Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.1714

(01/2007)

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

Aspects relatifs au protocole Internet – Gestion, exploitation et maintenance

Gestion et cadre général d'exploitation, d'administration et de maintenance des réseaux MPLS

Recommandation UIT-T Y.1714

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

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

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	**Y.1700–Y.1799**
Taxation	Y.1800–Y.1899
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899

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

Recommandation UIT-T Y.1714

Gestion et cadre général d'exploitation, d'administration et de maintenance des réseaux MPLS

Résumé

La présente Recommandation porte sur l'exploitation, l'administration et la maintenance (OAM, *operation, administration and maintenance*) du plan utilisateur de commutation multiprotocolaire par étiquetage (MPLS, *multiprotocol label switching*), les aspects relatifs au plan de commande et les aspects de la gestion MPLS liés au réseau de gestion des télécommunications (RGT). Plus particulièrement, les mécanismes abordés dans la présente Recommandation sont actuellement à l'étude au sein de différents organismes de normalisation, principalement l'UIT-T et le Groupe de travail d'ingénierie Internet (IETF, *Internet engineering task force*).

La présente Recommandation traite principalement des aspects OAM propres aux technologies MPLS du modèle de RGT de la Rec. UIT-T M.3010. Le domaine d'application de la présente Recommandation se limite aux composants et interfaces qui relient entre eux les éléments de réseau (plan utilisateur et plan de commande), ainsi que les éléments de réseau au système de gestion d'élément (EMS, *element management system*) et au système de gestion de réseau (NMS, *network management system*).

Source

La Recommandation UIT-T Y.1714 a été approuvée le 13 janvier 2007 par la Commission d'études 13 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Introduction

La présente Recommandation est une Recommandation-cadre visant à faciliter les travaux sur tous les aspects de la gestion de la commutation multiprotocolaire par étiquetage (MPLS, *multiprotocol label switching*). La présente Recommandation porte sur l'exploitation, l'administration et la maintenance (OAM, *operation, administration and maintenance*) du plan utilisateur de commutation MPLS, les aspects relatifs au plan de commande et les aspects de la gestion MPLS liés au réseau de gestion des télécommunications (RGT). Il est bien connu que ces travaux recoupent ceux qui sont menés dans le cadre de nombreuses commissions d'études et Questions de l'UIT-T, ainsi qu'au sein d'autres organismes de normalisation.

De nombreux aspects de la gestion MPLS ont été mis au point en même temps que la présente Recommandation. Les divers aspects de gestion qui n'étaient pas prêts pour être inclus dans les références normatives à la date de publication seront examinés dans le cadre des procédures normales de mise à jour des documents de l'UIT et sont signalés dans la présente Recommandation par la mention "à étudier".

Recommandation UIT-T Y.1714

Gestion et cadre général d'exploitation, d'administration et de maintenance des réseaux MPLS

1 Domaine d'application

La présente Recommandation porte sur l'exploitation, l'administration et la maintenance (OAM, *operation, administration and maintenance*) du plan utilisateur de commutation multiprotocolaire par étiquetage (MPLS, *multiprotocol label switching*), les aspects relatifs au plan de commande et les aspects de la gestion MPLS liés au réseau de gestion des télécommunications (RGT). Les mécanismes abordés dans la présente Recommandation sont actuellement à l'étude au sein de différents organismes de normalisation, principalement l'UIT-T et le Groupe de travail d'ingénierie Internet (IETF, *Internet engineering task force*).

La présente Recommandation traite principalement des aspects OAM propres aux technologies MPLS du modèle de RGT de [UIT-T M.3010]. Le domaine d'application de la présente Recommandation se limite aux composants et interfaces qui relient entre eux les éléments de réseau (plan utilisateur et plan de commande), ainsi que les éléments de réseau au système de gestion d'élément (EMS, *element management system*) et au système de gestion de réseau (NMS, *network management system*) (l'interface "Q").

Le diagramme suivant (Figure 1) indique le domaine d'application de la présente Recommandation et l'interaction avec les autres commissions d'études de l'UIT-T et les organismes de normalisation.

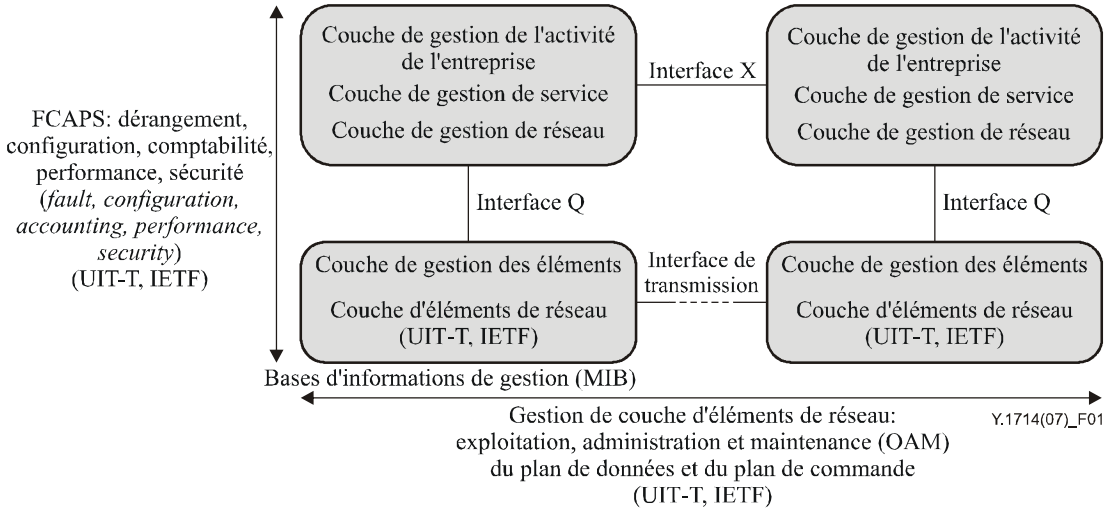

Figure 1 – Modèle de RGT générique

2 Références normatives

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

[UIT-T G.8110] Recommandation UIT-T G.8110/Y.1370 (2005), *Architecture du réseau de couche MPLS*.

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

[UIT-T M.3010] Recommandation UIT-T M.3010 (2000), *Principes du réseau de gestion des télécommunications*.

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

[UIT-T X.84] Recommandation UIT-T X.84 (2004), *Prise en charge des services à relais de trames sur les réseaux noyau MPLS*.

[UIT-T Y.1411] Recommandation UIT-T Y.1411 (2003), *Interfonctionnement des réseaux ATM et MPLS – Interfonctionnement dans le plan utilisateur en mode cellule*.

[UIT-T Y.1561] Recommandation UIT-T Y.1561 (2004), *Paramètres de performance et de disponibilité des réseaux MPLS*.

[UIT-T Y.1710] Recommandation UIT-T Y.1710 (2002), *Prescriptions relatives à la fonctionnalité d'exploitation et de maintenance pour les réseaux MPLS*.

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

[UIT-T Y.1712] Recommandation UIT-T Y.1712 (2004), *Fonctionnalité d'exploitation et de maintenance pour l'interfonctionnement des réseaux ATM et MPLS*.

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

[UIT-T Y.1720] Recommandation UIT-T Y.1720 (2003), *Commutation de protection pour les réseaux MPLS*.

[UIT-T Y.2011] Recommandation UIT-T Y.2011 (2004), *Principes généraux et modèle de référence général pour les réseaux de prochaine génération*.

[IETF RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol*.

[IETF RFC 2206] IETF RFC 2206 (1997), *RSVP Management Information Base using SMIv2*.

[IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.

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

[IETF RFC 3107] IETF RFC 3107 (2001), *Carrying Label Information in BGP-4*.

[IETF RFC 3209] IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP tunnels*.

[IETF RFC 3212] IETF RFC 3212 (2002), *Constraint-Based LSP Setup using LDP*.

[IETF RFC 3478] IETF RFC 3478 (2003), *Graceful Restart Mechanism for Label Distribution Protocol*.

[IETF RFC 3479] IETF RFC 3479 (2003), *Fault Tolerance for the Label Distribution Protocol (LDP)*.

