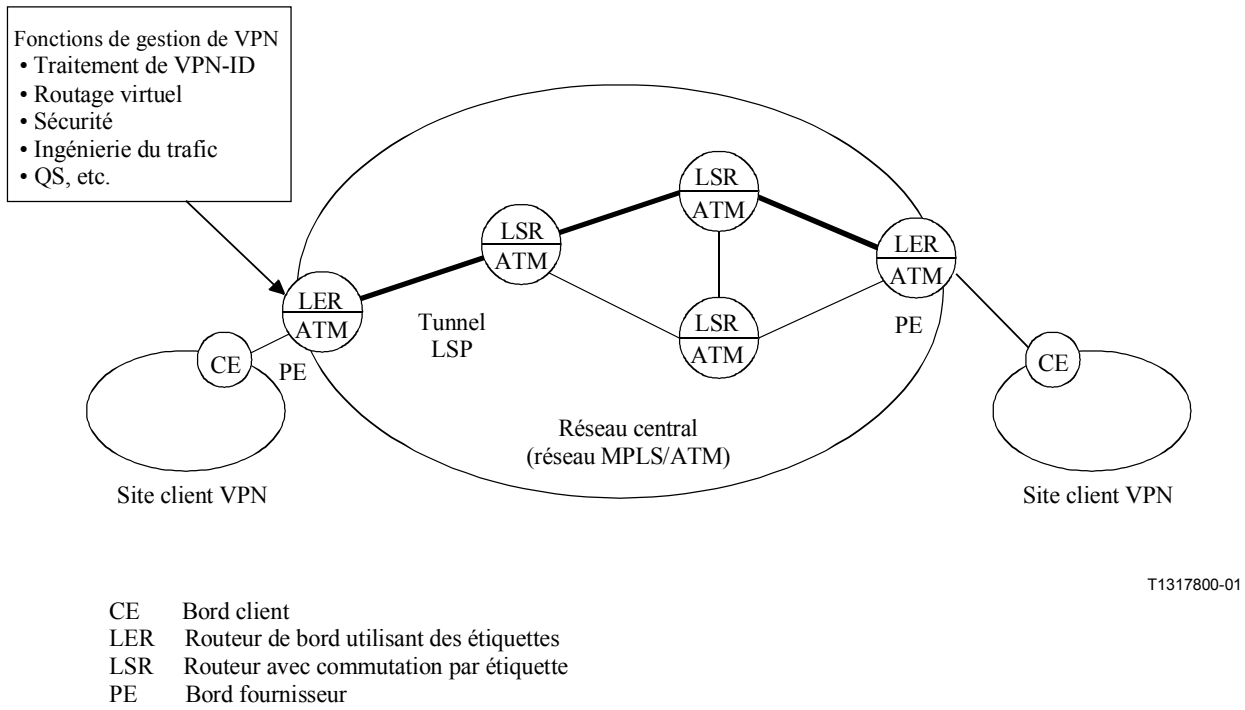
IV.1 Introduction

Le présent appendice décrit des exemples de méthode permettant d'utiliser la commutation MPLS pour offrir des services de réseau privé virtuel IP dans un réseau public. La commutation MPLS fournit une base souple et évolutive pour créer des services IP-VPN. Le sous-paragraphe 7.2 définit le service IP-VPN et donne quelques spécifications de ce service.

Il est entendu que les fournisseurs de services décideront de la conception permettant de prendre en charge des IP-VPN fondés sur leur réseau interne et les besoins des clients. Le présent appendice, qui décrit des exemples de méthode, ne vise pas à imposer de contrainte à la mise en place de VPN dans le réseau d'un exploitant.

Le concept IP-VPN a été élaboré pour la prise en charge de clients de type entreprise par des exploitants, mais les mêmes méthodes peuvent être utilisées par les fournisseurs de services pour prendre en charge d'autres fournisseurs de services (par exemple l'exploitant d'un exploitant).

La Figure IV.1 illustre un scénario générique pour les IP-VPN:



CE Bord client
LER Routeur de bord utilisant des étiquettes
LSR Routeur avec commutation par étiquette
PE Bord fournisseur

Figure IV.1/Y.1310 – Scénario générique pour les IP-VPN utilisant la commutation MPLS

Le routeur CE est le routeur du bord client qui sert d'interface entre un site client et le réseau du fournisseur de services. Le routeur PE est le routeur du bord fournisseur de services qui sert d'interface avec le routeur CE du client.

Un site est un ensemble de (sous-)réseaux qui appartiennent au réseau du client et il est raccordé au VPN via une ou plusieurs liaisons PE/CE. Un VPN est une collection de sites partageant des informations de routage communes. Un site peut faire partie de différents VPN.

