UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T G.7712/Y.1703

(03/2003)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE G: SYSTÈMES ET SUPPORTS DE TRANSMISSION, SYSTÈMES ET RÉSEAUX NUMÉRIQUES

Equipements terminaux numériques – Fonctionnalités de gestion, d'exploitation et de maintenance des équipements de transmission

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

Aspects relatifs au protocole Internet – Gestion, exploitation et maintenance

Architecture et spécification du réseau de communication de données

Recommandation UIT-T G.7712/Y.1703

RECOMMANDATIONS UIT-T DE LA SÉRIE G

SYSTÈMES ET SUPPORTS DE TRANSMISSION, SYSTÈMES ET RÉSEAUX NUMÉRIQUES

CONNEXIONS ET CIRCUITS TÉLÉPHONIQUES INTERNATIONAUX	G.100–G.199
CARACTÉRISTIQUES GÉNÉRALES COMMUNES À TOUS LES SYSTÈMES ANALOGIQUES À COURANTS PORTEURS	G.200–G.299
CARACTÉRISTIQUES INDIVIDUELLES DES SYSTÈMES TÉLÉPHONIQUES INTERNATIONAUX À COURANTS PORTEURS SUR LIGNES MÉTALLIQUES	G.300–G.399
CARACTÉRISTIQUES GÉNÉRALES DES SYSTÈMES TÉLÉPHONIQUES INTERNATIONAUX HERTZIENS OU À SATELLITES ET INTERCONNEXION AVEC LES SYSTÈMES SUR LIGNES MÉTALLIQUES	G.400–G.449
COORDINATION DE LA RADIOTÉLÉPHONIE ET DE LA TÉLÉPHONIE SUR LIGNES	G.450–G.499
EQUIPEMENTS DE TEST	G.500–G.599
CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION	G.600–G.699
EQUIPEMENTS TERMINAUX NUMÉRIQUES	G.700–G.799
RÉSEAUX NUMÉRIQUES	G.800–G.899
SECTIONS NUMÉRIQUES ET SYSTÈMES DE LIGNES NUMÉRIQUES	G.900–G.999
QUALITÉ DE SERVICE ET DE TRANSMISSION – ASPECTS GÉNÉRIQUES ET ASPECTS LIÉS À L'UTILISATEUR	G.1000–G.1999
CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION	G.6000–G.6999
EQUIPEMENTS TERMINAUX NUMÉRIQUES	G.7000–G.7999
Généralités	G.7000–G.7099
Codage des signaux analogiques en modulation par impulsions et codage	G.7100–G.7199
Codage des signaux analogiques par des méthodes autres que la MIC	G.7200–G.7299
Principales caractéristiques des équipements de multiplexage primaires	G.7300–G.7399
Principales caractéristiques des équipements de multiplexage de deuxième ordre	G.7400–G.7499
Caractéristiques principales des équipements de multiplexage d'ordre plus élevé	G.7500–G.7599
Caractéristiques principales des équipements de transcodage et de multiplication numérique	G.7600–G.7699
Fonctionnalités de gestion, d'exploitation et de maintenance des équipements de transmission	**G.7700–G.7799**
Caractéristiques principales des équipements de multiplexage en hiérarchie numérique synchrone	G.7800–G.7899
Autres équipements terminaux	G.7900–G.7999
RÉSEAUX NUMÉRIQUES	G.8000–G.8999

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

Recommandation UIT-T G.7712/Y.1703

Architecture et spécification du réseau de communication de données

Résumé

La présente Recommandation définit les exigences d'architecture pour un réseau de communication de données (RCD) qui peut assurer le traitement réparti des communications se rapportant au réseau de gestion des télécommunications (RGT), des communications sémaphores réparties se rapportant au réseau de transport à commutation automatique (ASTN) et d'autres communications réparties (par exemple, les communications de service ou vocales, la téléimportation de logiciel). L'architecture RCD s'intéresse aux réseaux qui sont en protocole IP seulement, en protocole OSI seulement et mixtes (c'est-à-dire acceptant les deux protocoles, IP et OSI). L'interfonctionnement entre les parties du RCD acceptant seulement le protocole IP, les parties acceptant seulement le protocole OSI et les parties acceptant à la fois le protocole IP et l'OSI est aussi spécifié.

Diverses applications (par exemple RGT, ASTN, etc.) nécessitent un réseau de communication par paquets pour transporter les informations entre les différents composants. Par exemple, le RGT a besoin d'un réseau de communication, appelé *réseau de communication de gestion* (RCG) pour transporter les messages de gestion entre les composants du RGT (par exemple, le composant NEF et le composant OSF). L'ASTN a besoin d'un réseau de communication, appelé *réseau de communication de signalisation* (RCS) pour transporter les messages de signalisation entre les composants de l'ASTN (par exemple, les composants CC). La présente Recommandation spécifie les fonctions de communications de données qui peuvent être utilisées à l'appui d'un ou de plusieurs réseaux de communication d'application.

Les fonctions de communications de données fournies dans la version 11/2001 de cette Recommandation acceptent les services réseau en mode sans connexion. La présente révision de la Recommandation ajoute la prise en charge des services RCS en mode connexion par l'inclusion d'un mécanisme spécifiquement fondé sur la commutation en environnement multiprotocolaire avec étiquette des flux (MPLS, *multi-protocol label switched*).

La présente Recommandation fait partie d'une série de Recommandations traitant des réseaux de transport.

Source

La Recommandation G.7712/Y.1703 de l'UIT-T, élaborée par la Commission d'études 15 (2001-2004) de l'UIT-T, a été approuvée le 16 mars 2003 selon la procédure définie dans la Résolution 1 de l'AMNT.

Historique du document	
Version	**Notes**
1.0	Résultat de la réunion du Groupe Q14/15 en octobre 2001
1.1	Résultat de la réunion du Groupe Q14/15 en avril 2002
1.2	Epuration de la version 1.1
1.3	Résultat de la réunion du Groupe Q14/15 en octobre 2002
1.4	Epuration de la version 1.3: remplacement des numéros de § 7.1.a, etc., § 7.1.13, etc.; suppression des remarques de l'éditeur
1.5	Résultat de la réunion du Groupe Q14/15 et soumission pour approbation

Mots clés

Interface de système ouvert (OSI, *open system interface*), protocole Internet (IP), réseau de communication de données.

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 responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

Recommandation UIT-T G.7712/Y.1703

Architecture et spécification du réseau de communication de données

1 Domaine d'application

La présente Recommandation définit les exigences en matière d'architecture pour un réseau de communication de données (RCD) qui peut accepter les communications de gestion répartie se rapportant au réseau de gestion des télécommunications (RGT), les communications de signalisation répartie se rapportant au réseau de transport à commutation automatique (ASTN) et les autres communications réparties (par exemple, communications de service ou vocales, téléimportation de logiciel). L'architecture RCD s'intéresse aux réseaux qui sont en protocole IP seulement, en protocole OSI seulement, et mixtes (c'est-à-dire acceptant les deux protocoles, IP et OSI). L'interfonctionnement entre les parties du RCD acceptant seulement le protocole IP, les parties acceptant seulement le protocole OSI et les parties acceptant à la fois le protocole IP et l'OSI est aussi spécifié.

Le RCD assure des fonctions de couche 1 (Physique), de couche 2 (Liaison de données) et de couche 3 (Réseau). Il consiste en fonctions de routage/commutation interconnectées via des liaisons qui peuvent être implémentées sur des interfaces variées, au nombre desquelles des interfaces de réseau régional (WAN, *wide area network*), des interfaces de réseau local (LAN, *local area network*) et des canaux de commande intégrés (ECC, *embedded control channel*).

Diverses applications (par exemple, RGT, ASTN, etc.) nécessitent un réseau de communication par paquets afin de transporter les informations entre les différents composants. Par exemple, le RGT a besoin d'un réseau de communication, appelé *réseau de communication de gestion* (RCG) pour transporter les messages de gestion entre les composants du RGT (par exemple, le composant NEF et le composant OSF). L'ASTN a besoin d'un réseau de communication, appelé *réseau de communication de signalisation* (RCS) pour transporter les messages de signalisation entre les composants de l'ASTN (par exemple, les composants CC). La présente Recommandation spécifie les fonctions de communications de données qui peuvent être utilisées à l'appui d'un ou de plusieurs réseaux de communications d'application.

Les fonctions de communications de données fournies dans la présente Recommandation acceptent les services réseau en mode sans connexion. Il est possible que des versions futures de la présente Recommandation comportent des fonctions additionnelles permettant d'accepter des services réseau en mode connexion.

2 Références normatives

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

– Recommandation UIT-T G.707/Y.1322 (2000), *Interface de nœud de réseau pour la hiérarchie numérique synchrone*.

– Recommandation UIT-T G.709/Y.1331 (2003), *Interfaces pour le réseau de transport optique*.

– Recommandation UIT-T G.783 (2000), *Caractéristiques des blocs fonctionnels des équipements de la hiérarchie numérique synchrone*.

– Recommandation UIT-T G.784 (1999), *Gestion de la hiérarchie numérique synchrone*.

– Recommandation UIT-T G.798 (2002), *Caractéristiques des blocs fonctionnels des équipements à hiérarchie numérique du réseau de transport optique*.

– Recommandation UIT-T G.807/Y.1302 (2001), *Prescriptions relatives aux réseaux de transport à commutation automatique*.

– Recommandation UIT-T G.872 (2001), *Architecture des réseaux de transport optiques*.

– Recommandation UIT-T G.874 (2001), *Aspects gestion de l'élément de réseau optique de transport*.

– Recommandation UIT-T G.7710/Y.1701 (2001), *Prescriptions de la fonction de gestion d'équipements communs*.

– Recommandation UIT-T G.8080/Y.1304 (2001), *Architecture des réseaux optiques à commutation automatique (ASON)*.

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

– Recommandation UIT-T M.3013 (2000), *Considérations relatives aux réseaux de gestion des télécommunications*.

– Recommandation UIT-T M.3016 (1998), *Aperçu général de la sécurité du RGT.*

– Recommandation UIT-T Q.811 (1997), *Profils des protocoles des couches inférieures pour les interfaces Q3 et X.*

– Recommandation UIT-T X.263 (1998) | ISO/CEI TR 9577:1999, *Technologies de l'information – Identification des protocoles dans la couche Réseau*.

– ISO/CEI 9542:1988, *Systèmes de traitement de l'information – Téléinformatique – Protocole de routage d'un système d'extrémité à un système intermédiaire à utiliser conjointement avec le protocole fournissant le service de réseau en mode sans connexion (ISO 8473)*.

– ISO/CEI 10589:2002, *Technologies de l'information – Communication de données et échange d'informations entre systèmes – Protocole intra-domaine de routage d'un système intermédiaire à un système intermédiaire à utiliser conjointement avec le protocole fournissant le service de réseau en mode sans connexion (ISO 847*3).

– IETF RFC 791 (1981), *Internet Protocol DARPA Internet Program Protocol Specification (Protocole Internet DARPA – Spécification du protocole de programme Internet)*.

– IETF RFC 792 (1981), *Internet Control Message Protocol (Protocole de commande de message Internet)*.

– IETF RFC 826 (1982), *An Ethernet Address Resolution Protocol (Protocole de résolution des adresses Ethernet)*.

– IETF RFC 894 (1984), *A Standard for the Transmission of IP Datagrams over Ethernet Networks (Norme pour la transmission de datagrammes IP sur les réseaux Ethernet)*.

– IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers (Exigences pour les serveurs Internet – Couches communication)*.

– IETF RFC 1172 (1990), *The Point-to-Point Protocol (PPP) Initial Configuration Options (Les options de configuration initiale du protocole point à point)*.

– IETF RFC 1195 (1990), *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (Utilisation du routage IS-IS de l'OSI pour le routage dans les environnements TCP/IP et doubles)*.

– IETF RFC 1332 (1992), *The PPP Internet Protocol Control Protocol (IPCP) (Le protocole PPP de commande du protocole Internet)*.

– IETF RFC 1377 (1992), *The PPP OSI Network Layer Control Protocol (OSINLCP) (Le protocole PPP de commande de la couche Réseau OSI)*.

– IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP) (Le protocole point à point (PPP))*.

– IETF RFC 1662 (1994), *PPP in HDLC-like Framing (Protocole PPP en verrouillage de trame quasi HDLC)*.

– IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers (Exigences pour les routeurs IP version 4)*.

– IETF RFC 2328 (1998), *OSPF Version 2*.

– IETF RFC 2460 (1998), *Spécification du protocole Internet, version 6 (IPv6)*.

– IETF RFC 2463 (1998), *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (Protocole de message de commande Internet (ICMPv6) pour le protocole Internet version 6 (Ipv6))*.

– IETF RFC 2472 (1998), *IP Version 6 sur PPP*.

– IETF RFC 2740 (1999), *OSPF pour IPv6*.

– IETF RFC 2784 (2000), *Generic Routing Encapsulation (GRE) (Encapsulage de routage générique)*.

3 Termes et définitions

3.1 La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T G.709/Y.1331:

a) unité de données de canal optique (ODUk, *optical channel data unit*)

b) unité de transport de canal optique (OTUk, *optical channel transport unit*)

c) signal d'en-tête optique (OOS, *optical overhead signal*)

3.2 La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T G.784:

a) canal de communications de données (DCC, *data communications channel*)

3.3 La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T G.807/Y.1302:

a) réseau de transport à commutation automatique (ASTN)

b) interface réseau–réseau (NNI, *network-network interface*)

c) interface utilisateur–réseau (UNI, *user-network interface*)

3.4 La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T G.8080/Y.1304:

a) contrôleur d'appel (CallC, *call controller*)

b) contrôleur de connexion (CC)

c) interface de contrôleur de connexion (CCI, *connection controller interface*)

d) contrôleur de sous-réseau (SNCr, *subnetwork controller*)

3.5 La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T G.874:

a) canal des communications générales (GCC, *general communications channel*)

b) en-tête de communications de gestion générale (COMMS OH, *general management communications overhead*)

3.6 La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T G.7710/Y.1701:

a) réseau de gestion X *(X management network*)

b) sous-réseau de gestion X *(X management subnetwork*)

3.7 La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T G.872:

a) réseau optique de transport (OTN, *optical transport network*)

3.8 La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T M.3010:

a) dispositif d'adaptation (AD, *adaptation device*)

b) fonction de communications de données (DCF, *data communications function*)

c) dispositif de médiation (MD, *mediation device*)

d) élément de réseau (NE, *network element*)

e) fonction d'élément de réseau (NEF, *network element function*)

f) système d'exploitation (OS, *operations system*)

g) fonction de système d'exploitation (OSF, *operations system function*)

h) interface Q (*Q-interface*)

i) fonction de traduction (*translation function*)

j) fonction de station de travail (WSF, *workstation function*)

3.9 La présente Recommandation utilise les termes suivants définis dans la Rec. UIT-T M.3013:

a) fonction de communication de message (MCF, *message communications function*)

3.10 La présente Recommandation définit les termes suivants:

3.10.1 réseau de communication de données (RCD): réseau qui assure les fonctions de couche 1 (Physique), de couche 2 (Liaison de données), et de couche 3 (Réseau). Un RCD peut être conçu pour assurer le transport des communications de gestion répartie se rapportant au RGT, des communications de signalisation répartie se rapportant à l'ASTN, et d'autres communications de fonctionnement (par exemple, des communications de service/vocales, téléimportation de logiciels, etc.).

3.10.2 canal de commande intégré (ECC, *embedded control channel*): canal de fonctions logiques entre éléments de réseau. Le canal physique servant de support au canal ECC est spécifique de la technologie utilisée. Comme exemples de canaux physiques servant de support au canal ECC, on aura: un canal DCC en hiérarchie SDH, un canal GCC dans une unité OTUk/ODUk du réseau OTN ou l'en-tête COMMS OH contenu dans le signal OOS du réseau OTN.

3.10.3 fonction d'interfonctionnement de routage IP: fonction qui permet de faire passer une topologie ou des routes IP d'un protocole de routage IP donné à un autre protocole de routage IP incompatible. Une fonction d'interfonctionnement de routages IP peut par exemple former une passerelle entre un RCD à routage par routage IS-IS intégré et un RCD à routage OSPF.

3.10.4 fonction d'interfonctionnement de couche Réseau: fonction qui assure l'interopérabilité entre des nœuds qui prennent en charge des protocoles incompatibles de couche Réseau. Exemple de fonction d'interfonctionnement de couche Réseau: les tunnels statiques d'encapsulage GRE ou une fonction AE-DCF.

3.10.5 fonction de communication de données à encapsulage automatique (AE-DCF): fonction qui encapsule automatiquement des paquets lorsque cela est nécessaire afin qu'ils puissent être routés par des éléments de réseau qui, sinon, seraient incapables de les réexpédier. Une fonction AE-DCF contient une sous-fonction inverse de désencapsulage afin de rétablir les paquets dans leur forme originale une fois qu'ils ont traversé des éléments de réseau incompatibles.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

AD	dispositif d'adaptation (*adaptation device*)
AE-DCF	fonction de communication de données à encapsulage automatique (*automatic encapsulating data communication function*)
ARP	protocole de résolution d'adresse (*address resolution protocol*)
ASON	réseau optique à commutation automatique (*automatic switched optical network*)
ASTN	réseau de transport à commutation automatique (*automatic switched transport network*)
ATM	mode de transfert asynchrone (*asynchronous transfer mode*)
CallC	contrôleur d'appel (*call controller*)
CC	contrôleur de connexion
CCI	interface de contrôleur de connexion (*connection controller interface*)
CLNP	protocole de couche Réseau en mode sans connexion (*connectionless network layer protocol*)
CLNS	service de couche Réseau en mode sans connexion (*connectionless network layer service*)
COMMS OH	en-tête général de communications de gestion (*general management communications overhead*)
DCC	canal de communication de données (*data communication channel*)
DCF	fonction de communication de données (*data communication function*)
DF	ne pas fragmenter (*don't fragment*)
ECC	canal de commande intégré (*embedded control channel*)
EMF	fonction de gestion des équipements (*equipment management function)*
ES	système d'extrémité (*end system*)
ESH	préappel de système d'extrémité selon l'ISO 9542 (*end system hello*)
ES-IS	routage de système d'extrémité à système intermédiaire (*end system-to-intermediate system*)

GCC	canal des communications générales (*general communication channel*)
GNE	élément de passerelle réseau (*gateway network element*)
GRE	encapsulage de routage générique (*generic routing encapsulation*)
HDLC	commande de liaison de données de haut niveau (*high level data link control*)
ICMP	protocole de message de commande Internet (*Internet control message protocol*)
ID	identificateur
IIH	préappel IS-IS (*IS-IS hello*)
IntISIS	routage intégré de système intermédiaire à système intermédiaire (*integrated intermediate system-to-intermediate system*)
IP	protocole Internet (*Internet protocol*)
IPCP	protocole de commande du protocole Internet (*Internet protocol control protocol*)
IPv4	protocole Internet version 4 (*Internet protocol version 4*)
IPv6	protocole Internet version 6 (*Internet protocol version 6*)
IS	système intermédiaire (*intermediate system*)
ISH	préappel de système intermédiaire selon ISO 9542 (*intermediate system hello*)
IS-IS	routage de système intermédiaire à système intermédiaire (*intermediate system-to-intermediate system*)
IWF	fonction d'interfonctionnement (*interworking function*)
LAN	réseau local (*local area network*)
LAPD	procédure d'accès à la liaison sur canal D (*link-access procedure D-channel*)
LSP	unité PDU d'état de liaison (*link state protocol data unit*)
MAC	commande de moyen d'accès (*media access control*)
MCF	fonction de communication de message (*message communication function*)
MD	dispositif de médiation (*mediation device*)
MTU	unité de transmission maximale (*maximum transmission unit*)
NE	élément de réseau (*network element*)
NEF	fonction d'élément de réseau (*network element function*)
NLPID	identificateur de protocole de couche Réseau (*network layer protocol identifier*)
NNI	interface réseau-réseau (*network-to-network interface*)
NSAP	point d'accès au service de réseau (*network service access point*)
ODUk	unité de données de canal optique (*optical channel data unit*)
OOS	signal d'en-tête de module optique de transport (*OTM overhead signal*)
OS	système d'exploitation (*operations system*)
OSC	canal optique de supervision (*optical supervisory channel*)
OSF	fonction de système d'exploitation (*operations system function*)
OSI	interface de système ouvert (*open system interface*)

OSINLCP	protocole OSI de commande de couche Réseau (*OSI network layer control protocol*)
OSPF	ouvrir d'abord le plus court chemin (*open shortest path first*)
OTM	module optique de transport (*optical transport module*)
OTN	réseau optique de transport (*optical transport network*)
OTUk	unité de transport de canal optique (*optical channel transport unit*)
PDU	unité de données protocolaire (*protocol data unit*)
PPP	protocole point à point
RCD	réseau de communication de données
RCG	réseau de communication de gestion
RCL	réseau de communication local
RCS	réseau de communication de signalisation
RFC	appel à commentaires (*request for comment*)
RGT	réseau de gestion des télécommunications
RNIS	réseau numérique à intégration de services
SDH	hiérarchie numérique synchrone (*synchronous digital hierarchy*)
SID	identificateur de système (*system identifier*)
SNCr	contrôleur de sous-réseau (*subnetwork controller*)
SP	segmentation autorisée (*segmentation permitted*)
SPF	plus court chemin en premier (*shortest path first*)
TCP	protocole de commande de transmission (*transmission control protocol*)
TF	fonction de traduction (*translation function*)
TLV	type longueur valeur
TNE	élément de réseau de transport (*transport network element*)
UNI	interface utilisateur vers réseau (*user-to-network interface*)
WAN	réseau régional (*wide area network*)
WS	poste de travail (*work station*)
WSF	fonction de poste de travail (*work station function*)
xMS	sous-réseau de gestion X (*X management subnetwork*)

5 Conventions

Les conventions suivantes sont utilisées tout au long de la présente Recommandation:

RCD mixte: un RCD mixte accepte des protocoles de couche Réseau multiples (par exemple, OSI et IPv4). Dans un RCD mixte, il est possible que le chemin entre deux entités communicantes (par exemple un système d'exploitation et un élément du réseau de gestion) traverse certaines parties qui n'acceptent qu'un seul protocole de couche Réseau (par exemple, OSI) et d'autres parties qui n'acceptent qu'un autre protocole de couche Réseau (par exemple, IPv4). Pour permettre la communication entre de telles entités, un protocole de couche Réseau devrait être encapsulé dans l'autre protocole de couche Réseau à la frontière des parties qui acceptent les différents protocoles de couche Réseau.

RCD à protocole OSI-seulement: un RCD à protocole OSI-seulement n'accepte que le protocole CLNP comme protocole de couche Réseau. Le chemin de bout en bout entre deux entités communicantes (par exemple, un système d'exploitation et un élément du réseau de gestion) acceptera donc le protocole CLNP; l'encapsulage d'un protocole de couche Réseau dans un autre protocole de couche Réseau n'est pas nécessaire pour traiter de telles communications.

RCD à protocole IPv4 seulement: un RCD à protocole IPv4 seulement n'accepte que le protocole IPv4 comme protocole de couche Réseau. Le chemin de bout en bout entre deux entités communicantes (par exemple, un système d'exploitation et un élément du réseau de gestion) acceptera donc IPv4; l'encapsulage d'un protocole de couche Réseau dans un autre protocole de couche Réseau n'est pas nécessaire pour traiter de telles communications.

RCD à protocole IPv6 seulement: un RCD à protocole IPv6 seulement n'accepte que le protocole IPv6 comme protocole de couche Réseau. Le chemin de bout en bout entre deux entités communicantes (par exemple, un système d'exploitation et un élément du réseau de gestion) acceptera donc Ipv6; l'encapsulage d'un protocole de couche Réseau dans un autre protocole de couche Réseau n'est pas nécessaire pour traiter de telles communications.

6 Caractéristiques du RCD

Diverses applications (par exemple, RGT, ASTN, etc.) requièrent un réseau de communication par paquets pour transporter les informations entre les divers composants. Par exemple, le RGT a besoin d'un réseau de communication, connu sous le nom de *réseau de communication de gestion* (RCG) pour transporter les messages de gestion entre les composants du RGT (par exemple, un composant NEF et un composant OSF). L'ASTN a besoin d'un réseau de communication, connu sous le nom de *réseau de communication de signalisation* (RCS) pour transporter les messages de signalisation entre les composants de l'ASTN (par exemple, les composants contrôleur de connexion). La présente Recommandation spécifie les fonctions de communications de données qui peuvent être utilisées afin de prendre en charge un ou plusieurs réseaux de communications d'application.

La Figure 6-1 illustre des exemples d'applications qui peuvent être traitées via le RCD. Chaque application peut être traitée sur des réseaux RCD séparés ou sur le même RCD selon la conception du réseau.

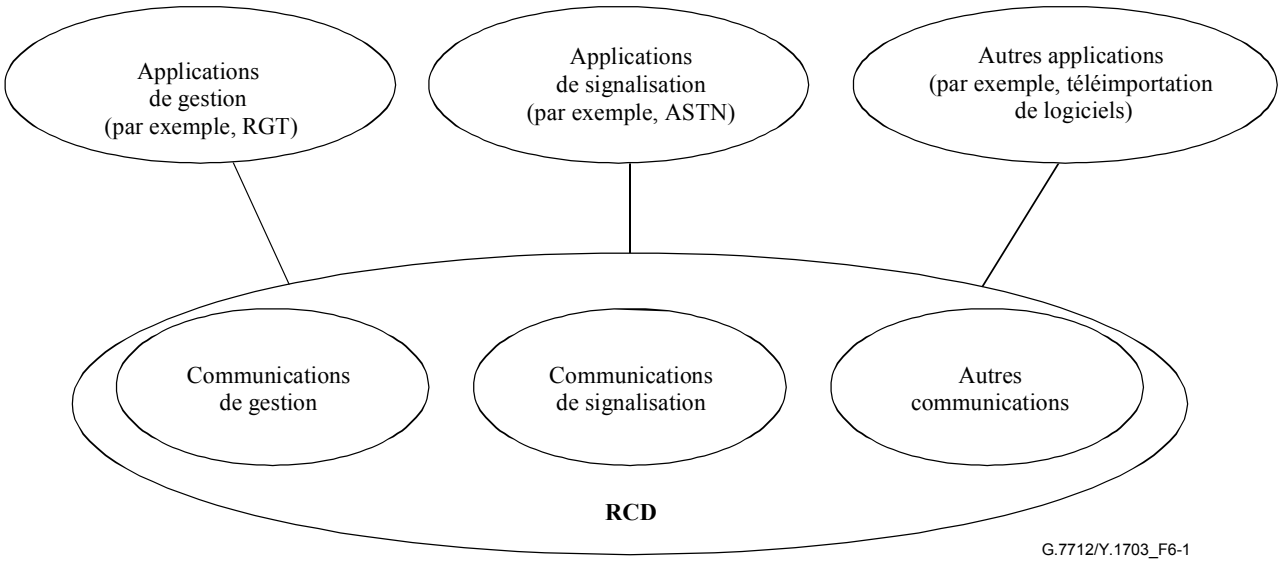


Figure 6-1/G.7712/Y.1703 – Exemple d'applications prises en charge par un RCD

Le concept de RCD est un ensemble de ressources permettant de traiter le transfert des informations entre les composants répartis. Comme indiqué ci-dessus, les communications de gestion répartie se rapportant au RGT et les communications de signalisation répartie se rapportant à l'ASTN sont des exemples de communication répartie qui peuvent être traités par le RCD. Dans le cas d'un RCD acceptant les communications de gestion répartie, les composants répartis sont les composants du RGT (éléments de réseau, AD, OS, MD, et WS contenant des fonctions RGT telles que OSF, TF, NEF, WSF). Les Recommandations UIT-T M.3010 et M.3013 donnent les spécifications détaillées des fonctions du RGT. Dans le cas d'un RCD acceptant les communications de signalisation répartie, les composants répartis sont les composants de l'ASTN (éléments de réseau contenant des fonctions SNCr de l'ASTN). Les Recommandations UIT-T G.807/Y.1302 et G.8080/Y.1304 donnent les spécifications détaillées des fonctions ASTN.

Un certain nombre de technologies des télécommunications peuvent accepter les fonctions de RCD telles que la commutation de circuit, la commutation de paquet, les réseaux LAN, le mode ATM, la hiérarchie SDH, et le réseau OTN. Les aspects importants du RCD sont la qualité de service, le débit de transfert des informations et la diversité de routage pour satisfaire les exigences de fonctionnement spécifiques des communications réparties traitées sur le RCD (par exemple, les communications de gestion répartie, les communications de signalisation répartie).

L'objectif d'une spécification d'interface est de garantir l'efficacité de l'échange des données entre les dispositifs interconnectés à travers un RCD afin de remplir une fonction donnée (par exemple, une fonction de RGT, une fonction de l'ASTN). Une interface est conçue pour assurer l'indépendance de ce type d'appareil ou du fournisseur. Cela requiert des protocoles de communication compatibles et des représentations de données compatibles pour les messages, y compris des définitions de message générique pour les fonctions de gestion pour le RGT et pour les fonctions de commande de l'ASTN.

Le RCD est responsable de la fourniture de communications compatibles à la couche Réseau (couche 3), à la couche Liaison de données (couche 2), et à la couche Physique (couche 1).

Les interfaces devraient être prises en considération dans le traitement de la compatibilité avec les fonctions de transport de données les plus efficaces disponibles pour chaque élément de réseau individuel (par exemple liaisons louées, connexions par circuit commuté, connexions par commutation de paquet, système de signalisation n° 7, canaux de communication intégrés de la hiérarchie SDH, OTN, et canaux B et D de l'accès réseau RNIS).

La présente Recommandation spécifie les trois couches inférieures pour la communication de données et donc tout interfonctionnement entre protocoles au sein des trois couches inférieures. Un tel interfonctionnement est assuré par la fonction de communications de données (DCF, *data communication function*). Des exemples de tels interfonctionnements sont illustrés à la Figure 6-2. Noter qu'un tel interfonctionnement ne met pas fin aux protocoles de couche 3. On en a un exemple avec l'interfonctionnement entre différentes couches Physiques via un protocole commun de couche 2 (par exemple, pour relier des trames MAC d'une interface de réseau LAN à un canal ECC). Un autre exemple est l'interfonctionnement entre différents protocoles de couche de Liaison de données via un protocole commun de couche 3 (par exemple, pour acheminer des paquets IP d'une interface de réseau LAN à un canal ECC). Le troisième exemple, illustré par la Figure 6-2, montre l'interfonctionnement entre différents protocoles de couche Réseau via une fonction de tunnellisation de couche 3 (dans cet exemple, l'OSI est encapsulé/tunnellisé sous IP, bien que l'encapsulage/la tunnellisation du protocole IP sous OSI soit aussi possible).

Le type d'informations transportées entre les composants répartis dépend du type d'interface accepté entre les composants. Un RCD acceptant les communications de gestion répartie se rapportant au RGT doit accepter le transport des informations associées aux interfaces RGT définies dans la Rec. UIT-T M.3010. Un RCD acceptant les communications de signalisation répartie se rapportant au ASTN doit accepter le transport des informations associées aux interfaces de l'ASTN définies dans la Rec. UIT-T G.807/Y.1302.

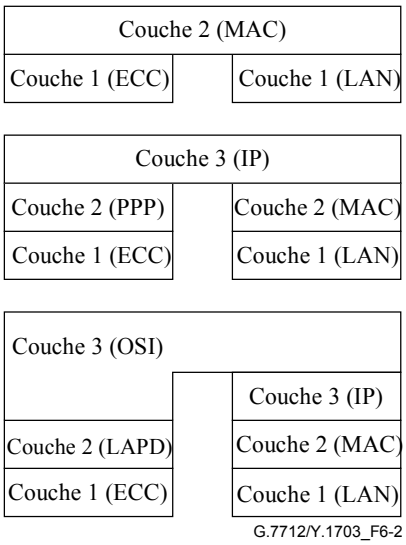


Figure 6-2/G.7712/Y.1703 – Exemples d'interfonctionnement du RCD

6.1 Application au RGT

Le RGT nécessite un réseau de communication, qu'on appelle *réseau de communication de gestion* (RCG) pour transporter les messages de gestion entre les composants du RGT (par exemple, le composant NEF et le composant OSF). La Figure 6-3 illustre un exemple de relation entre le RCG et le RGT. Les interfaces entre les divers éléments (par exemple, système d'exploitation, station de travail, élément de réseau) et le RCG, comme illustré à la Figure 6-3, sont logiques et peuvent être traitées sur une interface physique RCG simple ou par des interfaces RCG multiples.

La Figure 6-4 illustre un exemple d'implémentation physique d'un RCG acceptant des communications de gestion répartie. Selon le choix de l'implémentation du RCG, les éléments physiques peuvent traiter toutes les combinaisons d'interfaces ECC, d'interfaces LAN et d'interfaces WAN. La Figure 6-4 illustre aussi les types de blocs fonctionnels du plan de gestion qui peuvent être acceptés dans les différents éléments physiques. Voir les Recommandations UIT-T M.3010 et M.3013 pour des spécifications détaillées de ces blocs fonctionnels de gestion. Une

fonction de communications de données (DCF, *data communication function*) est incluse dans chaque élément physique et fournit les fonctions de communications de données.