[IETF RFC 3811] IETF RFC 3811 (2004), *Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management*.

[IETF RFC 3812] IETF RFC 3812 (2004), *Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)*.

[IETF RFC 3813] IETF RFC 3813 (2004), *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)*.

[IETF RFC 3814] IETF RFC 3814 (2004), *Multiprotocol Label Switching (MPLS) Forwarding Equivalence Class To Next Hop Label Forwarding Entry (FEC-To-NHLFE) Management Information Base (MIB)*.

[IETF RFC 3815] IETF RFC 3815 (2004), *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)*.

[IETF RFC 3985] IETF RFC 3985 (2005), *Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*.

[IETF RFC 4090] IETF RFC 4090 (2005), *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*.

[IETF RFC 4221] IETF RFC 4221 (2005), *Multiprotocol Label Switching (MPLS) Management Overview*.

[IETF RFC 4364] IETF RFC 4364 (2006), *BGP/MPLS IP Virtual Private Networks (VPNs)*.

[IETF RFC 4377] IETF RFC 4377 (2006), *Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks*.

[IETF RFC 4378] IETF RFC 4378 (2006), *A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM)*.

[IETF RFC 4379] IETF RFC 4379 (2006), *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise le terme suivant défini ailleurs:

3.1.1 plan de commande: [UIT-T Y.2011].

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 plan utilisateur: désigne l'ensemble des composants de transmission de trafic acheminant le flux de trafic.

NOTE – Le "plan utilisateur" est également appelé "plan de transport" dans d'autres Recommandations de l'UIT-T.

3.2.2 fonction de supervision de réseau: fonction qui coordonne un ensemble de mécanismes pour surveiller l'état de défaut du conduit commuté par étiquette (LSP, *label switched path*).

3.2.3 protection de la liaison: type de protection dans lequel, durant la panne, tous les conduits LSP qui utilisent la liaison protégée comme interface de sortie sont reroutés sur le seul conduit LSP de secours. Un conduit LSP de secours qui contourne une seule liaison du conduit LSP protégé est appelé conduit LSP de contournement par saut au routeur suivant (NHOP).

3.2.4 protection du nœud: forme de protection analogue à la protection de la liaison à cette différence près que le conduit LSP de secours aboutit au premier nœud situé en aval du point de panne. En général, la protection du nœud utilise le premier nœud situé en aval du point de panne; dans le cas présent, le conduit LSP de secours est appelé "conduit LSP de contournement par saut au routeur qui suit le routeur suivant (NNHOP).

Lorsqu'un nœud tombe en panne, les conduits LSP sont reroutés intégralement par contournement du nœud en panne.

3.2.5 protection du conduit: protection de bout en bout, depuis son extrémité de départ jusqu'à son extrémité d'arrivée, d'un conduit LSP donné. Pour plus de précisions, voir [UIT-T Y.1720].

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

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

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

CE extrémité client (*customer edge*)

CsC opérateur de l'opérateur (*carrier's carrier*)

eBGP protocole BGP externe (*external BGP*)

FEC classe équivalente de transmission (*forwarding equivalent class*)

FR relais de trames (*frame relay*)

FTN FEC-NHLFE

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

IP protocole Internet (*Internet protocol*)

IWF fonction d'interfonctionnement (*interworking function*)

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

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

LSR routeur commuté par étiquette (*label switched router*)

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

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

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

NHLFE entrée de réexpédition par étiquette de saut suivant (*next hop label forwarding entry*)

NHP saut suivant (*next hop*)

NNHP saut qui suit le saut suivant (*next next hop*)

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

PE bord fournisseur (*provider edge*)

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

RGT	réseau de gestion des télécommunications
RRO	objet record route (enregistrement de route) (*record route object*)
RSVP	protocole de réservation de ressources (*resource reservation protocol*)
TDM	multiplexage par répartition dans le temps (*time division multiplexing*)
TE	ingénierie du trafic (*traffic engineering*)
VCCV	vérification de connectivité de voie virtuelle (*virtual channel connectivity verification*)
VPN	réseau privé virtuel (*virtual private network*)

5 Conventions

Aucune.

6 Modèles de réseau

Les modèles de réseau incluent les cas dans lesquels les réseaux MPLS constituent la partie centrale des réseaux de service, alors que les autres technologies de couche 2 (ATM, relais de trames, Ethernet, par exemple) sont utilisées pour acheminer des services de bout en bout qui constituent la couche client et la portion MPLS. Comme exemples de modèles de réseau, on peut citer les réseaux IP-VPN à commutation MPLS [IETF RFC 4364], les réseaux ATM (ou toute technologie de couche 2 de type Ethernet ou à relais de trames, par exemple), les réseaux MPLS, les réseaux mis en interfonctionnement comportant le réseau central MPLS entre les connexions de bout en bout de couche 2, et les réseaux qui acheminent des signaux vocaux par le réseau dorsal MPLS (également connus sous la dénomination de "voix sur MPLS").

6.1 Infrastructure de commutation MPLS

[IETF RFC 3031] définit l'architecture de commutation MPLS, dans laquelle les paquets sont assignés à une classe équivalente de transmission (FEC, *forwarding equivalent class*) donnée au moment où ils entrent dans le réseau. [UIT-T G.8110] est la référence UIT-T correspondante pour l'architecture de commutation MPLS définie dans [IETF RFC 3031]. La classe FEC à laquelle le paquet est assigné est ensuite codée sous la forme d'une étiquette. Lors des sauts suivants, aucune analyse approfondie de l'en-tête de couche Réseau du paquet n'est effectuée. Au lieu de cela, l'étiquette est utilisée comme un indice dans un tableau qui spécifie le saut suivant et une nouvelle étiquette. L'ancienne étiquette est remplacée par la nouvelle, et le paquet est transmis à son saut suivant. L'architecture de commutation MPLS précise que chaque routeur commuté par étiquette (LSR, *label switched router*) dans le réseau dorsal MPLS informe ses routeurs homologues des rattachements d'étiquette ou de classe FEC qu'il a effectués. Cet ensemble de procédures est appelé protocole de distribution d'étiquettes. Le protocole de distribution d'étiquettes englobe également les négociations que doivent engager deux entités homologues de distribution d'étiquettes pour s'informer mutuellement de leurs capacités de commutation MPLS. Deux routeurs LSR qui utilisent un protocole de distribution d'étiquettes pour échanger entre eux des informations de rattachement d'étiquette ou de classe FEC sont appelés "entités homologues de distribution d'étiquettes" compte tenu des informations de rattachement qu'ils échangent.

L'architecture de commutation MPLS ne spécifie pas un protocole de distribution d'étiquettes unique. Le choix du protocole de distribution d'étiquettes dépend du but à atteindre. Dans certains cas, il est souhaitable de rattacher l'étiquette aux classes équivalentes de transmission qui peuvent être identifiées avec des routes à destination des préfixes d'adresse via le protocole LDP [IETF RFC 3036] ou le protocole BGP [IETF RFC 3107]. De même, lorsque des ressources doivent être réservées sur le parcours du conduit, notamment des ressources associées à l'ingénierie du

trafic, il est souhaitable d'établir un conduit explicitement routé, de l'entrée jusqu'à la sortie, au moyen d'un protocole de distribution d'étiquettes adapté tel que le protocole RSVP-TE [IETF RFC 3209] ou le protocole CR-LDP [IETF RFC 3212].

La prise en charge de conduits LSP d'ingénierie du trafic à commutation MPLS entre différentes zones de protocole de passerelle intérieure (IGP, *interior gateway protocol*) ou entre systèmes autonomes est réalisée moyennant l'apport d'améliorations à la signalisation RSVP-TE et au protocole de distribution d'étiquettes (voir [b-IETF RFC 4105]).

L'architecture de commutation MPLS permet, de plus, au routeur LSR $n-1$ dans un conduit commuté par étiquette de supprimer l'étiquette et de transmettre le paquet en fonction des informations obtenues de la couche Réseau dudit routeur. C'est ce qu'on appelle la suppression à l'avant-dernier saut (PHP, *penultimate hop popping*), qui permet au routeur LSR de sortie d'effectuer une seule recherche (au lieu de deux).