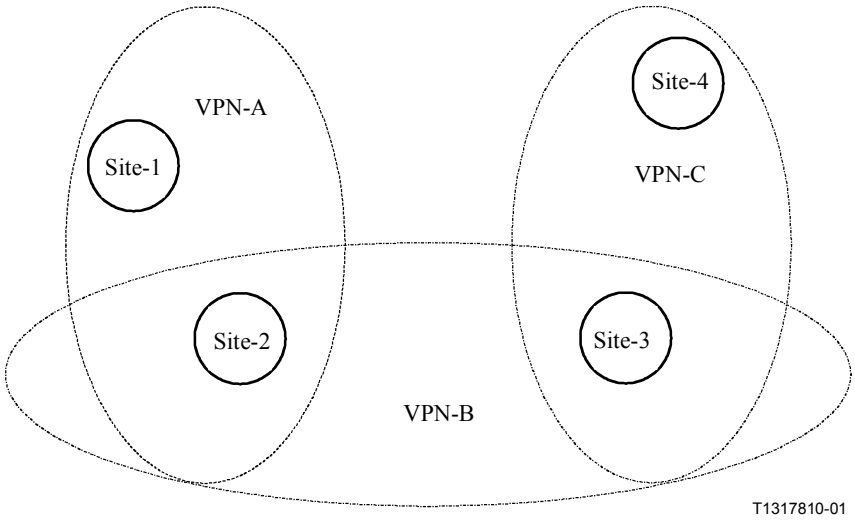


Figure IV.2/Y.1310 – Illustration de plusieurs VPN

La Figure IV.2 illustre le cas où un fournisseur de services prend en charge plusieurs VPN. Comme montré, un site peut appartenir à plusieurs VPN. Un site appartenant à plusieurs VPN ne fournit pas nécessairement de transit entre deux VPN, cela dépend de la politique adoptée (les modalités n'entrent pas dans le cadre de la présente Recommandation UIT-T). Si un site appartient à plusieurs VPN, il doit avoir un espace d'adresses qui soit unique parmi ces VPN.

IV.2 Scénario 1

Le présent sous-paragraphe décrit un exemple de méthode permettant d'utiliser la commutation MPLS pour offrir des services de réseau IP-VPN dans un réseau public. La commutation MPLS et son protocole LDP fournissent une base très souple et puissante pour créer des services de réseau IP-VPN. En tant qu'opération normale du protocole LDP, l'établissement de base d'un conduit LSP a lieu conformément à une méthode dépendante de la topologie. Il s'agit de l'établissement de base d'un conduit LSP avec utilisation d'une étiquette de base. Dans ce cas, 2 niveaux de tunnelisation LSP (empilage d'étiquettes) sont utilisés pour le routage intra-VPN.

IV.2.1 Configuration de réseau simple

IV.2.1.1 Aperçu général de l'architecture

La Figure IV.3 présente un exemple de configuration comprenant des routeurs LER et LSR pour des services de réseau IP-VPN dans un réseau central MPLS/ATM.