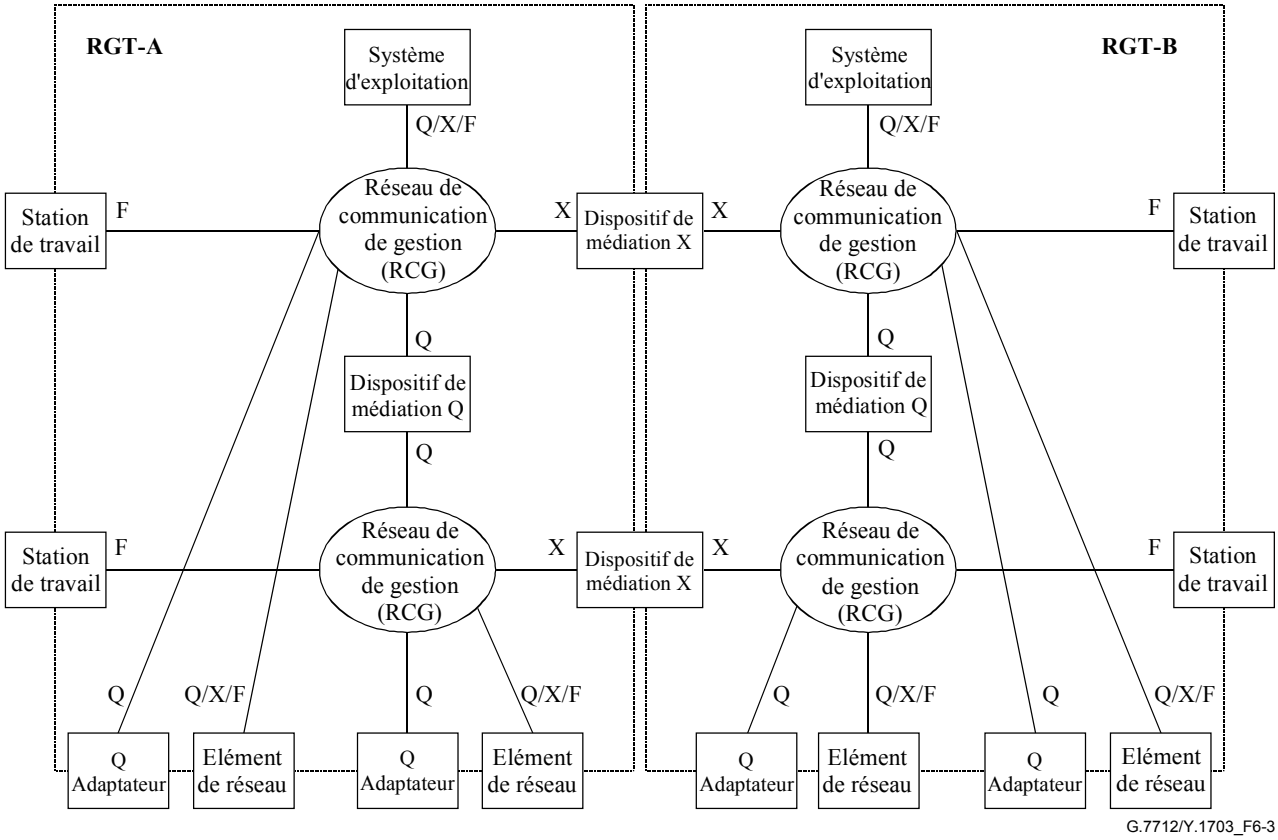


Figure 6-3/G.7712/Y.1703 – Exemple de relation entre interfaces RGT et RCG

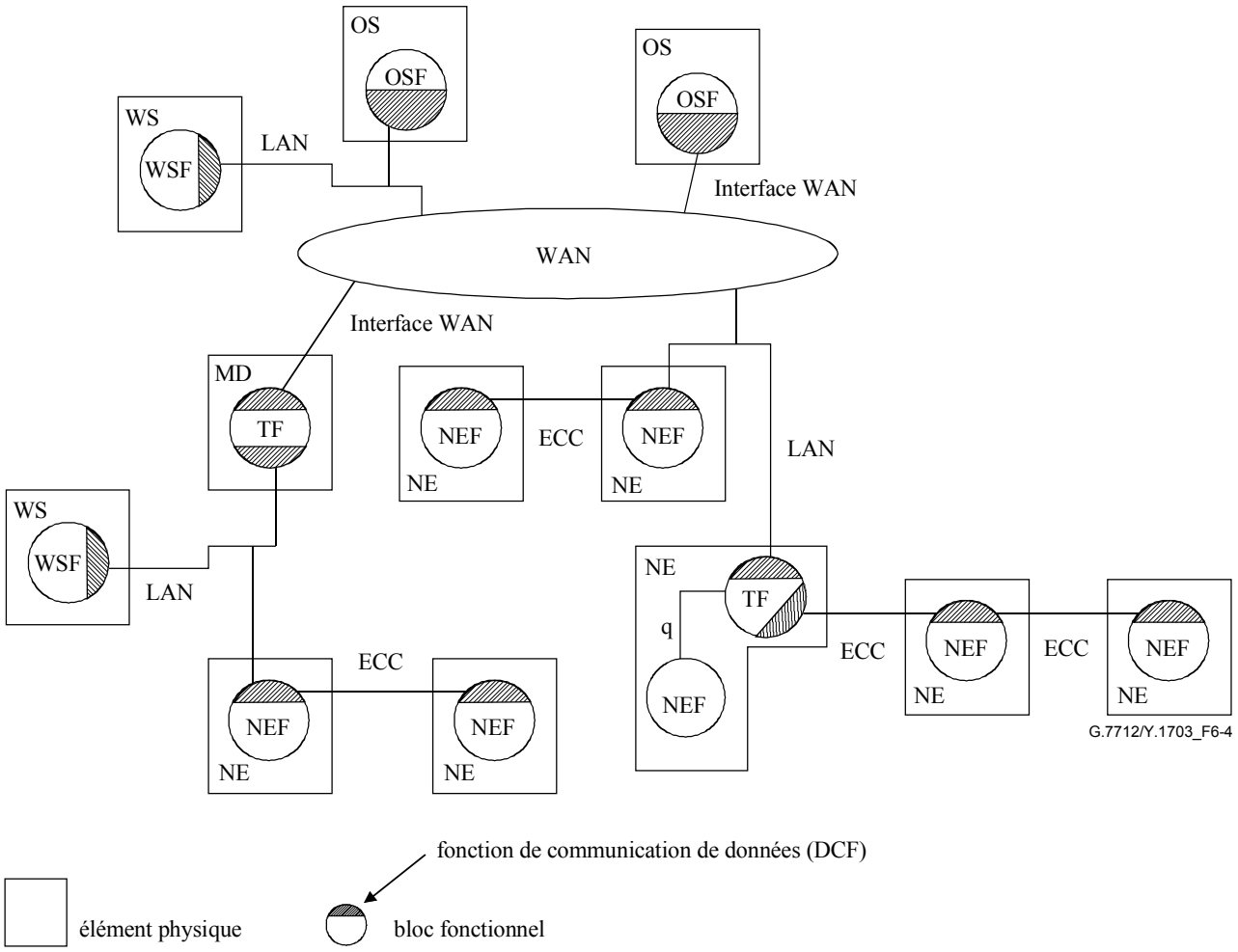


Figure 6-4/G.7712/Y.1703 – Exemple d'implémentation physique de RGT acceptant le RCG

6.1.1 Architecture de sous-réseau de gestion X

Dans la Figure 6-5, il faut noter un certain nombre de points au sujet de l'architecture d'un sous-réseau de gestion X (xMS):

– *éléments de réseau multiples sur un seul site*

des éléments de réseau adressables en hiérarchie SDH ou sur un réseau OTN peuvent apparaître sur un site donné. Par exemple, dans la Figure 6-5, les éléments NE_E et NE_G peuvent être colocalisés en un seul site d'équipement;

– *éléments de réseau SDH/OTN et leurs fonctions de communication*

la fonction de communication de message d'un élément de réseau en hiérarchie SDH ou sur un réseau OTN termine (au sens des couches de protocole inférieures), achemine ou traite de toute autre manière les messages sur le canal ECC, ou connectés via une interface externe.

i) Tous les éléments de réseau doivent terminer le canal ECC. Cela signifie que chaque élément de réseau doit être capable de remplir les fonctions d'une terminaison de système OSI ou d'un serveur IP.

ii) On peut aussi demander aux éléments de réseau de router les messages du canal ECC entre les accès conformément aux informations de commande de routage contenues dans l'élément de réseau. Cela signifie qu'on peut demander à un élément de réseau de remplir les fonctions d'un système OSI intermédiaire ou d'un routeur IP.

– *Communications entre sites en SDH/OTN*

les liaisons de communication entre éléments de réseau en SDH/OTN situés dans différents sites ou commutateurs peuvent être établies au moyen de canaux ECC en SDH/OTN;

– *communications à l'intérieur d'un site en SDH/OTN*

à l'intérieur d'un site particulier, les éléments de réseau en SDH/OTN peuvent communiquer via un canal ECC situé dans ce site ou via un réseau de communication local (RCL). La Figure 6-5 illustre les deux instances de cette interface.

NOTE – Un réseau RCL normalisé a été proposé comme variante à l'utilisation d'un canal ECC pour communiquer entre éléments de réseau colocalisés. Le réseau RCL pourrait être utilisé comme réseau de communication de site général desservant les éléments de réseau en SDH, OTN et autres que SDH/OTN (NNE, non SDH/OTN NE).

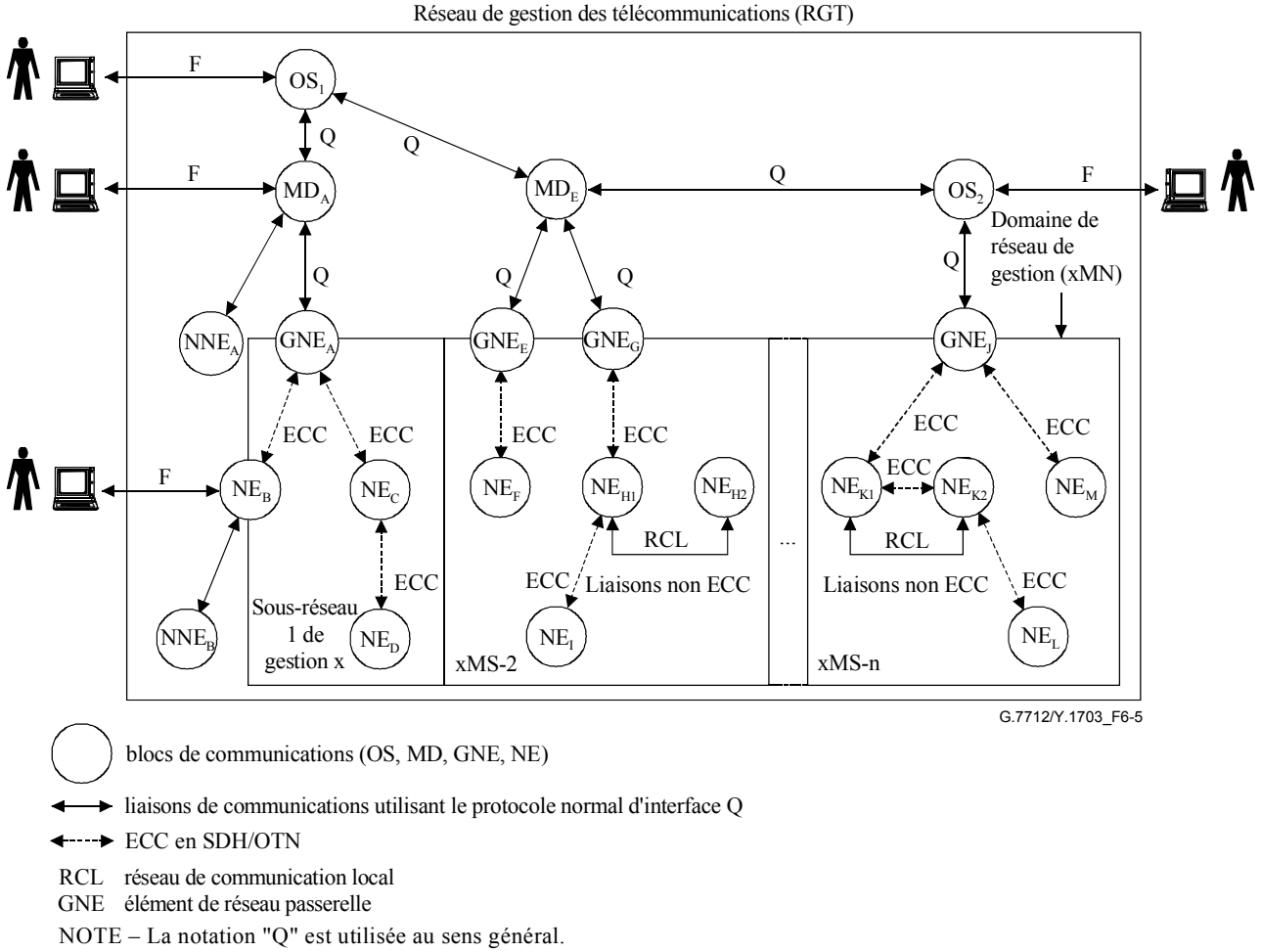


Figure 6-5/G.7712/Y.1703 – Modèle de RGT avec réseau et sous-réseau de gestion

6.1.1.1 Topologie de sous-réseau de gestion

La Figure 6-6 illustre un exemple de topologies de RCG telles que topologie linéaire, topologie annulaire, topologie maillée et topologie radiale utilisant des canaux ECC et/ou des réseaux de communication locaux (RCL) (par exemple LAN Ethernet) comme liens physiques interconnectant les éléments de réseau. La Figure 6-7 illustre comment un sous-réseau de gestion peut être traité sur chaque topologie. Les passerelles doubles (GNE_1 et GNE_2) sont communes à chaque topologie, ce qui permet un accès fiable aux éléments de réseau dans le sous-réseau de gestion. Un autre aspect commun à chaque topologie donnée en exemple est que chacune d'elles permet des chemins multiples entre chaque élément de réseau au sein du sous-réseau de gestion et du système d'exploitation (OS, *operations system*).

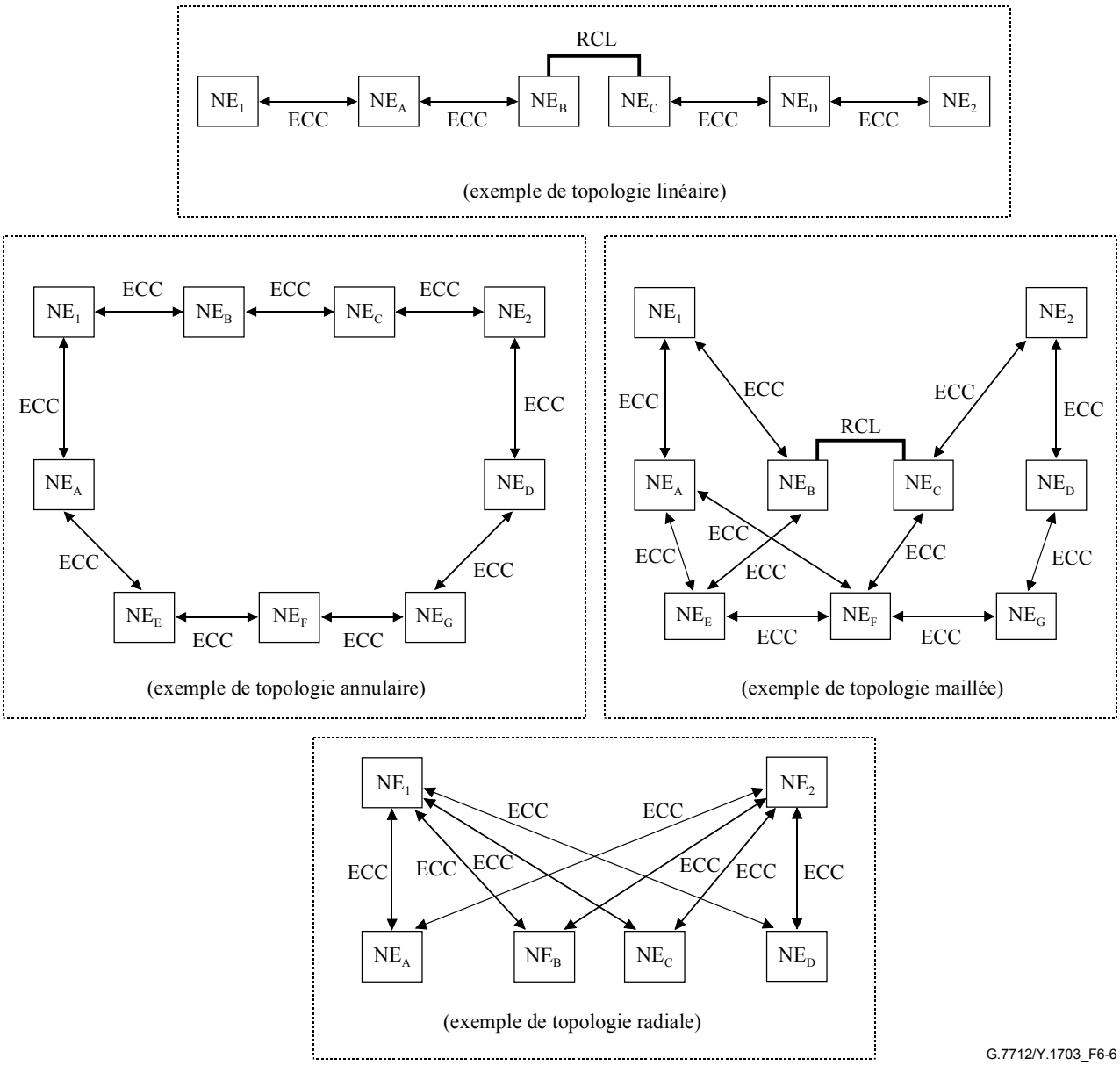


Figure 6-6/G.7712/Y.1703 – Exemples de topologies

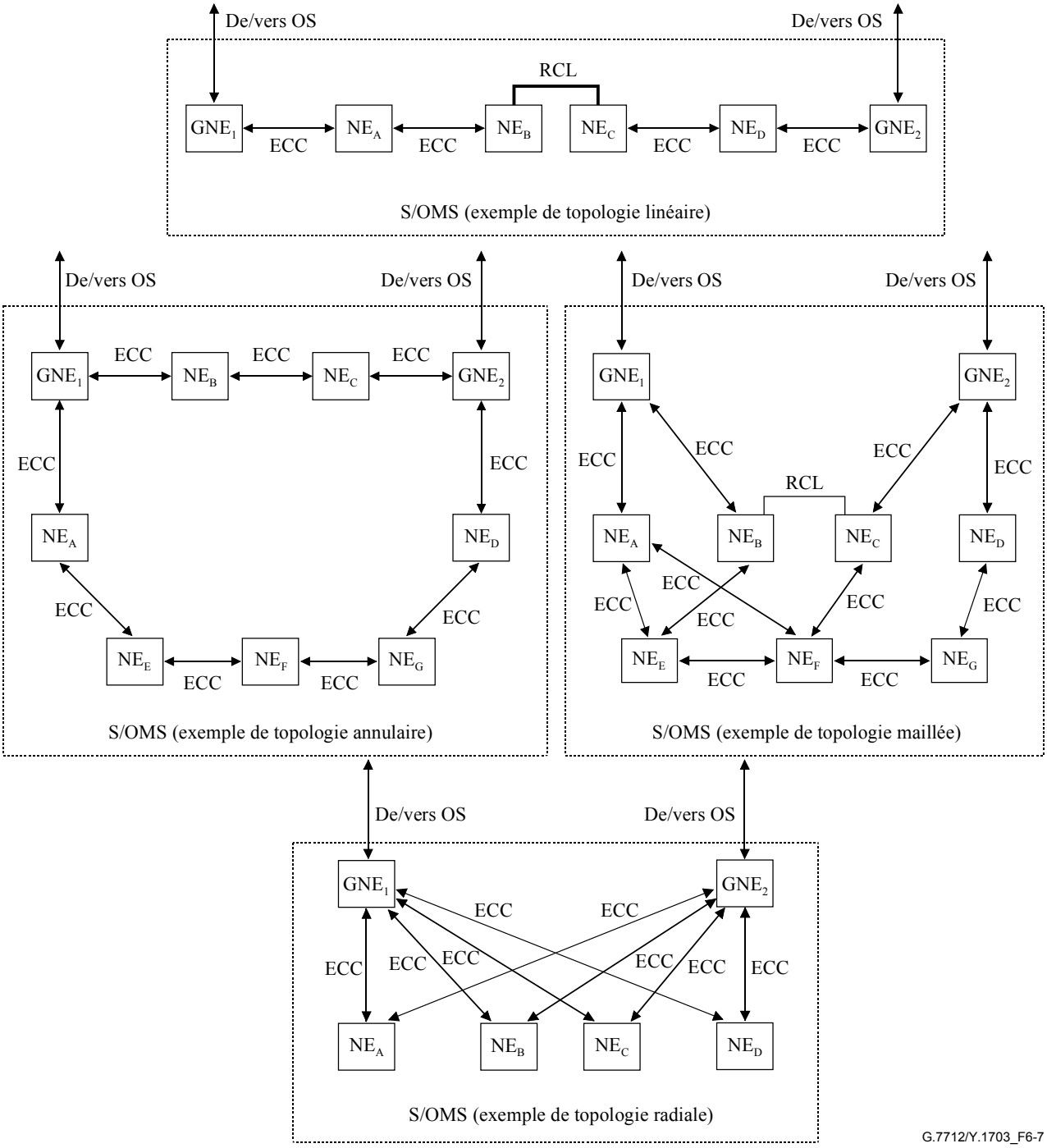


Figure 6-7/G.7712/Y.1703 – Prise en charge d'un sous-réseau de gestion dans diverses topologies

6.1.2 Fiabilité du RCG

Un RCG devrait être conçu pour empêcher qu'un défaut isolé puisse rendre impossible le transfert de messages de gestion essentiels.

Un RCG devrait être conçu pour garantir qu'un encombrement dans le RCG ne provoque pas le blocage ou des retards excessifs des messages de gestion du réseau qui sont destinés à corriger une panne ou un défaut.

Les systèmes d'exploitation et les éléments de réseau qui assurent une fonction d'urgence peuvent requérir des canaux d'accès de secours ou doublés afin d'assurer la redondance.

6.1.3 Sécurité du RCG

Voir la Rec. UIT-T M.3016 pour les exigences de sécurité du RCG.

6.1.4 Fonctions de communications de données du RCG

Au sein des entités du RGT, la fonction DCF doit traiter la fonctionnalité de système d'extrémité (ES, *end system*) (en termes OSI) ou de serveur (en termes IP).

- Lorsque, dans les entités du RGT, la fonction DCF accepte les interfaces ECC, les fonctions suivantes doivent être acceptées:
  - la fonction d'accès au canal ECC (comme spécifié au § 7.1.1);
  - la fonction de terminaison de Liaison de données de canal ECC (comme spécifié au § 7.1.2);
  - la fonction d'encapsulage (unité PDU de couche Réseau vers canal ECC de couche Réseau) (comme spécifié au § 7.1.3).
- Lorsque, dans les entités du RGT, la fonction DCF accepte les interfaces LAN Ethernet, les fonctions suivantes doivent être acceptées:
  - la fonction de terminaison de couche Physique du LAN Ethernet (comme spécifié au § 7.1.4);
  - la fonction d'encapsulage (unité PDU de couche Réseau vers trame Ethernet) (comme spécifié au § 7.1.5).

Au sein des entités du RGT, la fonction DCF peut fonctionner comme un système intermédiaire (IS, *intermediate system*) (en termes OSI) ou comme un routeur (en termes IP). Au sein des entités du RGT qui fonctionnent comme systèmes intermédiaires/routeurs, la fonction DCF doit être capable de router dans leur zone de niveau 1 et doit donc fournir les fonctionnalités d'un système intermédiaire/routeur de niveau 1. De plus, au sein d'une entité du RGT, la fonction DCF peut être prévue comme IS/routeur de niveau 2, ce qui lui donne la capacité de router d'une zone à une autre. La fonctionnalité de système intermédiaire/routeur de niveau 2 n'est pas nécessaire dans la fonction DCF de toutes les entités du RGT. Un exemple de fonction DCF acceptant la fonctionnalité de système intermédiaire/routeur de niveau 2 pourrait être celui de la fonction DCF au sein d'un élément de réseau passerelle.

- Lorsque, dans les entités du RGT, la fonction DCF fonctionne comme un système intermédiaire/routeur, elle doit accepter les fonctions suivantes:
  - fonction de renvoi des unités PDU de couche Réseau (comme spécifié au § 7.1.6);
  - fonction de routage dans la couche Réseau (comme spécifié au § 7.1.10).

Au sein d'une entité du RGT, la fonction DCF qui accepte le protocole Internet peut être connectée directement à la fonction DCF d'une entité du RGT voisine qui n'accepte que l'OSI.

- Lorsque, dans une entité du RGT qui accepte IP, la fonction DCF est directement connectée à une fonction DCF dans une entité du RGT voisine qui n'accepte que l'OSI, la fonction suivante doit être acceptée dans la fonction DCF qui accepte IP:
  - fonction d'interfonctionnement d'unité PDU de couche Réseau (comme spécifié au § 7.1.7).

Au sein d'une entité du RGT, la fonction DCF peut avoir à réexpédier une unité PDU de couche Réseau à travers un réseau qui n'accepte pas le même type de couche Réseau.

- Lorsque, au sein d'une entité du RGT, la fonction DCF doit réexpédier une unité PDU à travers un réseau qui n'accepte pas le même type de couche Réseau, les fonctions suivantes doivent être acceptées:
  - fonction d'encapsulage d'unité PDU de couche Réseau (comme spécifié au § 7.1.8);

– fonction de tunnellisation d'unité PDU de couche Réseau (comme spécifié au § 7.1.9).

Au sein d'une entité du RGT qui accepte le protocole IP en utilisant le routage OSPF, la fonction DCF peut être connectée directement à une fonction DCF située dans une entité de RGT voisine, qui accepte le protocole IP, en utilisant un routage IntISIS.

- Lorsque, dans une entité du RGT qui accepte le protocole IP en utilisant le routage OSPF, la fonction DCF est connectée directement à la fonction DCF d'une entité du RGT voisine qui accepte le protocole IP en utilisant un système IntISIS, la fonction suivante doit être acceptée dans la fonction DCF acceptant le routage OSPF:
  – fonction d'interfonctionnement de routage IP (comme spécifié au § 7.1.11).

6.2 Application de l'ASTN

L'ASTN requiert un réseau de communication appelé *réseau de communication de signalisation* (RCS) pour transporter les messages de signalisation entre les composants ASTN (par exemple, composants contrôleurs de connexion).

La Figure 6-8 illustre un exemple de relation entre le RCS et l'ASTN. Les interfaces entre les différents éléments et le RCS, comme illustré à la Figure 6-8, sont logiques et peuvent être traitées sur une seule interface RCS physique ou sur des interfaces RCS multiples.

La Figure 6-9 illustre un exemple d'implémentation physique d'un RCS acceptant les communications de signalisation répartie. Selon le choix de la mise œuvre du RCS, les éléments physiques peuvent traiter toutes combinaisons d'interfaces de canal ECC, d'interfaces LAN, et d'interfaces WAN. La Figure 6-9 illustre aussi les types de blocs fonctionnels du plan de commande qui peuvent être traités dans divers éléments physiques. Voir les Recommandations UIT-T G.807/Y.1302 et G.8080/Y.1304 pour des spécifications détaillées concernant ces blocs fonctionnels de commande. Une fonction de communications de données (DCF) fait partie de chaque élément physique et fournit la fonction de communications de données.

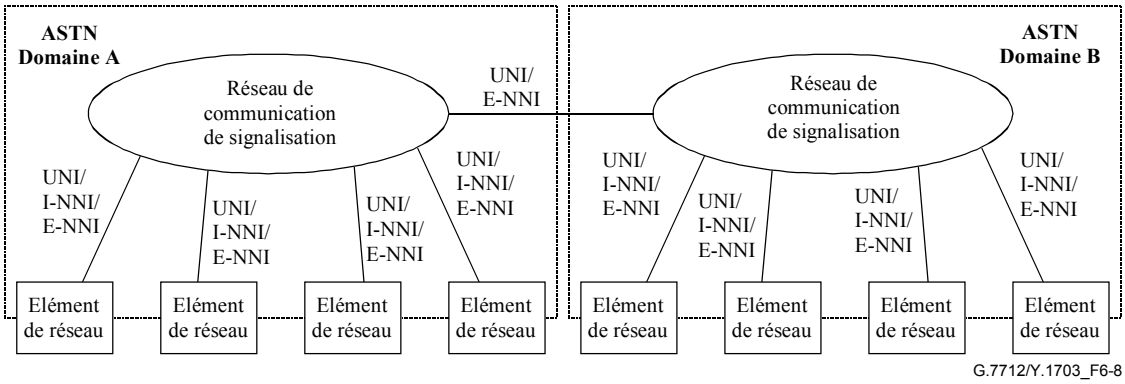


Figure 6-8/G.7712/Y.1703 – Exemple de relation d'interfaces d'ASTN avec un RCS

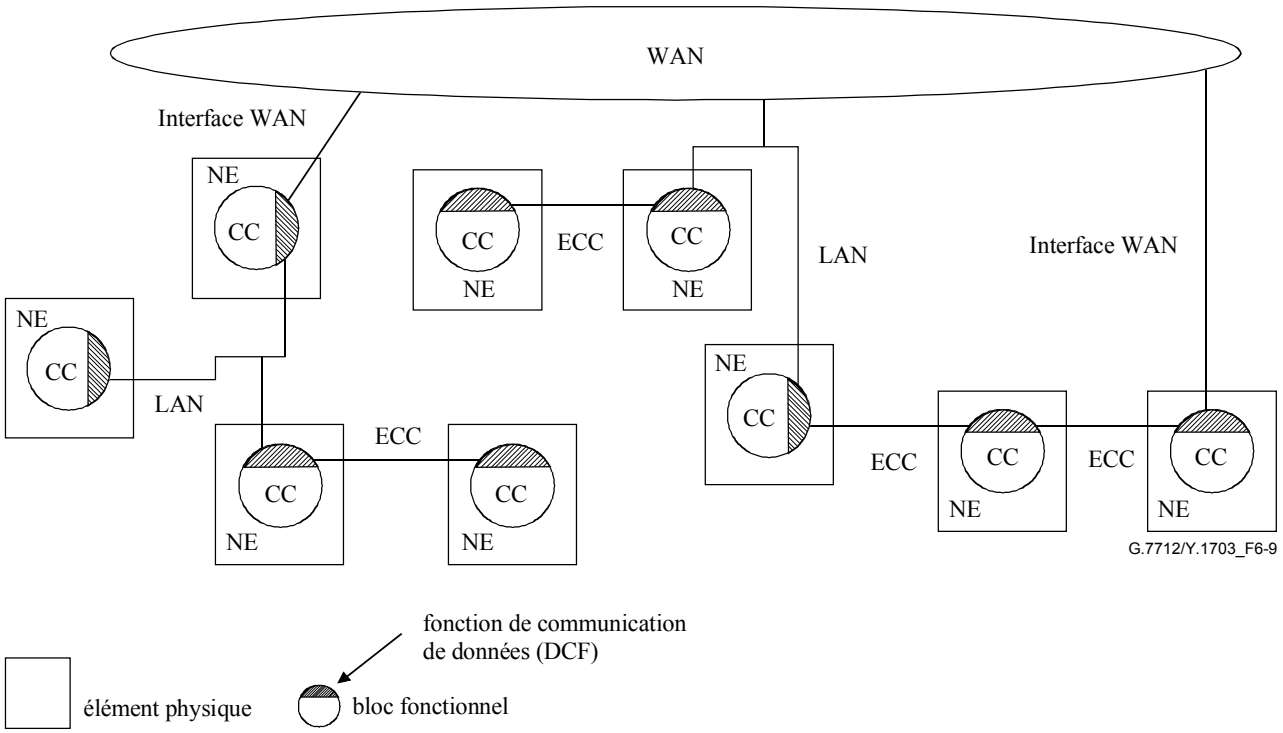


Figure 6-9/G.7712/Y.1703 – Exemple d'implémentation physique d'un ASTN prenant en charge un RCS

6.2.1 Topologie du RCS

La Figure 6-10 illustre un exemple de topologies telles que topologie linéaire, topologie annulaire, topologie maillée et topologie radiale utilisant des canaux ECC et/ou des réseaux de communications locaux (RCL) (par exemple LAN Ethernet) comme liens physiques interconnectant les éléments de réseau. La Figure 6-11 illustre comment un réseau de signalisation ASTN pourrait être traité sur chaque topologie. Dans chaque topologie, il existe diverses voies en variante entre les entités communicantes (c'est-à-dire, les éléments de réseau acceptant un ASTN). Noter que, pour traiter les diverses voies en variante entre les éléments de ASTN communicants selon une topologie linéaire, une liaison WAN externe pourrait être fournie entre les éléments d'ASTN périphériques.