6.2 Conduit LSP d'interfonctionnement

Un conduit LSP d'interfonctionnement est un conduit LSP à commutation MPLS assorti d'informations d'adaptation permettant d'émuler les attributs essentiels d'un service (ligne louée T1, mode ATM ou relais de trames, par exemple) sur un réseau à commutation de paquets. Un conduit LSP d'interfonctionnement équivaut à une construction d'étiquette à pseudo-trame telle que définie dans [IETF RFC 3985].

Un conduit LSP d'interfonctionnement est censé assurer la fonctionnalité nécessaire pour émuler le service avec le degré de fidélité requis. Toute opération de commutation, traduction ou autre imposant de connaître la sémantique de la charge utile, relève de la fonction d'interfonctionnement.

La Figure 2 illustre le modèle de référence générique pour un "service local" (NS, *native service*) en commutation MPLS où le "service local" peut être le mode ATM, le relais de trames, le multiplexage TDM, l'Ethernet, etc.

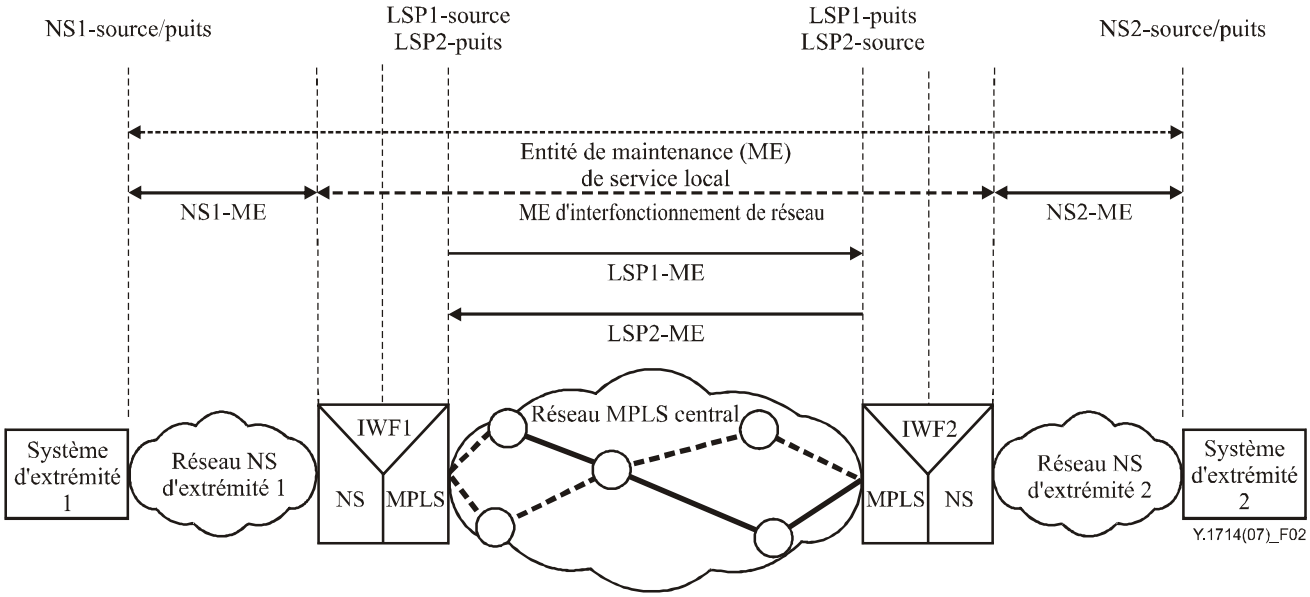

Figure 2 – Modèle de référence de réseaux à conduits LSP d'interfonctionnement

Parmi les fonctions que doivent assurer les conduits LSP d'interfonctionnement, mentionnons l'encapsulation des flux binaires, cellules ou unités PDU arrivant à un port d'entrée propres au service, et le transport de ces flux binaires, cellules ou unités PDU via un conduit ou tunnel. Dans certains cas, il est nécessaire d'effectuer une autre opération (gestion de la synchronisation et de l'ordre de ces flux binaires, cellules ou unités PDU, par exemple) pour émuler le comportement et les caractéristiques de service afin de les porter au degré de fidélité requis.

Du point de vue d'un système d'extrémité, le conduit LSP d'interfonctionnement se caractérise comme étant une liaison ou un circuit non partagé du service choisi.

La Figure 2b représente l'architecture de référence de réseaux à conduits LSP d'interfonctionnement basée sur le modèle fonctionnel G.805 [b-UIT-T G.805].

[UIT-T Y.1711] ainsi que l'utilitaire ping (*packet Internet grouper*) et la fonction de trace de conduit LSP définissent les mécanismes OAM pour le conduit LSP de transport. Toutefois, les procédures d'interaction au niveau d'une fonction d'interfonctionnement entre le conduit LSP de transport et le service local sont à étudier.

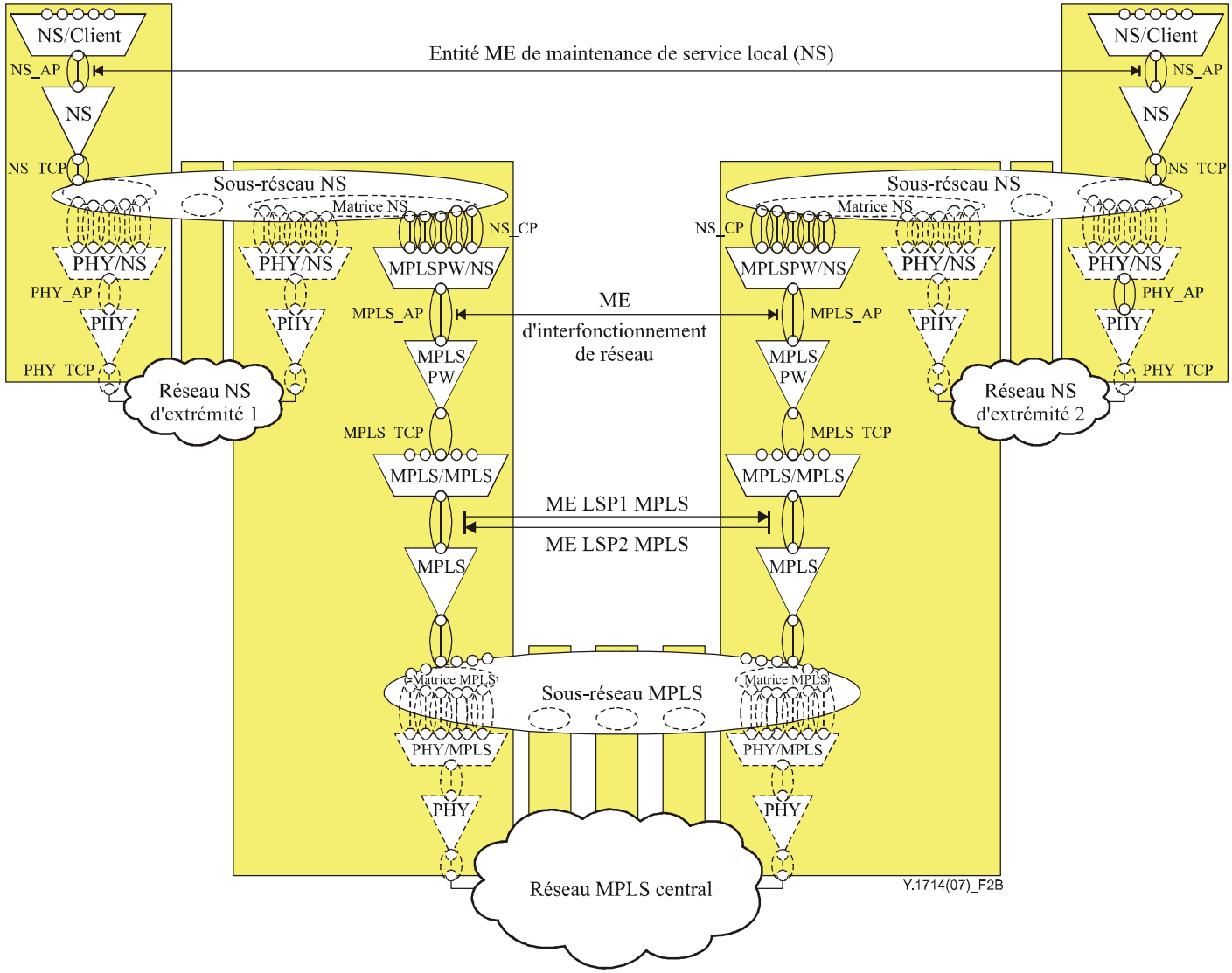

Figure 2b – Architecture de référence des réseaux à conduits LSP d'interfonctionnement basée sur la Rec. UIT-T G.805