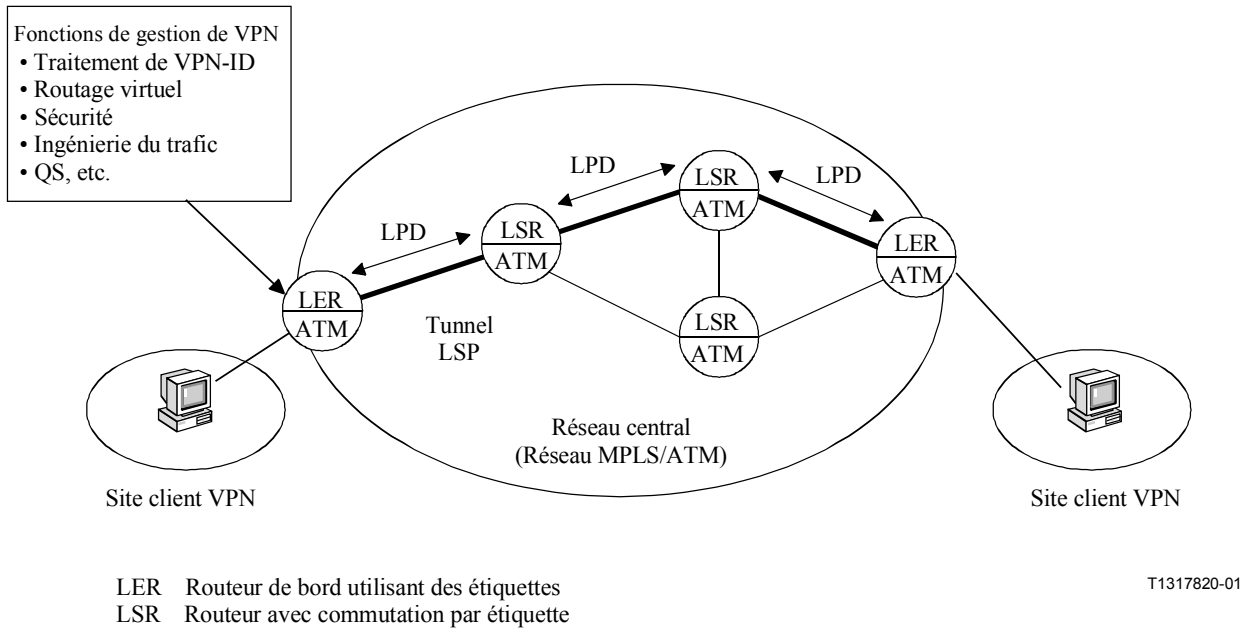


Figure IV.3/Y.1310 – Modèle de réseau pour la prise en charge de services IP-VPN dans un réseau public MPLS/ATM

IV.2.2 Composants du réseau

IV.2.2.1 Routeur LER (routeur de bord utilisant des étiquettes)

Les routeurs LER sont des routeurs de limite avec commutation MPLS situés au bord du réseau MPLS/ATM du fournisseur. Ils servent de points d'entrée et de sortie du tunnel LSP pour le trafic IP des clients VPN. Si un routeur LER est partagé par de nombreux clients, il doit réaliser un routage

virtuel, ce qui signifie qu'il tient des tables d'acheminement distinctes pour chaque VPN qu'il dessert puisqu'il est possible que leurs espaces d'adresses IP ne soient pas distincts.

IV.2.2.2 Routeur LSR (routeur avec commutation par étiquette)

Le réseau central MPLS/ATM est le réseau sous-jacent du fournisseur qui est partagé par les services IP-VPN des clients.

IV.2.2.3 Opérations d'établissement de zones IP-VPN

Un fournisseur de réseau qui souhaite proposer des services IP-VPN doit avant tout configurer un domaine MPLS. Dans ce cas, un domaine MPLS signifie une zone IP-VPN. Une zone IP-VPN est constituée de routeurs LER et de routeurs LSR. En tant qu'opération normale du protocole LDP, l'établissement de base d'un conduit LSP a lieu conformément à une méthode dépendante de la topologie, définie comme un établissement de base ou de niveau 1 d'un conduit LSP avec utilisation d'une étiquette de base. Pour le routage intra-VPN, deux niveaux de tunnelisation LSP (empilage d'étiquettes) sont utilisés.

IV.2.2.4 Détection d'appartenance à un VPN

Chaque routeur LER détecte tous les autres routeurs LER dans la zone VPN desservant le même réseau IP-VPN. Le processus de lancement de session LDP est utilisé comme méthode de détection de routeurs LER homologues, puisque le but ultime du schéma est d'établir un second niveau de tunnels MPLS. Chaque routeur LER envoie un message de salutation LDP dans chaque conduit LSP de réseau de base sortant. Les messages de salutation sont encapsulés avec l'étiquette MPLS de base de sorte qu'ils sont acheminés jusqu'au routeur LER cible. Le message de salutation LDP est une sorte de demande pour déterminer si un routeur LER pour le même VPN (un homologue) réside au niveau du routeur LER cible. Lorsqu'une contiguïté de salutation est enregistrée, le routeur LER correspondant lance une session LDP avec son homologue. L'un des deux routeurs LER lancera une connexion TCP vers l'autre. Une fois que la connexion TCP existe et que les messages de lancement nécessaires ont été échangés, une session LDP est établie entre les routeurs LER homologues. Dès que la session LDP est établie, chacun des deux routeurs LER propose une étiquette à l'autre pour établir un tunnel LSP dans sa direction. Si le tunnel LSP est un tunnel imbriqué, son étiquette est poussée sur la pile d'étiquette de paquets avant l'étiquette LSP de réseau de base.

IV.2.2.5 Appartenance à un VPN et diffusion d'informations d'atteignabilité

Le routeur LER apprend les préfixes d'adresse IP des sites clients auxquels il est directement connecté en échangeant des informations de routage. Le routeur LER doit identifier ses routeurs LER homologues. Il doit découvrir quels autres routeurs LER dans la même zone VPN desservent son VPN. Le routeur LER propose d'établir une session LDP directe avec chaque autre routeur LER dans la zone VPN. Mais seuls les routeurs LER desservant un même VPN se détecteront les uns les autres et établiront des sessions LDP les uns avec les autres. Les sessions LDP peuvent uniquement être établies correctement entre des routeurs LER qui prennent en charge le même VPN.