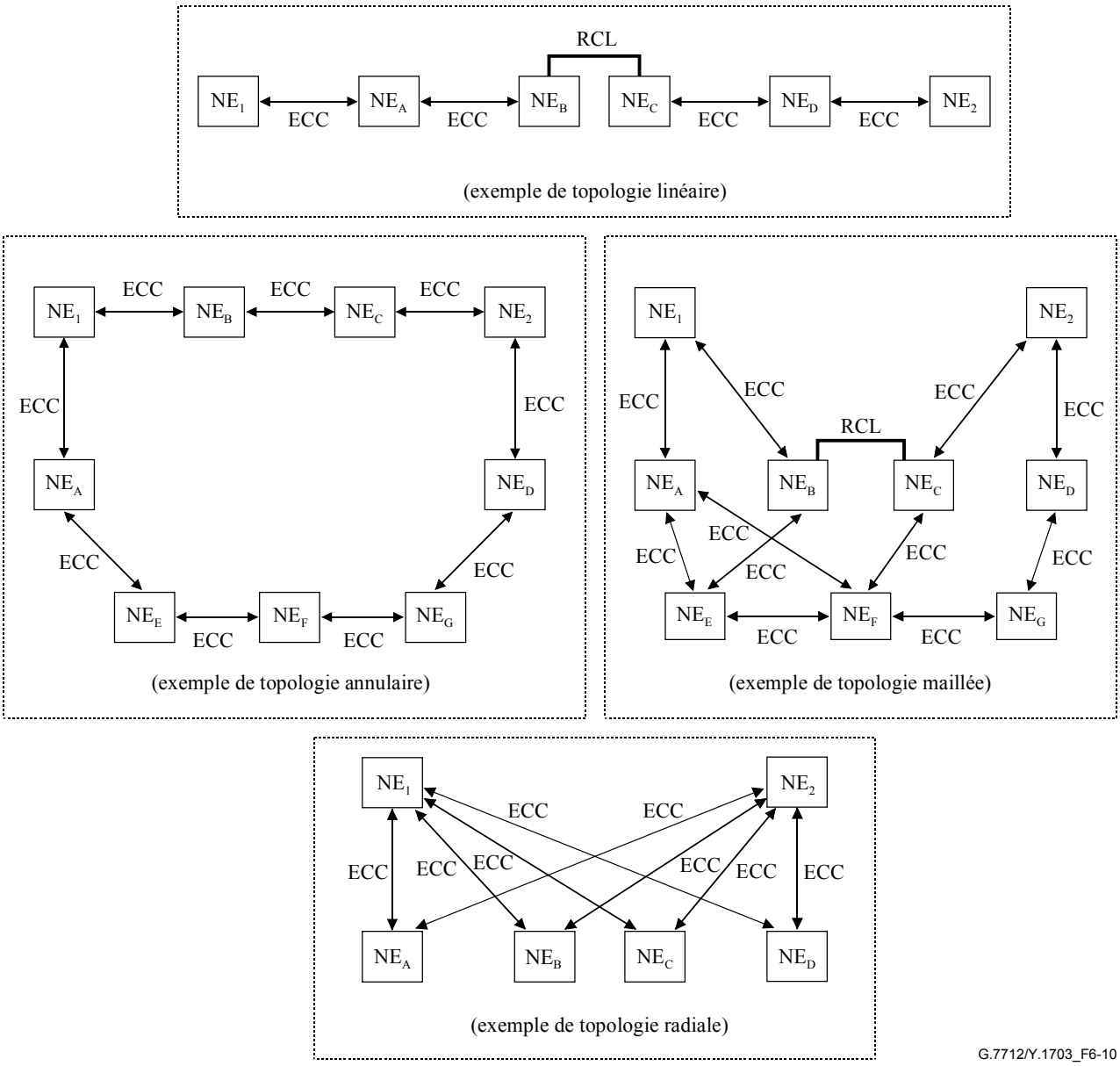


Figure 6-10/G.7712/Y.1703 – Exemples de topologies

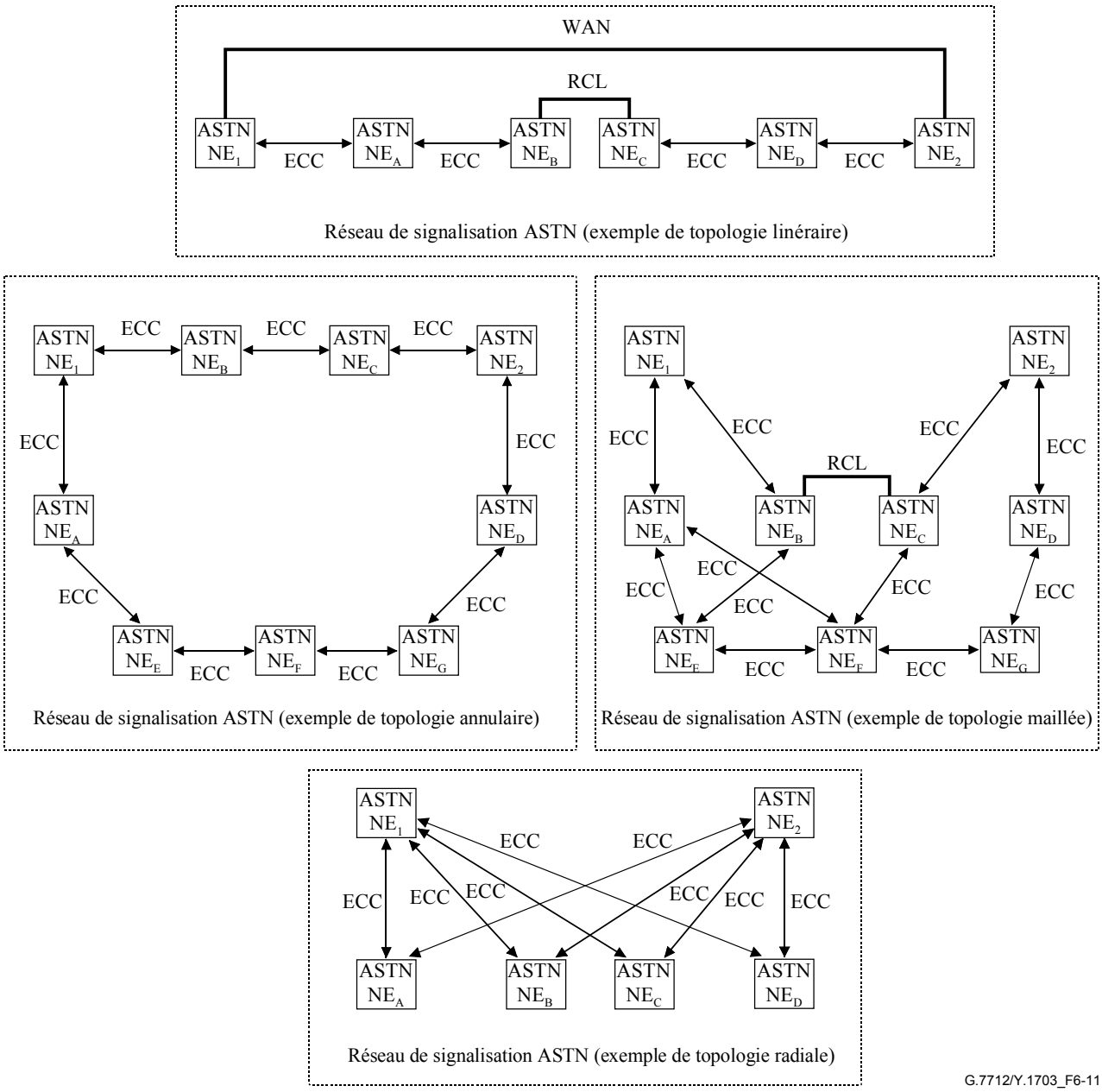


Figure 6-11/G.7712/Y.1703 – Prise en charge d'un réseau de signalisation d'ASTN dans diverses topologies

La Figure 6-12 illustre comment le réseau de signalisation d'ASTN peut consister en trois portions différentes: la portion utilisateur-réseau, la portion administrative intradomaniale, et la portion administrative interdomaniale. Cet exemple montre une topologie maillée utilisant des canaux ECC, des réseaux de communications locaux (par exemple LAN Ethernet), et des liaisons louées (par exemple DS1/E1, VC-3/4) comme liaisons physiques interconnectant les éléments d'ASTN. La topologie de la portion administrative intradomaniale permet à la signalisation d'avoir diverses voies en variante entre deux éléments d'ASTN communicants. La topologie de la portion administrative interdomaniale dépend des accords entre les domaines administratifs A et B. Cet exemple illustre des points d'accès doubles entre les domaines administratifs. La topologie de la portion usager-réseau dépend des accords entre l'abonné et le fournisseur de service. Cet exemple illustre un point d'accès unique entre l'abonné et le réseau.

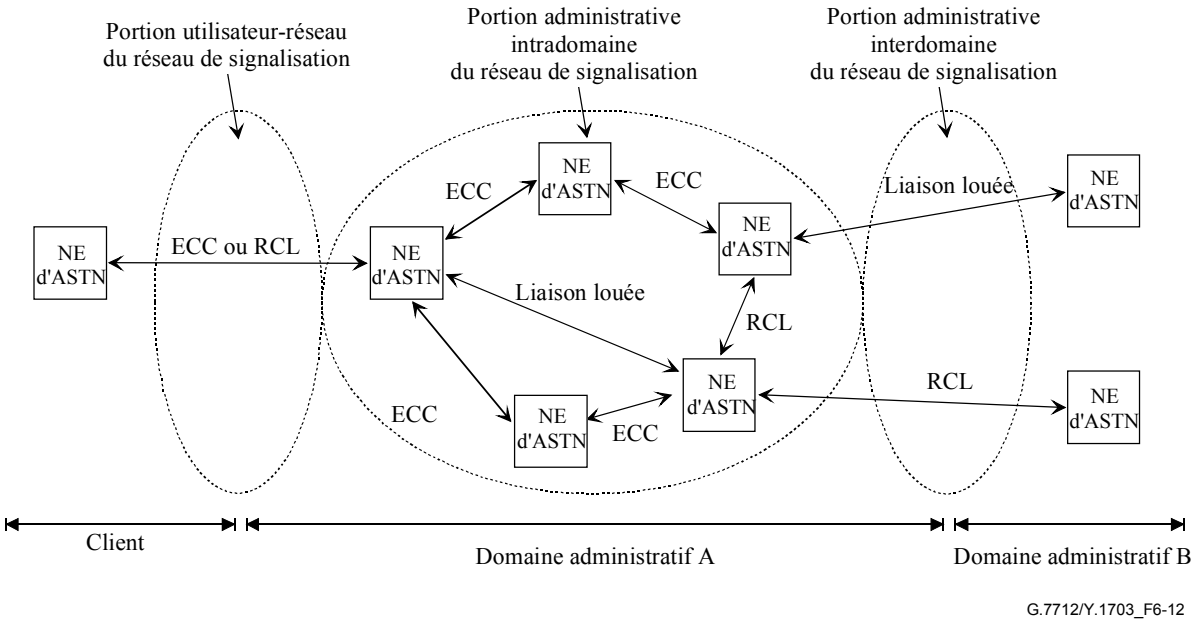


Figure 6-12/G.7712/Y.1703 – Exemple de RCS

6.2.2 Fiabilité du RCS

La Figure 6-13 illustre des messages de commande d'ASTN en cours de transport sur un RCS. Cela illustre les interfaces logiques suivantes:

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

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

CCI interface de contrôleur de connexion (*connection controller interface*).

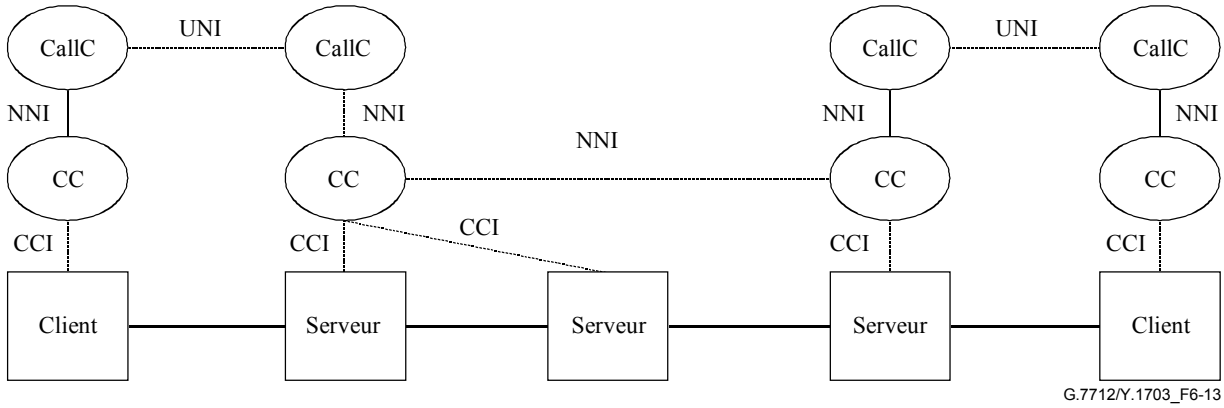


Figure 6-13/G.7712/Y.1703 – Interfaces ASTN prises en charge par un RCS

Dans cet exemple, les interfaces logiques UNI, NNI, et CCI sont portées via le RCS, qui peut consister en divers sous-réseaux dans certains desquels des liaisons logiques peuvent partager des routes physiques communes avec le réseau de transport sans que cela soit exigé ni exclu.

Il est possible que le RCS subisse une défaillance indépendante du réseau de transport. Un tel scénario est illustré dans les Figures 6-14 et 6-15. Dans cet exemple, qui est centré sur les messages ASTN transportés sur le RCS, une défaillance indépendante du RCS affecterait les nouvelles demandes d'établissement et de libération de connexion.

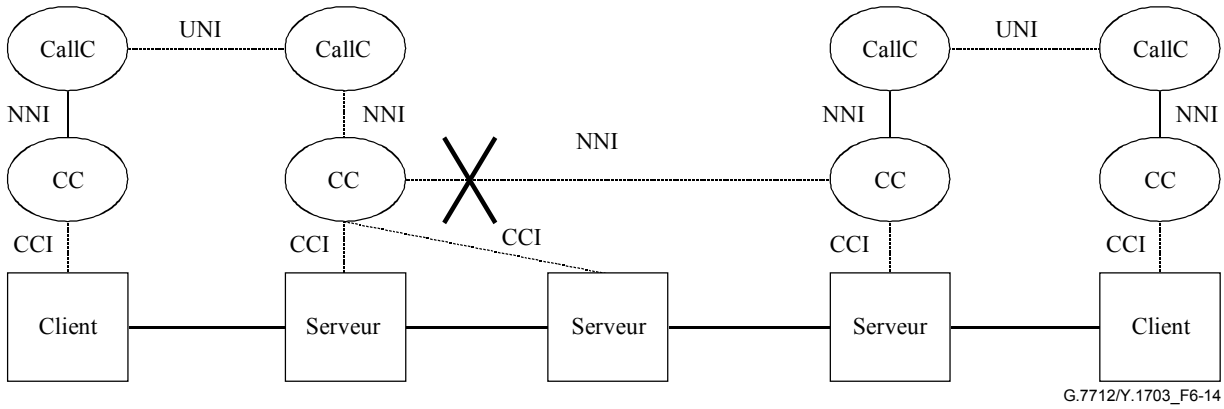


Figure 6-14/G.7712/Y.1703 – Défaillance de RCS ayant une incidence sur l'interface de signalisation

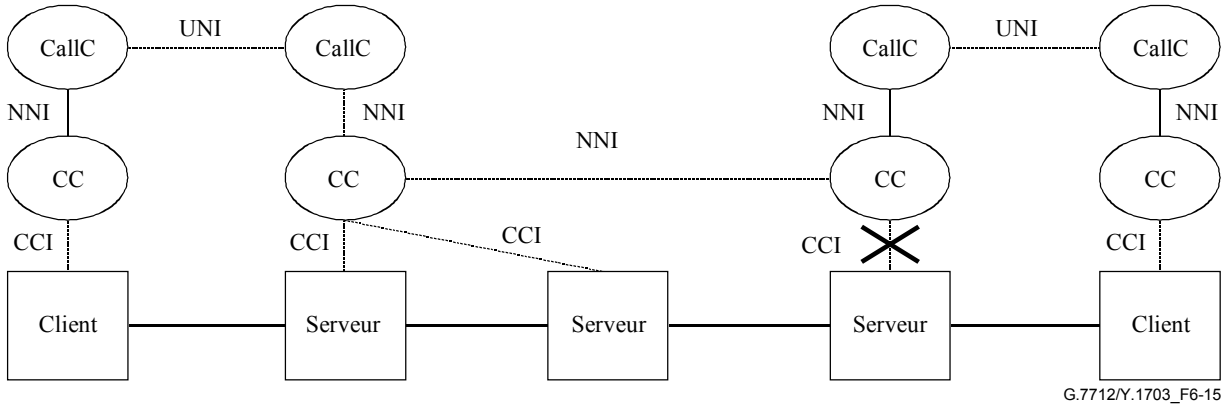


Figure 6-15/G.7712/Y.1703 – Défaillance de RCS ayant une incidence sur une interface CCI

Conformément à la Figure 6-15, il est aussi possible que certaines liaisons logiques au sein du RCS partagent les routes physiques du réseau de transport. Dans ce cas, il est possible que le RCS subisse une défaillance non indépendante du réseau de transport (c'est-à-dire qui interrompt à la fois le trafic du RCS et celui du réseau de transport), conformément à la Figure 6-16. Dans cet exemple, centré sur les messages ASTN transportés sur le RCS, une telle défaillance peut influencer le rétablissement lorsque l'ASTN est utilisé pour fournir le rétablissement des connexions existantes. Il est donc essentiel que le RCS présente une certaine robustesse lors du transport de messages de rétablissement.

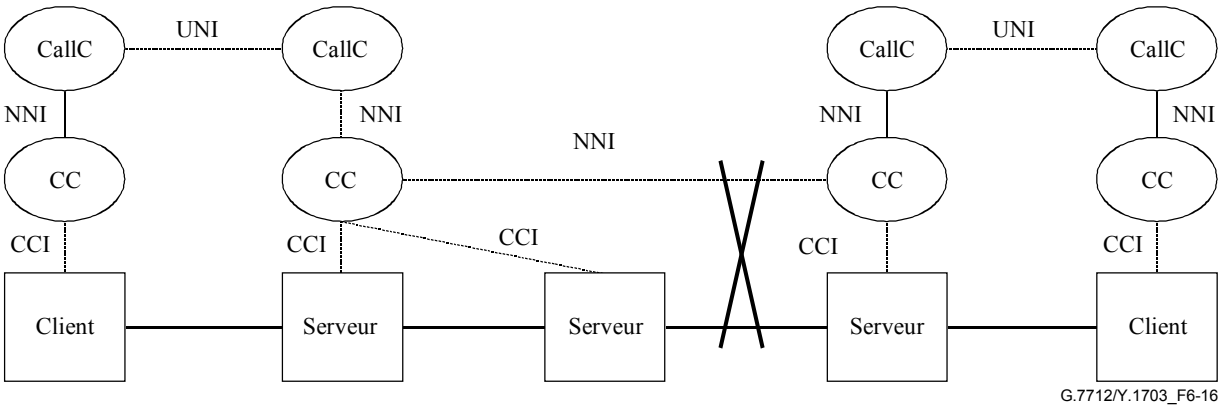


Figure 6-16/G.7712/Y.1703 – Défaillance du RCS ayant une incidence sur les interfaces de signalisation et de données

Si l'application de l'ASTN n'est utilisée que pour fournir l'établissement et la libération de la connexion, un RCS en mode sans connexion peut être suffisant. Cependant, si l'application de l'ASTN est aussi utilisée pour fournir le rétablissement, un RCS en mode connexion peut être nécessaire. Un RCS en mode connexion nécessiterait la spécification de fonctions supplémentaires pour accepter des services réseau en mode connexion.

Les exigences de fiabilité du RCS sont les suivantes:

le RCS doit accepter différents niveaux de rétablissement selon les exigences de fiabilité des composants communicants auxquels il fournit le transport (c'est-à-dire que le rétablissement peut être pris en charge par les composants communicants qui exigent des communications très fiables sans nécessiter que le rétablissement soit pris en charge par tous les composants communicants).

Une façon d'obtenir un RCS fiable est d'utiliser une protection doublée (1+1) des paquets pour un protocole en mode connexion tel que la commutation MPLS décrite au § 6.2.4.

Le RCS peut assurer le transport des messages de rétablissement. Dans ce cas, le RCS doit fournir des vitesses de rétablissement qui permettent un fonctionnement approprié des connexions commandées par les messages de rétablissement.

6.2.3 Sécurité du RCS

Un RCS acceptant les messages ASTN peut assurer la connexité entre différents domaines administratifs. Lorsqu'un RCS assure la connexité entre des frontières administratives, des précautions doivent être prises pour que seuls les messages qui sont autorisés à passer entre les deux domaines administratifs aient la capacité de traverser l'interface tandis que les messages qui ne sont pas autorisés à passer entre les domaines administratifs sont empêchés de traverser l'interface. Le RCS doit s'assurer que seul un ensemble choisi de messages qui sont autorisés par les parties administratives de part et d'autre de l'interface est réellement capable de traverser l'interface.

6.2.4 Fonctions de communications de données du RCS

Dans les entités ASTN, la fonction DCF doit accepter la fonctionnalité de système d'extrémité (ES, *end system*) (en termes OSI) ou serveur (en termes IP).

- Lorsque, dans les entités ASTN, la fonction DCF accepte les interfaces ECC, les fonctions suivantes doivent être acceptées:
  - fonction d'accès au canal ECC (comme spécifié au § 7.1.1);
  - fonction de terminaison de Liaison de données de canal ECC (comme spécifié au § 7.1.2);

  - fonction d'encapsulage ("unité PDU de couche Réseau vers couche de Liaison de données de canal ECC") (comme spécifié au § 7.1.3).

- Lorsque, dans les entités ASTN, la fonction DCF accepte les interfaces LAN Ethernet, les fonctions suivantes doivent être acceptées:
  - fonction de terminaison de couche Physique de LAN Ethernet (comme spécifié au § 7.1.4);
  - fonction d'encapsulage ("unité PDU de couche Réseau vers trame Ethernet") (comme spécifié au § 7.1.5).

Dans les entités ASTN, la fonction DCF peut fonctionner comme un système intermédiaire (IS) (en termes OSI) ou comme un routeur (en termes IP). La fonction DCF, au sein des entités ASTN qui fonctionnent comme IS/routeurs, doit être capable de router dans la zone de niveau 1 et doit donc fournir la fonctionnalité d'un IS/routeur de niveau 1. De plus, la fonction DCF dans une entité ASTN doit fonctionner comme IS/routeur de niveau 2, qui donne la capacité de router d'une zone à l'autre. La fonctionnalité IS/routeur de niveau 2 n'est pas nécessaire dans la fonction DCF de toutes les entités ASTN.

- Lorsque, dans les entités ASTN, la fonction DCF fonctionne comme un IS/routeur, les fonctions suivantes doivent être acceptées:
  - fonction de renvoi des unités PDU de couche Réseau (comme spécifié au § 7.1.6);
  - fonction de routage de couche Réseau (comme spécifié au § 7.1.10).

Dans une entité ASTN acceptant IP, la fonction DCF peut être connectée directement à une fonction DCF d'une entité ASTN voisine qui n'accepte que l'OSI.

- Lorsque, dans une entité ASTN qui accepte IP, la fonction DCF est connectée directement à une fonction DCF dans une entité voisine du RGT qui n'accepte que l'OSI, les fonctions suivantes doivent être acceptées dans la fonction DCF qui accepte IP:
  - fonction d'interfonctionnement d'unité PDU de couche Réseau (comme spécifié au § 7.1.7).

Dans une entité ASTN, la fonction DCF peut avoir à réexpédier une unité PDU de couche Réseau à travers un réseau qui n'accepte pas le même type de couche Réseau.

- Lorsque la fonction DCF d'une entité ASTN doit réexpédier une unité PDU de couche Réseau à travers un réseau qui n'accepte pas le même type de couche Réseau, les fonctions suivantes doivent être acceptées:
  - fonction d'encapsulage d'unité PDU de couche Réseau (comme spécifié au § 7.1.8);
  - fonction de tunnellisation d'unité PDU de couche Réseau (comme spécifié au § 7.1.9).

Dans une entité ASTN qui accepte IP en utilisant un routage OSPF, la fonction DCF peut être connectée directement à une fonction DCF d'une entité ASTN voisine qui accepte IP en utilisant IntISIS.

- Lorsque la fonction DCF d'une entité ASTN qui accepte IP en utilisant un routage OSPF est connectée directement à une fonction DCF d'une entité ASTN voisine qui accepte IP en utilisant IntISIS, les fonctions suivantes doivent être acceptées dans la fonction DCF qui accepte OSPF:
  - fonction d'interfonctionnement de routage IP (comme spécifié au § 7.1.11).

La fonction DCF contenue dans les entités ASTN peut jouer le rôle de routeur périphérique utilisant des étiquettes (LER, *label edge router*).

Lorsque la fonction DCF contenue dans les entités ASTN joue le rôle de routeur LER, les fonctions suivantes doivent être prises en charge:

- la fonction d'encapsulage ("unité PDU de commutation MPLS vers couche Liaison de données de canal ECC") si la fonction DCF prend en charge les interfaces de canal ECC, (comme spécifié au § 7.1.13);
- la fonction d'encapsulage ("unité PDU de commutation MPLS vers trame Ethernet") si la fonction DCF prend en charge les interfaces de réseau local (LAN), (comme spécifié au § 7.1.14);
- la fonction de signalisation d'unité LSP en commutation MPLS (comme spécifié au § 7.1.15);
- la fonction de réexpédition d'unité LSP en commutation MPLS (comme spécifié au § 7.1.16);
- la fonction de calcul de chemin d'unité LSP en commutation MPLS (comme spécifié au § 7.1.17);
- la fonction d'encapsulage ("unité PDU de couche Réseau vers commutation MPLS") (comme spécifié au § 7.1.18).

La fonction DCF contenue dans les entités ASTN peut jouer le rôle de routeur commutateur d'étiquettes (LSR, *label switch router*).

Lorsque la fonction DCF contenue dans les entités ASTN joue le rôle de routeur LSR, les fonctions suivantes doivent être prises en charge:

- la fonction d'encapsulage ("unité PDU de commutation MPLS vers couche Liaison de données de canal ECC") si la fonction DCF prend en charge les interfaces de canal ECC, (comme spécifié au § 7.1.13);
- la fonction d'encapsulage ("unité PDU de commutation MPLS vers trame Ethernet") si la fonction DCF prend en charge les interfaces de réseau local (LAN), (comme spécifié au § 7.1.14);
- la fonction de signalisation d'unité LSP en commutation MPLS (comme spécifié au § 7.1.15);
- la fonction de réexpédition d'unité LSP en commutation MPLS (comme spécifié au § 7.1.16).

La fonction DCF contenue dans les entités ASTN peut offrir la capacité de protection doublée des paquets.

Les exigences minimales pour offrir le service de protection doublée des paquets sont les suivantes:

- aucune capacité additionnelle n'est requise des nœuds internes du réseau;
- il y a lieu que le réseau prenne en charge l'établissement de connexions routées en diversité;
- *un nœud de réception*
  - doit être capable d'associer les deux connexions utilisées afin de fournir la protection doublée des paquets entre deux nœuds extrêmes;
  - doit prendre en charge le transport d'un identificateur dans le paquet qui sera utilisé afin d'identifier les duplicata d'un paquet au nœud d'émission;
  - doit être capable de dédoubler chaque paquet simultanément dans ces deux connexions appariées;
- *un nœud d'émission*
  - doit être capable d'associer les deux connexions utilisées afin de fournir la protection doublée des paquets entre deux nœuds extrêmes;

– doit être capable d'identifier, au moyen de l'identificateur, les duplicata d'un paquet dédoublé;
– doit être capable de sélectionner et de réexpédier une et une seule copie d'un paquet.

Le mécanisme permettant d'associer les deux connexions en diversité ainsi que le format et l'emplacement de l'identificateur de séquence doit être conforme au § 7.1.19.

6.3 Autres applications nécessitant des réseaux de communications

A côté des applications de RGT et d'ASTN, d'autres applications comme les communications vocales (par exemple ligne de service, téléimportation de logiciels, communications spécifiques des opérateurs) requièrent un réseau de communication pour assurer le transport des informations entre les composants.

6.4 Séparation de diverses applications

Selon la conception du réseau, la taille du réseau, la capacité des liaisons, les exigences de sécurité et de performance, divers niveaux de séparation entre les multiples applications (par exemple RGT, ASTN) sont possibles. Le niveau de séparation qui est fourni est un choix qui est fait entre opérateurs et vendeurs quand ils conçoivent le réseau. Les exemples suivants montrent divers niveaux de séparation.

Option A: le RCD peut être conçu de telle sorte que le RCG, le RCS et les autres applications (par exemple les communications spécifiques des opérateurs) soient traités sur le même réseau de couche 3 (par exemple, en partageant le réseau IP).

Option B: le RCD peut être conçu de telle sorte que le RCG, le RCS et les autres applications (par exemple, les communications spécifiques des opérateurs) soient traités sur des réseaux de couche 3 séparés, en pouvant toutefois partager certaines liaisons physiques.

Option C: le RCD peut être conçu de telle sorte que le RCG, le RCS et les autres applications (par exemple, les communications spécifiques des opérateurs) soient traités sur des réseaux physiques séparés (c'est-à-dire, séparer des réseaux de couche 3 qui ne partagent aucune liaison physique).

7 Architecture fonctionnelle et exigences du RCD

Dans le présent paragraphe, les exigences d'architecture du RCD s'appliquent aux domaines IP seulement, OSI seulement, et mixtes IP+OSI. Les exigences d'architecture RCD ne dépendent pas de la technologie utilisée. Des recommandations particulières pour des technologies spécifiques comme la Rec. UIT-T G.784 pour la hiérarchie SDH et la Rec. UIT-T G.874 pour le réseau OTN précisent quelles exigences sont applicables pour ces technologies particulières.

Le RCD est informé des protocoles de couche 1, de couche 2 et de couche 3 et est transparent aux protocoles des couches supérieures utilisés par les applications dont il effectue le transport.

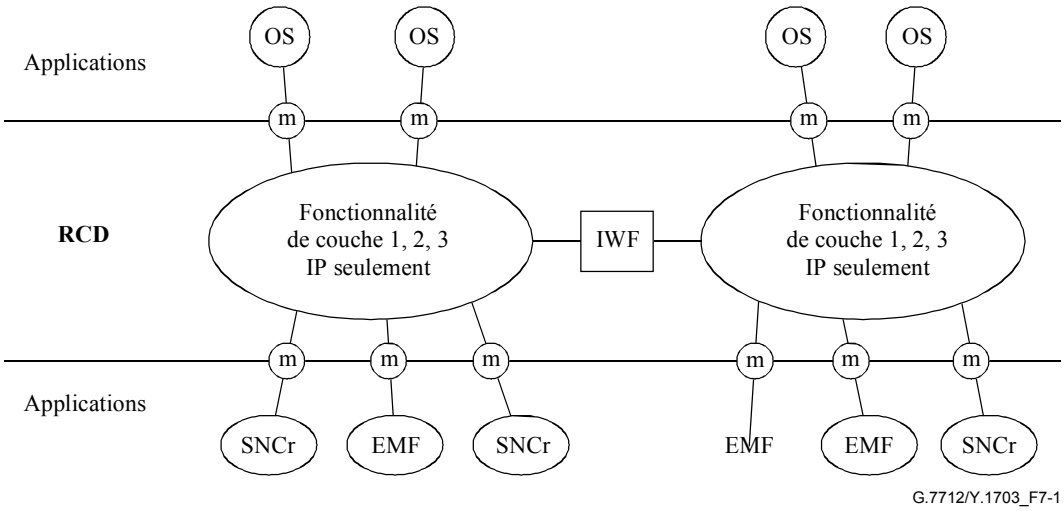
Un RCD peut être conçu de façon qu'il n'accepte que le protocole IP. Un RCD n'acceptant que le protocole IP peut consister en différents sous-réseaux utilisant différents protocoles de couche Physique et de Liaison de données, mais tous les sous-réseaux devront accepter IP comme protocole de couche Réseau.

Cependant, dans la mesure où les réseaux RCD intégrés acceptent l'OSI, certains RCD peuvent comporter des parties qui acceptent IP seulement, des parties qui acceptent OSI seulement, et des parties qui acceptent à la fois IP et OSI.

Les parties du RCD qui acceptent IP (c'est-à-dire les parties qui n'acceptent que le protocole IP ou les parties qui acceptent IP et OSI) peuvent consister en fonctions DCF qui acceptent IP seulement (c'est-à-dire une seule pile de fonctions DCF qui prennent en charge le protocole IP seulement) et/ou des fonctions DCF acceptant IP et OSI (par exemple, une fonction DCF à double pile qui est

capable de router à la fois les paquets IP et les paquets OSI). Les parties du RCD n'acceptant que l'OSI consisteraient en fonctions DCF qui traitent l'OSI seulement (c'est-à-dire une seule pile de fonctions DCF qui prennent en charge le protocole OSI seulement).

La Figure 7-1 illustre l'architecture fonctionnelle du RCD. Comme indiqué ci-dessus, le RCD peut être composé de parties qui n'acceptent que l'IP, de parties qui n'acceptent que l'OSI, et de parties qui acceptent à la fois IP et OSI. Une fonction d'interfonctionnement (IWF, *interworking function*) entre les parties du RCD traitant l'IP seulement, l'OSI seulement, et IP+OSI, et des fonctions de mappage qui attribuent des applications à la couche IP, sont également spécifiées. Pour assurer un tel transport, le RCD traite les fonctionnalités de couche 1 (Physique), de couche 2 (Liaison de données), et de couche 3 (Réseau). Les exigences d'architecture pour les parties du RCD n'acceptant que l'IP, que l'OSI ainsi que les exigences pour l'interfonctionnement entre les parties du RCD acceptant l'IP seulement, l'OSI seulement, et IP+OSI sont spécifiées. Le nuage de la Figure 7-1, représentant la partie IP seulement du RCD, est une représentation abstraite du RCD et peut donc aussi s'appliquer à un seul élément de réseau IP interconnecté à des éléments de réseau OSI via une fonction IWF.



IWF fonction d'interfonctionnement
SNCr contrôleur de connexion de sous-réseau
EMF fonction de gestion d'équipement
OS système d'exploitation
m mappage entre application et RCD

Figure 7-1/G.7712/Y.1703 – Architecture fonctionnelle du RCD

7.1 Spécification des fonctions de communications de données

Le présent paragraphe spécifie différentes fonctions de communications de données se rapportant aux interfaces de canal ECC, aux interfaces de LAN Ethernet, et aux capacités de couche Réseau.

7.1.1 Fonction d'accès au canal ECC

Une fonction d'accès au canal ECC donne accès au flux binaire ECC. Cette fonction est définie dans les Recommandations relatives aux équipements spécifiques des diverses technologies (par exemple, les Recommandations UIT-T G.783 et G.798). Les débits et les définitions des divers canaux ECC (par exemple DCC, GCC, et l'en-tête COMMS OH dans le canal OSC) sont indiqués dans les Recommandations propres aux diverses technologies (par exemple les Recommandations UIT-T G.784 et G.874).

7.1.2 Fonction de terminaison de couche Liaison de données pour canal ECC

Une fonction de terminaison de couche Liaison de données pour canal ECC assure le traitement commun de la couche Liaison de données sans considération des unités PDU de la couche Réseau encapsulés dans la trame de la couche Liaison de données. La mise en place de la trame de couche Liaison de données dans le canal ECC est aussi assurée par cette fonction. Cette fonction est spécifiée dans les Recommandations spécifiques des diverses technologies. On donne cependant ci-dessous la spécification pour la fonction de terminaison de couche Liaison de données pour un canal ECC en hiérarchie SDH.

7.1.2.1 Fonction de terminaison de couche Liaison de données pour un canal ECC en hiérarchie SDH

7.1.2.1.1 Mappage de la trame de couche de Liaison de données SDH dans le canal ECC

Le signal verrouillé en trames HDLC est un flux binaire sériel contenant des trames justifiées et entourées par une ou plusieurs séquences de fanions. Le format du signal à trames HDLC est défini dans la Rec. UIT-T Q.921 pour le protocole LAPD et dans le commentaire RFC 1662 pour les liaisons PPP à trames HDLC. Une trame HDLC consiste en N octets conformément à la Figure 7-2. La trame HDLC est transmise de droite à gauche et de haut en bas. Un bit 0 est inséré après toute séquence de cinq bits 1 consécutifs dans le contenu de la trame HDLC (octets 2 à N-1) pour garantir qu'une séquence de fanions ou d'interruption n'est pas simulée à l'intérieur d'une trame.

Le mappage du signal à trames HDLC dans le canal DCC est synchrone au bit près (plutôt que synchrone à l'octet près) dans la mesure où la trame justifiée HDLC ne contient pas nécessairement un nombre entier d'octets par suite du processus d'insertion des 0. Il n'y a donc pas de mappage direct d'une trame HDLC justifiée sur les octets d'un canal DCC. Le générateur de signaux HDLC dérive sa temporisation de la fonction Couche serveur/DCC_A (c'est-à-dire du signal DCC_CI_CK) pour la hiérarchie SDH. Les fonctions Couche serveur/DCC_A suivantes sont définies dans la Rec. UIT-T G.783: la fonction MSn/DCC_A, la fonction MS256/DCC_A et la fonction RSn/DCC_A.

Le signal de trame HDLC est un flux de bits sériels qui doit être inséré dans le canal DCC de telle sorte que les bits soient transmis par le module STM-N dans l'ordre où ils ont été reçus du générateur de signal de trames HDLC.

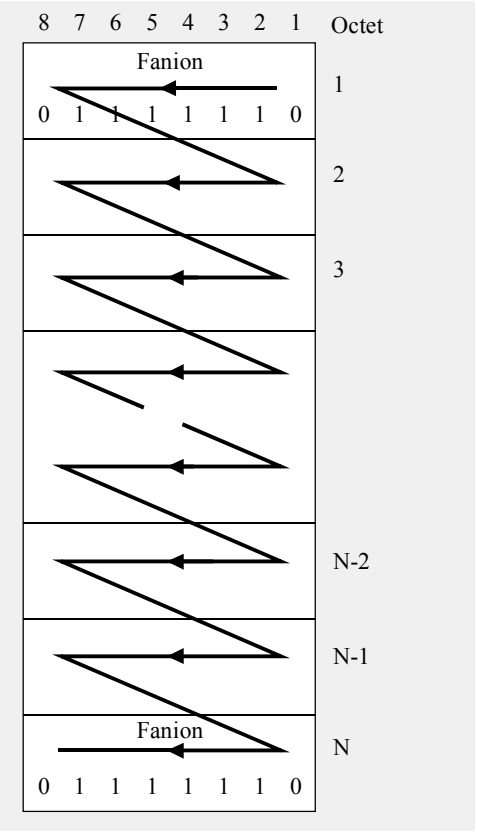


Figure 7-2/G.7712/Y.1703 – Format de trame HDLC

7.1.2.1.2 Spécification du protocole de couche de Liaison de données pour canal ECC en hiérarchie SDH

Les trois types d'interfaces identifiés sont les suivants: interfaces IP seulement, interfaces OSI seulement et interfaces doubles (les interfaces doubles sont des interfaces qui peuvent transporter aussi bien les paquets IP que les paquets OSI). Lors du transport de paquets IP seulement dans le canal DCC, le verrouillage de trames PPPinHDLC doit être utilisé comme protocole de couche de Liaison de données. Comme les interfaces doubles peuvent prendre en charge les deux protocoles IP et OSI, il est possible qu'une interface double soit connectée aussi bien à une interface IP seulement, à une interface OSI seulement, ou à une autre interface double. Les interfaces OSI seulement existent aujourd'hui dans les réseaux, et le protocole de Liaison de données utilisé sur de telles interfaces est la procédure LAPD définie dans la Rec. UIT-T G.784. Pour permettre aux interfaces doubles de se connecter soit à une interface IP seulement soit à une interface OSI seulement, le protocole de la couche Liaison de données accepté sur une interface double doit être configurable de façon à accepter le protocole PPPinHDLC ou LAPD. Une exception est permise pour les éléments de réseau SDH intégrés acceptant la procédure LAPD dans des appareils qui ont été mis à niveau pour accepter des interfaces doubles. Pour limiter la quantité de mises à niveau à effectuer sur les matériels, il est permis aux éléments de réseau améliorés en hiérarchie SDH de n'accepter que la procédure LAPD.