6.3 Interfonctionnement de réseaux ATM et MPLS

Appliqués aux réseaux ATM, la Figure 2 définit le modèle de référence générique des fonctions OAM pour les réseaux MPLS et pour l'interfonctionnement des réseaux ATM et MPLS; les fonctions de la couche client devraient être indépendantes les unes des autres. [UIT-T Y.1712] recommande une instanciation propre aux réseaux ATM/MPLS. Dans le cas présent, les fonctions OAM pour les réseaux ATM sont définies dans [UIT-T I.610] et les fonctions OAM pour les réseaux MPLS sont définies dans [UIT-T Y.1711]. Les fonctions de diagnostic sont à étudier.

NOTE – [UIT-T Y.1712] contient en outre des informations sur les procédures d'interfonctionnement (IWF) OAM pour le scénario d'interfonctionnement de couches de réseau (interfonctionnement de services), qui n'est pas abordé dans la présente Recommandation.

6.4 Réseaux VPN L3 dans un environnement MPLS

[IETF RFC 4364] décrit une méthode permettant d'utiliser un réseau dorsal MPLS pour mettre en œuvre des réseaux privés virtuels (VPN, *virtual private network*) IP. Cette méthode utilise un "modèle homologue", dans lequel les routeurs d'extrémité client ("routeurs CE") envoient leurs routes aux routeurs de l'extrémité fournisseur (réseau dorsal) ("routeurs PE"). On utilise ensuite le protocole de passerelle frontière (BGP, *border gateway protocol*) dans la couche centrale pour échanger les routes d'un réseau VPN donné entre les routeurs PE qui sont rattachés à ce réseau VPN. Ce faisant, on veille à ce que les routes en provenance de différents réseaux VPN demeurent distinctes et séparées, même si deux réseaux VPN ont un espace d'adressage en chevauchement. La Figure 3 représente la corrélation entre sites VPN L3 dans un environnement MPLS.

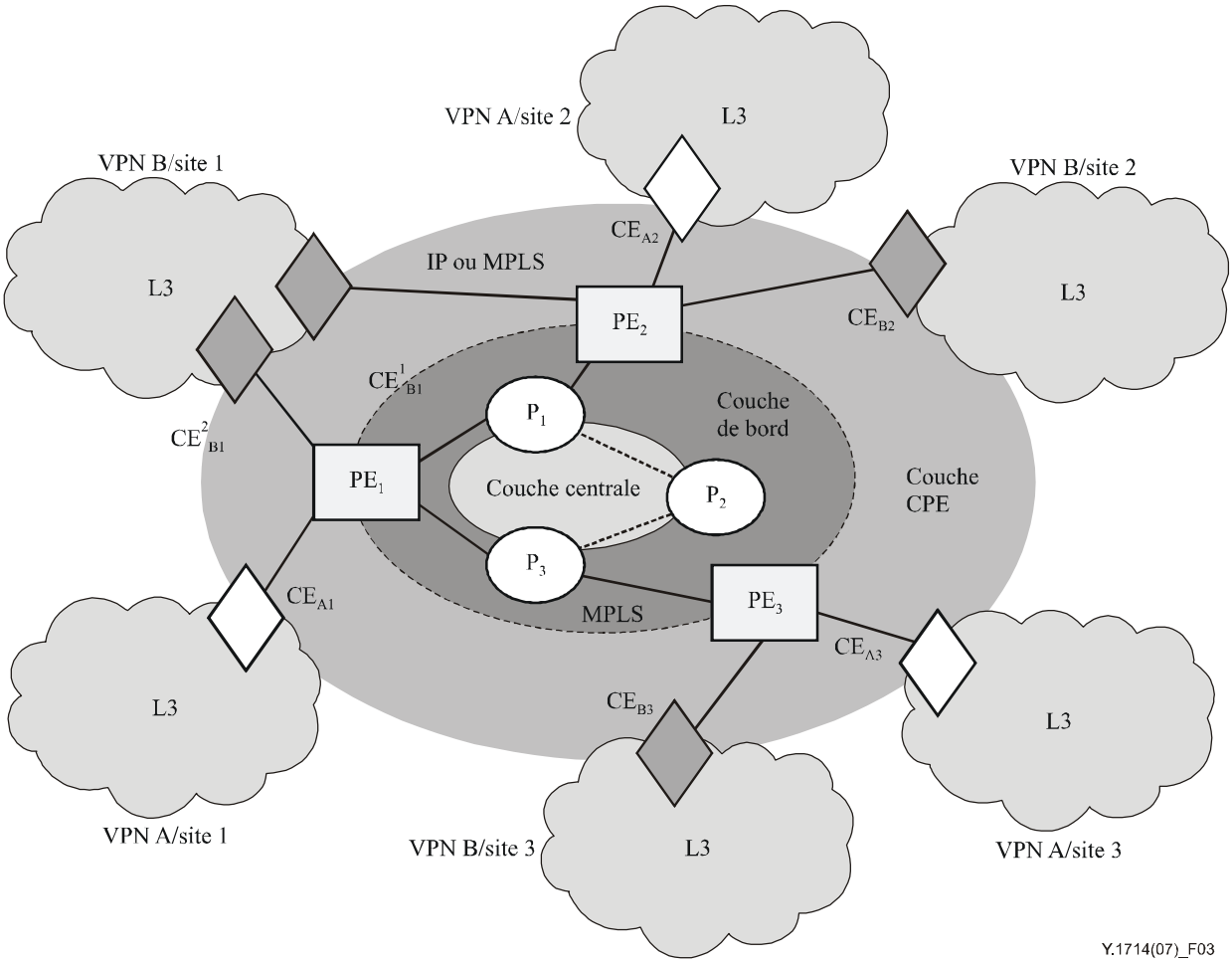

Figure 3 – Modèle de référence d'un réseau VPN L3 dans un environnement MPLS

Les sites VPN peuvent aussi constituer, parfois, un réseau d'un fournisseur de services, qui offrira alors un service VPN à ses clients finals. Dans ce cas, il est nécessaire que les routeurs de l'extrémité client (CE, *customer edge*) prennent en charge la commutation MPLS. C'est ce qu'on appelle le modèle de l'opérateur de l'opérateur (CsC, *carrier's carrier*), dont le principe est exactement le même que celui du réseau VPN L3 à commutation MPLS "normal". De même, bien qu'il puisse constituer un réseau de transit pour les routes extérieures au réseau VPN du client, le réseau VPN ne participe pas en principe à l'échange de routage pour les routes externes. Il n'y a pas véritablement d'accord entre homologues entre le bord fournisseur (PE, *provider edge*) et l'extrémité client (CE). La portion fournisseur du réseau VPN n'est pas perçue comme un système autonome distinct par le système de routage et n'est pas non plus comptabilisée séparément dans les mesures de transit. L'extrémité client (CE) doit seulement distribuer au bord fournisseur (PE) les routes internes au réseau VPN. Les routeurs autres que du type "porte-parole BGP" (*non-BGP speaker*) dans le réseau client sont censés avoir des routes par défaut à destination des routeurs "porte-parole BGP" du client.

Une autre variante du réseau VPN L3 à commutation MPLS correspond à la situation dans laquelle deux sites d'un réseau VPN sont connectés à des systèmes autonomes (AS, *autonomous system*) différents (ce qui pourrait être le cas, par exemple, lorsque les réseaux VPN sont connectés à deux fournisseurs de services différents).