IV.2.2.6 Atteignabilité intra-VPN

Le premier trafic qui circulera sur les tunnels imbriqués sera l'échange d'informations de routage entre les routeurs LER. Il est supposé que lors de la première configuration d'un routeur LER pour un IP-VPN, une partie de l'information de configuration est le protocole de routage que ce routeur doit utiliser en "intra-VPN". Il est également supposé que le routeur LER obtiendra tous les pouvoirs en termes de sécurité dont il peut avoir besoin pour participer en tant que routeur voisin pour les autres routeurs LER. Après une phase de découverte du schéma de routage "intra-VPN", chaque routeur LER annoncera les préfixes d'adresse propres aux clients VPN qu'il permettra d'atteindre.

IV.2.2.7 Réacheminement de paquets IP

A la suite des échanges d'informations de routage entre les routeurs LER, chaque routeur LER établira une table de réacheminement qui associe les préfixes d'adresse propres aux clients VPN (FEC: classes d'équivalence de réacheminement) au prochain saut. Lors de l'arrivé de paquets IP dont le prochain saut est un routeur LER, le processus de réacheminement pousse d'abord l'étiquette pour le routeur homologue (étiquette de tunnel imbriquée). Puis l'étiquette de base, pour le premier saut du conduit LSP de réseau de base qui mène au routeur LER, est poussée sur le paquet. Le paquet doublement étiqueté est ensuite transmis au routeur LSR suivant dans le conduit LSP de réseau de base. Lorsque le paquet arrive au routeur LER cible, l'étiquette extérieure peut avoir changé plusieurs fois, mais l'étiquette imbriquée est inchangée. Lorsque la pile d'étiquettes est dépilée, l'étiquette imbriquée est utilisée pour transmettre le paquet au bon routeur LER. A un routeur LER donné, l'espace d'étiquettes imbriquées utilisé par chaque VPN doit être disjoint de celui de tous les autres VPN pris en charge par le même routeur LER.

IV.3 Scénario 2

Le présent sous-paragraphe décrit un exemple de méthode permettant d'utiliser la commutation MPLS et le protocole de passerelle limite multiprotocole pour offrir des services de réseau IP-VPN dans un réseau public, comme défini dans la référence [29]. Le présent sous-paragraphe donne un aperçu. Pour les détails, on se reportera à la référence [29].

IV.3.1 Aperçu général de l'architecture

La Figure IV.1 présente un exemple de configuration comprenant des routeurs LER et LSR pour des services de réseau IP-VPN dans un réseau central MPLS/ATM.

La Figure IV.4 illustre le modèle de réseau sur la base de la référence [29].

IV.3.2 Composants du réseau

Le présent sous-paragraphe décrit les composants du réseau à utiliser pour la prise en charge du réseau IP-VPN et précise la terminologie utilisée.

IV.3.2.1 Routeur du bord fournisseur (PE)

Le routeur PE est le routeur du bord fournisseur de services qui sert d'interface avec les routeurs du bord client (CE). Dans le cadre de la présente Recommandation UIT-T, ce routeur est un routeur LSR de bord (c'est-à-dire que l'interface entre le client et le fournisseur n'utilise pas la commutation MPLS).

IV.3.2.2 Routeur du bord client (CE)

Le routeur CE est le routeur du bord client qui sert d'interface avec les routeurs du bord fournisseur de services (PE). Dans le cadre du présent scénario, le routeur CE n'utilise pas la commutation MPLS et c'est un routeur IP. Il n'a pas besoin de prendre en charge de protocole de routage ou de signalisation propre au VPN.

IV.3.2.3 Routeur du fournisseur (P)

Les routeurs P sont les routeurs avec commutation par étiquette situés dans le centre.

IV.3.2.4 Site

Un site est un ensemble de (sous-)réseaux qui font partie du réseau du client et il est raccordé au VPN via une ou plusieurs liaisons PE/CE. Un site peut appartenir à différents VPN.

IV.3.2.5 Désignateur de route

Le fournisseur assigne à chaque VPN un identificateur unique appelé désignateur de route (RD, *route distinguisher*) qui est différent pour chaque Intranet ou Extranet au sein du réseau du fournisseur. Les tables de réacheminement dans les routeurs PE contiennent des adresses uniques, appelées adresses VPN-IP, créées par la concaténation du désignateur de route avec les adresses IP des clients. Les adresses VPN-IP sont uniques pour chaque point d'extrémité du réseau du fournisseur de services et sont stockées dans les tables de réacheminement de chaque nœud du VPN (c'est-à-dire chaque routeur PE du VPN).