7.1.2.1.2.1 Interface IP seulement

Les interfaces IP seulement sont illustrées à la Figure 7-3.

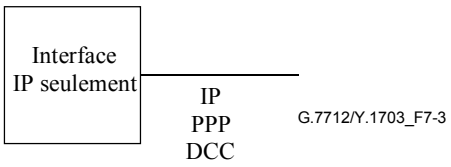


Figure 7-3/G.7712/Y.1703 – Interface IP seulement

Les interfaces IP seulement doivent utiliser des liaisons en protocole PPP comme indiqué dans le commentaire RFC 1661.

7.1.2.1.2.2 Interface OSI seulement

Les interfaces OSI seulement sont illustrées à la Figure 7-4.

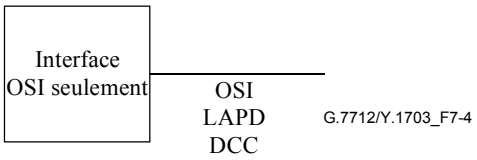


Figure 7-4/G.7712/Y.1703 – Interface OSI seulement

Les interfaces OSI seulement doivent utiliser la procédure LAPD conformément à la Rec. UIT-T G.784.

7.1.2.1.2.3 Interface double (IP+OSI)

Les interfaces doubles (qui peuvent transporter des paquets OSI et des paquets IP) peuvent être connectées à des interfaces IP seulement, à des interfaces OSI seulement, ou à d'autres interfaces doubles. Pour permettre aux interfaces doubles d'être connectées à d'autres interfaces IP seulement ou à d'autres interfaces OSI seulement, le protocole de Liaison de données sur l'interface double doit être configurable de façon à pouvoir passer du protocole PPP en verrouillage de trames HDLC (comme indiqué dans le commentaire RFC 1662) à la procédure LAPD (indiquée dans la Rec. UIT-T G.784), comme illustré à la Figure 7-5. Noter que les éléments de réseau intégrés en hiérarchie SDH acceptant la procédure LAPD dans des appareils qui ont été mis à niveau pour accepter le protocole IP ne sont pas tenus d'accepter le protocole PPP en verrouillage de trames HDLC sur leurs interfaces doubles. Il est donc simplement demandé aux interfaces doubles de ces éléments d'accepter la procédure LAPD.

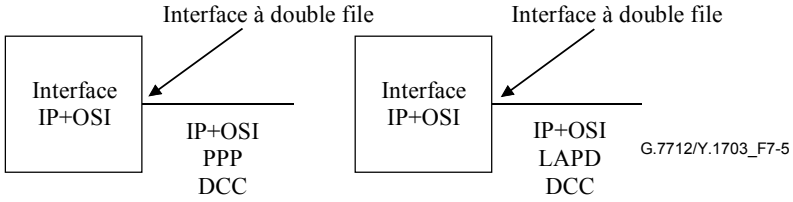


Figure 7-5/G.7712/Y.1703 – Interface double

Les interfaces doubles acceptant le protocole PPP doivent l'utiliser comme indiqué dans le commentaire RFC 1661.

Les interfaces doubles acceptant la procédure LAPD doivent l'utiliser conformément à la Rec. UIT-T G.784.

7.1.3 Fonction d'encapsulage ("unité PDU de couche Réseau dans trame de couche Liaison de données de canal ECC")

Une fonction d'encapsulage ("unité PDU de couche Réseau dans trame de couche Liaison de données de canal ECC") encapsule et désencapsule les unités PDU de couche Réseau dans la trame de couche Liaison de données. Cette fonction traite aussi l'identificateur de protocole. Cette fonction est définie dans les Recommandations sur les technologies spécifiques. La spécification pour la fonction d'encapsulage ("unité PDU de couche Réseau dans trame de couche Liaison de données de canal ECC en hiérarchie SDH") est toutefois donnée ci-dessous.

7.1.3.1 Fonction d'encapsulage ("unité PDU de couche Réseau dans trame de couche Liaison de données de canal ECC en hiérarchie SDH")

La spécification de la fonction d'encapsulage ("unité PDU de couche Réseau dans trame de couche Liaison de données de canal ECC en hiérarchie SDH") pour les interfaces IP seulement, les interfaces OSI seulement, et les interfaces doubles est donnée ci-dessous.

7.1.3.1.1 Interface IP seulement

Les interfaces IP seulement ne doivent utiliser que le mode PPPinHDLCframing/DCC comme indiqué dans le commentaire RFC 1662.

Une interface IP seulement se définit comme suit:

l'extrémité d'émission:

– doit mettre les paquets IS-IS directement dans le champ d'information PPP comme indiqué dans le commentaire RFC 1661 avec la valeur de protocole OSI comme indiqué dans le commentaire RFC 1377 dans le champ de protocole PPP;

– doit mettre les paquets IPv4 directement dans le champ d'information PPP comme indiqué dans le commentaire RFC 1661 avec la valeur de protocole IPv4 comme indiqué dans le commentaire RFC 1332 dans le champ de protocole PPP;

– doit mettre les paquets IPv6 directement dans le champ d'information PPP comme indiqué dans le commentaire RFC 1661 avec la valeur de protocole IPv6 comme dans le commentaire RFC 2472 dans le champ de protocole PPP.

L'extrémité de réception:

– un paquet IS-IS est identifié si le champ de protocole PPP a la valeur de protocole OSI indiquée dans le commentaire RFC 1377 et si le paquet a l'identificateur NLPID pour IS-IS comme spécifié dans la Rec. UIT-T X.263 | ISO/CEI 9577;

– un paquet IPv4 est identifié si le champ de protocole PPP a la valeur de protocole IPv4 indiquée dans le commentaire RFC 1332;

– un paquet IPv6 est identifié si le champ de protocole PPP a la valeur de protocole IPv6 indiquée dans le commentaire RFC 2472.

7.1.3.1.2 Interface OSI seulement

Les interfaces OSI seulement ne doivent utiliser que le canal LAPD/DCC comme indiqué dans la Rec. UIT-T G.784.

Une interface OSI seulement est définie comme suit:

l'extrémité d'émission:

– doit mettre les paquets CLNP, IS-IS et ES-IS directement dans la charge utile de la procédure LAPD comme indiqué dans la Rec. UIT-T G.784;

l'extrémité de réception:

– doit inspecter l'identificateur de protocole situé dans le premier octet de la charge utile de la procédure LAPD. La valeur de cet identificateur est cohérente avec la valeur allouée dans la Rec. UIT-T X.263 | ISO/CEI 9577. Si l'unité PDU reçue est destinée à un protocole non accepté par le récepteur, cette unité PDU doit alors être ignorée.

7.1.3.1.3 Interface double (IP+OSI)

Une interface double acceptant PPP comme protocole de Liaison de données se définit comme suit:

l'extrémité d'émission:

– doit mettre les paquets CLNP, IS-IS et ES-IS directement dans le champ d'information du protocole PPP comme indiqué dans le commentaire RFC 1661 avec la valeur de protocole OSI comme indiqué dans le commentaire RFC 1377 dans le champ de protocole PPP;

– doit mettre les paquets IPv4 directement dans le champ d'information du protocole PPP comme indiqué dans le commentaire RFC 1661 avec la valeur de protocole IPv4 comme indiqué dans le commentaire RFC 1332 dans le champ de protocole PPP;

– doit mettre les paquets IPv6 directement dans le champ d'information du protocole PPP comme indiqué dans le commentaire RFC 1661 avec la valeur de protocole IPv6 comme indiqué dans le commentaire RFC 2472 dans le champ de protocole PPP.

L'extrémité de réception:

– un paquet OSI est identifié si le champ de protocole PPP a la valeur de protocole OSI comme indiqué dans le commentaire RFC 1377;

– un paquet IPv4 est identifié si le champ de protocole PPP a la valeur de protocole IPv4 comme indiqué dans le commentaire RFC 1332;

– un paquet IPv6 est identifié si le champ de protocole PPP a la valeur de protocole IPv6 comme indiqué dans le commentaire RFC 2472.

Une interface double acceptant la procédure LAPD comme protocole de Liaison de données se définit comme suit:

l'extrémité d'émission:

– doit mettre les paquets CLNP, IS-IS et ES-IS directement dans la charge utile de la procédure LAPD comme indiqué dans la Rec. UIT-T G.784;

– doit mettre les paquets IP directement dans la charge utile de la procédure LAPD, avec un identificateur de protocole d'un seul octet prémarqué. Cet identificateur doit être cohérent avec les valeurs allouées pour Ipv4 et Ipv6 dans la Rec. UIT-T X.263 | ISO/CEI 9577.

L'extrémité de réception:

– doit inspecter l'identificateur de protocole situé dans le premier octet de la charge utile de la procédure LAPD. La valeur de cet identificateur est cohérente avec les valeurs allouées dans la Rec. UIT-T X.263 | ISO/CEI 9577. Si l'unité PDU reçue est pour un protocole non accepté par le récepteur, cette unité PDU doit alors être ignorée.

7.1.4 Fonction de terminaison physique de LAN Ethernet

Une fonction de terminaison physique de LAN Ethernet termine l'interface physique Ethernet.

Un ou plusieurs des débits suivants doivent être acceptés: 1 Mbit/s, 10 Mbit/s, 100 Mbit/s.

L'accès aux canaux ECC à terminaison physique est autorisé par les éléments de réseau qui acceptent les interfaces LAN Ethernet. Il n'est pas nécessaire que tous les éléments de réseau acceptant les canaux ECC acceptent les accès LAN Ethernet, pourvu qu'il y ait une voie ECC à

partir d'un élément de réseau terminant le canal ECC et un autre élément de réseau fournissant les accès LAN Ethernet.

7.1.5 Fonction d'encapsulage ("unité PDU de couche Réseau dans trame Ethernet")

Cette fonction encapsule et désencapsule une unité PDU de couche Réseau dans une trame 802.3 ou Ethernet (version 2).

Elle doit encapsuler les unités PDU de couche Réseau dans des trames 802.3 ou Ethernet (version 2) conformément aux règles suivantes:

- elle doit encapsuler et désencapsuler les unités PDU CLNP, IS-IS, et ES-IS dans des trames 802.3 comme indiqué dans la Rec. UIT-T Q.811;
- elle doit encapsuler et désencapsuler les paquets IP en trames Ethernet (version 2) comme indiqué dans le commentaire RFC 894;
- les adresses IP doivent être mappées avec les adresses MAC Ethernet en utilisant le Protocole de résolution d'adresse du commentaire RFC 826.

Elle doit déterminer le type de trame reçue (802.3 ou Ethernet version 2) comme indiqué au § 2.3.3 du commentaire RFC 1122.

7.1.6 Fonction de renvoi d'unité PDU de couche Réseau

La fonction de renvoi d'unité PDU de couche Réseau renvoie les paquets de couche Réseau.

Si cette fonction renvoie les paquets CLNP, elle doit procéder comme indiqué dans la Rec. UIT-T Q.811.

Si cette fonction renvoie les paquets IPv4, elle doit procéder comme indiqué dans le commentaire RFC 791.

Si cette fonction renvoie les paquets IPv6, elle doit procéder comme indiqué dans le commentaire RFC 2460.

Le format d'adresse préféré est IPv6. Le protocole de routage IP doit être capable de traiter l'adressage IPv6 et IPv4.

7.1.7 Fonction d'interfonctionnement d'unité PDU de couche Réseau

La fonction d'interfonctionnement d'unité PDU de couche Réseau veille à ce que des fonctions DCF voisines, traitant différents protocoles de couche, Réseau puissent communiquer. Il est nécessaire que la fonction DCF acceptant IP accepte OSI pour permettre la communication avec la fonction DCF voisine n'acceptant que l'OSI.

7.1.8 Fonction d'encapsulage d'unité PDU de couche Réseau

La fonction d'encapsulage d'unité PDU de couche Réseau encapsule et désencapsule une même unité PDU de couche Réseau dans une autre unité PDU de couche Réseau.

Les paquets CLNP doivent être encapsulés en protocole IP au moyen de l'encapsulage de routation général (GRE, *generic routing encapsulage*), comme spécifié dans le commentaire RFC 2784, en tant que charge utile d'un paquet IP en utilisant un numéro de protocole IP égal à 47 (décimal) et avec le bit DF ne pas fragmenter (DF, *don't fragment*) non établi. Comme indiqué dans le commentaire RFC 2784, l'encapsulage GRE doit contenir un Ethertype pour indiquer quel protocole de couche Réseau doit être encapsulé. On doit utiliser la norme industrielle pour Ethertype OSI, qui est 00FE (hex).

Les paquets IP doivent être encapsulés en protocole CLNS au moyen de l'encapsulage GRE, comme spécifié dans le commentaire RFC 2784, en tant que charge utile de données d'une unité PDU de type de données CLNP comme spécifié dans l'ISO/CEI 8473-1, en utilisant une valeur de sélecteur NSAP égale à 47 (décimal) et avec le fannion SP (segmentation permise) établi. Des informations complémentaires sont disponibles dans le commentaire RFC 3147.

Les paquets IP doivent être encapsulés en protocole IP au moyen de l'encapsulage GRE, comme spécifié dans le commentaire RFC 2784, en tant que charge utile d'un paquet IP en utilisant un numéro de protocole IP égal à 47 (décimal) et avec le bit DF (ne pas fragmenter) non établi.

En option, la fonction d'encapsulage d'unité PDU de couche Réseau peut réexpédier des unités PDU par des nœuds incompatibles au moyen de la procédure d'encapsulage automatique qui est décrite dans l'Annexe B. Noter qu'une fonction DCF prenant en charge la procédure d'encapsulage décrite dans l'Annexe B est compatible avec une fonction DCF qui ne prend pas en charge la procédure d'encapsulage automatique et qu'elle peut être déployée dans la même zone.

7.1.9 Fonction de tunnellisation de couche Réseau

La fonction de tunnellisation d'unité PDU de couche Réseau fournit un tunnel statique entre deux fonctions DCF traitant la même unité PDU de couche Réseau. Pour un tunnel avec une taille d'unité MTU configurée, tout paquet IP qui ne peut pas être renvoyé par le tunnel parce qu'il est plus grand que la taille de la MTU, et qui a son bit DF établi, doit être rejeté et un message ICMP d'erreur due à une inaccessibilité (en particulier le code "fragmentation nécessaire et DF établi") devrait être renvoyé à la source du paquet.

7.1.10 Fonction de routage de couche Réseau

La fonction de routage de couche Réseau achemine les paquets de la couche Réseau.

Une fonction DCF acceptant le routage OSI doit accepter IS-IS comme indiqué dans l'ISO/CEI 10589.

Une fonction DCF acceptant le routage OSI doit accepter le routage IS-IS intégré (voir au § 7.1.10.1 les exigences pour le routage IS-IS intégré) et peut aussi accepter le routage OSPF ainsi que d'autres protocoles de routage IP.

7.1.10.1 Exigences pour le routage IS-IS intégré

Une fonction DCF acceptant le routage IS-IS intégré doit être conforme au commentaire RFC 1195.

Une fonction DCF acceptant le routage IS-IS intégré doit accepter la prise de contact à trois voies (voir à l'Annexe A les exigences pour la prise de contact à trois voies). La prise de contact à trois voies modifie la création de contiguïtés et le comportement de maintenance spécifiés dans l'ISO/CEI 10589.

7.1.10.1.1 Création de contiguïtés compatibles avec le protocole de couche Réseau

La fonction DCF doit inclure un nuplet TLV "protocoles pris en charge" dans toutes les unités PDU de préappel IIH ou ISH à toutes les interfaces et dans toutes les unités LSP portant le numéro 0, conformément au commentaire RFC 1195.

Dès réception d'une unité PDU de préappel IIH ou ISH à routage IS-IS, la fonction DCF doit contrôler cette unité PDU afin de déterminer si elle contient un nuplet TLV à routage IS-IS"protocoles pris en charge". Cette détection doit s'effectuer à toutes les interfaces, qu'il s'agisse de liaisons LAN, DCC etc. Si une unité PDU de préappel IIH ou ISH ne contient pas de TLV "protocoles pris en charge", elle doit être traitée comme si elle contenait un TLV "protocoles pris en charge" contenant seulement l'identificateur NLPID pour le protocole CLNP.

La fonction DCF doit comparer les identificateurs NLPID énumérés dans le TLV "protocoles pris en charge" (en supposant par défaut le protocole CLNP si aucun identificateur n'est présent) aux protocoles de couche Réseau que la fonction DCF est elle-même capable de réexpédier.

Si aucune contiguïté n'existe avec l'entité voisine qui a envoyé le préappel ISH ou IIH, et si la fonction DCF n'est capable de réexpédier aucun des protocoles de couche Réseau énumérés dans le TLV "protocoles pris en charge" du préappel ISH ou IIH reçu de l'entité voisine, alors la fonction DCF ne doit pas former de contiguïté avec cette entité voisine.

Si une contiguïté existe bien avec l'entité voisine qui a envoyé le préappel ISH ou IIH et si la fonction DCF n'est capable de réexpédier aucun des protocoles de couche Réseau énumérés dans le TLV "protocoles pris en charge" du préappel ISH ou IIH reçu de l'entité voisine, alors la fonction DCF doit supprimer la contiguïté avec cette entité voisine et produire un évènement de discordance entre protocoles pris en charge.

Si la fonction DCF est par elle-même capable de réexpédier un ou plusieurs des protocoles de couche Réseau énumérés dans le TLV "protocoles pris en charge" d'un préappel ISH ou IIH reçu, alors cette fonction DCF doit traiter le préappel ISH ou IIH comme étant normal.

La fonction DCF ne doit pas tenir compte de la valeur du TLV "protocoles pris en charge" des unités LSP au cours de ce processus.

Une fonction DCF qui ne peut pas réexpédier des unités PDU du protocole CLNP ne doivent pas tenir compte des unités PDU de préappel ESH et, par conséquent, ne doivent pas annoncer l'accessibilité des systèmes d'extrémité OSI.

7.1.10.1.2 Distribution de préfixe IP dans tout le domaine IS-IS

Les fonctions DCF acceptant le routage IS-IS intégré de niveau 1 à niveau 2 doivent accepter l'annonce de préfixes de destination IP configurés et acquis via des unités LSP de niveau 2 à niveau 1, ainsi que de préfixes de destination IP acquis via des unités LSP de niveau 1 à niveau 2. Le comportement par défaut, lorsque aucun préfixe de destination IP n'a été configuré, doit être de ne transformer aucun préfixe de niveau 2 en unités LSP de niveau 1, tandis que tous les préfixes acquis de niveau 1 doivent être transformés en unités LSP de niveau 2.

7.1.10.1.2.1 Préfixes de configuration

L'opérateur doit prévoir deux tableaux qui commandent la transformation des préfixes. Un tableau doit commander la transformation du niveau 1 au niveau 2, tandis que l'autre commande la transformation du niveau 2 au niveau 1.

7.1.10.1.2.2 Balisage des préfixes transformés

Dans la mesure où la transformation des préfixes du niveau 2 au niveau 1 et ensuite du niveau 1 au niveau 2 peut introduire des boucles de routage, une balise est nécessaire pour identifier la source du préfixe. Cette balise, dite *fanion de montée/descente*, est stockée dans le bit de poids fort (bit 8) précédemment inutilisé du champ d'Objet métrologique par défaut contenu dans les nuplets TLV d'accessibilité IP interne et externe. Les mises en œuvre existantes de routage IS-IS qui acceptent le commentaire RFC 1195 ne seront pas touchées par la redéfinition de ce bit car le commentaire RFC 1195 demande qu'il soit mis à zéro lors de l'émission des unités LSP, et ignoré lors de leur réception. De plus amples détails sont disponibles dans le commentaire RFC 2966.

Les nuplets TLV d'accessibilité IP interne et externe doivent être traités de la même manière. Le type de TLV reçu sera celui qui est utilisé lorsque le préfixe est transformé d'une zone de niveau 2 en zone de niveau 1, ainsi que d'une zone de niveau 1 en zone de niveau 2.

Ce qui précède diffère du commentaire RFC 1195, qui contraint les valeurs de TLV d'accessibilité IP externe à n'apparaître que dans les unités LSP de niveau 2.

7.1.10.1.2.2.1 Transmission d'unités LSP avec nuplets TLV d'accessibilité IP interne et externe

Comme dans le commentaire RFC 1195 normal, la valeur du fanion de montée/descente doit être mise à zéro pour tous les nuplets TLV de protocole IP dans les unités LSP de niveau 2. La valeur du fanion de montée/descente doit être mise à zéro pour les unités LSP de niveau 1 émises dans une zone de niveau 1.

Le fanion de montée/descente doit être mis à un dans les nuplets TLV de protocole IP d'unité LSP de niveau 1 quand un élément de réseau de routage IS-IS intégré aux niveaux 1 et 2 transforme un préfixe configuré de niveau 2 en niveau 1.

7.1.10.1.2.2.2 Réception d'unités LSP avec nuplets TLV d'accessibilité interne et externe

Une fonction DCF acceptant le routage intégré de systèmes IS-IS doit ignorer la valeur du fanion de montée/descente lorsqu'elle développe des routes à utiliser dans une zone de niveau 1 ou 2.

Une fonction DCF acceptant le routage IS-IS intégré aux niveaux 1 et 2, qui reçoit une unité LSP avec un nuplet TLV de protocole IP pour un préfixe qui convient à une entrée dans le tableau de transformation de niveau 1 en niveau 2, doit annoncer le préfixe approprié du niveau 1 au niveau 2.

Une fonction DCF acceptant le routage IS-IS intégré aux niveaux 1 et 2, qui reçoit une unité LSP avec un nuplet TLV de protocole IP avec le fanion de montée/descente mis à un, ne doit jamais utiliser le préfixe pour la transformation des informations du niveau 1 au niveau 2.

7.1.10.1.2.2.3 Utilisation du fanion de montée/descente dans les unités LSP de niveau 2

L'utilisation du fanion de montée/descente dans les unités LSP de niveau 2 fera l'objet d'études ultérieures.

7.1.10.1.2.3 Préférence de routage

Etant donné que les préfixes peuvent maintenant passer du niveau 2 au niveau 1, les préférences de routage spécifiées dans le commentaire RFC 1195 doivent être mises à jour pour prendre en compte cette nouvelle source. L'ordre de préférence de routage est le suivant:

1) routes intrazones de niveau 1 avec objet métrique interne;
   routes externes de niveau 1 avec objet métrique interne;
2) routes intrazones de niveau 2 avec objet métrique interne;
   routes externes de niveau 2 avec objet métrique interne;
   routes interzones passées de niveau 1 à niveau 2 avec objet métrique interne;
   routes externes interzones passées de niveau 1 à niveau 2 avec objet métrique interne;
3) routes interzones passées de zone de niveau 2 à zone de niveau 1 avec objet métrique interne;
   routes externes passées de zone de niveau 2 à zone de niveau 1 avec objet métrique interne;
4) routes externes de niveau 1 avec objet métrique externe;
5) routes externes de niveau 2 avec objet métrique externe;
   routes externes interzones passées de niveau 1 à niveau 2 avec objet métrique externe;
6) routes externes interzones passées de niveau 2 à zone de niveau 1 avec objet métrique externe.

7.1.11 Fonction d'interfonctionnement de routage IP

Une fonction DCF acceptant la fonction d'interfonctionnement de routage IP doit accepter les mécanismes de filtrage de routage indiqués aux § 7.5 et 7.6 du commentaire RFC 1812 de façon que les réseaux ayant deux protocoles de routage puissent être connectés via plus d'un point de commutation.

7.1.12 Fonction de mappage ("d'applications sur la couche Réseau")

Les applications OSI fonctionnant sur (tout ou partie du) RCD, qui n'acceptent que le protocole IP peuvent être mappées en protocole IP comme spécifié au § 2.1.6/Q.811 qui traite du profil de protocole RFC 1006/TCP/IP. Un tel mappage est une solution de couche 4 et sort donc du domaine d'application de la présente Recommandation. Une autre option pour le transport des applications

OSI dans (tout ou partie du) RCD, qui n'accepte que le protocole IP, consiste à fournir l'OSI par encapsulage dans la couche 3 du protocole IP comme spécifié au § 7.1.8.

Le mappage d'applications IP sur (tout ou partie du) RCD qui accepte le protocole IP doit être conforme aux spécifications des suites IP.

7.1.13 Fonction d'encapsulage ("d'unité PDU de commutation MPLS vers couche Liaison de données")

Cette fonction encapsule et désencapsule une unité PDU de commutation MPLS dans une trame de couche Liaison de données par canal ECC.

Si le protocole de Liaison de données pris en charge est PPP à l'interface avec le canal ECC, ce qui suit est requis:

– *à l'extrémité d'émission*:

  les paquets MPLS doivent être insérés directement dans le champ d'informations PPP conformément à RFC 1661 avec la valeur de protocole MPLS égale à 0281 hex insérée dans le champ de protocole PPP conformément au § 4.3 du RFC 3032 pour l'unidiffusion par commutation MPLS;

– *à l'extrémité de réception*:

  un paquet MPLS est identifié si le champ de protocole PPP a la valeur de protocole MPLS de 0281 hex conformément au § 4.3 du RFC 3032 pour l'unidiffusion MPLS.

7.1.14 Fonction d'encapsulage ("d'unité PDU de commutation MPLS vers trame Ethernet")

Cette fonction encapsule et désencapsule une unité PDU de commutation MPLS dans une trame Ethernet (version 2).

Elle doit encapsuler les unités PDU de commutation MPLS dans les trames Ethernet (version 2) conformément au RFC 894 au moyen d'une valeur d'Ethertype égale à 8847 hex conformément au § 5 du RFC 3032 pour l'unidiffusion MPLS.

7.1.15 Fonction de signalisation d'unité LSP en commutation MPLS

La fonction de signalisation d'unité LSP (*label switched path*) en commutation MPLS assure la signalisation nécessaire pour établir les chemins LSP de commutation MPLS.

Une fonction DCF prenant en charge la fonction de signalisation d'unité LSP en commutation MPLS doit prendre en charge le modèle de réservation suivant: chemin explicite avec route stricte via des nœuds simples (adresses IP de 32 bits) pour chemins LSP unidiffusés de point à point, via le style de réservation "FF" par protocole IPv4.

Le message "Path" est réexpédié vers la destination sur un chemin spécifié par une liste d'adresses IP dans l'objet de route explicite (ERO, *explicit route object*). Chaque nœud (routeur LSR) contenu dans le chemin enregistre l'objet ERO. Au moyen de l'objet Demande d'étiquette, les nœuds (routeurs LSR) assurent l'association des étiquettes au cours de la session. Voir RFC 3209 – RSVP-TE, § 2.2, 3.1, 4.2 et 4.3.

Le nœud de destination répond par un message Resv qui est envoyé en amont vers l'expéditeur, dans l'ordre inverse de la liste de nœuds contenue dans l'objet ERO. L'étiquette contenue dans l'objet Etiquette du message Resv est utilisée dans chaque routeur LSR intermédiaire afin d'associer le trafic sortant au chemin d'unités LSP correspondant. Si le nœud n'est pas l'expéditeur, il attribue une nouvelle étiquette et l'insère dans l'objet Etiquettte du message Resv qu'il envoie en amont au bond précédent (PHOP, *previous hop*). Voir RFC 3209 – RSVP-TE, § 2.2, 3.2 et 4.1.

Si le nœud ne peut pas répondre à la demande, il envoie un message PathErr ou ResvErr au nœud expéditeur. Voir RFC 3209 – RSVP-TE, § 4.5.

La procédure d'états conditionnels du protocole RSVP implique l'expédition périodique d'une représentation complète de l'état du chemin d'unités LSP dans des messages Resv et Path afin de maintenir le chemin d'unités LSP. Le message Srefresh est utilisé à la place de l'expédition périodique de messages Path et Resv normalisés. Chaque identificateur de message contenu dans le message Srefresh représente un message Path ou Resv complet dont l'état n'est pas modifié. Voir RFC 2961 – RSVP-ORE, § 5.5.

Un objet MESSAGE_ID_NACK est utilisé afin d'indiquer qu'un identificateur de message ne correspond pas et qu'un message Path ou Resv complet est nécessaire afin de rétablir le chemin d'unités LSP. Voir RFC 2961 – RSVP-ORE, § 5.4.

Un objet MESSAGE_ID_ACK est utilisé afin d'accuser réception de messages contenant l'objet MESSAGE_ID et pour lesquels le fanion ACK_Desired est activé. Cet objet fait partie de l'algorithme de réexpédition Srefresh comme décrit en RFC 2961 – RSVP-ORE, § 6.3.

7.1.16 Fonction de réexpédition d'unité LSP en commutation MPLS

La fonction de réexpédition d'unité LSP en commutation MPLS réexpédie le paquet MPLS entrant vers une interface sortante sur la base de son étiquette MPLS et de son entrée de réexpédition par étiquette de prochain bond (NHLFE, *next hop label forwarding entry*) conformément à RFC 3031.

La séquence des paquets doit être conservée à l'intérieur d'un chemin d'unités LSP.

7.1.17 Fonction de calcul de chemin d'unité LSP en commutation MPLS

La fonction de calcul d'unité LSP en commutation MPLS calcule le chemin pour une voie LSP unidirectionnelle. Cette fonction doit être en mesure de calculer des chemins pour deux voies LSP unidirectionnelles vers la même destination de façon que ces chemins ne traversent pas le même nœud ou sous-réseau.

7.1.18 Fonction d'encapsulage ("de paquet de couche Réseau vers commutation MPLS")

La fonction d'encapsulage ("de paquet de couche Réseau vers commutation MPLS") ajoute/retranche l'entrée de pile d'étiquette MPLS du paquet de couche Réseau conformément au RFC 3032.

7.1.19 Fonction de protection doublée (1+1) de paquets MPLS

7.1.19.1 Association de deux chemins LSP

Les nœuds de réception et d'émission doivent identifier et associer les deux chemins LSP fournissant le service de protection doublée de paquet. Cette association entre deux chemins LSP peut être établie soit par interface de gestion de réseau soit par signalisation.

Dans le cas de la signalisation, un identificateur doit être transféré dans chacun des divers chemins LSP. Cet identificateur doit être identique dans chacun des divers chemins LSP et doit être unique parmi les chemins LSP ouverts par le nœud de réception et parmi les chemins LSP terminés par le nœud d'émission.

Le mécanisme spécifique d'attribution de l'identificateur ainsi que la façon dont l'identificateur est transporté à l'intérieur du protocole de signalisation feront l'objet d'une étude complémentaire. Ce mécanisme sera analogue à celui qui est requis afin d'associer des chemins LSP à d'autres mécanismes en mode MPLS tels que la protection 1+1 ou 1:1.

Afin de répondre à l'exigence qu'aucune extension de signalisation n'est requise aux nœuds intermédiaires, l'identificateur et le type de service LSP (c'est-à-dire en paquets à protection doublée) doivent être transportés par des objets opaques.

7.1.19.2 Format d'identificateur de séquence

Le numéro de séquence doit être utilisé comme identificateur pour la protection doublée des paquets. Chaque exemplaire du paquet dédoublé est affecté du même numéro de séquence unique par le nœud de réception. Le numéro de séquence du paquet suivant est produit par ajout d'une unité au numéro de séquence actuel.

Le nœud d'émission utilise le numéro de séquence pour vérifier que seul le premier exemplaire reçu du paquet est sélectionné, tandis que le deuxième exemplaire reçu est rejeté. Le nœud d'émission enlève le numéro de séquence du paquet immédiatement après sa sélection et avant sa transmission à la couche supérieure de la pile. Noter que le processus de rétablissement par protection doublée est indépendant des applications/protocoles pris en charge au-dessus de la commutation MPLS.

Le numéro de séquence doit être transporté dans chaque paquet sous la forme des quatre premiers octets d'en-tête de compensation de chacun des chemins LSP offrant la protection doublée de paquet. Le numéro de séquence initial qui est attribué au premier paquet par le nœud de réception doit être convenu entre les nœuds de réception et d'émission. Sa valeur par défaut est zéro.

Le numéro de séquence est situé après les 4 octets de l'en-tête d'encapsulage MPLS comme illustré à la Figure 7-6. Noter que la protection doublée des paquets peut être assurée à un niveau hiérarchique quelconque d'un chemin d'unités LSP imbriqué.

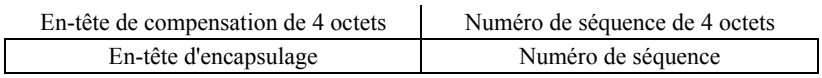


Figure 7-6/G.7712/Y.1703 – Format d'identificateur de séquence

7.2 Exigences de fourniture

Chaque élément de réseau doit accepter la création d'une interface qui n'ait aucune manifestation physique. Cette interface doit pouvoir être fournie avec une adresse IP.

La longueur des unités LSP doit être configurable.

Cela permet de fixer la longueur de l'unité MTU au sein du domaine.

La fourniture d'un identificateur de zone par interface, y compris les canaux ECC et LAN, est nécessaire pour le routage OSPF.

7.3 Exigences de sécurité

Il faut veiller à éviter des interactions intempestives (adresses, etc.) entre un réseau IP public et un RCD acceptant IP.

Annexe A[1]

Exigences pour la prise de contact à trois voies

La procédure de prise de contact à trois voies est fondée sur la fonction de prise de contact à trois voies du Groupe de travail IS-IS de l'IETF (RFC 3373) et est conçue de façon à être compatible avec cette fonction.

A.1 Nuplet TLV de contiguïté à trois voies point à point

Une fonction DCF prenant en charge les routages IS-IS intégrés doit inclure un nuplet TLV dans toutes les unités PDU de préappel IIH point à point. La structure de ce nuplet TLV doit être la suivante:

Type = 0xF0 (décimal 240)

Longueur = 5 à 17 octets

Valeur:

Etat de contiguïté à trois voies (un octet):

0 = montée

1 = initialisation

2 = descente

Identificateur de circuit local étendu, de quatre octets

Identificateur de système voisin, de zéro à huit octets si connu

Identificateur de circuit local étendu de système voisin, de quatre octets si connu

L'identificateur de circuit local étendu doit être attribué par la fonction DCF lors de la création du circuit et la fonction DCF doit utiliser une valeur différente pour chaque circuit point à point qu'elle contrôle.