Il existe quatre méthodes pour établir la connectivité MPLS VPN L3 entre systèmes autonomes:

1) établissement de connexion de transmission de routage virtuelle à connexion de transmission de routage virtuelle dans les routeurs périphériques des systèmes autonomes;
2) redistribution, par le protocole eBGP, de routes VPN-IPv4 étiquetées d'un système autonome (AS) au système AS voisin;
3) redistribution multisaut, par le protocole eBGP, de routes VPN-IPv4 étiquetées entre les systèmes AS d'origine et de destination, avec redistribution, par le protocole eBGP, de routes IPv4 étiquetées d'un système AS au système AS voisin;
4) pour améliorer l'évolutivité, on peut faire en sorte que les connexions eBGP multisaut existent uniquement entre un réflecteur de route d'un système AS et un réflecteur de route d'un autre système AS.

6.5 Réseaux VPN L2 dans un environnement MPLS

A étudier.

7 Recommandations connexes et contexte

NOTE – Le présent paragraphe ne s'applique pas aux conduits LSP d'interfonctionnement.

7.1 Aspects relatifs au plan utilisateur

7.1.1 Prescriptions relatives à la gestion du plan utilisateur MPLS

[UIT-T Y.1710] et [IETF RFC 4377] définissent les prescriptions relatives à la gestion du plan utilisateur MPLS. [IETF RFC 4378] définit le cadre général de gestion du plan utilisateur MPLS.

7.1.2 Définition de la disponibilité et mécanismes de gestion des dérangements dans un environnement MPLS

Un des mécanismes suivants peut être utilisé pour la gestion des dérangements:

1) [UIT-T Y.1711] contient la définition de la disponibilité point à point et définit les outils protocolaires de prise en charge pour la mesure de la disponibilité, la détection des dérangements et la notification des dérangements (y compris la gestion des alarmes).

2) Le protocole de détection de transmission bidirectionnelle (BFD, *bidirectional forwarding detection*) est censé détecter les dérangements dans le conduit bidirectionnel entre deux moteurs de transmission, ayant potentiellement une très faible latence, et peut être utilisé en plus de l'utilitaire ping de conduit LSP MPLS pour détecter les pannes dans le plan de données. Le protocole BFD est décrit dans l'Appendice IV.

3) [UIT-T Y.1561] définit les paramètres qui peuvent être utilisés pour spécifier et évaluer la performance en termes de rapidité, de précision, de sûreté de fonctionnement et de disponibilité du transfert de paquets sur un conduit commuté par étiquette (LSP, *label switched path*) dans un réseau à commutation multiprotocolaire par étiquetage (MPLS, *multi-protocol label switching*). Les paramètres définis s'appliquent aux conduits LSP point à point et multipoint à point de bout en bout et à tout domaine MPLS qui fournit ou qui contribue à fournir des services de transfert de paquets.

7.1.3 Détection de mauvais branchement dans les réseaux MPLS

La fonction de vérification de connectivité pour la classe FEC (FEC-CV), définie dans [UIT-T Y.1713], offre un mécanisme permettant de détecter la transmission erronée, dans le plan de données, de paquets entre conduits LSP non surveillés au moyen des mécanismes Y.1711, et entre conduits LSP non surveillés et surveillés.

7.1.4 Outils de diagnostic

Un des mécanismes suivants peut être utilisé comme outil de diagnostic selon le conduit commuté par étiquette:

1) L'utilitaire ping de conduit LSP [IETF RFC 4379] peut être utilisé pour la capacité ping et de fonction de trace du plan de données. L'utilitaire ping de conduit LSP est un outil de diagnostic qui peut être utilisé pour vérifier la connectivité unidirectionnelle ainsi que le traçage des conduits commutés par étiquette MPLS. L'utilitaire ping de conduit LSP est un outil qui utilise le protocole UDP/IP et qui s'applique à la fois aux conduits LSP point à point et aux conduits LSP multipoint à point. En outre, il est doté de capacités lui permettant de prendre en charge des conduits de coût égal (ECMP, *equal cost multi-path*) et la suppression d'étiquette à l'avant-dernier saut (PHP, *penultimate hop popping*).

2) La vérification de connectivité de voie virtuelle (VCCV, *virtual channel connectivity verification*), associée à l'utilitaire ping de conduit LSP, peut être utilisée comme outil de diagnostic sur des conduits LSP d'interfonctionnement. La vérification VCCV offre un mécanisme permettant de diagnostiquer, dans le plan de données, la transmission erronée de paquets entre conduits LSP d'interfonctionnement. Cette vérification est effectuée à l'aide d'un canal de contrôle associé à chaque conduit LSP d'interfonctionnement. La vérification VCCV est décrite dans l'Appendice II.

3) Le test automatique de routeur commuté par étiquette (LSR, *label switched router*) définit un moyen de tester automatiquement un routeur LSR pour vérifier que son plan de données fonctionne pour certaines applications essentielles de commutation multiprotocolaire par étiquetage (MPLS), dont la transmission en monodiffusion utilisant le protocole LDP et les tunnels d'ingénierie du trafic utilisant le protocole RSVP-TE. Ce test automatique est décrit dans l'Appendice II.

7.1.5 Dérangements

[UIT-T Y.1711] définit les dérangements dans un réseau MPLS qui reflètent:

– une perte totale de connectivité entre les points source et puits d'un chemin;

– des problèmes de transmission erronée qui ont une incidence maximale sur les caractéristiques de transfert d'un ou de plusieurs conduits LSP point à point (P2P).

[UIT-T Y.1713] ajoute à cette liste les dérangements observés par le biais de la transmission erronée de conduits LSP et, par conséquent, la transmission erronée de tests OAM pour les conduits LSP non surveillés point à point (P2P) ou multipoint à point (MP2P) qui indiquent indirectement une perte totale de connectivité entre un point source et puits dans le réseau.

Il existe d'autres états de dérangement qui ne sont pas explicitement liés aux conduits et qui peuvent avoir une incidence sur une partie seulement du trafic transporté par un conduit LSP. Ces états peuvent ne pas être mesurables par l'utilisation de techniques de gestion des dérangements faisant appel à des tests OAM, du fait qu'ils se manifestent comme des problèmes de gestion de la performance. Ces états ne se traduiront pas par des dérangements entraînant une perte totale de connectivité, mais ils auront une incidence sur les modèles de disponibilité définis dans [UIT-T Y.1561] étant donné qu'ils se manifesteront sous forme de paquets erronés. Ces autres états de dérangement sont les suivants:

7.1.5.1 Unité de transmission maximale (MTU) dépassée

Le réseau MPLS n'est pas doté d'un mécanisme de fragmentation et l'unité MTU du conduit LSP en cours pour une classe FEC n'est pas toujours connue à l'entrée du conduit LSP. Il s'ensuit que les paquets situés dans la couche centrale ne peuvent pas être fragmentés et ne peuvent pas être transmis. Ces paquets seront perçus par le système de gestion comme des paquets rejetés via les tableaux de performance de base MIB de routeur LSR.

7.1.5.2 Perte de paquets pour cause d'encombrement

Une perte de paquets pour cause d'encombrement se produit lorsque la charge offerte sur une liaison dépasse la capacité de cette liaison et que cette charge se maintient de telle sorte que la capacité disponible de mise en mémoire tampon est dépassée au niveau d'un routeur LSR dans le conduit de transmission. Ces paquets perdus seront perçus par le système de gestion comme des paquets rejetés via les tableaux de performance de base MIB de routeur LSR.

7.1.5.3 Mauvais ordonnancement

Le mauvais ordonnancement est instrumenté pour les conduits LSP d'interfonctionnement qui utilisent un mot de commande contenant un numéro de séquence. Souvent, les implémentations rejetteront les unités PDU reçues hors de séquence, si bien que le mauvais ordonnancement sera perçu comme un rejet de paquets au niveau du routeur LSR d'interfonctionnement de sortie. Les paquets rejetés pour cause de remise en ordre dispersé ne sont pas expressément comptabilités dans aucune des bases MIB actuellement définies, aussi seront-ils perçus par le système de gestion comme des pertes pour cause d'encombrement du réseau.