IV.3.2.6 Modèle de connexion

La Figure IV.4 ci-dessous illustre le modèle de connexion pour le VPN MPLS/BGP.

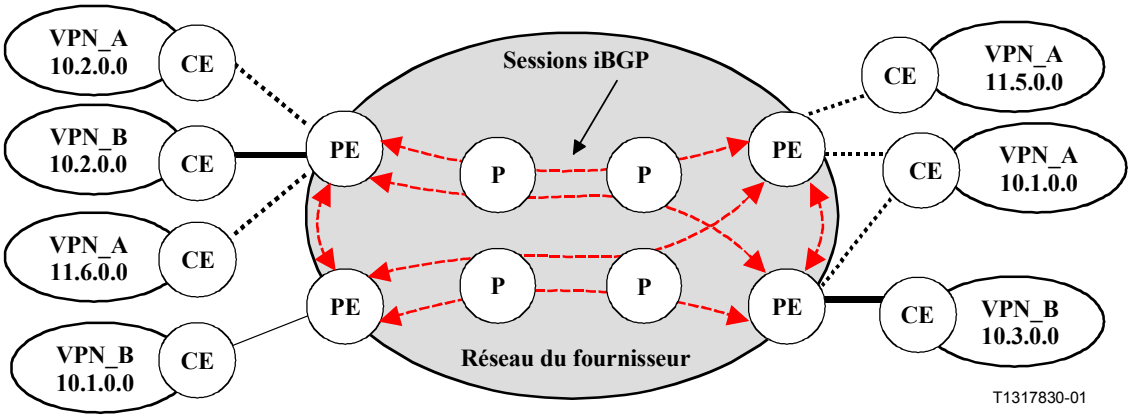


Figure IV.4/Y.1310 – Modèle de connexion pour des IP-VPN utilisant MPLS/BGP

Les routeurs P sont situés dans le centre du réseau MPLS. Les routeurs PE utilisent la commutation MPLS pour communiquer avec le réseau MPLS central et le routage IP pour communiquer avec les routeurs CE. Les routeurs P et PE utilisent un protocole de routage IP (protocole de passerelle interne) pour établir des routes IP dans le centre MPLS et le protocole LDP pour la distribution d'étiquettes entre routeurs.

Les routeurs PE utilisent le protocole BGP-4 multiprotocole pour communiquer entre eux pour échanger des étiquettes et la politique de chaque VPN. Ils constituent une structure entièrement maillée BGP (à moins qu'un réflecteur de route ne soit utilisé). Plus particulièrement, comme ils se trouvent dans le même système autonome, ils utilisent un protocole BGP interne (iBGP, *internal BGP*).

Les routeurs P n'utilisent pas le protocole BGP et n'ont absolument pas connaissance des VPN. Ils utilisent des procédures et des protocoles MPLS normaux.

Les routeurs PE peuvent échanger des routes IP avec des routeurs CE via un protocole de routage IP. On peut aussi utiliser des routes statiques. Des procédures de routage normales sont utilisées entre les routeurs CE et PE. Le routeur CE n'a pas à mettre en œuvre la commutation MPLS ou à avoir une connaissance particulière du VPN.

Les routeurs PE distribuent les routes des clients aux autres routeurs PE via le protocole iBGP. L'adresse VPN-IP (créée à partir du désignateur de route et de l'adresse IPv4) est utilisée dans le protocole BGP pour distribuer les routes. Par conséquent, différents VPN peuvent utiliser des espaces d'adresses IPv4 se chevauchant sans qu'il en résulte d'adresses VPN-IP en double.

Les routeurs PE mettent en correspondance les routes qu'ils ont apprises grâce au protocole BGP dans leurs tables de routage pour transmettre les paquets reçus en provenance des routeurs CE dans le bon conduit LSP.

Deux niveaux d'étiquette sont utilisés. L'étiquette intérieure sert à identifier le bon VPN pour le routeur PE. L'étiquette extérieure est utilisée par les routeurs LSR dans le réseau MPLS pour router les paquets vers le bon routeur PE.

IV.3.2.7 Opérations d'établissement de zones IP-VPN

Un fournisseur de réseau qui souhaite offrir un service IP-VPN doit concevoir et mettre en place le réseau conformément aux spécifications de connectivité.

Chaque routeur PE doit être configuré pour les VPN qu'il doit prendre en charge et pour les VPN auxquels chaque routeur CE rattaché appartient. Une relation entre homologues iBGP doit être configurée entre routeurs PE dans le réseau MPLS ou un réflecteur de route est utilisé. On peut utiliser des capacités normales d'évolutivité du protocole iBGP.