L'état des trois voies de contiguïté signalé dans le TLV doit être conforme au § A.2.

A.2 Etat des trois voies de contiguïté

Une fonction DCF prenant en charge un routage IS-IS intégré pour chaque circuit point à point doit avoir un état des trois voies de contiguïté. Cet état diffère de celui qui est spécifié dans l'ISO/CEI 10589.

Si aucune contiguïté n'existe dans une liaison, l'état des trois voies de contiguïté doit être mis à la valeur "descente".

Si une fonction DCF reçoit un préappel sur une liaison point à point et qu'il en résulte la création d'une nouvelle contiguïté avec l'état de contiguïté "initialisation", cet état des trois voies de contiguïté doit être mis à la valeur "descente".

Si une fonction DCF reçoit un préappel IIH point à point qui ne contient pas de nuplet TLV des trois voies de contiguïté, cette fonction DCF doit se comporter conformément à l'ISO/CEI 10589 mais doit inclure, dans les unités PDU de préappel IIH sur cette liaison, un TLV indiquant la valeur "descente" de l'état des trois voies de contiguïté.

---

[1] NOTE – Cette nouvelle Annexe A remplace celle de la version 2001 de la Rec. UIT-T G.7712/Y.1703.

Si une fonction DCF reçoit une unité PDU de préappel point à point qui contient un TLV de contiguïté à trois voies, cette fonction DCF doit se comporter différemment du processus de traitement d'unité PDU de préappel IIH, selon l'ISO/CEI 10589, comme suit:

– si l'identificateur de système voisin et l'identificateur de circuit local étendu de système voisin du TLV sont présents et si l'identificateur de système voisin ne correspond pas à l'identificateur de la fonction DCF, ou si l'identificateur de circuit local étendu du système voisin ne correspond pas à l'identificateur étendu de la fonction DCF, l'unité PDU de préappel IIH doit être rejetée et ne doit pas être traitée;

– si l'unité PDU de préappel IIH a pour résultat que les tables d'état ISO/CEI 10589 produisent une valeur "montée" ou "accepter", et si l'état reçu des trois voies de contiguïté est "descente", alors la fonction DCF doit mettre son état des trois voies de contiguïté à la valeur "initialisation";

– si l'unité PDU de préappel IIH a pour résultat que les tables d'état ISO/CEI 10589 produisent une valeur "montée" ou "accepter" et si l'état reçu des trois voies de contiguïté est "initialisation", alors la fonction DCF doit modifier son état des trois voies de contiguïté afin de passer de la valeur "descente" ou "initialisation" à "montée" puis produire un événement "AdjacencyChangeState(Up)";

– si l'unité PDU de préappel IIH a pour résultat que les tables d'état ISO/CEI 10589 produisent une valeur "montée" ou "accepter", que l'état reçu des trois voies de contiguïté soit "initialisation" et que la fonction DCF ait déjà un état des trois voies de contiguïté de valeur "montée", cette unité doit maintenir cet état;

– si l'unité PDU de préappel IIH a pour résultat que les tables d'état ISO/CEI 10589 produisent une valeur "montée" ou "accepter", que l'état reçu des trois voies de contiguïté soit "montée" et que la fonction DCF ait déjà un état des trois voies de contiguïté de valeur "descente", cette unité produira un évènement "AdjacencyStateChange(Down)" avec la raison "voisin relancé" et la contiguïté doit être supprimée sans autre traitement d'unité PDU de préappel IIH;

– si l'unité PDU de préappel IIH a pour résultat que les tables d'état ISO/CEI 10589 produisent une valeur "montée" ou "accepter", que l'état reçu des trois voies de contiguïté soit "montée" et que la fonction DCF ait déjà un état des trois voies de contiguïté de valeur "initialisation", cette unité fera passer son état des trois voies de contiguïté à la valeur "montée" et produira un évènement "AdjacencyStateChange(Up)";

– si l'unité PDU de préappel IIH a pour résultat que les tables d'état ISO/CEI 10589 produisent une valeur "montée" ou "accepter", que l'état reçu des trois voies de contiguïté soit "montée" et que la fonction DCF ait déjà un état des trois voies de contiguïté de valeur "montée", cette unité doit maintenir cet état;

– ensuite, la comparaison de l'identificateur d'origine extrait de l'unité PDU avec l'identificateur du système local et la manipulation de l'identificateur de circuit ne doivent pas être effectuées.

Si l'unité PDU de préappel IIH a pour résultat que les tables d'état ISO/CEI 10589 produisent une valeur "montée" ou "accepter", alors la fonction DCF doit:

1) copier les entrées de contiguïté d'adresse de zone du système voisin extraites du champ d'adresses de zone de l'unité PDU;

2) régler la valeur du temporisateur de maintien dans le champ de durée de maintien extrait de l'unité PDU;

3) régler l'identificateur de système voisin à la valeur de l'identificateur d'origine extrait de l'unité PDU conformément à l'ISO/CEI 10589.

Annexe B

Exigences pour l'encapsulage automatique

B.1 Introduction

La présente annexe spécifie la fonction facultative AE-DCF qui permet à des nœuds, qui prennent en charge le routage de différents protocoles de couche Réseau incompatibles (comme CLNS, IPv4 ou IPv6), d'être présents dans une même zone de niveau 1 ou dans un même sous-domaine de niveau 2 d'un routage IS-IS. La fonction AE-DCF encapsule automatiquement un protocole de couche Réseau dans un autre protocole selon les besoins, à condition que tous les nœuds prennent en charge le routage par routage IS-IS, intégré ou non intégré.

B.2 Domaine d'application

La fonction AE-DCF est facultative. Lorsqu'elle est offerte, elle doit fonctionner comme spécifié dans la présente annexe, dont les prescriptions ne s'appliquent qu'aux fonctions DCF qui contiennent la fonctionnalité additionnelle d'encapsulage automatique (AE-DCF). Celle-ci nécessite également certains comportements de la part des fonctions DCF qui n'incluent pas la fonctionnalité AE, afin d'interfonctionner avec elles. Les exigences pour les fonctions DCF qui n'incluent pas la fonctionnalité AE se trouvent dans le § 7.1.10.1 pour les nœuds en protocoles IP et doubles, et dans l'ISO/CEI 10589 pour les nœuds en protocole OSI.

B.3 Description de la fonction AE-DCF

B.3.1 Introduction

Le routage IS-IS intégré qui est spécifié en RFC 1195 était originellement conçu pour permettre de router les protocoles IP et CLNS au moyen d'un seul protocole de routage et d'un seul algorithme SPF. Il représente à cette fin des adresses IPv4 et des masques de sous-réseau sous forme d'un nombre de 64 bits qui est ensuite traité par l'algorithme SPF comme s'il s'agissait d'adresses de système d'extrémité OSI. Les nœuds à routage IS-IS intégré sont tenus d'avoir une adresse de zone IS-IS et un identificateur de système, qui est traité de la même façon qu'une adresse de point NSAP dans un nœud à protocole OSI seulement. Les nœuds à routage IS-IS intégré forment ensuite des contiguïtés ainsi que des identificateurs et des mesures de système de déversement dans l'ensemble de leur zone de niveau 1 (routeurs de niveau 1) ou de leur sous-domaine de niveau 2 (routeurs de niveau 2), de la même façon que les nœuds IS-IS en protocole OSI-seulement.

Les identificateurs de système (SID, *system identifier*) et les mesures correspondant à d'autres identificateurs SID sont déversés dans toute une zone de niveau 1 ou tout un sous-domaine de niveau 2 au moyen d'unités d'état de liaison (LSP) qui sont communes aux nœuds à routage IS-IS aussi bien intégré que non intégré. Des informations propres au protocole IP sont ensuite ajoutées à ces unités LSP au moyen d'extensions TLV qui ne sont interprétées que par les nœuds ayant la capacité IP. Les routeurs OSI seulement ne peuvent pas décoder ces nuplets TLV mais continuent à les déverser vers toutes leurs contiguïtés. Une arborescence de routage SPF peut ainsi être construite par tout nœud à routage IS-IS intégré ou non intégré pouvant router des paquets CLNS, IPv4 ou IPv6, selon le cas. Les nœuds à capacité OSI calculeront les plus courts chemins vers les systèmes d'extrémité OSI. Les nœuds à capacité IPv4 calculeront les plus courts chemins vers des adresses ou préfixes IPv4, tandis que les nœuds à capacité IPv6 calculeront les plus courts chemins vers des adresses ou préfixes IPv6.

Une des conséquences de ce qui précède est qu'un nœud OSI seulement calculera le plus court chemin vers un système d'extrémité OSI en traversant un nœud IP seulement, bien que celui-ci ne puisse pas réexpédier les paquets CLNS. De même, un nœud IP seulement calculera le plus court chemin vers une destination IP en traversant un nœud OSI seulement, bien que celui-ci ne puisse

pas réexpédier les paquets IP. Un nœud à capacité OSI seulement ne doit donc jamais être placé dans une partie de réseau où il y ait la moindre possibilité qu'il se trouve sur le plus court chemin vers des destinations IP; et un nœud IP seulement ne doit pas être placé dans une partie du réseau où il y ait la moindre possibilité qu'il se trouve sur le plus court chemin vers un système d'extrémité OSI.

L'algorithme de routage IS-IS intégré ne peut utiliser qu'un seul algorithme de routage SPF pour au moins deux protocoles de couche Réseau en raison du principe que tous les protocoles de couche Réseau ont accès aux mêmes ressources ou, autrement dit, au même réseau avec la même topologie. Un routage IS-IS intégré implique donc que tout nœud de zone de niveau 1 ou de sous-domaine de niveau 2 soit en mesure de router tout protocole de couche Réseau présent dans la zone ou le sous-domaine, selon le cas.

C'est pourquoi le RFC 1195 impose des limitations topologiques aux réseaux qui sont routés par routage IS-IS intégré, en exigeant que tous les nœuds prennent en charge les deux protocoles IP et CLNS dans une zone contenant du trafic CLNS comme IP.

Par conséquent, conformément à RFC 1195, si un nœud réexpédie des paquets IP après remise à niveau, tous les autres nœuds contenus dans la zone de niveau 1 ou dans le sous-domaine de niveau 2 doivent également être remis à niveau.

La solution proposée ici permet de supprimer cette limitation topologique afin d'encapsuler automatiquement les paquets CLNS dans des paquets IP pour réexpédition de part et d'autre de nœuds IP seulement et d'encapsuler des paquets IP dans des paquets CLNS pour réexpédition de part et d'autre de nœuds OSI seulement. La solution proposée ici est entièrement compatible avec les nœuds OSI seulement qui existent actuellement et qui n'auront besoin d'aucune remise à niveau. Elle impose une seule exigence aux nœuds IPv4 seulement ou IPv6 seulement par rapport aux exigences de RFC 1195, à savoir la fonction de création de contiguïtés compatibles avec le protocole de couche Réseau, spécifiée au § 7.1.10.1.1.

B.3.2 Concept fondamental

Cette option tire parti du fait que tous les nœuds à routage IS-IS intégré ou non intégré partagent de la même façon des informations topologiques de base ainsi que du comportement des nœuds OSI seulement, qui essaieront de réexpédier un paquet de part et d'autre d'un nœud IP seulement et vice versa, bien que ces nœuds soient en fait incapables de réexpédier le paquet. Il en résultera normalement une perte de paquet mais une fonction AE-DCF encapsulera les paquets avant qu'ils soient réexpédiés de part et d'autre de nœuds incompatibles, de façon qu'ils ne soient pas perdus.

Lorsque deux îlots de nœuds à routage IS-IS intégré ou non intégré à capacité IP sont connectés au moyen d'un réseau central qui ne prend en charge que le protocole OSI et lorsque tous ces nœuds participent à la même zone (dans le cas de nœuds de niveau 1), alors les nœuds à capacité IP recevront les unités LSP en provenance de tous les autres nœuds à capacité IP, même de ceux de l'autre îlot, ainsi que les unités LSP en provenance de tous les nœuds IP seulement situés au centre. Ces nœuds calculeront donc les plus courts chemins entre les nœuds OSI seulement pour les destinations IP situées dans l'îlot distant. Ce n'est que lorsqu'un nœud à capacité IP réexpédie réellement un paquet IP vers un nœud OSI seulement que des erreurs se produisent et que le paquet est perdu, ce qui explique les limitations topologiques dans RFC 1195.

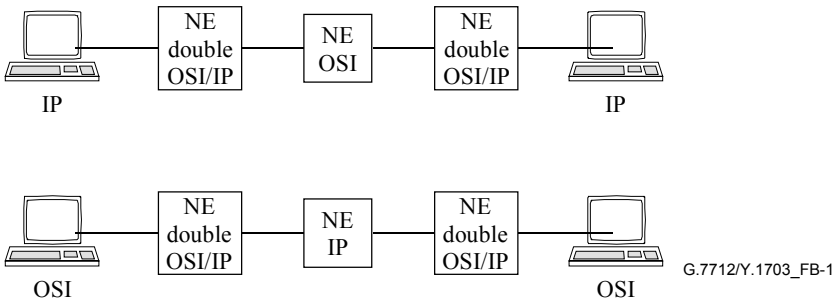


Figure B.1/G.7712/Y.1703 – Topologies illégales

Les simples réseaux décrits ci-dessus dans la Figure B.1 sont des topologies illégales aux termes du RFC 1195. Dans le réseau du haut, les paquets IP seront routés d'un bout à l'autre du réseau mais seront rejetés lorsqu'ils arriveront au nœud OSI seulement. De même, dans le réseau du bas, les paquets CLNS seront routés d'un bout à l'autre du réseau mais seront rejetés lorsqu'ils arriveront au nœud IP seulement. Une fonction AE-DCF, ici spécifiée, corrigera ce comportement.

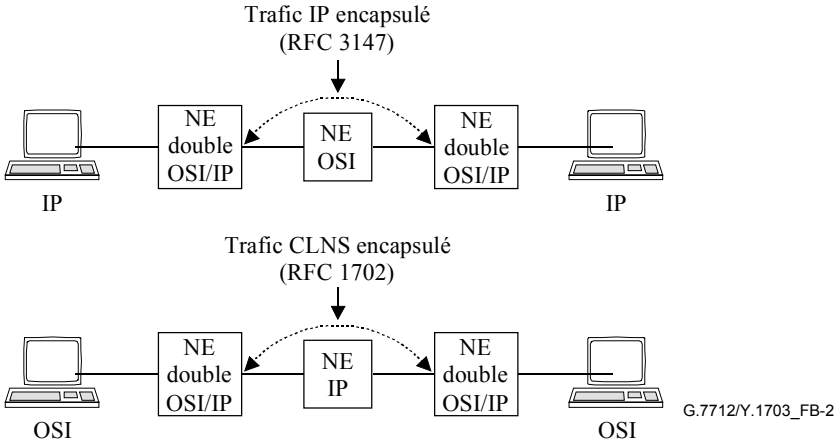


Figure B.2/G.7712/Y.1703 – "Réparation" par encapsulation

La fonction AE-DCF réside dans les nœuds à double protocole et leur permet de détecter le fait qu'un certain système voisin va rejeter un certain trafic et leur permet donc d'encapsuler ce trafic sous une forme qui ne sera pas rejetée (voir Figure B.2). Cette opération "répare" le réseau de façon que la partie du réseau qui est située entre les nœuds doubles se comporte comme si elle était composée uniquement de nœuds doubles alors qu'en fait un ou plusieurs de ses nœuds ne sont pas doubles.

Une fonction AE-DCF n'altère pas le chemin parcouru par un paquet dans le réseau: chaque paquet continuera à traverser le réseau en utilisant le plus court chemin calculé par l'algorithme SPF normal de routage IS-IS.

La fonction de création de contiguïtés compatibles avec le protocole de couche Réseau spécifiée au § 7.1.10.1.1 force le trafic à traverser des nœuds qui prennent en charge les deux protocoles, IP et OSI, chaque fois que le plus court chemin fait passer le trafic par une frontière entre parties à capacité IP et à capacité OSI d'une zone. La fonction AE-DCF permet alors à ces nœuds doubles d'encapsuler un paquet si nécessaire, de façon qu'il puisse être réexpédié par des nœuds qui ne prennent pas en charge ce protocole de couche Réseau. Cet encapsulage n'intervient que lorsqu'il est nécessaire, de sorte que ces tunnels sont créés automatiquement et sont dynamiques. Les tunnels ainsi créés ne sont jamais conservés et n'existent qu'en tant qu'entrées dans les tables de

réexpédition. En ce qui concerne le protocole de routage, les tunnels n'apparaissent ni sous forme de circuits ni sous forme d'interfaces. Les paquets continuent donc à traverser le réseau par le plus court chemin calculé normalement par chaque nœud, de sorte qu'il n'est pas nécessaire d'encapsuler les paquets IS-IS, seul le trafic IP ou CLNS étant encapsulé.

B.4 Exigences et limitations

B.4.1 Exigences pour nœuds OSI seulement

Afin d'assurer l'interfonctionnement avec la fonction AE-DCF, les nœuds OSI seulement sont tenus d'être conformes à l'ISO/CEI 10589.

B.4.2 Exigences pour nœuds à capacité IP

Afin d'assurer l'interfonctionnement avec la fonction AE-DCF, les nœuds IP seulement sont tenus d'être conformes au RFC 1195.

Les nœuds à capacité IP sont en particulier tenus d'ignorer le nuplet TLV "protocole pris en charge" dans les unités LSP des nœuds qu'ils visent comme candidats aux plus courts chemins lors de l'application de l'algorithme SPF.

Un nœud à capacité IP n'incluant que des nœuds à capacité IP dans son calcul de routage SPF ne serait pas conforme à RFC 1195, qui précise ceci:

– extrait de la page 26 de RFC 1195: "Le calcul de l'algorithme de Dijkstra ne tient pas compte du fait qu'un routeur est IP-seulement, OSI seulement ou à double protocole. Les limitations topologiques spécifiées au § 1.4 garantissent que les paquets IP ne seront envoyés que par des routeurs à capacité IP et que les paquets OSI ne seront envoyés que par des routeurs à capacité OSI".

La fonction AE-DCF est compatible avec les implémentations RFC 1195 qui sont conformes à ce qui est mentionné ci-dessus. Une implémentation qui ne comporte que des nœuds à capacité IP dans son calcul de routage SPF ne considérera pas les chemins passant par des nœuds OSI seulement comme des routes appropriées et ne tirera donc pas parti de la fonction AE-DCF.

Afin d'interfonctionner avec la fonction AE-DCF, les nœuds IP sont tenus d'être conformes au § 7.1.10.1.1, pour la raison indiquée ci-dessous:

– Cette solution dépend de la question de savoir si les paquets IP qui arrivent à un nœud OSI seulement n'ont d'abord traversé qu'une fonction AE-DCF et de la question de savoir si les paquets CLNS qui arrient à un nœud IP seulement n'ont d'abord traversé qu'une fonction AE-DCF. Celle-ci est en effet chargée d'encapsuler ces paquets de façon qu'ils puissent être réexpédiés.
– Un nœud IP seulement ne doit donc jamais avoir de contiguïté avec un nœud OSI seulement.
– Si cette solution est utilisée afin d'associer des nœuds IPv4 et IPv6 dans la même zone de niveau 1 ou dans le même sous-domaine de niveau 2, alors un nœud IPv4 seulement ne doit jamais non plus avoir de contiguïté avec un nœud IPv6 seulement.
– Cette exigence est satisfaite si tous les nœuds à capacité IP sont conformes au § 7.1.10.1.1. Noter que cette exigence n'est pas présente dans le commentaire RFC 1195.

En variante, un opérateur peut s'assurer manuellement que les nœuds qui ne prennent pas en charge un protocole de couche Réseau commun n'ont pas de contiguïtés entre eux.

B.4.3 Exigences pour nœuds doubles ou multilingues à encapsulage automatique

Si cette caractéristique doit être utilisée dans une zone de niveau 1 ou dans un domaine de niveau 2, alors les nœuds qui prennent en charge plusieurs protocoles de couche Réseau mais qui ne prennent pas en charge la fonction AE-DCF peuvent être utilisés avec précaution. Une option plus sûre consiste soit à observer les limitations topologiques du RFC 1195 soit à n'utiliser que des nœuds doubles ou multilingues qui contiennent la fonction AE-DCF.

B.4.3.1 Nuplet TLV de capacité d'encapsulage

La fonction AE-DCF inclura un nouveau nuplet TLV dans les unités LSP dont le numéro est égal à zéro. Ce nouveau TLV aura la structure suivante:

Code: 16 (décimal)
Longueur: celle de la valeur
Valeur: partie de longueur variable contenant ce qui suit:
Type de sous-TLV: 1
Longueur de sous-TLV: 3 fois le nombre de modes d'encapsulage contenu dans le sous-TLV
Valeur de sous-TLV:
47, indiquant que les deux octets suivants sont un encapsulage GRE;
l'identificateur NLPID d'un paquet qui peut être encapsulé (interne);
l'identificateur d'un paquet qui transporte le paquet encapsulé (externe);
octets 4, 5, 6: un deuxième mode d'encapsulage (si nécessaire);
octets 7, 8, 9: un troisième mode d'encapsulage (si nécessaire);
etc.

Les identificateurs NLPID utilisés sont ceux qui sont spécifiés dans la Rec. UIT-T X.263 | ISO/CEI 9577. Les nœuds qui transmettent ce nuplet TLV doivent indiquer les formats qu'un nœud peut aussi bien recevoir qu'émettre. Les nœuds doivent toujours être capables d'encapsuler comme de désencapsuler automatiquement les formats qui sont décrits dans le TLV, de façon que le trafic puisse être reçu et être renvoyé dans le sens inverse.

Il est recommandé que les nœuds doubles prenant en charge une fonction AE-DCF aient la capacité d'encapsuler/de désencapsuler A vers B et B vers A (où A et B sont les deux protocoles de couche Réseau pris en charge) afin d'offrir deux modes d'encapsulage dans un nœud double normal.

Par exemple, le contenu du nuplet TLV d'une fonction normale AE-DCF en protocoles OSI et IPv4 sera le suivant:

16: le code;
8: la longueur de valeur (dans cet exemple);
1: type 1 de sous-TLV;
6: longueur de sous-TLV (dans cet exemple);
47: les deux prochains octets sont en mode de prise en charge d'encapsulage GRE;
129: identificateur IPI pour CLNP d'après la Rec. UIT-T X.263 | ISO/CEI 9577;
204: identificateur IPI pour IPv4 d'après la Rec. UIT-T X.263 | ISO/CEI 9577;
47: les deux prochains octets sont en mode de prise en charge d'encapsulage GRE;
204: identificateur IPI pour IPv4 d'après la Rec. UIT-T X.263 | ISO/CEI 9577;
129: identificateur IPI pour CLNP d'après la Rec. UIT-T X.263 | ISO/CEI 9577.

Une fonction AE-DCF pour protocoles OSI, IPv4 et IPv6 utilisera donc, normalement, six modes d'encapsulage afin d'indiquer la transition de CLNP vers IPv4, de CLNP vers IPv6, d'IPv4 vers CLNS, d'IPv4 vers IPv6, d'IPv6 vers CLNS et d'IPv6 vers IPv4, ce qui donne une longueur de valeur égale à 20.

Ce nuplet TLV ne sera pas inclus dans les unités LSP pseudonodales.

Une fonction AE-DCF qui ne possède pas d'adresses IPv4 ne doit insérer aucun format d'encapsulage dans ses TLV de type égal à 16 contenant IPv4 comme identificateur NLPID de transport d'encapsulage (externe) tant qu'une adresse IPv4 n'est pas préconfigurée et annoncée.

Une fonction AE-DCF qui ne possède pas d'adresses IPv6 ne doit insérer aucun format d'encapsulage dans ses TLV de type égal à 16 contenant IPv6 comme identificateur NLPID de transport d'encapsulage (externe) tant qu'une adresse IPv6 n'est pas préconfigurée et annoncée.

B.4.3.2 Processus de réexpédition

Bien qu'elle ne modifie pas le chemin suivi par un paquet, la fonction AE-DCF peut calculer le plus court chemin pour un paquet IP dont le résultat sera que le prochain bond sera un nœud OSI-seulement.

Lorsque cela se produit, la fonction AE-DCF ne doit pas simplement réexpédier un paquet vers un nœud adjacent qui ne prend pas en charge ce type de protocole de couche Réseau. La fonction AE-DCF doit au contraire encapsuler le paquet à l'intérieur d'un nouveau paquet d'un type que le prochain bond prend effectivement en charge. Le critère permettant de déterminer si un nœud adjacent prend ou non en charge un protocole de couche Réseau particulier est le fait que ce protocole de couche Réseau est énuméré dans le TLV "protocoles pris en charge" contenu dans les unités PDU de préappel IS-IS reçues du nœud se trouvant à la contiguïté qui est le prochain bond pour cette destination.

Ce nouveau paquet nécessite, afin d'encapsuler le paquet initial, un protocole de couche Réseau, une adresse de destination et une adresse d'origine, comme suit:

– le protocole de couche Réseau du nouveau paquet doit être un de ceux qui sont pris en charge par le prochain bond comme défini par le TLV "protocoles pris en charge" des unités PDU de préappel reçues du prochain bond;
– l'adresse de destination du nouveau paquet doit toujours être égale à l'identité du prochain nœud sur le plus court chemin vers la destination originale qui a transmis un mode d'encapsulage contenant aussi bien le type de protocole de couche Réseau que le paquet original possède selon l'identificateur NLPID (interne) encapsulé, que le protocole de couche Réseau qui est pris en charge par le prochain bond (tel que défini par le TLV "protocoles pris en charge" des unités PDU de préappel reçues du prochain bond) selon l'identificateur NLPID (externe) de transport d'encapsulage;
– cette opération doit être réalisée au moyen d'un contrôle du nouveau TLV de type égal à 16 à partir des unités LSP reçues de chaque nœud sur le chemin vers la destination, jusqu'à ce que l'on trouve la première unité qui répond à l'exigence ci-dessus;
– lors du contrôle des nuplets TLV de type égal à 16, une fonction AE-DCF doit négliger tous les éventuels sous-TLV qu'elle ne peut pas interpréter et doit sauter au prochain sous-TLV et le contrôler jusqu'à ce qu'elle trouve tous les modes d'encapsulage qu'elle recherche ou jusqu'à ce qu'elle atteigne la fin du TLV;
– l'adresse d'origine du nouveau paquet doit toujours être égale à l'identité de la fonction AE-DCF qui construit le nouveau paquet d'encapsulage.

Si une fonction AE-DCF peut réexpédier un paquet sans encapsulage parce que le prochain bond prend en charge ce type de paquet, la fonction AE-DCF doit réexpédier ce paquet sans l'encapsuler.

Une fonction AE-DCF peut envoyer des unités LSP contenant des informations d'accessibilité IP depuis un nœud IP seulement vers un nœud à double pile ou inversement. Elle peut donc être appelée à encapsuler des paquets destinés à un nœud à double pile ou à désencapsuler des paquets reçus d'un tel nœud.

Un nœud à double pile d'encapsulage automatique doit donc suivre aussi le même processus de contrôle des unités LSP des nœuds situés entre lui-même et la destination, à la recherche d'un nœud possédant un format d'encapsulage approprié.

Noter qu'un nœud à double pile peut avoir la capacité de recevoir un paquet IPv4 encapsulé seulement dans un paquet CLNS, par exemple. Dans ce cas, le nœud à double pile ne transmettra que "CLNS" dans le champ "protocoles pris en charge" de ses paquets de préappel et n'inclura dans ses unités LSP et dans son TLV de type égal à 16 qu'un seul mode d'encapsulage. Cet unique mode d'encapsulage spécifiera "IPv4" en tant qu'identificateur NLPID (interne) de paquet encapsulé et "CLNS" en tant qu'identificateur NLPID (externe) de transport d'encapsulage.

B.4.3.3 Processus de réception

Lorsqu'une fonction AE-DCF reçoit un paquet qui lui est destiné, elle doit le contrôler afin de déterminer s'il contient un autre paquet encapsulé. Le paquet désencapsulé CLNS, IPv4 ou IPv6 résultant doit ensuite être réexpédié selon la procédure normale. Si le paquet désencapsulé résultant contient en fait un autre paquet destiné à ce nœud, le processus se répète car de multiples couches d'encapsulage peuvent nécessiter un désencapsulage par une seule fonction AE-DCF.

Les paquets de routage IS-IS ne sont pas compatibles avec les paquets IP et ne peuvent pas être réexpédiés dans l'Internet public ou dans d'autres réseaux IP-seulement. C'est un avantage de sécurité car cela rend difficile à une entité malveillante de lancer à distance des paquets IS-IS dans des nœuds de routage IS-IS intégré ou non intégré du réseau Internet public. Afin de ne pas perdre cet avantage, si un paquet IS-IS ou ES-IS arrive encapsulé dans un autre paquet destiné à une fonction AE-DCF, celle-ci doit alors le rejeter, sauf s'il provient d'un nœud avec lequel la fonction AE-DCF a préconfiguré manuellement un tunnel avec un routage IS-IS préconfiguré pour le traverser. En option, un rapport d'erreur peut être propagé afin d'informer le gestionnaire du réseau du fait qu'un tel paquet a été reçu et rejeté, de son origine, ou du fait qu'il constitue peut-être un évènement malveillant.

Tous les paquets doivent être encapsulés au moyen de la méthode d'encapsulage GRE spécifiée au § 7.1.8.

B.4.3.4 Exigences relatives à la longueur des unités MTU et à la fragmentation

L'encapsulage d'un même paquet à l'intérieur d'un autre paquet peut se traduire par un nouveau paquet qui est plus long que l'unité MTU de la liaison par laquelle ce nouveau paquet doit être réexpédié. Ce nouveau paquet d'encapsulage GRE ne doit pas être rejeté. Ces paquets ne doivent donc pas avoir le bit "ne pas fragmenter" activé s'il s'agit de paquets IPv4 et ces paquets doivent avoir le fanion "segmentation permise" activé s'il s'agit de paquets CLNS conformément au § 7.1.8.

Les paquets d'encapsulage résultants doivent donc être fragmentés avant d'être réexpédiés si leur longuer dépasse maintenant la limite de l'unité MTU de la liaison.

Il n'est pas nécessaire de fragmenter un paquet avant de l'encapsuler car le paquet d'encapsulage résultant sera fragmenté si nécessaire.

B.4.3.5 Exigences pour fonction AE-DCF avec interfaces de diffusion (LAN)

B.4.3.5.1 Processus de sélection pseudonodale

Conformément au § 7.1.10.1.1, les nœuds IP-seulement ne sont pas autorisés à former une contiguïté avec les nœuds OSI seulement et les nœuds IPv4 seulement ne sont pas autorisés à former une contiguïté avec les nœuds IPv6 seulement.

Lorsque des nœuds IP seulement et OSI seulement sont connectés au même réseau LAN dans la même zone de niveau 1 ou dans le même sous-domaine de niveau 2, les nœuds IP seulement formeront des contiguïtés les uns avec les autres et choisiront un pseudo-nœud tandis que les nœuds OSI seulement formeront des contiguïtés distinctes et choisiront un autre pseudo-nœud. Il y aura

donc deux pseudo-nœuds distincts dans le réseau LAN, l'un pour les nœuds OSI seulement et l'autre pour les nœuds IP seulement.

Un processus analogue peut se produire si des nœuds IPv4 seulement et IPv6 seulement sont connectés au même réseau LAN.

Une fonction AE-DCF doit donc participer à ces processus distincts de sélection de pseudo-nœud indépendamment pour chaque couche Réseau qu'elle prend en charge. Une fonction AE-DCF de niveau 1/niveau 2 doit participer à deux processus de sélection de pseudo-nœud pour chaque protocole de couche Réseau qu'elle prend en charge (un pour le niveau 1 et un autre pour le niveau 2).

Chaque pseudo-nœud du LAN, résidant dans un nœud de protocole de couche Réseau compatible avec la fonction AE-DCF, possédera une contiguïté avec la fonction AE-DCF. Dans un réseau LAN en protocoles IP et OSI, la fonction AE-DCF sera donc correctement celle qui possède des contiguïtés valides avec le pseudo-nœud IP et avec le pseudo-nœud OSI (si plusieurs pseudo-nœuds sont présents dans le LAN). La fonction AE-DCF possédera une contiguïté avec le pseudo-nœud IP et avec le pseudo-nœud OSI mais le pseudo-nœud IP ne possédera pas de contiguïté directe avec le pseudo-nœud OSI, et inversement. Au contraire, il n'obtiendra sa connexité qu'au moyen de la fonction AE-DCF, ce qui garantira que les paquets CLNS seront encapsulés par la fonction AE-DCF avant d'être réexpédiés vers des nœuds IP seulement, et que les paquets IP seront encapsulés par la fonction AE-DCF avant d'être réexpédiés vers des nœuds OSI seulement.

Une fonction AE-DCF à capacité IP et OSI peut être choisie comme routeur désigné par les nœuds à capacité IP dans le LAN mais ne peut l'être par les nœuds à capacité OSI. Dans ce cas, la fonction AE-DCF doit créer un pseudo-nœud; mais celui-ci ne doit déclarer les contiguïtés dans ses unités LSP qu'avec les nœuds à capacité IP du LAN.

De même, une fonction AE-DCF à capacité IP et OSI peut être choisie comme routeur désigné par les nœuds à capacité OSI dans le LAN mais ne peut l'être par les nœuds à capacité IP. Dans ce cas, la fonction AE-DCF doit créer un pseudo-nœud; mais celui-ci ne doit déclarer les contiguïtés dans ses unités LSP qu'avec les nœuds à capacité OSI du LAN.

Une fonction AE-DCF à capacité IP et OSI peut être choisie comme routeur désigné aussi bien par les nœuds à capacité IP que par les nœuds à capacité OSI dans le LAN. Dans ce cas, la fonction AE-DCF doit créer un pseudo-nœud qui déclare les contiguïtés dans ses unités LSP avec les nœuds du LAN.

En principe, une fonction AE-DCF participe à un processus de sélection distinct pour chaque protocole de couche Réseau qu'elle prend en charge. Si elle réussit à être choisie lors d'un quelconque des processus de sélection, elle crée un pseudo-nœud qui cependant ne déclarera dans ses unités LSP que les contiguïtés avec l'ensemble (les ensembles) des nœuds qui l'ont choisi.

Par conséquent, les nœuds OSI seulement ou IP seulement peuvent recevoir des unités LSP issues d'un pseudo-nœud qui énumèrent des contiguïtés qu'ils ne possèdent pas avec des nœuds du LAN. Si un paquet devait avoir besoin d'être réexpédié via un tel nœud, il devrait être envoyé au système intermédiaire désigné, conformément à l'ISO/CEI 10589, § C.2.5, point h) et conformément au commentaire RFC 1195, § C.1.4, étape 0, § 8, page 73. Noter que ces paragraphes de l'ISO/CEI 10589 et du RFC 1195 ne sont pas normatifs. Il est possible qu'il y ait des implémentations qui ne manifestent pas ce comportement. Une telle implémentation abandonnera les paquets au lieu d'envoyer le trafic vers une fonction AE-DCF pour encapsulage automatique, si cette fonction AE-DCF est le routeur désigné et s'il y a des nœuds non compatibles sur le plus court chemin du même réseau LAN.