NOTE – Ces paquets ne sont pas expressément identifiés comme étant rejetés pour cause de mauvais ordonnancement dans les modèles d'information de gestion actuels.

7.2 Mécanismes de retour à l'exploitation normale du plan de données

7.2.1 Commutation de protection de couche MPLS

La protection peut être soit de bout en bout (protection de conduit) soit locale (reroutage rapide).

7.2.1.1 Protection de conduit

[UIT-T Y.1720] décrit un mécanisme de protection de conduits pour les scénarios 1+1 et 1:1.

Les mécanismes de protection partagée entre mailles qui permettent de partager les ressources de protection entre plusieurs entités en service, sont à étudier.

7.2.1.2 Protection locale par le mécanisme de reroutage rapide

Le reroutage rapide, tel qu'il est décrit dans [IETF RFC 4090], est un mécanisme permettant de faire face aux pannes de liaison et de nœud en procédant à une réparation locale. Ce mécanisme pourrait

être utilisé pour protéger plusieurs conduits LSP au moyen d'un tunnel de secours unique. En outre, il est doté de capacités permettant de rerouter les conduits LSP de manière indépendante. Le reroutage rapide offre également la capacité de prendre en charge la même largeur de bande entre conduits LSP protégés et conduits LSP de protection. Le reroutage rapide s'applique uniquement aux conduits LSP utilisant la signalisation RSVP-TE.

7.3 Aspects relatifs au plan de commande

7.3.1 Détection des pannes dans le plan de commande

La détection des pannes dans le plan de commande est à étudier.

7.3.2 Retour à l'exploitation normale à la suite de pannes du plan de commande

Il existe des procédures expressément définies qui permettent le retour à l'exploitation normale à la suite d'interruptions non catastrophiques du plan de commande sans qu'il soit nécessaire d'interrompre la connectivité du plan de données ni de réinstancier l'état du plan de données.

Le retour à l'exploitation normale du plan de commande pour le protocole de signalisation LDP peut être assuré au moyen du redémarrage en douceur (*graceful*) décrit dans [IETF RFC 3478], associé au mécanisme de reprise sur défaillance défini dans [IETF RFC 3479].

Pour une session BGP, telle que spécifiée dans [IETF RFC 4364], le redémarrage en douceur pour la commutation MPLS permet de réduire au minimum les effets négatifs sur la transmission MPLS causés par le redémarrage du plan de commande du routeur commuté par étiquette.

7.3.3 Outils de diagnostic du plan de commande

L'objet d'enregistrement de route (RRO, *record route object*) RSVP-TE, tel qu'il est décrit dans [IETF RFC 3209], fournit des informations indiquant le routage concret d'un conduit LSP point à point (P2P) établi avec le protocole RSVP-TE. L'objet RRO peut être comparé avec les résultats de l'outil de diagnostic du plan de données.

7.4 Aspects relatifs à la gestion

7.4.1 Base d'informations de gestion (MIB) de conventions textuelles en commutation MPLS (MPLS TC)

La base MIB MPLS TC contient des conventions textuelles représentant les informations de gestion de commutation MPLS couramment utilisées. Les conventions textuelles devraient être importées par les modules MIB qui gèrent les réseaux MPLS [IETF RFC 3811].

7.4.2 Aperçu général de la gestion des réseaux MPLS

Le document intitulé "Aperçu général de la gestion des réseaux MPLS" [IETF RFC 4221] décrit l'architecture de gestion des réseaux MPLS et indique les liens réciproques entre les différents modules MIB utilisés pour la gestion des réseaux MPLS. On trouvera dans l'Appendice III de plus amples précisions sur les différents modules MIB.

7.4.3 Bases MIB pour la gestion du plan utilisateur

7.4.3.1 Bases MIB de routeur commuté par étiquette MPLS

Le plan de données MPLS est géré avec la base MIB de routeur commuté par étiquette MPLS [IETF RFC 3813]. Celle-ci décrit les objets gérés pour configurer et/ou surveiller un routeur commuté par étiquette MPLS.

7.4.3.2 Base MIB FTN

La base MIB FTN (FEC-NHLFE) de routeur LSR, qui achemine le mappage des classes FEC sur des conduits LSP dans un routeur LSR, est gérée à l'aide de la base MIB FTN [IETF RFC 3814].

Elle décrit les objets gérés permettant de définir, de configurer et de surveiller les classes équivalentes de transmission (FEC, *forwarding equivalence class*) pour les mappages d'entrée de réexpédition par étiquette de saut suivant (NHLFE) ainsi que les actions correspondantes à utiliser avec la commutation multiprotocolaire par étiquetage.

7.4.4 Bases MIB pour la gestion du plan de commande

7.4.4.1 Bases MIB du protocole de distribution d'étiquettes MPLS

Le plan de commande du protocole de distribution d'étiquettes (LDP) MPLS est géré avec la base MIB du protocole de distribution d'étiquettes [IETF RFC 3815].

7.4.4.2 Base MIB MPLS-TE

Le plan de commande d'ingénierie du trafic MPLS (MPLS-TE) est géré par la base MIB MPLS-TE [IETF RFC 3812].

7.4.4.3 Base MIB du protocole RSVP

La base MIB du protocole RSVP définit une partie de la base d'informations de gestion (MIB) à utiliser avec les protocoles de gestion de réseau dans les réseaux Internet TCP/IP. En particulier, elle définit les objets permettant de gérer le protocole de réservation de ressources (RSVP) dans les attributs d'interface définis dans le modèle avec intégration des services [IETF RFC 2206].

7.5 Sécurité

La présente Recommandation n'introduit pas de nouvelles questions de sécurité dans l'architecture MPLS. Nous renvoyons le lecteur aux diverses spécifications visées ici relatives à telle ou telle question de sécurité.

7.5.1 Fonctions de gestion du plan utilisateur

Pour les réseaux VPN utilisant le protocole BGP/IP ou le protocole MPLS IP [IETF RFC 4364], la séparation du trafic dans le plan de données est obtenue par l'extrémité fournisseur (PE) d'entrée en ajoutant comme préfixe aux paquets une étiquette propre au réseau VPN. Les paquets avec les étiquettes VPN sont envoyés via le réseau central à l'extrémité fournisseur (PE) de sortie, où l'étiquette VPN est utilisée pour déterminer le réseau VPN adéquat. Compte tenu de la séparation de l'adressage, du routage et du trafic via un réseau central VPN BGP/MPLS IP, il est à présumer que cette architecture offre à cet égard la même sécurité que des réseaux VPN de couche 2 comparables tels que des réseaux ATM ou à relais de trames. Toute intrusion d'un réseau VPN ou du réseau central dans d'autres réseaux VPN via le réseau VPN BGP/MPLS IP est impossible, sauf si ce dernier réseau a été configuré expressément à cet effet. Entre deux réseaux VPN de couche 3 qui ne s'interpénètrent pas, dans le cas d'un service VPN, il est à présumer que l'espace d'adresse entre réseaux VPN différents est entièrement indépendant. Il s'ensuit que, par exemple, deux réseaux VPN qui ne s'interpénètrent pas doivent pouvoir tous les deux utiliser le réseau 10/8 (adresse non publique) sans que cela n'entraîne aucun brouillage.

De plus, le trafic en provenance d'un réseau VPN ne doit jamais entrer dans un autre réseau VPN. Cela implique la séparation des informations protocolaires de routage, de manière à disposer également de tableaux de routage séparés par réseau VPN.

En particulier:

- un réseau VPN quelconque doit pouvoir utiliser le même espace d'adresse que tout autre réseau;
- un réseau VPN quelconque doit pouvoir utiliser le même espace d'adresse que le réseau central MPLS;
- le flux de trafic en provenance d'un réseau VPN ne doit jamais passer dans un autre réseau VPN;

- les informations de routage, ainsi que la distribution et le traitement de ces informations, pour une instance de VPN, doivent être indépendantes de toute autre instance de VPN.

Du point de vue de la sécurité, l'impératif premier est d'éviter que les paquets destinés à un serveur dans un réseau VPN donné ne parviennent à un serveur ayant la même adresse dans un autre réseau VPN ou dans le réseau central, ou soit routés vers un autre réseau VPN même si l'adresse du serveur n'existe pas dans ce réseau.