Il faut réaliser une configuration normale du protocole de routage pour les communications avec les routeurs CE.

Il faut réaliser une configuration MPLS normale (LDP, IGP, etc.) pour les communications avec le réseau central MPLS.

Les routeurs P ne devraient pas avoir à être configurés pour prendre en charge les VPN (au-delà de la prise en charge normale de la commutation MPLS).

IV.3.2.8 Appartenance à un VPN et diffusion d'informations d'atteignabilité

Le routeur PE apprend les préfixes d'adresse IP des sites clients auxquels il est directement raccordé en échangeant des informations de routage via un protocole de routage IP ou via une configuration (routes statiques).

Le routeur PE échange des préfixes d'adresse VPN-IP avec ses homologues BGP pour apprendre les routes vers les sites VPN de destination. Il échange aussi des étiquettes via le protocole BGP avec les routeurs PE homologues afin d'identifier le conduit LSP à utiliser pour la connectivité entre routeurs PE. Ces étiquettes sont utilisées comme des étiquettes de second niveau et ne sont pas vues par les routeurs P.

Les routeurs PE tiennent à jour des tables de routage et de réacheminement distinctes pour chaque VPN qu'ils prennent en charge. Chaque routeur CE rattaché à un routeur PE utilisera la table de routage appropriée en fonction de l'interface à laquelle il est rattaché.

IV.3.2.9 Réacheminement de paquets IP

A la suite des échanges d'informations de routage entre les routeurs PE, chaque routeur PE établira une table de réacheminement pour chaque VPN dans laquelle les préfixes d'adresse propres aux clients VPN sont mis en relation avec les routeurs PE du prochain saut.

Lorsque des paquets IP arrivent en provenance d'un routeur CE, le routeur PE cherchera, dans la table de réacheminement, le VPN identifié avec cette interface. Si une correspondance est trouvée, le routeur procédera comme suit:

- si le prochain saut correspond à un routeur PE, le processus de réacheminement pousse d'abord l'étiquette pour le routeur PE homologue (étiquette de tunnel imbriquée) identifiée par la table de routage;
- le routeur PE pousse alors l'étiquette de base sur le paquet, pour le premier saut du conduit LSP de réseau de base qui mène au routeur PE cible. Le paquet doublement étiqueté est ensuite transmis au routeur LSR suivant dans le conduit LSP de réseau de base;

- les routeurs P (LSR) utilisent les étiquettes du niveau supérieur et leurs tables de routage pour router le paquet vers le routeur PE cible;
- lorsque le paquet arrive au routeur PE cible, l'étiquette la plus à l'extérieur peut avoir changé plusieurs fois mais l'étiquette imbriquée n'a pas changé;
- lorsque le routeur PE reçoit un paquet, il utilise l'étiquette imbriquée pour identifier le VPN. A un routeur PE donné, l'espace d'étiquettes imbriquées utilisé par chaque VPN doit être disjoint de celui de tous les autres VPN pris en charge par le même routeur PE. Le routeur PE consulte la table de routage associée à ce VPN pour déterminer sur quelle interface le paquet doit être transmis.

Si aucune correspondance n'est trouvée dans la table de routage du VPN, le routeur PE consulte la table de routage Internet (si cette capacité est mise à disposition par le fournisseur) pour déterminer les possibilités de routage. Si aucune route n'est trouvée, le paquet est supprimé.

Les tables de réacheminement du VPN-IP contiennent des étiquettes qui correspondent à des adresses VPN-IP. Ces étiquettes permettent de router le trafic vers chaque site d'un VPN. Comme on utilise des étiquettes et non des adresses IP, les clients peuvent conserver leurs plans d'adressage privés, dans l'Internet d'entreprise, sans nécessiter que la traduction d'adresse de réseau (NAT, *network address translation*) fasse transiter le trafic par le réseau du fournisseur. Le trafic est séparé entre les VPN au moyen d'une table de réacheminement distincte sur le plan logique pour chaque VPN. Sur la base de l'interface d'entrée, le commutateur sélectionne une table de réacheminement donnée, dans laquelle figurent uniquement les destinations valables dans le VPN, grâce au protocole BGP. Pour créer des Extranets, un fournisseur configure explicitement l'atteignabilité entre VPN. (Des configurations NAT peuvent être nécessaires.)

IV.3.2.10 Sécurité

Dans le réseau du fournisseur, des désignateurs de route sont associés à chaque paquet par le routeur PE, de sorte qu'un utilisateur ne peut pas "parodier" un flux ou un paquet dans le VPN d'un autre client. Il est à noter que les désignateurs de route ne sont pas transportés dans les paquets de données utilisateur. Les utilisateurs ne peuvent participer à un Intra-net ou à un Extra-net que s'ils résident à un port physique correct et ont les désignateurs de route corrects configurés dans le routeur PE. Cela rend pratiquement impossible toute entrée et fournit les mêmes niveaux de sécurité que ceux auxquels les utilisateurs sont habitués dans un service en mode relais de trames, de type ligne louée ou en mode ATM.