Les réalisateurs et les opérateurs ont donc un choix à effectuer entre les deux options suivantes:

1) fixer la priorité de la fonction AE-DCF à une valeur élevée. Dans ce cas, un seul pseudo-nœud apparaîtra dans le LAN, pris en charge par une fonction AE-DCF. L'inconvénient de cette option est la faible probabilité qu'il existe déjà dans le LAN une implémentation qui ne réexpédie pas le trafic vers une fonction AE-DCF si un nœud non compatible se trouve sur le plus court chemin du LAN;

2) fixer la priorité de la fonction AE-DCF à une valeur basse. Dans ce cas, un seul pseudo-nœud apparaîtra dans le LAN pour chaque protocole de couche Réseau pris en charge, qui enverra explicitement à une fonction AE-DCF le trafic destiné à des nœuds non compatibles. Cela améliorea l'interopérabilité mais doublera le nombre d'unités LSP transmises dans le LAN, avec une éventuelle réduction de la modularité.

Il est recommandé que la priorité d'une fonction AE-DCF soit configurable par l'opérateur.

B.4.3.5.2 Processus de mise à jour des unités LSP

L'ISO/CEI 10589 indique, au § 7.3.15.1, qu'une unité LSP reçue sans provenir d'une contiguïté valide doit être rejetée. Une implémentation strictement OSI seulement rejettera donc les unités LSP qui sont transmises par un nœud IP seulement sur une interface de réseau LAN, car ce nœud IP seulement a déjà rejeté la contiguïté conformément au § 7.1.10.1.1. Le nœud OSI seulement ne pourra donc recevoir de telles unités LSP que d'une fonction AE-DCF. Sans modification de comportement, un nœud double ne réexpédiera de telles unités LSP qu'au cours de la synchronisation périodique de la base de données LSP.

Une fonction AE-DCF est donc tenue d'avoir modifié le comportement de déversement d'unités LSP de façon que les nœuds OSI seulement ou IP seulement n'aient pas besoin d'attendre le prochain événement de synchronisation de la base de données LSP.

Une fonction AE-DCF doit toujours vérifier les unités LSP entrantes qui arrivent sur les interfaces de LAN afin de déterminer si elles proviennent d'un système voisin qui prend en charge les mêmes protocoles de couche Réseau qu'elle-même. Cette vérification doit être effectuée par contrôle du TLV "protocoles pris en charge" dans les paquets de préappel reçus de ce système voisin.

Si l'unité LSP est reçue d'un voisin qui ne prend pas en charge tous les protocoles de couche Réseau que la fonction AE-DCF prend en charge, celle-ci doit se comporter conformément à l'ISO/CEI 10589 et doit désactiver le fanion SRM pour cette unité LSP à l'interface LAN si elle possède déjà l'unité LSP, ou doit la déverser à la sortie de toutes les autres interfaces si elle ne possède pas déjà l'unité LSP.

Si l'unité LSP est reçue d'un voisin qui ne prend pas en charge tous les protocoles de couche Réseau que la fonction AE-DCF prend en charge et si celle-ci ne possède pas déjà l'unité LSP, la fonction AE-DCF doit activer le fanion SRM pour cette unité LSP à l'interface LAN par laquelle l'unité LSP a été reçue, en plus de toutes les autres interfaces, ce qui a pour résultat que la fonction AE-DCF retransmet l'unité LSP dans le réseau LAN.

De cette façon, si une unité LSP est transmise sur le LAN par un nœud IP seulement, une fonction AE-DCF retransmet cette unité de façon qu'elle puisse être reçue par des nœuds OSI seulement sur une contiguïté valide du LAN et inversement.

B.4.3.5.3 Réacheminements

Si une fonction AE-DCF émet une demande de réacheminement par protocole ICMP, cette demande ne doit pas réacheminer les paquets IPv4 d'un nœud à capacité IPv4 vers un nœud sans capacité IPv4. De même, si une fonction AE-DCF émet des unités PDU de réacheminement selon l'ISO/CEI 9542, le réacheminement ne doit pas réexpédier des paquets CLNS d'un nœud à capacité OSI vers un nœud sans capacité OSI.

B.4.3.5.4 Association dans un LAN de nœuds doubles RFC 1195 et de nœuds à encapsulage automatique

Un nœud double qui est conforme au RFC 1195 mais qui ne prend pas en charge une fonction AE-DCF ne doit pas résider dans la même zone de niveau 1 ou dans le même sous-domaine de niveau 2 d'un LAN que des nœuds aussi bien IP seulement qu'OSI seulement car il peut réexpédier du trafic IP vers un nœud OSI seulement ou du trafic CLNS vers un nœud IP seulement, ce qui entraîne une perte de paquet. Il s'agit d'une limitation topologique du RFC 1195.

Un nœud double qui est conforme au RFC 1195 mais qui ne prend pas en charge une fonction AE-DCF peut résider dans la même zone de niveau 1 ou dans le même sous-domaine de niveau 3 d'un réseau LAN qu'une fonction AE-DCF.

Un tel nœud peut par ailleurs résider dans un LAN possédant un nœud OSI seulement s'il ne peut réexpédier que du trafic CLNS vers ce nœud; dans un LAN possédant un nœud IPv4 seulement s'il ne peut réexpédier que du trafic IPv4 vers ce nœud; ou dans un LAN possédant un nœud IPv6-seulement s'il ne peut réexpédier que du trafic IPv6 vers ce nœud.

B.4.4 Exigences pour nœuds à double pile d'encapsulage automatique

Un nœud à double pile émet et reçoit les paquets d'un type de protocole de couche Réseau qu'il ne peut pas réexpédier par défaut dans ses canaux DCC. La seule façon dont un tel nœud peut émettre ou recevoir de tels paquets est que ceux-ci soient sous forme encapsulée.

Cette solution est particulièrement utile pour ajouter une carte IP dans un nœud principalement OSI ou dans un nœud qui sera – par exemple – installé à l'intérieur d'un réseau OSI existant. Il pourra également être plus facile de mettre à niveau un élément de réseau de passerelle OSI afin d'en faire un nœud à double pile plutôt qu'une double fonction AE-DCF, de façon que le trafic IP puisse entrer et sortir du réseau dont ce nœud est une passerelle.

Le nœud à double pile doit pouvoir effectuer le routage interne de tous les paquets qu'il reçoit avec un protocole de couche Réseau faisant partie de ceux qui sont énumérés dans les nuplets TLV "protocoles pris en charge" de ses unités LSP de routage IS-IS.

Un nœud à double pile doit toujours utiliser le TLV "protocoles pris en charge" contenu dans les unités PDU de préappel IS-IS afin d'indiquer seulement les protocoles de couche Réseau qu'il peut recevoir et réexpédier par défaut à toute interface individuelle (ou ne jamais prendre en charge ce TLV s'il s'agit d'une interface OSI seulement).

En d'autres termes, un nœud IP-sur-OSI peut router par défaut des paquets CLNS dans ses canaux DCC et peut router le trafic IP qui arrive pour lui par des paquets IP-sur-OSI à encapsulage GRE, ou éventuellement par une interface Ethernet.

Un nœud à double pile peut donc indiquer un seul protocole de couche Réseau dans le TLV "protocoles pris en charge" de certains paquets de préappel à une interface donnée, et indiquer un autre protocole de couche Réseau dans le TLV "protocoles pris en charge" de certains paquets de préappel à une autre interface. Un tel nœud sera en mesure d'effectuer le routage interne des deux protocoles de couche Réseau et l'annoncera dans les TLV "protocoles pris en charge" de ses unités LSP.

Un nœud à double pile doit toujours utiliser des TLV d'accessibilité IP dans les unités LSP de routage IS-IS afin d'indiquer l'étendue d'adressage des paquets encapsulés qu'il est en mesure de recevoir.

Un nœud à double pile peut recevoir des extensions d'accessibilité IP en provenance d'un nœud IP-seulement via une double fonction AE-DCF. Le nœud à double pile doit donc être en mesure d'envoyer du trafic vers une fonction AE-DCF qu'il utilisera afin d'encapsuler ses paquets. A cette fin, un nœud à double pile doit toujours rechercher, sur le chemin vers chaque destination, le

prochain nœud capable d'effectuer le désencapsulage ou rechercher une destination à double pile, exactement comme le fait une fonction AE-DCF.

Un nœud à double pile d'encapsulage automatique doit annoncer les modes d'encapsulage qu'il prend en charge, au moyen du TLV de capacité d'encapsulage indiqué au § B.4.3.1.

Lorsqu'un nœud à double pile reçoit un paquet qui lui est destiné, il doit contrôler ce paquet afin de vérifier s'il comporte un autre paquet encapsulé. Si c'est le cas, le paquet subira un traitement interne, à moins qu'il ne s'agisse d'un paquet IS-IS ou ES-IS, auquel cas il doit être rejeté (à moins qu'un tunnel ait été préconfiguré manuellement avec un routage IS-IS préconfiguré pour le traverser) comme le ferait une double fonction AE-DCF.

Comme le ferait une double fonction AE-DCF, un nœud à double pile doit prendre en charge l'encapsulage GRE conformément au § 7.1.8.

B.4.5 Utilisation avec la fonction AE-DCF de nœuds IP non conformes au § 7.1.10.1.1

Les nœuds IPv4 seulement ou IPv6 seulement qui sont conformes au RFC 1195 mais qui ne prennent pas en charge la fonction de création de contiguïtés compatibles avec le protocole, spécifiée au § 7.1.10.1.1, peuvent être utilisés comme fonction AE-DCF mixte dans la même zone de niveau 1 ou dans le même sous-domaine de niveau 2 mais le gestionnaire du réseau doit toujours s'assurer manuellement qu'un tel nœud ne possède pas de contiguïtés avec d'autres nœuds qui pourraient lui réexpédier des paquets qu'il ne prend pas en charge.

B.4.6 Utilisation dans la même zone IS-IS de nœuds doubles sans fonction AE-DCF et de nœuds doubles avec fonction AE-DCF

Les nœuds doubles qui sont conformes au RFC 1195 mais qui ne prennent pas en charge de fonction AE-DCF peuvent être utilisés à titre mixte avec une fonction AE-DCF dans les zones de niveau 1 et dans les sous-domaines de niveau 2 avec les restrictions suivantes.

Les nœuds (ou grappes de nœuds) de routage IS-IS intégré qui prennent en charge plusieurs protocoles de couche Réseau mais qui ne prennent pas en charge une fonction AE-DCF restent soumis aux limitations topologiques du RFC 1195. En d'autres termes, le gestionnaire du réseau doit s'assurer qu'un tel nœud ne peut pas transmettre de paquets à un nœud voisin qui n'a pas la capacité de réexpédier ce type de paquet.

Dans les combinaisons suivantes, le terme "double" désigne un nœud double de routage IS-IS intégré qui est conforme au RFC 1195 mais qui ne contient pas de fonction AE-DCF:

OSI-AEDCF-double-AEDCF-IP est une combinaison sûre;

OSI-AEDCF-double-double-double-AEDCF-IP est une combinaison sûre;

IPv4-AEDCF-double IPv4&IPv6-AEDCF-IPv6 est une combinaison sûre;

double-AEDCF-OSI-AEDCF-double est une combinaison sûre;

OSI-IPv4&OSIAEDCF-double IPv4&OSI-double IPv4&IPv6-IPv4&IPv6 AEDCF-IPv6 n'est pas une combinaison sûre;

OSI-IPv4&OSIAEDCF-double IPv4&OSI-IPv4&IPv6&OSI-double IPv4&IPv6-IPv4&IPv6 AEDCF-IPv6 n'est pas une combinaison sûre.

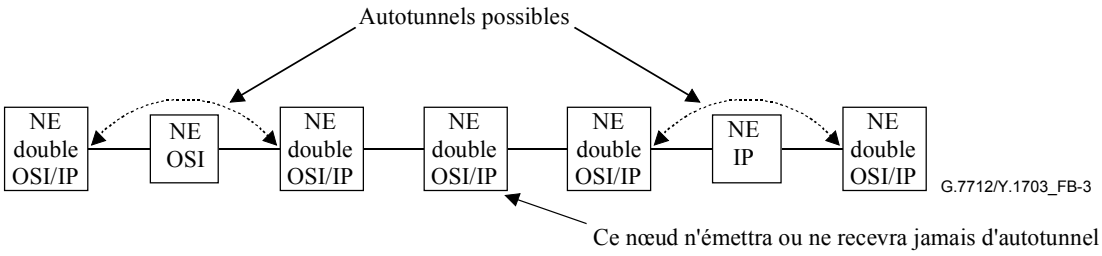


Figure B.3/G.7712/Y.1703 – Prescriptions topologiques pour les nœuds doubles de routage IS-IS

B.4.7 Exigences pour nœuds de niveau 1, niveau 2

Il est recommandé que les nœuds, qui prennent en charge le routage aux deux niveaux 1 et 2, et qui sont présents dans une zone où des fonctions AE-DCF sont utilisées, prennent en charge:

– soit tous les protocoles de couche Réseau qui sont présents dans les sous-domaines des deux niveaux 1 et 2 auxquels ces nœuds participent et qu'ils prennent en charge une fonction AE-DCF;

– tous les protocoles de couche Réseau qui sont présents dans les sous-domaines des deux niveaux 1 et 2 auxquels ces nœuds participent et qu'ils soient connectés, soit directement ou par l'intermédiaire de chaînes continues d'autres nœuds prenant en charge tous les protocoles de couche Réseau dans la zone, à un nœud prenant en charge une fonction AE-DCF et tous les protocoles de couche Réseau dans la zone.

Dans les combinaisons suivantes, le terme "double" désigne un nœud double de routage IS-IS intégré qui est conforme au RFC 1195 mais qui ne prend pas en charge de fonction AE-DCF:

sous-domaine L2-double L1/L2-non double est une combinaison sûre (conformément au RFC 1195);

sous-domaine L2-double L1/L2-double-double-non double est une combinaison sûre (conformément au RFC 1195);

sous-domaine L2-double L1/L2-AE-DCF-réseau mixte est une combinaison sûre;

sous-domaine L2-double L1/L2-double-double-AE-DCF-réseau mixte est une combinaison sûre;

sous-domaine L2-double L1/L2-non double-double n'est pas une combinaison sûre (à moins que les limitations RFC 1195 ne soient appliquées);

sous-domaine L2-double L1/L2-non double-AE-DCF n'est pas une combinaison sûre (à moins que les limitations RFC 1195 ne soient appliquées).

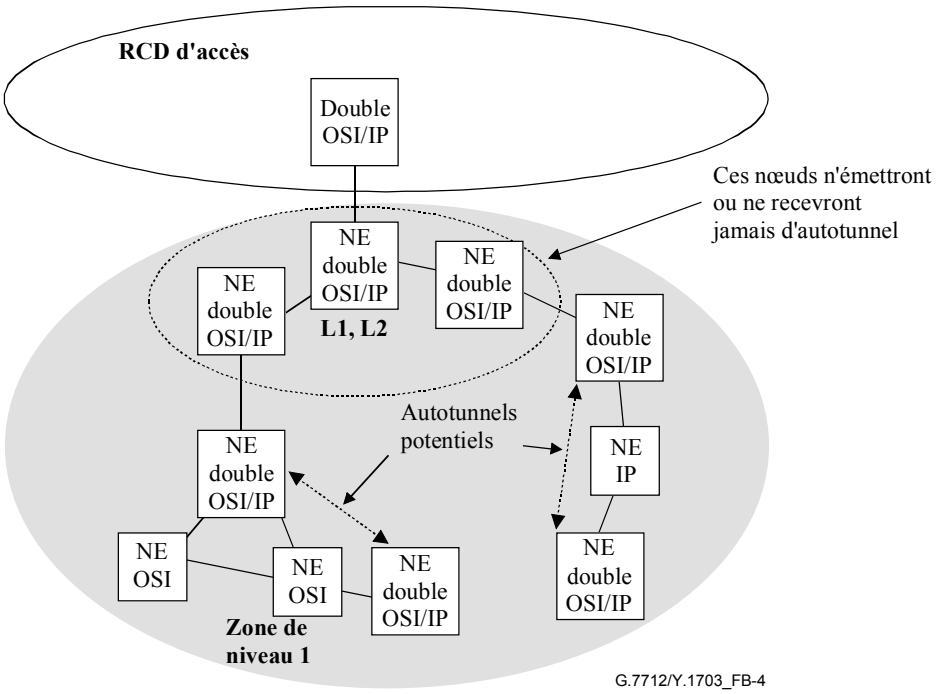


Figure B.4/G.7712/Y.1703 – Prescriptions pour les nœuds de niveau 1 et de niveau 2

Il est toutefois admis qu'un élément NE de passerelle et donc un routeur de niveaux L1, L2 peut être un dispositif OSI seulement existant. Dans ce cas, il est possible d'avoir le protocole IP et l'encapsulage automatique dans la zone en utilisant la méthode suivante, avec précaution.

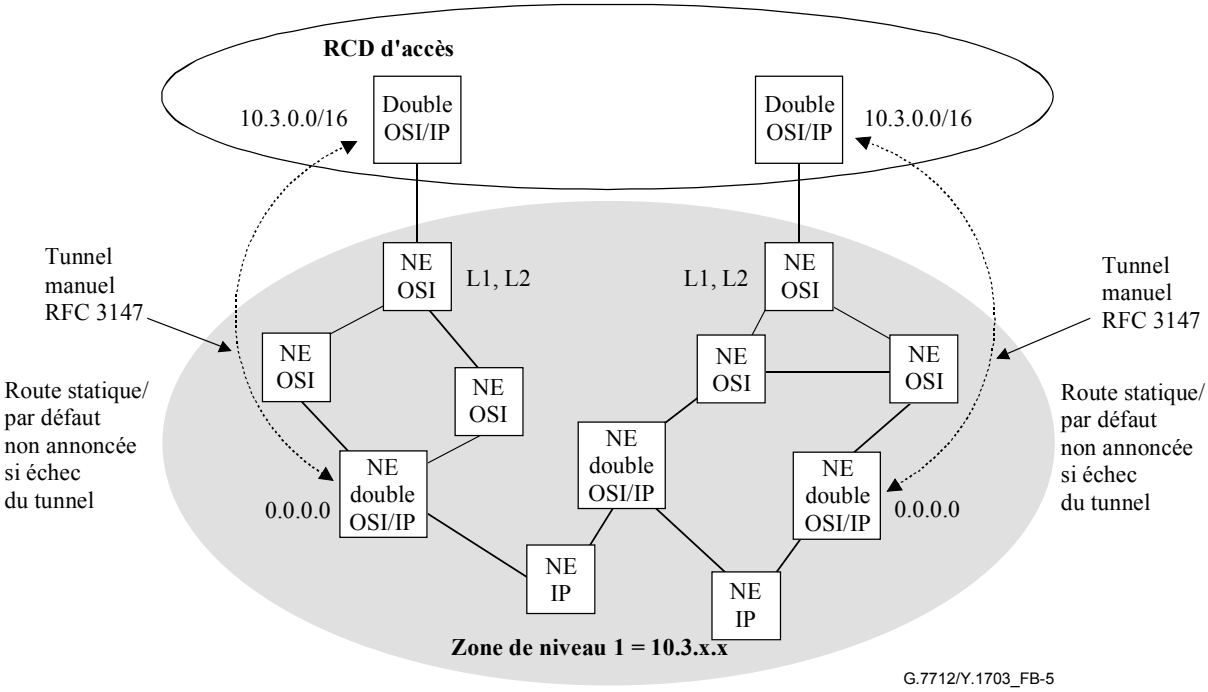


Figure B.5/G.7712/Y.1703 – Utilisation d'un dispositif OSI seulement comme passerelle

Un ou plusieurs nœuds doubles de la zone peuvent être choisis comme passerelles pour des paquets IP. Ces nœuds seront configurés de façon à annoncer une route par défaut (0.0.0.0) dans la zone, afin d'attirer vers eux tout le trafic IP "hors zone". Ces nœuds réexpédieront ensuite tout le trafic "hors zone" au moyen d'un tunnel GRE préconfiguré manuellement et passant par un nœud OSI seulement de niveau 1, niveau 2 vers un autre nœud situé à l'extérieur de la zone.

Le nœud double qui se trouve à l'extérieur de la zone doit toujours comporter un préfixe préconfiguré manuellement afin d'attirer à lui tout le trafic IP destiné à la zone et de l'envoyer dans le tunnel de cette zone. En option, un mécanisme comme un protocole de routage IP peut être préconfiguré dans le tunnel de façon que chaque extrémité puisse vérifier si l'autre est encore active. Si toutefois un routage IS-IS intégré est utilisé, il faut que ce soit une instance de routage différente de celle qui est généralement utilisée dans la zone car il s'agit alors en fait d'un domaine de routage différent.

Si un tel mécanisme est utilisé et que l'extrémité distante disparaisse, le nœud double situé à l'intérieur de la zone devra arrêter d'annoncer une route par défaut et le nœud double situé à l'extérieur de la zone devra arrêter d'annoncer le préfixe qui représente les nœuds dans cette zone, ce qui permettra de préconfigurer des passerelles IP redondantes.

Noter que le commentaire RFC 1195 indique que des routes par défaut ne devraient pas être annoncées dans les unités LSP de niveau 1. Cette solution nécessite que ce comportement soit effacé par recouvrement dès réception d'une annonce de route par défaut dans une unité LSP de niveau 1. Si cela n'est pas possible, une autre solution consiste à configurer les nœuds de passerelle IP avec une sélection de routes statiques couvrant toutes les destinations "hors zone" possibles qu'une pile IP est susceptible d'essayer d'atteindre dans la zone.

B.4.8 Exigences pour le sous-domaine de niveau 2

Il est acceptable que tous les protocoles présents par défaut dans le sous-domaine de niveau 2 soient routés conformément au RFC 1195, auquel cas aucun des nœuds de niveau 2 n'a besoin de prendre en charge une fonction AE-DCF. Mais ils doivent tous prendre en charge tous les protocoles de couche Réseau présents.

En variante, il est acceptable que l'on utilise des nœuds de niveau 2 ne prenant pas en charge la totalité des protocoles de couche Réseau présents dans le domaine, auquel cas les nœuds doubles ou multilingues de niveau 2 seront tenus de prendre en charge une fonction AE-DCF de façon que les paquets puissent être automatiquement encapsulés et puissent traverser de tels nœuds.

Appendice I[2]

Contraintes des fonctions d'interfonctionnement dans le RCD

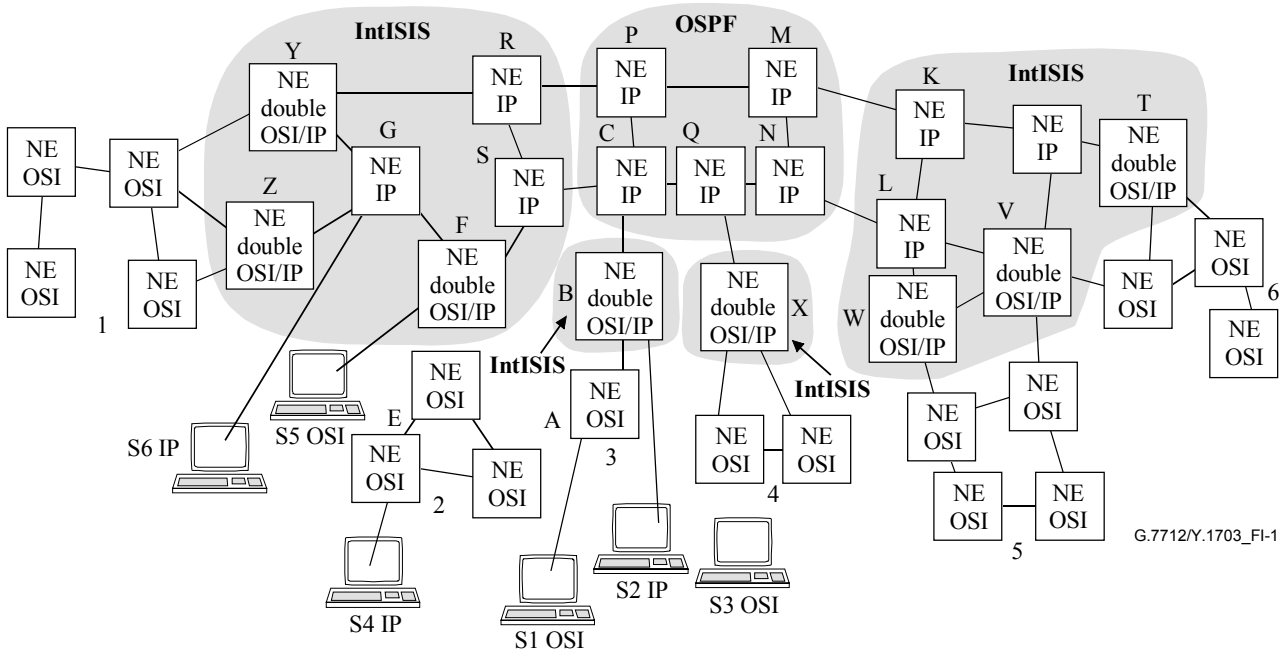


Figure I.1/G.7712/Y.1703 – Scénarios d'interfonctionnement

I.1 Hypothèses générales

Le RCD couvre la fonction IWF pour les couches 2-3 des piles IP-OSI. Les mécanismes d'interfonctionnement qui s'appliquent aux autres couches sont en dehors du domaine d'application de la présente Recommandation (c'est-à-dire, médiation).

Voir le § 7.1.7 pour une définition de l'interfonctionnement.

Les tunnels sont fondés sur les RFC.

Les éléments de réseau IP seulement acceptent le routage IP et peuvent contenir une redistribution entre routage IS-IS intégré et routage OSPF.

I.2 Elément commun à tous les scénarios

Le routage dynamique est accompli par redistribution des routes des informations d'adresse IP entre les éléments de réseau OSPF et IS-IS. La redistribution des routes est préformée sur les nœuds OSPF entre les paires (R,P), (S,C), (M,K), (N,L).

I.2.1 Scénario 1: système de gestion de type OSI connecté au nœud A

Il doit y avoir au moins un tunnel configuré de B à l'un au moins de Y ou Z.

Il doit y avoir un tunnel configuré de B à X.

Il doit y avoir un tunnel configuré de B à F.

Il doit y avoir au moins un tunnel configuré de B à l'un au moins de W, V ou T.

---

[2] NOTE – Le nouvel Appendice I remplace celui de l'édition 2001 de la Rec. UIT-T G.7712/Y1703.

Les tunnels ci-dessus auront probablement un routage IS-IS les traversant (à l'intérieur du tunnel). Des techniques de routage interdomaniales sont également possibles. Dans certaines conditions, certains tunnels pourraient subir des encombrements par suite des choix de routage effectués.

Un système de gestion de type OSI a maintenant la connexité CLNS avec tout élément de réseau OSI seulement ou à double pile du réseau, mais il n'a pas la connexité avec les éléments de réseau IP seulement. Bien qu'un gestionnaire de type OSI soit à même d'envoyer des paquets CLNS à un élément de réseau à double pile, il ne sera pas capable de le traiter à moins qu'il ne soit gérable en protocole OSI.

I.2.2 Scénario 2: systèmes de gestion de type IP connectés au nœud B

Dans ce réseau particulier, le trafic IP peut être renvoyé de B à tous les éléments de réseau IP sans qu'il y ait besoin de tunnels. Les éléments de réseau OSPF P, C, M et N doivent accepter la redistribution des routes IP en routage IS-IS intégré. Des filtres devront être configurés sur les nœuds OSPF P, C, M et N afin d'arrêter la formation de boucles de routage.

Un système de gestion de type IP a maintenant la connexité IP avec tout élément de réseau IP seulement ou à double pile dans le réseau, mais n'a pas la connexité avec les éléments de réseau OSI seulement. Bien qu'un gestionnaire de type IP soit à même d'envoyer des paquets IP à un élément de réseau à double pile, il ne sera pas capable de le traiter à moins qu'il ne soit gérable en protocole IP.

I.2.3 Scénario 3: systèmes de gestion de type OSI connectés au nœud C

L'élément de réseau C ne peut pas assurer la connexité OSI et les paquets CLNS ne peuvent donc pas être réexpédiés, de sorte qu'un système de gestion de type OSI ne peut pas fonctionner sur un tel site.

I.2.4 Scénario 4: systèmes de gestion de type IP connectés au nœud E

L'élément de réseau E ne peut pas assurer la connexité IP et les paquets IP ne peuvent donc pas être réexpédiés, de sorte qu'un système de gestion de type IP ne peut pas fonctionner sur un tel site.

I.2.5 Scénario 5: systèmes de gestion de type OSI connectés au nœud F

Le trafic CLNS peut passer à travers un élément de réseau F vers un réseau 2 en protocole OSI sans qu'il y ait besoin de tunnels car l'élément de réseau F peut par défaut réexpédier les paquets CLNS.

Un tunnel doit être configuré de F à B.

Il doit y avoir au moins un tunnel configuré de F vers l'un au moins de Z ou Y.

Il doit y avoir un tunnel configuré de F à X.

Il doit y avoir au moins un tunnel configuré de F vers l'un au moins de W, V ou T.

Les tunnels ci-dessus auront probablement un routage IS-IS les traversant (à l'intérieur du tunnel). Cependant des techniques de routage interdomaniales sont également possibles. Dans certaines conditions, certains tunnels pourraient subir des encombrements par suite des choix de routage effectués.

Un système de gestion de type OSI a maintenant la connexité CLNS avec tout élément de réseau OSI seulement ou à double pile dans le réseau, mais n'a pas la connexité avec les éléments de réseau IP seulement. Bien qu'un gestionnaire de type OSI soit à même d'envoyer des paquets CLNS à un élément de réseau à double pile, il ne sera pas capable de le traiter à moins qu'il ne soit gérable par l'OSI.

I.2.6 Scénario 6: systèmes de gestion de type IP connectés au nœud G

Dans ce réseau particulier, le trafic IP peut être renvoyé de G à tous les éléments de réseau IP sans qu'il y ait besoin de tunnels. Les éléments de réseau OSPF P, C, M et N doivent accepter la redistribution des routes IP par routage IS-IS intégré. Des filtres devront être configurés sur les nœuds OSPF P, C, M et N afin d'arrêter la formation de boucles de routage.

Un système de gestion de type IP a maintenant la connexité IP avec tout élément de réseau IP seulement ou à double pile dans le réseau, mais n'a pas la connexité avec les éléments de réseau OSI seulement. Bien qu'un gestionnaire de type IP soit à même d'envoyer des paquets IP à un élément de réseau à double pile, il ne sera pas capable de le traiter à moins qu'il ne soit gérable en protocole IP.

Appendice II

Exemple d'implémentation d'un encapsulage automatique

II.1 Introduction

Le présent appendice n'est pas normatif mais donne quelques détails à titre d'exemple sur la façon dont un nœud peut être mis en œuvre dans le cadre d'une des caractéristiques spécifiées dans la présente Recommandation.

La plus simple (mais non la seule) façon pour un nœud de calculer le prochain nœud sur le plus court chemin jusqu'à la destination finale d'un paquet capable d'encapsuler consiste à modifier l'algorithme SPF à cette fin.

L'algorithme peut être modifié afin de trouver, sur le plus court chemin vers la destination, le prochain nœud qui puisse accepter le trafic IP encapsulé sur OSI, ainsi que, sur le plus court chemin vers la destination, le prochain nœud qui puisse accepter le trafic OSI encapsulé sur IP. Noter que ces deux nœuds peuvent être confondus ou distincts. Un algorithme de Dijkstra est indiqué ci-après à cette fin.

Ce processus additionnel n'a besoin d'intervenir que lorsque le prochain bond ne prend pas en charge le protocole de couche Réseau du type qui correspond à l'adresse de destination pour ce chemin. Si le prochain bond prend effectivement en charge ce type de protocole de couche Réseau (tel que spécifié dans le TLV "protocoles pris en charge" présent dans les unités PDU de préappel de routage IS-IS reçues de ce nœud), alors les paquets allant vers cette destination peuvent simplement être réexpédiés par défaut puis oubliés, de sorte qu'il n'est pas nécessaire de rechercher sur le chemin de nœud à capacité d'encapsulage.

L'algorithme doit ensuite identifier une adresse IP pour ce prochain nœud d'encapsulage si la destination du chemin est un système d'extrémité OSI; et doit ensuite identifier une adresse OSI pour ce prochain nœud d'encapsulage si la destination du chemin est une adresse IP.

L'impossibilité de trouver une adresse IP pour ce prochain nœud d'encapsulage indique une erreur de configuration dans ce nœud (absence d'adresse IP), ce qui peut éventuellement se traduire par l'envoi d'un message d'erreur à l'administrateur du réseau. Une perte de paquet en résultera si un paquet CLNS nécessite une tunnellisation vers ce nœud par encapsulage sur IP car, sans adresse IP de destination, l'encapsulage sera sans doute impossible et le paquet sera au contraire rejeté.

L'impossibilité de trouver un nœud à capacité d'encapsulage indique une erreur de conception du réseau et plus précisément une impossibilité de respecter les limitations topologiques indiquées dans la présente Recommandation. Il devrait en résulter un compte rendu d'erreur de type "destination inaccessible".

Pour chaque destination IP qui nécessite un encapsulage afin d'aller au-delà du prochain bond, le nœud peut ensuite placer un marqueur dans la table de réexpédition IP afin d'indiquer l'adresse OSI de destination qui doit être utilisée afin d'encapsuler tous les paquets IP destinés à cette adresse.

Pour chaque destination OSI qui nécessite un encapsulage afin d'aller au-delà du prochain bond, le nœud peut ensuite placer un marqueur dans la table de réexpédition OSI afin d'indiquer l'adresse IP de destination qui doit être utilisée afin d'encapsuler tous les paquets OSI destinés à cette adresse.

Un nœud qui prend en charge les protocoles IPv4, IPv6 et OSI peut trouver deux adresses (par exemple une adresse IPv4 et une adresse IPv6) pouvant servir à encapsuler des paquets. Dans ce cas, ce nœud peut choisir l'une ou l'autre adresse du moment qu'il en résulte un paquet dont le type de protocole de couche Réseau est pris en charge par le prochain bond (comme spécifié dans le TLV "protocoles pris en charge" présent dans ses unités PDU de préappel de routage IS-IS reçues de ce nœud).

II.2 Mises à jour de l'algorithme de Dijkstra

Les paragraphes suivants contiennent l'ensemble de l'algorithme de Dijkstra y compris ses extensions de prise en charge de l'autotunnellisation. Il est fondé sur l'algorithme spécifié en RFC 1195. L'algorithme indiqué convient pour un nœud double IPv4 et CLNS à encapsulage automatique. Les modifications apportées à cet algorithme sont reproduites en caractères ***italiques gras***.

L'algorithme produit une base de données "PATHS" contenant, pour chaque destination, l'identité du premier nœud de S à N ayant la capacité d'encapsuler IP sur OSI, ainsi que l'identité du premier nœud de S à N ayant la capacité d'encapsuler OSI sur IP.

Pour chaque destination IP, le premier nœud de S à N ayant la capacité d'encapsuler IP sur OSI peut avoir son adresse OSI chargée dans la table de réexpédition IP en tant qu'adresse de destination à utiliser dans tout paquet CLNP utilisé afin d'encapsuler IP sur OSI, si le prochain bond ne prend pas en charge le protocole IP.