7.5.2 Fonctions de gestion du plan de commande

Les fonctions de gestion du plan de commande sont à étudier.

7.5.3 Plan de gestion

La sécurité du plan de gestion est à étudier.

7.6 Relation OAM entre les couches client et la couche serveur MPLS

L'interfonctionnement de réseaux et l'interfonctionnement de services sont abordés dans le présent paragraphe.

7.6.1 Interfonctionnement de réseaux IP et MPLS

L'utilitaire ping IP et l'outil traceroute (information de trace) IP basés sur le protocole des messages de commande Internet [IETF RFC 792] peuvent être utilisés via le point d'interfonctionnement. Les autres mécanismes d'interfonctionnement de réseaux IP et MPLS sont à étudier.

7.6.2 Interfonctionnement de réseaux ATM et MPLS

[UIT-T Y.1712] définit les procédures d'interfonctionnement entre réseaux basés sur [UIT-T I.610] et [UIT-T Y.1711] pour réseau ATM dans un environnement MPLS (selon les procédures définies dans [UIT-T Y.1411] ou des procédures analogues).

7.6.3 Interfonctionnement de réseaux à relais de trames (FR) et MPLS

1) **Relais de trames, mode 1:1**

   L'interfonctionnement OAM pour les réseaux FR et MPLS en mode 1:1 est à étudier.

2) **Relais de trames, mode port**

   L'indication de l'état des connexions virtuelles permanentes (PVC), telle qu'elle est définie dans [UIT-T Q.933], est transportée de manière transparente entre les extrémités fournisseur (PE). Toutefois, le mappage d'une panne du conduit LSP de transport MPLS est à étudier dans le cadre de [UIT-T X.84].

7.6.4 Interfonctionnement de réseaux Ethernet et MPLS

L'interfonctionnement des réseaux Ethernet et MPLS pour la gestion OAM est à étudier.

7.6.5 Interfonctionnement de réseaux vocaux et MPLS

Les aspects relatifs à l'interfonctionnement et à la gestion OAM sont à étudier.

8 Aspects relatifs au RGT dans un environnement MPLS

8.1 Fonction de supervision du réseau MPLS

La fonction de supervision du réseau MPLS coordonne les fonctions de gestion de réseau MPLS qui entrent dans le cadre de la présente Recommandation. Ces fonctions sont notamment les suivantes:

- détection et diagnostics des dérangements des conduits commutés par étiquette MPLS;
- outils de diagnostic;
- commutation de protection de couche MPLS;
- reroutage de couche MPLS;
- bases MIP MPLS.

Appendice I

Détection des dérangements dans le plan de données

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

Les dérangements dans le plan de données entrent dans trois catégories: les pannes d'interface de transmission, les pannes de nœud et les pannes de conduit.

I.1 Détection des pannes d'interface de transmission

Une panne de la couche Liaison se manifeste sous la forme d'une perte de lumière ou de porteuse ou de dérangements d'ordre supérieur tels qu'une perte de verrouillage de trames ou la non-détection d'erreurs. De même, certains réseaux de transport qui acheminent la commutation MPLS (pour le mode paquet sur réseau Sonet (POS) défini dans [b-IETF RFC 1619], par exemple) assurent leur propre fonctionnalité OAM (ECHO LCP, par exemple).

I.2 Détection des pannes de nœud

Traditionnellement, on utilise les non-adjacences du plan de commande pour la détection par "proxy" du plan de transmission et pour détecter les pannes de nœud. Cette technique, qui se justifie dans des réseaux utilisant la transmission en mode sans connexion, se justifie moins dans des réseaux utilisant la transmission en mode connexion (avec commutation de paquets ou de circuits) ou dans ceux dans lesquels le plan de commande et le plan de données sont disjoints. Citons, notamment, à titre d'exemples:

- *Adjacence de protocole LDP [IETF RFC 3212]/CR-LDP [IETF RFC 3209]*.

  Le protocole LDP incorpore un central d'accueil qui est utilisé pour ajouter artificiellement du trafic entre homologues LDP/CR-LDP en l'absence d'autre trafic. Cette opération est associée à une interruption d'activité.
- *Adjacence RSVP-TE [IETF RFC 3209]*

  Un central d'accueil a été ajouté entre les entités RSVP-TE homologues, qui peut être utilisé pour détecter les pannes.
- *Adjacence IGP/EGP*

  Les protocoles OSPF (*open shortest path first*) [b-IETF RFC 2328] etc., ont tous un central d'accueil.

Toutefois, l'explosion de la complexité des logiciels et la technicité croissante de l'implémentation du plan de commande ont conduit à une situation dans laquelle les éléments du protocole du plan de commande ne peuvent qu'exceptionnellement tomber en panne sans que cela ait des répercussions sur la transmission. En outre, ces types de pannes sont plus fréquentes que celles pour lesquelles la détection des dérangements du plan de commande (maintien de connexions (*keep-alive*), par exemple), a été initialement confiée à un proxy.

Cette situation a évolué pour déboucher sur un découplage (ou, du moins, un retard) opérationnel du "partage de sort" entre le plan de commande et le plan de transmission, et sur la définition de mécanismes assurant l'intégrité transactionnelle et le rétablissement de l'état du plan de commande entre différentes pannes de celui-ci. Cela a abouti à des définitions distinctes des pannes de nœud réparables et des pannes de nœud irréparables. La détection d'une panne de nœud irréparable a été différée en vertu du principe selon lequel une panne de nœud réparable (avec survie associée du plan de transmission) constitue le scénario le plus courant. La prise en charge du redémarrage du plan de commande est généralement négociée entre entités homologues et cette négociation prévoit l'établissement de temps d'attente de protection pour permettre le redémarrage en douceur. [IETF RFC 3478] donne un exemple de découplage du plan de commande et du plan de transmission.

I.3 Détection des pannes de conduit

Les pannes de conduit se manifestent sous diverses formes:

- interruptions du conduit dues à des défauts du niveau ou de la couche de desserte;
- interruptions du conduit dues à des défauts du niveau d'intensité de courant;
- acheminement erroné en raison d'une fusion involontaire du conduit avec un autre conduit;
- acheminement erroné en raison d'une erreur d'étiquetage involontaire du conduit, avec pour conséquence que le routeur LSR aval ne dispose d'aucune entrée du tableau d'étiquettes entrantes (ILM, *incoming label map*) pour ce conduit;
- en cas d'utilisation de la messagerie de vérification de connectivité (CV) OAM de Y.1711, l'identification de l'unité PDU CV en cas d'absence d'entrée ILM et l'extraction de l'identificateur de source de chemin (TTSI) de l'unité PDU CV permettent d'identifier le conduit LSP défectueux.

Appendice II

Outils de diagnostic

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

II.1 Vérification de connectivité de voie virtuelle

La vérification de connectivité de voie virtuelle (VCCV, *virtual channel connectivity verification*), telle qu'elle est décrite dans [b-pwe3-vccv], prend en charge les applications de vérification de connexion pour les PW quelle que soit la technologie de réseau de service public sous-jacente. La vérification VCCV utilise des protocoles IP pour exécuter des fonctions d'exploitation et de maintenance. A cet effet, elle utilise un canal de commande associé à chaque PW. Un opérateur de réseau peut utiliser les procédures de vérification VCCV pour tester la vivacité du plan de transmission du réseau.

II.2 Test automatique de routeur commuté par étiquette

Le test automatique de routeur commuté par étiquette, tel qu'il est décrit dans [b-mpls-lsr-self-test], offre la capacité de vérifier que son plan de données fonctionne pour certaines applications essentielles de commutation multiprotocolaire par étiquetage (MPLS), dont la transmission en monodiffusion et les tunnels d'ingénierie du trafic. Un nouveau type de classe équivalente de transmission en boucle est défini pour permettre à un voisin situé en amont de participer au test pour un coût modique. Les messages de demande et de réponse de vérification MPLS sont définis pour procéder au test proprement dit.