APPENDICE V

Bibliographie

Le présent appendice contient des références explicites imbriquées dans les documents RFC énumérés au 2.1.2. Les références imbriquées déjà incluses sous forme de références primaires ne sont pas répétées dans le présent appendice.

[1] POSTEL (J.): Internet Protocol, *RFC 760, USC/Information, Sciences Institute*, janvier 1980.

[2] POSTEL (J.): Transmission Control Protocol, *RFC 761, USC/Information Sciences Institute*, janvier 1980.

[3] POSTEL (J.): Internet Control Message Protocol – DARPA Internet Program Protocol Specification, *RFC 792, USC/Information Sciences Institute*, septembre 1981.

[4] POSTEL (J.): Service Mappings, *RFC 795, USC/Information Sciences Institute*, septembre 1981.

[5] POSTEL (J.): Address Mappings, *RFC 796, USC/Information Sciences Institute*, septembre 1981.

[6] BRADEN (R.): Requirements for Internet hosts – communication layers, *STD 3, RFC 1122*, octobre 1989.

[7] RIVEST (R.): The MD5 Message-Digest Algorithm, *RFC 1321*, avril 1992.

[8] ALMQUIST (P.): Type of Service in the Internet Protocol Suite, *RFC 1349*, juillet 1992.

[9] MALIS (A.): Multiprotocol Encapsulation over Frame Relay, *RFC 1490*, juillet 1993.

[10] MOY (J.): OSPF Version 2, *RFC 1583, Proteon Inc*, mars 1994.

[11] SIMPSON (W.): The Point-to-Point Protocol (PPP), *STD 51, RFC 1661*, juillet 1994.

[12] REYNOLDS (J.), POSTEL (J.): Assigned Numbers, *RFC 1700*, octobre 1994.

[13] REKHTER (Y.), LI (T.): A Border Gateway Protocol 4 (BGP-4), *RFC 1771*, mars 1995.

[14] BAKER (F.), Editor: Requirements for IP Version 4 Routers, *RFC 1812*, juin 1995.

[15] SCHULZRINNE (H.), CASNER (S.), FREDERICK (R.), JACOBSON (V.): RTP: A Transport Protocol for Real-Time Applications, *RFC 1889*, janvier 1996.

[16] McCANN (J.), MOGUL (J.), DEERING (S.): Path MTU Discovery for IP version 6, *RFC 1981*, août 1996.

[17] BRADNER (S.): Key words for use in RFCs to Indicate Requirement Levels, *BCP 14, RFC 2119*, mars 1997.

[18] BRADEN (R.) et al.: Resource ReSerVation Protocol (RSVP) – Version 1, Functional Specification, *RFC 2205*, septembre 1997.

[19] WROCLAWSKI (J.): The use of RSVP with IETF Integrated Services, *RFC 2210*, septembre 1997.

[20] WROCLAWSKI (J.): Specification of the Controlled-Load Network Element Service, *RFC 2211*, septembre 1997.

[21] SHENKER (S.), WROCLAWSKI (J.): General Characterization Parameters for Integrated Service Network Elements, *RFC 2215*, septembre 1997.

[22] SHENKER (S.), WROCLAWSKI (J.): Network Element Service Specification Template, *RFC 2216*, septembre 1997.

[23] HINDEN (R.), DEERING (S.): IP Version 6 Addressing Architecture, *RFC 2373*, juillet 1998.

[24] HEFFERNAN (A.): Protection of BGP Sessions via the TCP MD5 Signature Option, *RFC 2385*, août 1998.

[25] KENT (S.), ATKINSON (R.): Security Architecture for the Internet Protocol, *RFC 2401*, novembre 1998.

[26] KENT (S.), ATKINSON (R.): IP Authentication Header, *RFC 2402*, novembre 1998.

[27] KENT (S.), ATKINSON (R.): IP Encapsulating Security Protocol (ESP), *RFC 2406*, novembre 1998.

[28] NARTEN (T.), ALVESTRAND (H.): Guidelines for Writing an IANA Considerations Section in RFCs, *RFC 2434*, octobre 1998.

[29] DEERING (S.), HINDEN (R.): Internet Protocol, Version 6 (IPv6) Specification, *RFC 2460*, décembre 1998.

[30] CONTA (A.), DEERING (S.): ICMP for the Internet Protocol Version 6 (IPv6), *RFC 2463*, décembre 1998.