Pour chaque système d'extrémité OSI, le premier nœud de S à N ayant la capacité d'encapsuler OSI sur IP peut avoir une de ses adresses OSI chargée dans la table de réexpédition OSI en tant qu'adresse de destination à utiliser dans tout paquet IP utilisé afin d'encapsuler OSI sur IP, si le prochain bond ne prend pas en charge le protocole OSI.

II.2.1 Modifications apportées à la base de données

Il y a lieu de mettre à jour les bases de données PATHS et TENTS afin qu'elles contiennent une extension de l'élément {Adj(N)} du triplet. L'élément de contiguïté N contiendra deux entrées correspondantes de double prise en charge de protocoles (IDP(N)-ODP(N)) qui représenteront l'identificateur de système du premier double routeur sur le chemin de S à N ayant la capacité de désencapsuler les paquets tunnellisés IP sur OSI (IDP(N)) et qui représenteront l'identificateur de système du premier double routeur sur le chemin de S à N ayant la capacité de désencapsuler les paquets tunnellisés OSI sur IP (ODP(N)). Si aucun routeur *DP(N) n'existe sur le chemin PATH, alors cette valeur est mise à zéro. Si de multiples entrées Adj(N) existent dans la base de données TENTS ou PATHS, alors chaque contiguïté aura les entrées *DP(N) correspondantes. Chaque triplet prendra donc la forme <N,d(N),{Adj(N)-IDP(N)-ODP(N)}>.

Si la valeur de l'entrée IDP(N) est mise à 0, cela signifie qu'aucun double routeur n'existe sur le chemin vers la destination, ayant la capacité de désencapsuler et d'encapsuler des paquets IP sur OSI.

Si la valeur de l'entrée ODP(N) est mise à 0, cela signifie qu'aucun double routeur n'existe sur le chemin vers la destination, ayant la capacité de désencapsuler et d'encapsuler des paquets OSI sur IP.

II.2.2 Modifications apportées à l'algorithme

L'algorithme SPF spécifié au § C.1.4 de RFC 1195 est modifié comme suit.

Etape 0: initialiser les bases de données TENTS et PATHS à la valeur "vide". Initialiser la longueur "tentlength" à la valeur:
[internalmetric=0, externalmetric=0].

("tentlength" est la longueur de chemin des éléments contenus dans la base TENT que l'on examine.)

1) Ajouter à la base PATHS <SELF,0,W***-0-0***> où W est une valeur spéciale indiquant que le trafic vers SELF est communiqué à des processus internes (au lieu d'être réexpédié).

2) Précharger ensuite la base TENT avec la base de données de contiguïtés locales (chaque entrée dans TENT doit être marquée comme étant soit un système d'extrémité soit un routeur afin que l'on puisse effectuer correctement une vérification à la fin de l'étape 2 – Noter que chaque entrée d'accessibilité IP locale est incluse en tant que contiguïté et est marquée comme étant un système d'extrémité). Pour chaque contiguïté Adj(N) (y compris les contiguïtés manuelles OSI de niveau 1, ou les adresses OSI accessibles de niveau 2 activées, et les entrées d'accessibilité IP) sur des circuits activés, calculer pour le système N de SELF dans l'état "Montée":

   d(N) = coût du circuit parent de la contiguïté (N), obtenu à partir de l'objet métrologique "metric.k", où k = un des mesures suivantes: {mesure par défaut, mesure de délai, mesure monétaire, mesure d'erreur}.

   Adj(N)***-IDP(N)-ODP(N)*** = numéro de contiguïté de la contiguïté à N, ***l'identificateur du routeur de prochain bond sur le chemin vers le système voisin ayant la capacité de désencapsuler les paquets IP sur OSI et l'identificateur du routeur de prochain bond sur le chemin vers le système voisin ayant la capacité de désencapsuler les paquets OSI sur IP. Dans ce cas, c'est-à-dire au cours de l'initialisation, les deux valeurs DP seront mises à 0***

3) Si la base TENT contient un triplet <N,x,{Adj(M)***-IDP(N)-ODP(N)***}>, alors:

   Si x = d(N), alors {Adj(M)***-IDP(N)-ODP(N)***} <--- {Adj(M)***-IDP(M)-ODP(M)***}

   U {Adj(N)***-IDP(N)-ODP(N)***}.

4) Si N est un routeur ou une entrée de système d'extrémité OSI, et s'il y a maintenant plus de contiguïtés dans l'élément {Adj(M)} que la valeur "maximumPathSplits", alors supprimer les contiguïtés excédentaires comme décrit au § 7.2.7 de l'ISO/CEI 10589. Si N est une entrée d'accessibilité IP, alors les contiguïtés excédentaires peuvent être supprimées à volonté. Cela n'aura pas d'incidence sur le bien-fondé du routage mais pourra éliminer le déterminisme pour les routes IP (c'est-à-dire que les paquets continueront à suivre des routes optimales dans une zone mais, si plusieurs routes de même valeur existent, les paquets ne suivront pas nécessairement la route qu'un routeur particulier aura anticipée).

5) Si x < d(N), ne rien faire.

6) Si x > d(N), supprimer <N,x,{Adj(M)***-IDP(M)-ODP(M)***}> de TENT et ajouter le triplet <N,d(N),{Adj(N) ***-IDP(N)-ODP(N)***}>.

7) Si aucun triplet <N,x,{Adj(M)***-IDP(M)-ODP(M)*** }> ne se trouve dans TENT, ajouter <N,d(N),{Adj(N)***-IDP(N)-ODP(N)***}> à la base TENT.

8) Ajouter ensuite les systèmes avec lesquels le routeur local n'a pas de contiguïtés mais qui sont mentionnés dans les unités LSP de pseudo-nœuds voisins. La contiguïté avec de tels systèmes est réglée sur celle du routeur désignée. Noter que cela ne vise pas les entrées d'accessibilité IP issues d'unités LSP pseudonodales voisines qui, de toute façon, n'en contiennent pas.

9) Pour tous les circuits de diffusion à l'état "Actif", trouver l'unité LSP pseudonodale pour ce circuit (spécifiquement, l'unité LSP de numéro zéro dont les 7 premiers octets d'identificateur LSPID sont égaux à l'identificateur LnCircuitID pour ce circuit, où n est égal à 1 (pour le routage de niveau 1) ou à 2 (pour le routage de niveau 2). Si cette unité est présente, ajouter pour tous les systèmes voisins N, signalés dans toutes les unités LSP de ce pseudo-nœud mais qui n'existent pas dans la base TENT, une entrée <N,d(N),{Adj(N)***-IDP(N)-ODP(N)***}> où:

   d(N) = valeur "metric.k" du circuit.

   Adj(N) = numéro de la contiguïté avec le DR

10) Passer à l'étape 2

Etape 1: examiner l'unité LSP de numéro 0 de P, qui est le système situé exactement sur PATHS (c'est-à-dire l'unité LSP ayant les mêmes 7 premiers octets de LSPID que P et le numéro zéro).

1) Si cette unité LSP est présente et que le bit de "coût de rebonds infinis" est désactivé pour chaque paire Adj(*) – IDP(*) – ODP(*) dans la base de données PATHS pour le système P. S'il ne s'agit pas d'une unité LSP pseudonodale et si IDP(*) est égal à zéro, vérifier le champ de capacité d'encapsulage de cette unité LSP: si elle prend en charge le routage IP sur OSI, alors régler la valeur IDP(P) de cette contiguïté comme étant l'identificateur du système P. Si ODP(*) est égal à zéro, vérifier le champ de capacité d'encapsulage de cette unité LSP: si elle prend en charge le routage OSI sur IP, alors régler la valeur IDP(P) de cette contiguïté comme étant l'identificateur du système P.

2) Si cette unité LSP est présente et si le bit "coût de rebonds infinis" est désactivé, alors pour chaque unité LSP du système P (c'est-à-dire toutes les unités LSP ayant les mêmes 7 premiers octets de LSPID que P, quelle que soit la valeur du numéro d'unité LSP, calculer:

   dist(P, N) = d(P) + metric.k(P, N)

pour chaque système voisin N (système d'extrémité avec routeur) du système P. Si le bit "coût de rebonds infinis" est activé, ne considérer que les systèmes d'extrémité voisins du système P.

Noter que les systèmes d'extrémités voisins du système P contiennent les entrées d'adresses IP accessibles se trouvant dans les unités LSP issues du système P. Ici, d(P) est le deuxième élément du triplet suivant.

   <P,d(P),{Adj(P)***-IDP(P)-ODP(P)***}>

et "metric.k(P, N)" est le coût de la liaison de P à N comme indiqué dans l'unité PDU d'état de liaison (LSP) du système P.

3) Si dist(P, N) > MaxPathMetric, ne rien faire.

4) Si le triplet <N,d (N),{Adj (N) ***– IDP(N)-ODP(N)***}> se trouve dans la base PATHS, ne rien faire.

   NOTE – d(N) doit toujours être inférieur à dist(P,N), sinon N n'aurait pas été placé dans la base PATHS. Un contrôle de rectitude additionnel peut être effectué ici afin de vérifier que d(N) est en fait inférieur à dist(P,N)

5) Si un triplet <N,x,{Adj(N)***-IDP(N)-ODP(N)***}> se trouve dans TENT, alors:

   a) Si x = dist(P,N), alors {Adj(N), ***IDP(N)-ODP(N)***} <--

      {Adj(N) -***IDP(N)-ODP(N)***} U {Adj(P) ***-IDP(P)-ODP(N)***}.

   Noter que, même si la valeur d'Adj(N) est égale à celle d'Adj(P) mais que les valeurs correspondantes d'IDP(P) ou d'ODP(P) et d'IDP(N) ou ODP(N) soient différentes, cela doit être traité comme une contiguïté différente et doit représenter un autre chemin vers la destination.

   b) Si N est un routeur ou un système d'extrémité OSI, et s'il y a maintenant plus de contiguïtés dans l'élément {Adj(M)} que la valeur "maximumPathSplits", alors supprimer les contiguïtés excédentaires comme décrit au § 7.2.7 de l'ISO/CEI 10589. Si N est une entrée d'accessibilité IP, alors les contiguïtés excédentaires peuvent être supprimées à volonté. Cela n'aura pas d'incidence sur le bien-fondé du routage mais pourra éliminer le déterminisme pour les routes IP (c'est-à-dire que les paquets continueront à suivre des routes optimales dans une zone mais, si plusieurs routes de même valeur existent, les paquets ne suivront pas nécessairement la route qu'un routeur particulier aura anticipée).

   c) Si x < dist(P,N), ne rien faire.

   d) si x > dist(P,N), supprimer <N,x,{Adj(N)***- IDP(N)-ODP(N***)}> de TENT, et ajouter

      <N,dist(P,N),{Adj(P)***- IDP(P)-ODP(P)***}>

6) si aucun triplet <N,x,{Adj(N)}> ne se trouve dans TENT, ajouter alors

   <N,dist(P,N),{Adj(P)}> à TENT.

Etape 2: si TENT est vide, arrêter le processus. Sinon:

1) Trouver comme suit l'élément <P,x,{Adj(P)***-IDP(P)-ODP(P)***}> ayant x minimal:

   a) Si un élément <*,tentlength,*> reste dans la liste de longueurs "tentlength" de la base TENT, choisir cet élément. S'il y a plusieurs éléments dans la liste pour "tentlength", choisir un des éléments (s'ils existent) pour un système qui est un pseudo-nœud de préférence à un élément pour un système qui n'est pas un pseudo-nœud. S'il n'y a plus d'éléments dans la liste pour "tentlength", incrémenter "tentlength" et répéter l'étape 2.

   b) Supprimer <P,tentlength,{Adj(P)***-IDP(P)-ODP(P***)}> de TENT.

   c) Ajouter <P,d(P),{Adj(P) ***-IDP(P)-ODP(P)***}> à PATHS.

   d) Si c'est le processus de décision de niveau 2 qui est en cours et que le système vienne de s'ajouter lui-même à la liste de PATHS en tant que système intermédiaire de niveau 2 désigné par partition, alors ajouter également <AREA.P,d(P),{Adj(P)}> à PATHS, où AREA.P est le titre d'entité de réseau de l'autre extrémité de la liaison virtuelle, obtenu par extraction de la première valeur AREA énumérée dans l'unité LSP du système P puis par adjonction de l'identificateur du système P.

   e) Si le système qui vient de s'ajouter à PATHS était un système d'extrémité, passer à l'étape 2. Sinon, passer à l'étape 1.

   NOTE – Dans le contexte du niveau 2, le terme "systèmes d'extrémité" désigne l'ensemble des préfixes d'adresse accessible (pour l'OSI), l'ensemble des adresses de zone de coût nul (pour l'OSI également), plus l'ensemble des entrées d'accessibilité IP (internes aussi bien qu'externes).

Appendice III

Guide de mise en service pour éléments de réseau SDH en double environnement RFC 1195 et influence de l'option d'encapsulage automatique

III.1 Introduction

Le présent appendice donne des directives sur l'installation de nœuds de routage IS-IS intégré dans un réseau à double protocole IPv4 et OSI, ainsi que sur la façon d'utiliser la capacité facultative d'encapsulage automatique décrite dans l'Annexe B.

III.2 Routage IS-IS intégré sans encapsulage automatique

III.2.1 Introduction et règles du RFC 1195

Le protocole de routage IS-IS intégré spécifié dans le commentaire RFC 1195 avait initialement été rédigé en tant que protocole de double routage. Il a en particulier été rédigé afin de permettre le routage de paquets aussi bien IPv4 que CLNP au moyen d'un seul calcul SPF, d'un seul ensemble de mesures pour les deux protocoles IP et CLNP, et d'un seul ensemble de préappels et d'unités LSP.

Plus précisément, les routeurs de routage IS-IS intégré conformes au RFC 1195 calculent les plus courts chemins traversant une zone de niveau 1 ou un sous-domaine de niveau 2 sans tenir compte de la question de savoir si un routeur candidat peut effectivement réexpédier un type de paquet spécifique.

C'est ce qui est clairement indiqué au § 3.10 du RFC 1195:

– "Le calcul par l'algorithme de Dijkstra ne tient pas compte de la question de savoir si un routeur est IP seulement, OSI seulement ou à double protocole. Les limitations topologiques spécifiées au § 1.4 garantissent que les paquets IP ne seront envoyés que par des routeurs à capacité IP et que les paquets OSI ne seront envoyés que par des routeurs à capacité OSI."

Avec le routage IS-IS intégré, un routeur est simplement un routeur. L'hypothèse est que tout routeur du réseau peut gérer tous les types de paquets qui lui sont envoyés.

Les routeurs de routage IS-IS intégré calculent donc des routes et réexpédient les paquets sur la base de cette hypothèse. C'est à l'opérateur qu'il appartient de faire en sorte que cette hypothèse se vérifie bien.

Il y a donc les limitations topologiques du RFC 1195. L'incapacité à appliquer les limitations topologiques du RFC 1195 peut se traduire par une perte de paquets car ceux-ci disparaissent dans le trou noir d'un routeur qui rejette simplement les paquets qu'ils ne peut pas réexpédier parce qu'il ne les prend pas en charge.

Dans un simple réseau à zone de niveau 1 unique, les règles sont tout à fait simples. Ce sont les suivantes:

1) si des paquets IPv4 doivent être réexpédiés dans une zone, tous les routeurs de celle-ci doivent être en mesure de réexpédier des paquets IPv4;
2) si des paquets CLNP doivent être réexpédiés dans une zone, tous les routeurs de celle-ci doivent être en mesure de réexpédier des paquets CLNP;
3) si des paquets aussi bien IPv4 que CLNP doivent être réexpédiés dans une zone, tous les routeurs de celle-ci doivent être à double protocole, c'est-à-dire capable de renvoyer ces deux sortes de paquets.

Il est donc assez facile de classer les zones de niveau 1 des routages IS-IS comme suit: "zone OSI seulement", "zone IP seulement" et "zone double". C'est ce qui est représenté dans la Figure III.1.

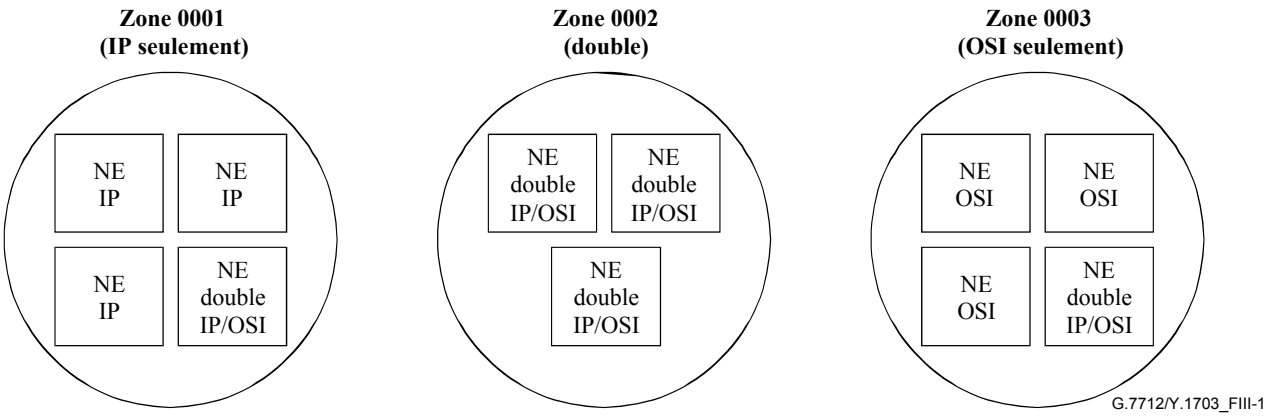


Figure III.1/G.7712/Y.1703 – Classification des zones de niveau 1 des routages IS-IS

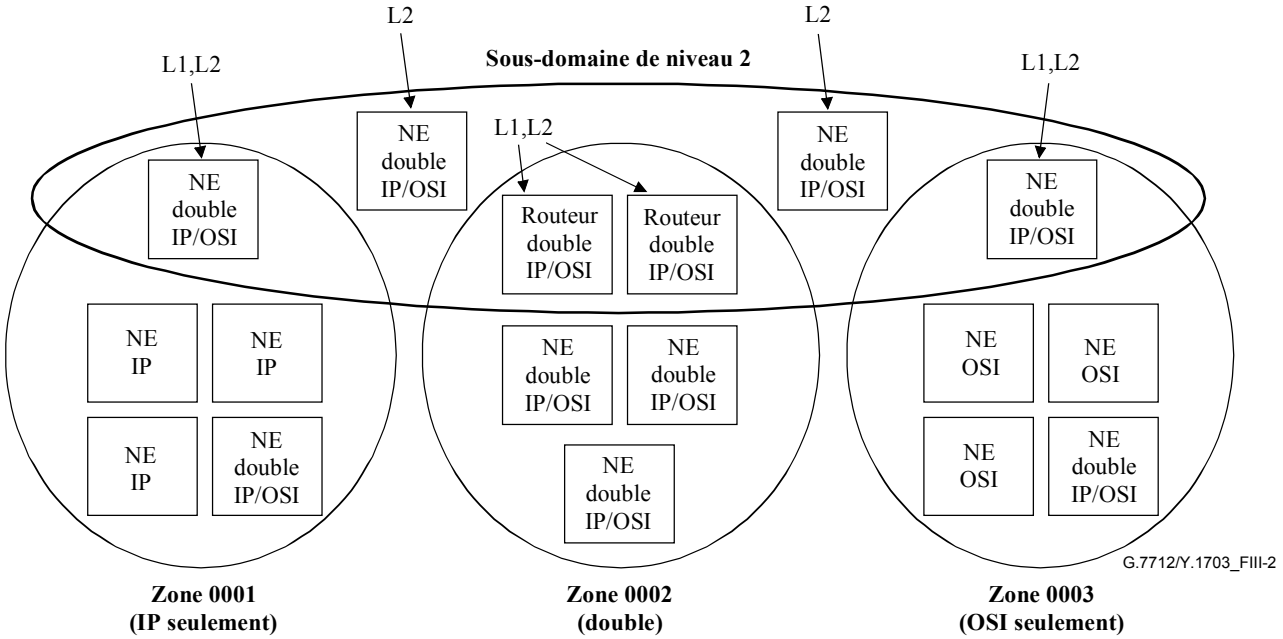
III.2.2 Sous-domaine de niveau 2

Si un très grand réseau est requis, nécessitant un routage de niveau 2, le sous-domaine de niveau 2 réexpédiera les paquets entre les zones de niveau 1 et devra donc prendre en charge tous les types de paquets présents dans toutes ces zones de niveau 1. Les règles applicables au sous-domaine de niveau 2 sont les suivantes:

1) si des paquets IPv4 sont reéexpédiés dans une des zones (IP seulement ou doubles), tous les routeurs du sous-domaine de niveau 2 doivent être en mesure de réexpédier ces paquets;

2) si des paquets CLNP sont réexpédiés dans une des zones (OSI seulement ou doubles), tous les routeurs du sous-domaine de niveau 2 doivent être en mesure de réexpédier ces paquets.

Si une des zones est double ou si les deux types de zone, OSI seulement et IP seulement coexistent, les routeurs du sous-domaine de niveau 2 doivent être à double protocole, comme illustré dans la Figure III.2.



Etant donné que les paquets IPv4 comme CLNP sont réexpédiés dans les zones de niveau 1, tous les nœuds du sous-domaine de niveau 2 doivent être à double protocole, même ceux qui sont présents dans des zones IP seulement ou OSI seulement.

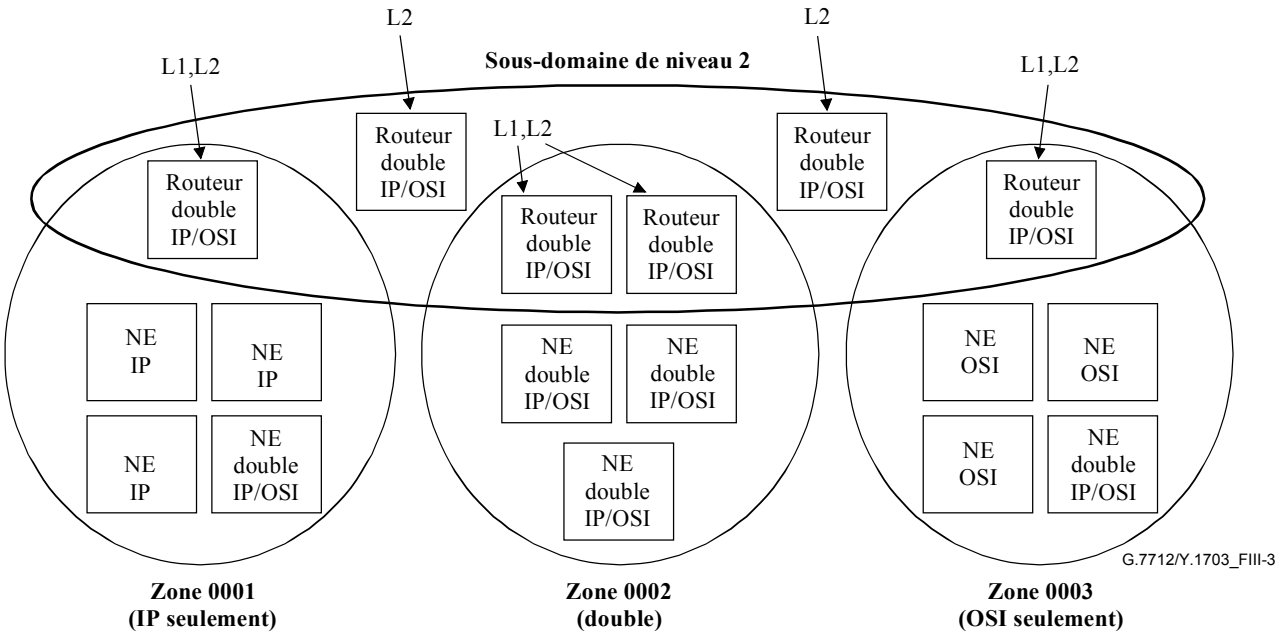
Un nœud est dans le sous-domaine de niveau 2 s'il exploite le routage de niveau 2.

Figure III.2/G.7712/Y.1703 – Sous-domaine de niveau 2

III.2.3 Sous-domaine de niveau 2 avec routeurs externes exploitant des routages IS-IS intégrés

De nombreux opérateurs exploitent actuellement le routage IS-IS de niveau 1 dans leurs éléments de réseau OSI seulement en hiérarchie SDH. Ils relient ensuite de multiples zones par routage IS-IS de niveau 2 dans un réseau routeur externe.

Si un opérateur souhaite utiliser un modèle analogue pour un réseau à double protocole, il peut exploiter le routage IS-IS intégré de niveau 1 dans chaque zone et le routage IS-IS intégré de niveau 2 dans un réseau routeur externe. Cela produit un réseau très semblable au précédent, comme indiqué dans la Figure III.3.



Etant donné que les paquets IPv4 comme CLNP sont réexpédiés dans les zones de niveau 1, tous les routeurs du sous-domaine de niveau 2 doivent être à double protocole, même ceux qui sont présents dans des zones IP seulement ou OSI seulement.

Figure III.3/G.7712/Y.1703 – Niveau 2 avec routeurs externes exploitant des routages IS-IS

III.2.4 Routeurs externes exploitant l'algorithme OSPF ou d'autres protocoles de routage IP

De nombreux opérateurs exploitent actuellement le routage IS-IS de niveau 2 dans leurs routeurs externes et l'algorithme OSPF ou d'autres protocoles de routage pour IP. Dans ce cas, le routeur externe doit rester le routeur de niveau 2 pour les éléments de réseau en hiérarchie SDH et un routeur à double routage IS-IS intégré doit donc exister pour une zone à double protocole. Le routeur peut toutefois être configuré de façon à router tous les paquets IP au moyen de l'algorithme OSPF par configuration d'une redistribution des routes IP entre routes IS-IS et routes OSPF. De cette façon, tous les paquets IP seront routés par OSPF tandis que les paquets CLNP continueront à suivre le routage IS-IS de niveau 2. C'est ce qui est représenté dans la Figure III.4.

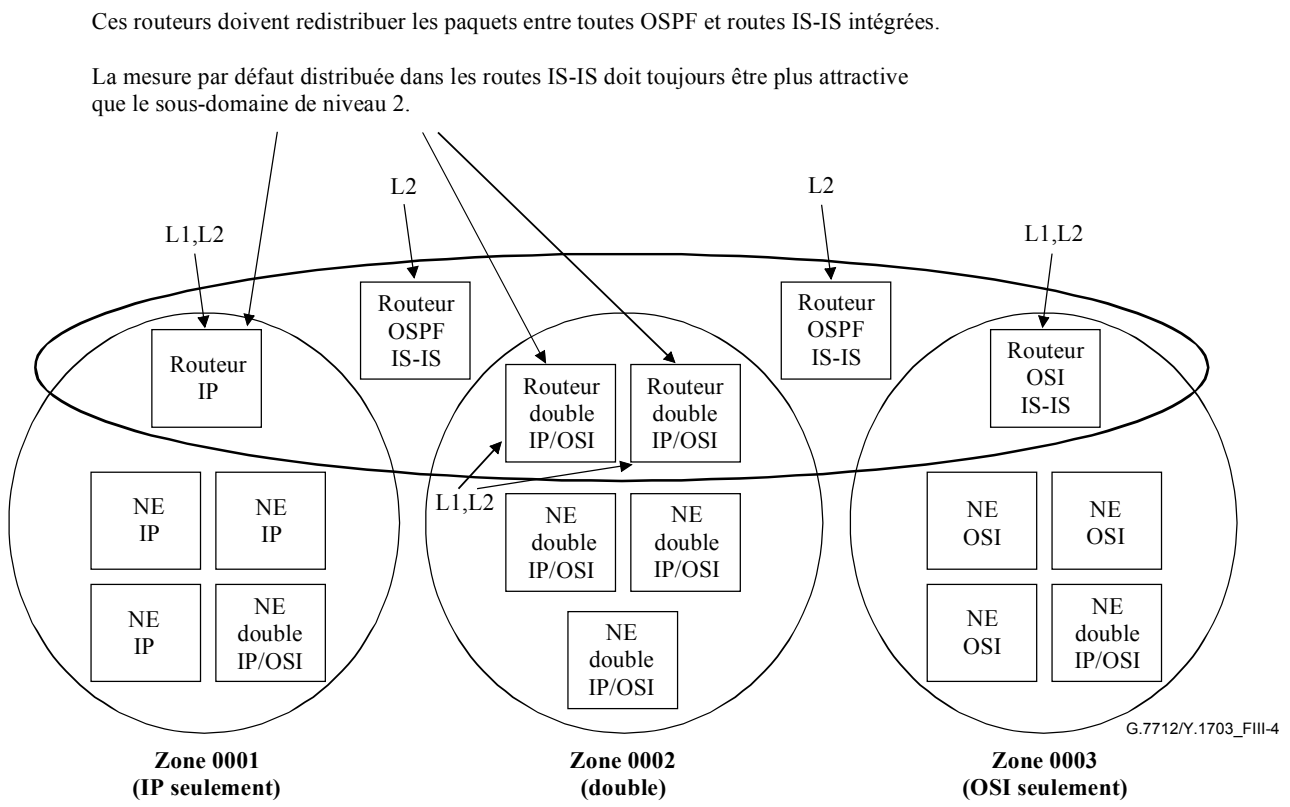


Figure III.4/G.7712/Y.1703 – Routeurs externes exploitant l'algorithme OSPF

Noter que la pile de routage IS-IS intégré dans les routeurs externes ne sera pas informée du fait que le sous-domaine de niveau 2 ne vise que les paquets CLNP. Les routes calculées par l'algorithme OSPF doivent donc être redistribuées en routes IS-IS intégrées avec une faible mesure par défaut afin de les rendre plus attractives pour les paquets IP que le sous-domaine de niveau 2.

III.3 Routage IS-IS intégré avec encapsulage automatique

III.3.1 Introduction et incidence sur les limitations topologiques

L'option d'encapsulage automatique permet de contourner les règles topologiques du RFC 1195. Pratiquement, l'encapsulage automatique permet à un nœud ou à un groupe de nœuds de paraître capable de réexpédier des paquets qu'en réalité ils ne peuvent pas réexpédier.

C'est ce qui est montré dans la Figure III.5.

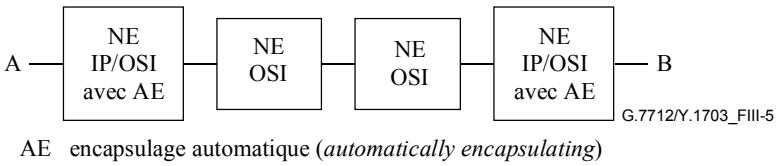


Figure III-5/G.7712/Y.1703 – Groupe de nœuds avec encapsulage automatique

Ce groupe de nœuds réexpédiera donc les paquets IPv4 comme CLNP du moment que ces paquets entrent au point A ou B, au moyen d'un des nœuds d'encapsulage automatique.

Le groupe de nœuds peut donc être placé sans difficulté dans une zone à double protocole ou dans un sous-domaine double de niveau 2, car la paire de nœuds d'encapsulage automatique réexpédiera les paquets IPv4 en les encapsulant dans des paquets CLNP de façon qu'ils puissent être réexpédiés par les éléments de réseau OSI seulement au lieu d'être rejetés.

Une double zone valide pourra donc ressembler à ce qui est indiqué dans la Figure III.6.

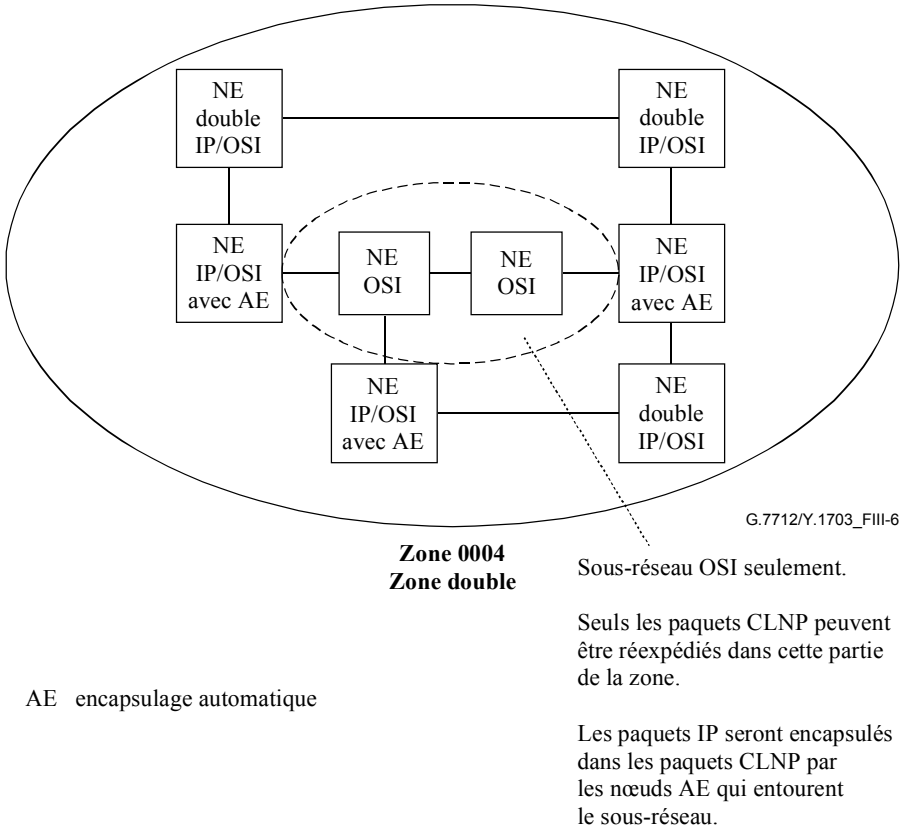


Figure III.6/G.7712/Y.1703 – Exemple de double zone valide

Noter que les nœuds OSI seulement ne doivent pas être directement connectés à un des nœuds doubles qui ne possèdent pas l'option d'encapsulage automatique. C'est seulement la présence des nœuds d'encapsulage automatique qui empêche les paquets IPv4 d'être envoyés à un nœud OSI seulement.

Un nœud double peut être connecté directement à un nœud OSI seulement s'il est également traité comme un nœud OSI seulement, comme indiqué dans la Figure III.7.

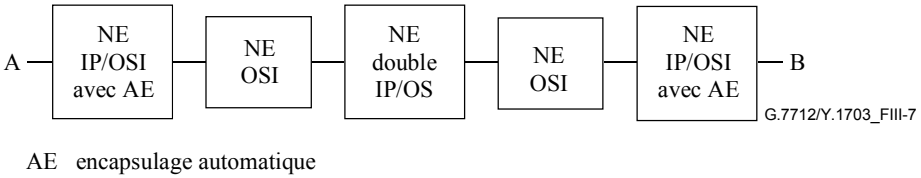


Figure III.7/G.7712/Y.1703 – Connexion d'un double nœud à un nœud OSI seulement

Dans ce cas, le réseau agit comme étant à double protocole pour les paquets allant du point A au point B mais les paquets IPv4 ne peuvent pas atteindre le double nœud central, qui se trouve à l'intérieur d'un sous-réseau OSI seulement. Ce double nœud ne pourra réexpédier que les paquets

CLNP et devra être géré par le service CLNS. Il ne doit pas y avoir d'autres connexions au double nœud central car, si des paquets IPv4 y étaient introduits, ils pourraient être réexpédiés vers un nœud OSI seulement et être rejetés.