Les messages de l'utilitaire ping de conduit LSP des messages de demande d'écho et de réponse d'écho MPLS sont étendus pour procéder au test proprement dit. Les messages de l'utilitaire ping sont envoyés à un voisin situé en amont, renvoyés via le routeur LSR soumis au test et interceptés, à l'expiration de la durée de vie (TTL, *time-to-live*), par un voisin situé en aval. Les extensions aux messages de l'utilitaire ping de conduit LSP sont définies pour permettre au voisin situé en aval de rendre compte des résultats du test.

Appendice III

Capacités de gestion MPLS

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

III.1 Gestion du plan de données MPLS

La base MIB de routeur commuté par étiquette (MIB LSR) MPLS est conçue pour satisfaire aux prescriptions et aux contraintes suivantes:

1) la base MIB prend en charge l'établissement d'un conduit LSP par un protocole de signalisation MPLS (dans lequel les paramètres du conduit LSP sont spécifiés au moyen de cette base MIB dans la tête de réseau du conduit LSP, l'établissement du conduit LSP de bout en bout étant accompli via la signalisation). La base MIB, en outre, prend en charge manuellement les conduits LSP configurés (c'est-à-dire ceux pour lesquels des associations d'étiquettes à chaque saut du conduit LSP sont fournies par l'administrateur via cette base MIB);
2) la base MIB prend en charge l'activation et la désactivation de la capacité MPLS sur les interfaces d'un routeur LSR dotées d'une telle capacité;
3) la base MIB autorise le partage de ressources entre deux conduits LSP ou plus, c'est-à-dire qu'elle permet de spécifier le partage de la largeur de bande et d'autres ressources LSR entre différents conduits LSP;
4) les espaces d'étiquettes par plate-forme et par interface sont pris en charge;
5) les paquets MPLS peuvent être transmis uniquement à partir d'une étiquette supérieure entrante [IETF RFC 3031], [b-IETF RFC 3032];
6) la prise en charge de la résolution du saut suivant est assurée lorsque l'interface sortante est une interface de médias partagés. Dans le cas de connexions point à multipoint, chaque segment sortant peut résider sur une interface de médias partagés différente;
7) la base MIB prend en charge les connexions point à point, point à multipoint et multipoint à point dans un routeur LSR;
8) pour les connexions multipoint à point, tous les paquets sortants peuvent avoir la même étiquette supérieure;
9) pour les connexions multipoint à point, les ressources sortantes des connexions fusionnées peuvent être partagées;
10) pour les connexions multipoint à point, les paquets provenant de connexions entrantes différentes peuvent avoir des piles d'étiquettes sortantes distinctes en dessous de l'étiquette supérieure (identique);
11) dans le cas de connexions point à multipoint, chaque connexion sortante a une pile d'étiquettes distincte incluant l'étiquette supérieure;
12) tous les membres d'une connexion point à multipoint peuvent partager les ressources attribuées aux segments d'entrée;
13) la base MIB assure la capacité d'interconnexion permettant de supprimer ("*pop*") une étiquette entrante et de transmettre le paquet avec le reste de la pile d'étiquettes en l'état et sans pousser aucune étiquette ("*pop-and-go*") [b-IETF RFC 3032];
14) la base MIB prend en charge les conduits LSP persistants ainsi que les conduits LSP non persistants;
15) des compteurs de performance sont fournis pour les segments entrants et les segments sortants, ainsi que pour mesurer la performance de la commutation MPLS sur chaque interface.

III.2 Gestion du plan de commande du protocole LDP de commutation MPLS

Les bases MIB de distribution d'étiquettes MPLS pour la gestion du plan utilisateur sont basées sur quatre objets principaux. On distingue quatre modules MIB: le module MPLS-LDP-MIB, le module MPLS-LDP-GENERIC-MIB, le module MPLS-LDP-ATM-MIB et le module MPLS-LDP-FRAME-RELAY-MIB.

1) Le module MPLS-LDP-MIB définit les objets qui sont communs à toutes les implémentations utilisant le protocole LDP.

2) Le module MPLS-LDP-GENERIC-MIB définit les objets espace d'étiquette par plate-forme de couche 2 à utiliser avec le module MPLS-LDP-MIB.

3) Le module MPLS-LDP-ATM-MIB définit les objets ATM (mode de transfert asynchrone) de couche 2 à utiliser avec le module MPLS-LDP-MIB.

4) Le module MPLS-LDP-FRAME-RELAY-MIB définit les objets à relais de trames de couche 2 à utiliser avec le module MPLS-LDP-MIB.

Le module MPLS-LDP-MIB et au moins un des modules MIB de couche 2 doivent être implémentés.

A titre d'exemple, si une implémentation de routeur LSR souhaite prendre en charge l'utilisation par le protocole LDP du média Ethernet de couche 2, alors les modules MPLS-LDP-MIB et MPLS-LDP-GENERIC-MIB seront implémentés.

Si une implémentation de routeur LSR souhaite prendre en charge l'utilisation par le protocole LDP du média ATM de couche 2, alors le module MPLS-LDP-MIB doit être implémenté et le module MPLS-LDP-ATM-MIB sera implémenté.

Si une implémentation de routeur LSR souhaite prendre en charge l'utilisation par le protocole LDP du média relais de trames (FRAME-RELAY) de couche 2, alors le module MPLS-LDP-MIB sera implémenté et le module MPLS-LDP-FRAME-RELAY-MIB sera implémenté. Une implémentation du protocole LDP qui utilise les trois médias de couche 2 (Ethernet, relais de trames et ATM) prendra en charge les quatre modules MIB.

Appendice IV

Gestion des dérangements

(Cet appendice ne fait pas partie intégrante de la présente Recommandation)

IV.1 Détection de transmission bidirectionnelle

La détection de transmission bidirectionnelle (BFD), telle qu'elle est décrite dans [b-bfd-base] [b-bfd-mpls], permet de détecter un dérangement de conduit LSP MPLS dans le plan de données de manière analogue à l'utilitaire ping de conduit LSP MPLS [IETF RFC 4379]. Toutefois, le traitement requis, dans le plan de commande, pour les paquets de commande BFD est réduit par rapport au traitement requis pour les messages de l'utilitaire ping de conduit LSP. Un traitement associant l'utilitaire ping LSP et la détection BFD peut être utilisé pour permettre une détection plus rapide des pannes dans le plan de données et/ou rendre possible l'utilisation d'une telle détection sur un plus grand nombre de conduits LSP.

Bibliographie

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

[b-IETF RFC 1619] IETF RFC 1619 (1994), *PPP over SONET/SDH*.

[b-IETF RFC 2328] IETF RFC 2328 (1998), *OSPF Version 2*.

[b-IETF RFC 3032] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*.

[b-IETF RFC 4105] IETF RFC 4105 (2005), *Requirements for Inter-Area MPLS Traffic Engineering*.

[b-bfd-base] IETF draft, *Bidirectional Forwarding Detection*, draft-ietf-bfd-base-06.txt, March 2007.

[b-bfd-mpls] IETF draft, *BFD for MPLS LSPs*, draft-ietf-bfd-mpls-04.txt, March 2007.

[b-ccamp-inter-domain-framework] IETF draft, *A Framework for Inter-Domain MPLS Traffic Engineering*, draft-ietf-ccamp-inter-domain-framework-06.txt, August 2006.

[b-mpls-bgp-mpls-restart] IETF draft, *Graceful Restart Mechanism for BGP with MPLS*, draft-ietf-mpls-bgp-mpls-restart-05.txt, August 2005

[b-mpls-lsr-self-test] IETF draft, *LSR Self Test*, draft-ietf-mpls-lsr-self-test-07.txt, May 2007.

[b-pwe3-oam-msg-map] IETF draft, *Pseudowire (PW) OAM Message Mapping*, draft-ietf-pwe3-oam-msg-map-05.txt, March 2007.

[b-pwe3-vccv] IETF draft, *Pseudo Wire Virtual Circuit Connectivity Verification*, draft-ietf-pwe3-vccv-14.txt, July 2007.

SÉRIES DES RECOMMANDATIONS UIT-T

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

Imprimé en Suisse
Genève, 2007