[31] AWDUCHE *et al*.: Requirements for Traffic Engineering Over MPLS, *RFC 2702*, septembre 1999.

[32] POSTEL (J.): Internet Name Server, *USC/Information Sciences Institute, IEN 116*, août 1979.

[33] SOLLINS (K.): The TFTP Protocol, *Massachusetts Institute of Technology, IEN 133*, janvier 1980.

[34] CERF (V.): The Catenet Model for Internetworking, *Information Processing Techniques Office, Defense Advanced Research Projects Agency, IEN 48*, juillet 1978.

[35] BERANEK (Bolt), NEWMAN: Specification for the Interconnection of a Host and an IMP, *BBN Technical Report 1822*, Révisé en mai 1978.

[36] SHOCH (J.): Inter-Network Naming, Addressing, and Routing, *COMPCON, IEEE Computer Society*, Automne 1978.

[37] SHOCH (J.): Packet Fragmentation in Inter-Network Protocols, *Computer Networks, Vol. 3, Nº 1*, février 1979.

[38] STRAZISAR (V.): How to Build a Gateway, *IEN 109, Bolt Beranek and Newman*, août 1979.

[39] CERF (V.), KAHN (R.): A Protocol for Packet Network Intercommunication, *IEEE Transactions on Communications*, Vol. COM-22, Nº 5, pp. 637-648, mai 1974.

[40] DALAL (Y.), SUNSHINE (C.): Connection Management in Transport Protocols, *Computer Networks*, Vol. 2, Nº 6, pp. 454-473, décembre 1978.

[41] DEMERS (A.), KESHAV (S.), SHENKER (S.): Analysis and Simulation of a Fair Queueing Algorithm, in *Internetworking: Research and Experience*, Vol. 1, Nº 1, pp. 3-26.

[42] ZHANG (L.): Virtual Clock: A New Traffic Control Algorithm for Packet Switching Networks, in *Proc. ACM SIGCOMM '90*, pp. 19-29.

[43] VERMA (D.), ZHANG (H.), FERRARI (D.), Guaranteeing Delay Jitter Bounds in Packet Switching Networks, in *Proc. Tricomm '91*.

[44] GEORGIADIS (L.), GUERIN (R.), PERIS (V.), SIVARAJAN (K.N.): Efficient Network QoS Provisioning Based on per Node Traffic Shaping, *IBM Research Report Nº RC-20064*.

[45] GOYAL (P.), LAM (S.S.), VIN (H.M.): Determining End-to-End Delay Bounds in Heterogeneous Networks, in P*roc. 5th Intl. Workshop on Network and Operating System Support for Digital Audio and Video*, avril 1995.

[46] FLOYD (S.), JACOBSON (V.): Link-sharing and Resource Management Models for Packet Networks, *IEEE/ACM Transactions on Networking*, Vol. 3, Nº 4, pp. 365-386, août 1995.

[47] SHREEDHAR (M.), VARGHESE (G.): Efficient Fair Queueing using Deficit Round Robin, *Proc. ACM SIGCOMM 95*, 1995.

[48] BENNETT (J.), ZHANG (Hui): Hierarchical Packet Fair Queueing Algorithms, *Proc. ACM SIGCOMM 96*, août 1996.

[49] STILIADIS (D.), VARMA (A.): Rate-Proportional Servers: A Design Methodology for Fair Queueing Algorithms, *IEEE/ACM Trans. on Networking*, avril 1998.

[50] WU (L.) *et al*.: LDP State Machine work in progress (*draft-ietf-mpls-ldp-state-00*), février 1999.

[51] DAVIE (B.), LAWRENCE (J.), McCLOGHRIE (K.), REKHTER (Y.), ROSEN (E.), SWALLOW (G.), DOOLAN (P.): Use of Label Switching With ATM, Work in Progress, septembre 1998.

[52] FELDMAN (N.), JAMOUSSI (B.), KOMANDUR (S.), VISWANATHAN (A.), WORSTER (T.): MPLS using ATM VP Switching, Work in Progress, février 1999.

[53] CONTA (A.), DOOLAN (P.), MALIS (A.): Use of Label Switching on Frame Relay Networks, Work in Progress, octobre 1998.

[54] NIKOLAOU (N.), RIGOLIO (G.), CASACA (A.), CIULLI (N.), STASSINOPOULOS (G.): Intégration de IP et ATM pour la prise en charge de classe QS et multimédia, *4e Conférence internationale distribuée (ICD 1999)*, 22-23 septembre 1999, Madrid, Espagne.

SÉRIES DES RECOMMANDATIONS UIT-T

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

Genève, 2001