III.3.2 Obtention du trafic à destination ou en provenance du réseau SDH imbriqué

III.3.2.1 Elément de réseau passerelle à capacité IP

Les paquets IP comme CLNP doivent toujours être en mesure de pénétrer et de quitter une zone double, que l'encapsulage automatique soit ou non utilisé. Normalement, le trafic pénètre et quitte une zone à routage IS-IS au moyen de routeurs de niveau 1, niveau 2, qui participent à la fois à la zone de niveau 1 et au sous-domaine de niveau 2.

Le moyen le plus simple pour construire ce routage est de veiller à ce que les routeurs de niveau 1, niveau 2 soient à double protocole, comme indiqué dans la Figure III.8.

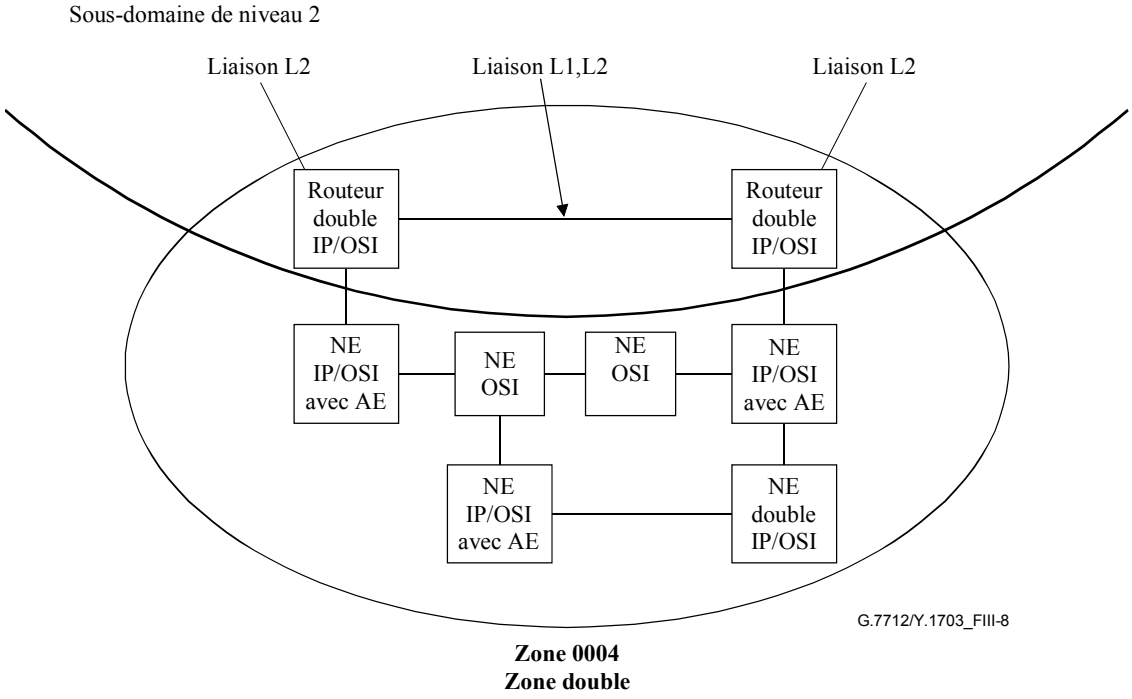
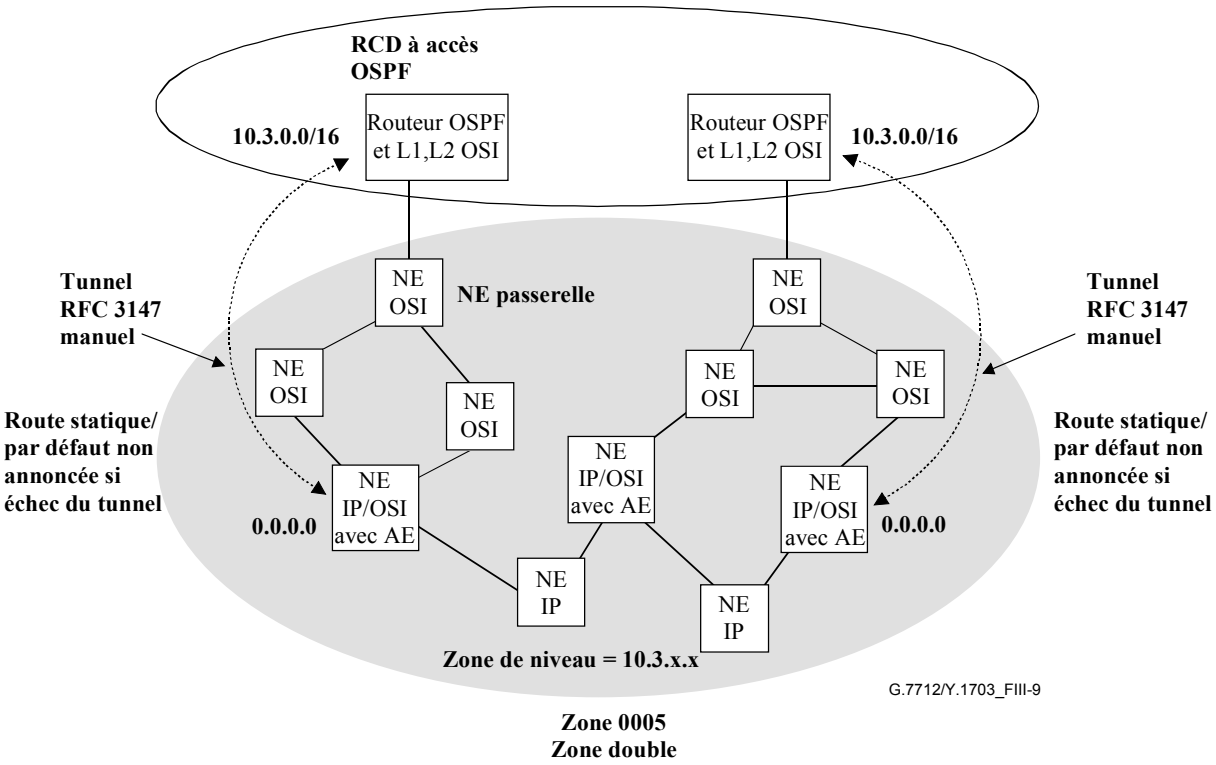


Figure III.8/G.7712/Y.1703 – Passerelle double

III.3.2.2 Elément de réseau passerelle à capacité OSI seulement

Occasionnellement, des nœuds d'encapsulage automatique seront utilisés afin de mettre à niveau une zone OSI seulement existante et de la transformer effectivement en zone à double protocole. Dans ce cas, les nœuds passerelles devront peut-être rester des nœuds OSI seulement et un réseau comme celui de la Figure III.9 pourra être construit.



AE encapsulage automatique

Figure III.9/G.7712/Y.1703 – Passerelle à capacité OSI seulement

Dans ce réseau, les paquets CLNP qui ont besoin de quitter la zone de niveau 1 continuent à aller vers le routeur OSI de niveau 1, niveau 2. Les nœuds qui ont un tunnel manuel sortant de la zone de niveau 1 l'annoncent comme route par défaut. Par conséquent, les nœuds à capacité IP ajouteront une entrée en bas de leur table de routage leur indiquant qu'ils doivent envoyer tous les paquets IPv4 à un des nœuds qui possède un tunnel manuel, à moins qu'ils n'aient une route plus spécifique. De cette façon, un paquet IPv4 ne sera jamais envoyé à un nœud de niveau 1, niveau 2 mais passera toujours par un des tunnels manuels.

Le routeur situé dans le RCD d'accès auquel le tunnel manuel aboutit n'a pas besoin d'exploiter le routage IS-IS intégré. Il peut exploiter tout protocole de routage IP qu'un opérateur souhaite utiliser. De cette façon, un réseau existant qui utilise les routages OSPF et IS-IS de niveau 2 dans le RCD d'accès, ainsi que le routage IS-IS de niveau 1 dans les éléments de réseau SDH, peut mettre à niveau ses zones de niveau 1 en zones à double protocole sans grande incidence sur les éléments de réseau OSI seulement existants en SDH ni sur le RCD d'accès.

Appendice IV

Exemple montrant la protection doublée des paquets

IV.1 Aperçu général de la protection doublée des paquets

La protection des paquets par double chemin (1+1) offre un service de protection au niveau des paquets semblable à certains égards au service conventionnel de protection doublée au niveau des connexions, avec plusieurs distinctions importantes. La protection doublée au niveau des paquets permet la sélection des paquets entrants par une connexion quelconque, quelle que soit la connexion à partir de laquelle le dernier paquet a été sélectionné. En d'autres termes, la protection doublée des paquets traite les deux connexions (de trafic et de secours) comme étant deux connexions de trafic alors que la protection doublée des connexions désigne une des connexions comme étant de trafic et l'autre de secours. Dans la protection des connexions, les paquets sont sélectionnés à partir de la connexion de trafic jusqu'à ce que la détection d'une défaillance dans cette connexion de trafic provoque une commutation sur la connexion de secours. En revanche, la protection doublée des paquets ne nécessite pas de détection de défaillance explicite ni de commutation sur secours. Cela permet au système de protection doublée des paquets de se rétablir instantanément et en transparence après une défaillance quelconque. Comme en protection doublée au niveau des connexions, seuls les nœuds périphériques ont besoin d'être compatibles avec le service, ce qui facilite l'interopérabilité.

Afin d'offrir le service de protection doublée des paquets entre deux nœuds périphériques de réseau en mode connexion, une paire de connexions est établie sur des chemins non consécutifs. Les paquets issus d'un flux applicatif abonné au service sont dédoublés sur ces deux connexions au niveau du nœud de réception. Dans le cas le plus simple, les chemins disjoints peuvent être séparés au niveau des liaisons ou au niveau des nœuds. Mais, en général, ils peuvent mettre en œuvre des notions plus complexes, comme les groupes à risque partagé. Au niveau du nœud périphérique d'émission, un des deux exemplaires reçus et possibles des paquets est choisi puis réexpédié, chacun traversant un chemin disjoint de l'autre. Cela étant, toute défaillance isolée dans le réseau, autre que celle du nœud de réception ou d'émission lui-même, pourra affecter au plus un seul exemplaire de chaque paquet, ce qui permettra au service de résister en transparence à une défaillance isolée. En termes de temps de rétablissement, cela peut être caractérisé comme une reprise instantanée puisqu'il n'est pas nécessaire de détecter, de notifier et de commuter explicitement sur connexion de secours. Ce procédé peut être facilement étendu à la protection contre des défaillances multiples par l'emploi de plusieurs chemins disjoints.

IV.2 Illustration de la protection doublée des paquets

La Figure IV.1 décrit une réalisation du service faisant appel à des numéros de séquence en tant qu'identificateurs. Après avoir traversé le classificateur, chaque paquet appelé à être réexpédié dans les chemins d'unités LSP correspondantes est affecté d'un numéro de séquence distinct par le nœud périphérique d'origine, compatible avec le service. Ce paquet, portant l'identification distincte, est ensuite dédoublé et réexpédié sur les deux chemins d'unités LSP disjoints. Le nœud d'émission ne doit sélectionner qu'un seul exemplaire du paquet dédoublé. Afin de sélectionner correctement le paquet une seule fois exactement, la destination doit être en mesure d'identifier les paquets dédoublés puis d'en choisir un avec prise en charge de toutes les variantes possibles. Ce processus de sélection au niveau des paquets n'est pas trivial parce que les paquets dédoublés peuvent ne pas arriver en même temps (en raison des délais de propagation et de la mise en tampon) et peuvent être perdus (en raison d'erreurs de transmission et de débordements de tampon).

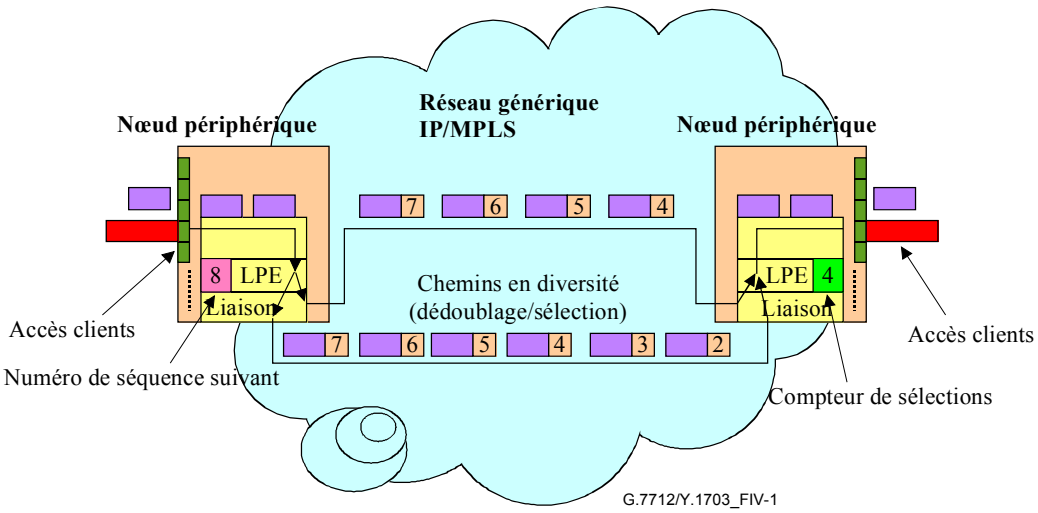


Figure IV.1/G.7712/Y.1703 – Protection doublée

Le nœud de réception insère le numéro de séquence comme indiqué au § 7.1.19.2. Le paquet est ensuite dédoublé et transporté dans les divers chemins d'unités LSP. Compte tenu de la diversité des chemins LSP, il y aura un LSP d'attaque et un LSP de traîne. Le LSP d'attaque acheminera les paquets au nœud d'émission plus rapidement que le LSP de traîne. En conditions de non-défaillance, le nœud d'émission choisira donc les paquets à partir du LSP d'attaque. Les paquets reçus du LSP de traîne seront des exemplaires redondants et seront donc rejetés.

La décision d'accepter ou de rejeter un paquet reçu est fondée sur le numéro de séquence de ce paquet et sur un compteur + une fenêtre glissante dans le nœud d'émission. Le compteur indique le numéro de séquence du prochain paquet attendu. Le compteur et la fenêtre glissante affichent les numéros de séquence acceptables. La fenêtre glissante est requise afin d'accepter et de rejeter correctement les paquets. Si le paquet reçu s'inscrit dans la fenêtre, il est considéré comme légitime et peut être accepté. Sinon, il est rejeté. La taille de la fenêtre devrait être supérieure au nombre maximal de paquets consécutifs qu'un chemin LSP de trafic (ou actif) peut perdre.

La fenêtre glissante sert à résoudre le problème de la perte de paquets sur le chemin LSP d'attaque lorsque le numéro de séquence du LSP d'attaque est très proche du point de débordement. La Figure IV.2 montre un chemin d'unités LSP d'attaque (LSP 1) qui remet un paquet dont le numéro de séquence est 29. Ce paquet est accepté et le compteur est incrémenté à 30. Si l'on suppose que 2 paquets consécutifs sont perdus (c'est-à-dire des paquets avec les numéros de séquence 30 et 31), le prochain paquet reçu sur LSP 1 sera 0. Sans fenêtre glissante, le nœud d'émission rejettera ce paquet étant donné que $0 < 30$. Ce problème peut être résolu en mettant en œuvre une fenêtre glissante plus grande que le nombre maximal de paquets consécutifs qu'un chemin LSP de trafic (actif) peut perdre. Par exemple, soit 5 le nombre maximal de paquets consécutifs qu'un LSP de trafic peut perdre. Dans ce cas, une fenêtre glissante de 6 peut être définie. Avec le même exemple mais en utilisant maintenant la fenêtre glissante, le nœud d'émission acceptera les paquets dans l'étendue de {30, 31, 0, 1, 2, 3, 4}. Même si 5 paquets sont perdus (c'est-à-dire le nombre maximal de paquets consécutifs qui peuvent être perdus sur un LSP de trafic), le prochain paquet reçu aura le numéro de séquence 3 et ce paquet sera accepté.

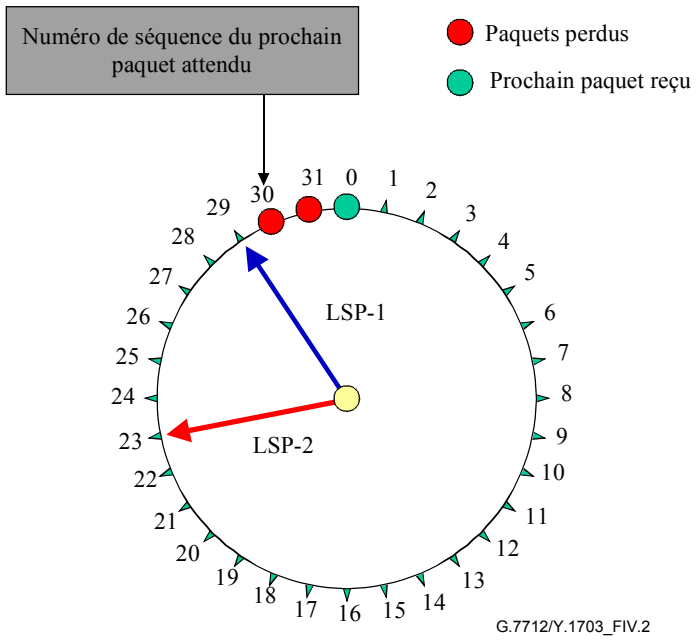


Figure IV.2/G.7712/Y.1703 – Fonctionnement de la fenêtre glissante

Noter que cette idée de fenêtre glissante ne fonctionne que si le chemin LSP de traîne ne peut pas se replier dans l'étendue de la fenêtre glissante. Si un paquet portant un numéro de séquence compris dans l'étendue de la fenêtre glissante est reçu en provenance du chemin LSP de traîne, ce paquet sera accepté par erreur. Un chemin LSP de traîne ne peut recevoir un paquet portant un numéro de séquence s'inscrivant dans l'étendue de la fenêtre glissante que si son repliement a une longueur supérieure à (2^N – longueur de la fenêtre glissante). Le nombre de bits "*N*" utilisé pour le numéro de séquence doit donc prendre en charge l'équation suivante:

$$2^N > \text{SlidingWindow} + \text{DelayWindow}$$

où:

SlidingWindow > nombre maximal de paquets consécutifs pouvant être perdus sur un chemin LSP

et où:

DelayWindow = nombre maximal de paquets que le chemin LSP de traîne peut laisser derrière le chemin LSP d'attaque.

Noter que le § 7.1.19.2 définit un champ de 4 octets pour l'acheminement du numéro de séquence. Ce champ de 4 octets permet une séquence de plus de 4 milliards de numéros ce qui est assez pour tenir compte du cas le moins favorable de pertes de paquets consécutifs et de différences de temps de propagation.

Un moyen logique de calculer la longueur des fenêtres glissante et de délai consiste à rendre la longueur de la fenêtre glissante égale à celle de la fenêtre de délai. (Noter que l'on part du principe que la longueur de la fenêtre de délai est généralement supérieure à celle de la fenêtre glissante.) Cela garantit la sélection de paquets issus du chemin LSP d'attaque dans tous les scénarios après réparation d'un LSP défaillant. Ce point est développé plus en détail dans le paragraphe suivant, qui examine divers scénarios de défaillance.

IV.3 Fonctionnement de l'algorithme sélecteur dans différents scénarios de défaillance

Une façon de considérer le fonctionnement de l'algorithme sélecteur consiste à représenter une horloge avec des intervalles de 2^N. La Figure IV.3 montre un exemple dans lequel N = 4 (c'est-à-dire un numéro de séquence de 4 bits). Les numéros de séquence sont donc compris entre 0 et 15.

Dans cet exemple, la fenêtre glissante est choisie égale à la fenêtre de délai, qui est de 5.

La Figure IV.3 montre que le chemin LSP d'attaque a une avance de 3 numéros de séquence sur le chemin LSP de traîne. Le chemin LSP d'attaque remet un paquet de numéro de séquence = 1 et le compteur est alors mis à 2.

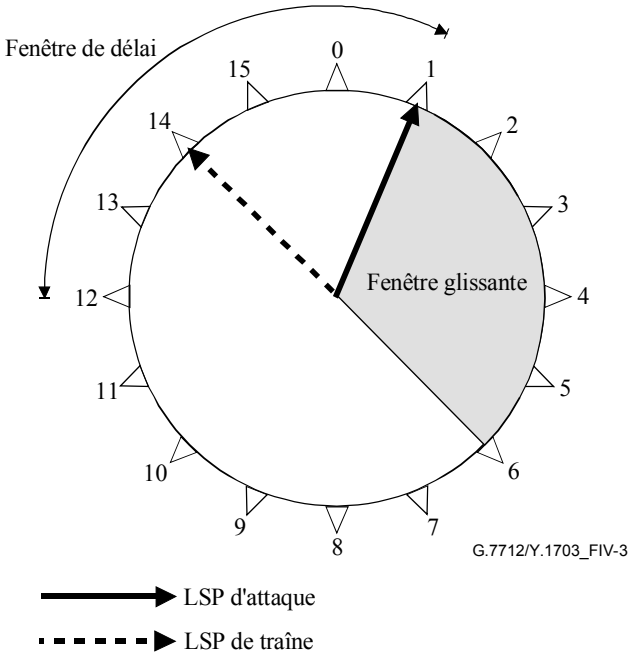


Figure IV.3/G.7712/Y.1703 – Fonctionnement de l'algorithme sélecteur

La Figure IV.4 montre qu'avant de recevoir un paquet ayant un numéro de séquence égal à 2 sur le chemin LSP d'attaque, celui-ci subit une défaillance. Tant que le paquet portant un numéro de séquence égal à 2 n'est pas remis par le chemin LSP de traîne, le nœud d'émission ne sélectionne plus de paquets et le compteur reste égal à 2.

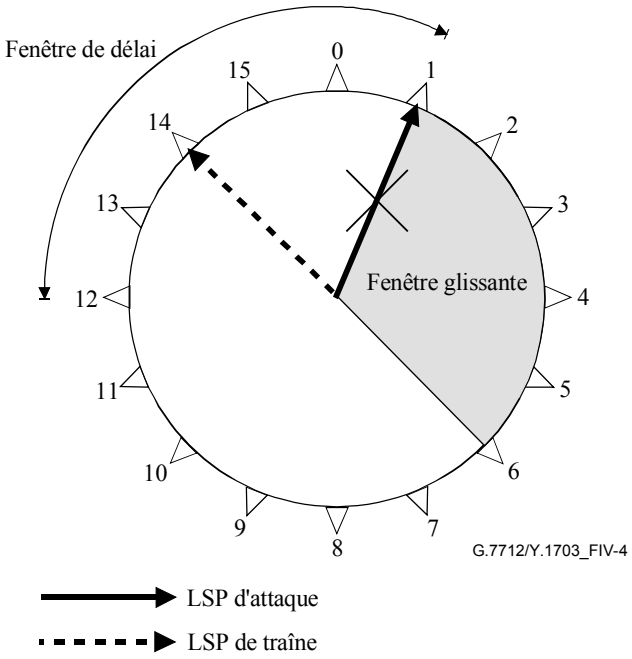


Figure IV.4/G.7712/Y.1703 – Défaillance sur le chemin LSP d'attaque

La Figure IV.5 montre que, lorsque le paquet de numéro de séquence égal à 2 est reçu sur le chemin LSP de traîne, le nœud d'émission incrémente le compteur à 3 et la fenêtre glissante se déplace de façon qu'un paquet portant un numéro de séquence compris entre 3 et 7 puisse être accepté.

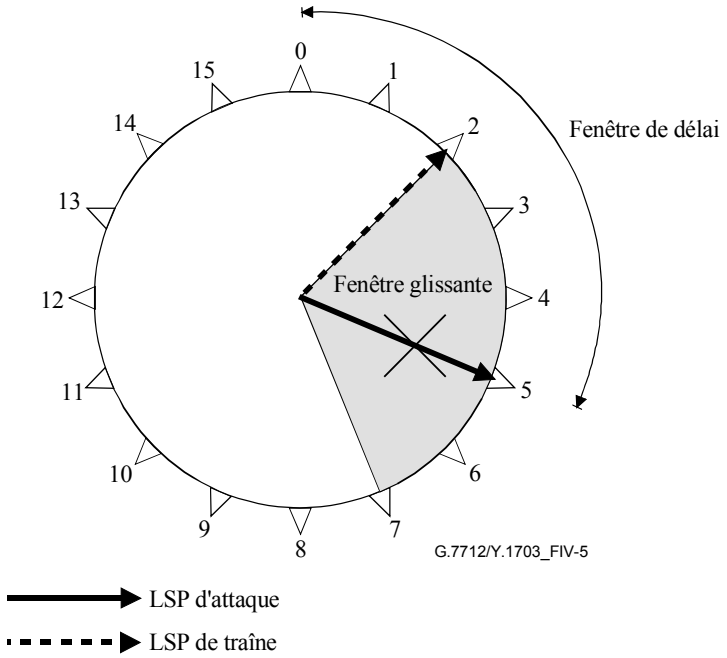


Figure IV.5/G.7712/Y.1703 – Réception du paquet 2 par le chemin LSP de traîne

La Figure IV.6 montre qu'avant de recevoir un paquet de numéro de séquence égal à 3 en provenance du chemin LSP de traîne, le chemin LSP d'attaque est réparé et qu'un paquet de séquence égal à 6 est reçu du chemin LSP d'attaque. Comme 6 s'inscrit dans l'étendue de la fenêtre glissante, le paquet est accepté. Noter qu'il importe que les paquets soient reçus du LSP d'attaque tant que ce chemin LSP fonctionne. Afin de garantir que le chemin LSP d'attaque remet, lorsqu'il

est réparé, un paquet portant un numéro de séquence dont la valeur s'inscrit dans l'étendue de la fenêtre glissante, celle-ci doit donc être égale ou supérieure à la fenêtre de délai, ce qui est le cas dans cet exemple.

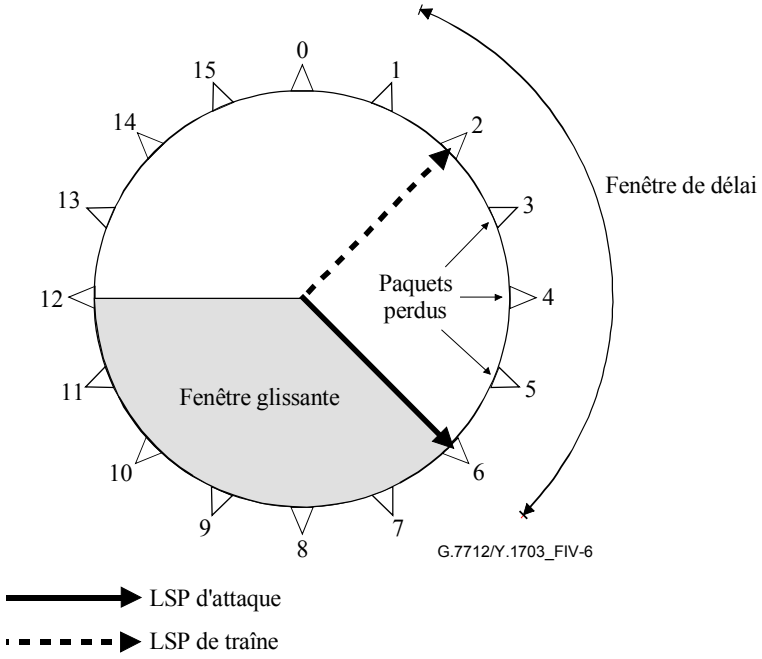


Figure IV.6/G.7712/Y.1703 – Réparation du chemin LSP d'attaque

Les Figures IV.7, IV.8 et IV.9 décrivent un problème qui se pose si la fenêtre glissante est réglée à une longueur inférieure à la fenêtre de délai. Dans ce cas, il est possible que le LSP d'attaque, s'il est réparé, remette des paquets portant des numéros de séquence tombant en dehors de la fenêtre glissante et que le nœud d'émission continue donc d'accepter des paquets issus du LSP de traîne. Si celui-ci tombe ultérieurement en panne, une perte de nombreux paquets est possible (le cas le moins favorable serait 2^N – *longueur_de_fenêtre_glissante*, où N est le nombre de bits utilisés pour le numéro de séquence).

La Figure IV.7 montre un exemple dans lequel la fenêtre glissante est réglée à 3 alors que la fenêtre de délai peut atteindre 7. Dans cet exemple, le chemin LSP de traîne retarde de 4 numéros de séquence par rapport au chemin LSP d'attaque. Comme celui-ci est en panne, les paquets sont sélectionnés à partir du LSP de traîne.

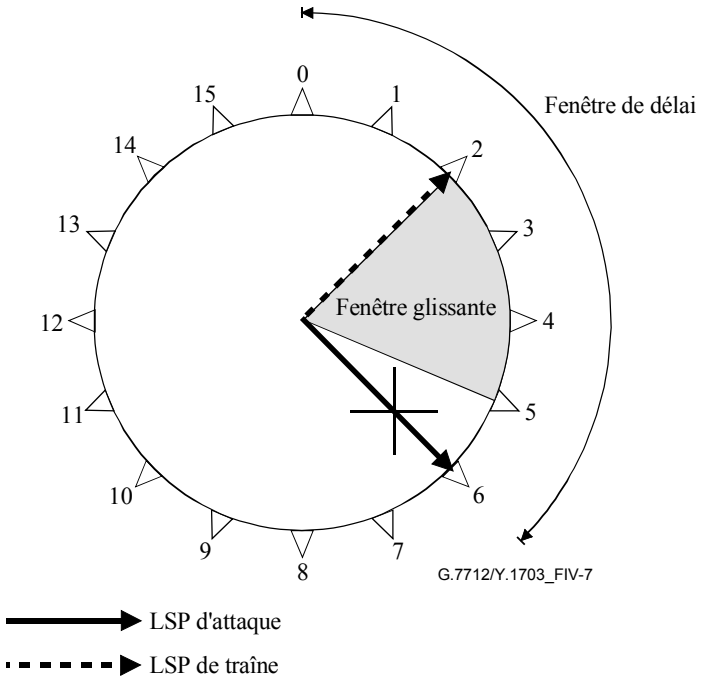


Figure IV.7/G.7712/Y.1703 – Fenêtre glissante trop petite: paquet sélectionné depuis le chemin LSP de traîne

La Figure IV.8 montre que le chemin LSP d'attaque remet, au moment où il est réparé, un paquet portant un numéro de séquence égal à 7, qui est donc extérieur à la fenêtre glissante et est donc rejeté. Les paquets continuent à être sélectionnés à partir du chemin LSP de traîne.

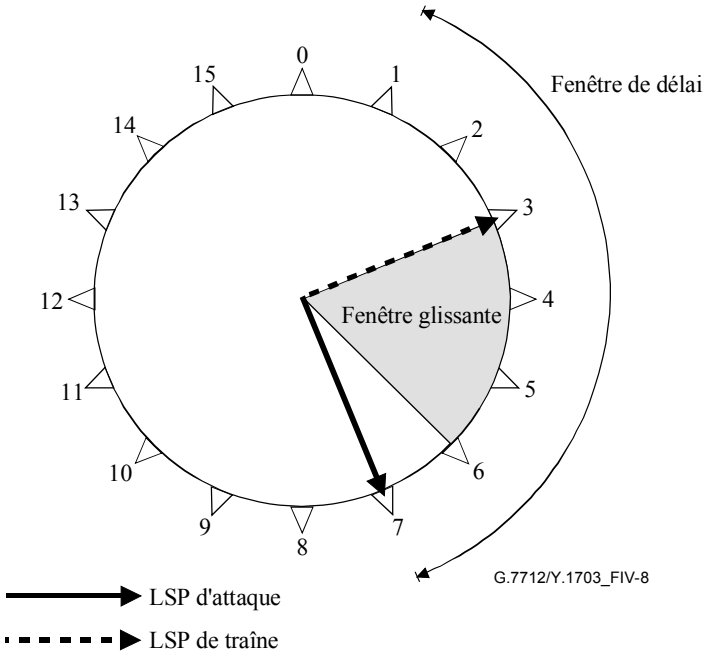


Figure IV.8/G.7712/Y.1703 – Fenêtre glissante trop petite: rejet des paquets remis par le chemin LSP d'attaque

La Figure IV.9 décrit une défaillance dans le chemin LSP de traîne. Comme le LSP d'attaque remet des paquets en dehors de la fenêtre glissante et que ces paquets sont donc rejetés, le nœud d'émission ne commence pas à accepter de paquets tant que le LSP d'attaque n'est pas complètement réparé et ne commence pas à remettre des paquets portant un numéro de séquence s'inscrivant dans la fenêtre glissante. Il peut en résulter un perte notable de paquets. Afin d'empêcher une telle circonstance, il est donc recommandé que ce type d'algorithme sélecteur rende la fenêtre glissante égale à la fenêtre de délai.

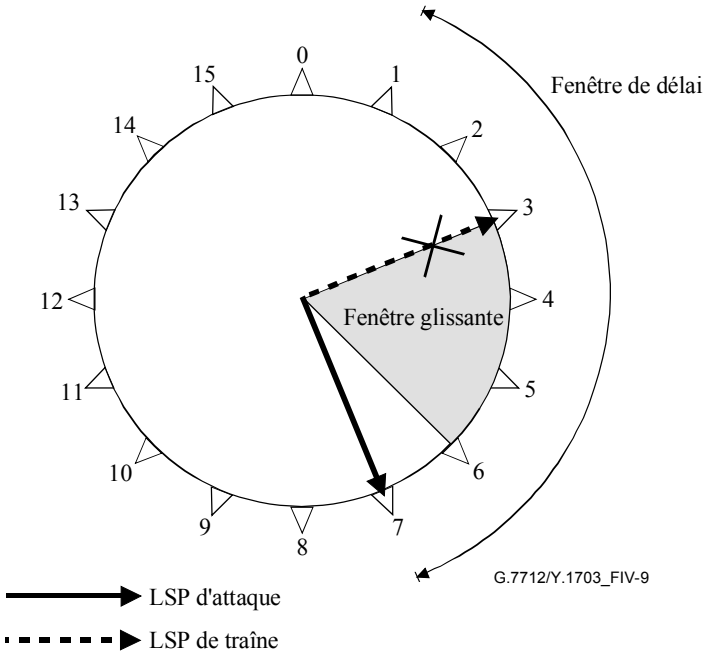


Figure IV.9/G.7712/Y.1703 – Fenêtre glissante trop petite: effet d'une défaillance du chemin LSP de traîne

Appendice V

Bibliographie

– IETF RFC 1006 (1997), *ISO Transport Service on top of the TCP Version 3* (Service de transport ISO sur la version 3 du protocole TCP).

– IETF RFC 2966 (2000), *Domain-wide Prefix Distribution with Two-Level IS-IS* (Distribution de préfixe sur toute la largeur du domaine avec routage IS-IS à 2 niveaux).

– IETF RFC 3147 (2001), *Generic Routing Encapsulation of CLNS Networks* (Encapsulage de routage générique dans les réseaux CLNS).

– IETF RFC 3373 (2002), *Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies* (Dialogue à trois voies pour contiguïtés point à point de système intermédiaire à système intermédiaire (IS-IS).

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.

SÉRIES DES RECOMMANDATIONS UIT-T

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

Imprimé en Suisse
Genève, 2003