

**UIT-T**

SECTEUR DE LA NORMALISATION  
DES TÉLÉCOMMUNICATIONS  
DE L'UIT

**G.8080/Y.1304**

**Amendement 2**  
(02/2005)

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

Aspects relatifs au protocole Ethernet sur couche  
Transport – Généralités

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

Aspects relatifs au protocole Internet – Transport

---

Architecture du réseau optique à commutation  
automatique (ASON)

**Amendement 2**

Recommandation UIT-T G.8080/Y.1304 (2001) –  
Amendement 2

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 RADIODÉLÉPHONIE ET DE LA TÉLÉPHONIE SUR LIGNES	G.450–G.499
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
DONNÉES SUR COUCHE TRANSPORT – ASPECTS GÉNÉRIQUES	G.7000–G.7999
ASPECTS RELATIFS AU PROTOCOLE ETHERNET SUR COUCHE TRANSPORT	G.8000–G.8999
<b>Généralités</b>	<b>G.8000–G.8099</b>
Aspects relatifs au protocole MPLS sur couche Transport	G.8100–G.8199
Objectifs de qualité et de disponibilité	G.8200–G.8299
RÉSEAUX D'ACCÈS	G.9000–G.9999

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

# **Recommandation UIT-T G.8080/Y.1304**

## **Architecture du réseau optique à commutation automatique (ASON)**

### **Amendement 2**

#### **Résumé**

Le présent amendement contient des informations additionnelles à incorporer dans la Rec. UIT-T G.8080/Y.1304, Architecture du réseau optique à commutation automatique (ASON). Le présent amendement remplace l'Amendement 1.

#### **Source**

L'Amendement 2 de la Recommandation UIT-T G.8080/Y.1304 (2001) a été approuvé le 22 février 2005 par la Commission d'études 15 (2005-2008) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

## AVANT-PROPOS

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

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

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

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

## NOTE

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

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

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

A la date d'approbation de la présente Recommandation, l'UIT avait 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.

© UIT 2005

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

## TABLE DES MATIÈRES

	<b>Page</b>
1) Domaine d'application .....	1
2) Paragraphe 2 Références .....	1
3) Paragraphe 3 Définitions .....	1
4) Paragraphe 4 Abréviations.....	2
5) Modification du numéro de certaines Figures .....	2
6) Paragraphe 5 .....	4
7) Paragraphe 5.1 Commandes d'appel et de connexion.....	5
8) Paragraphe 5.1.1 Commande d'appel .....	5
9) Nouveau paragraphe 5.2 Interaction entre plans de commande, de transport et de gestion.....	5
10) Paragraphe 6.1 Entités de transport .....	7
11) Paragraphe 6.2 Zones de routage.....	7
12) Nouveau paragraphe 6.2.1 Agrégation de liaisons et de zones de routage.....	8
13) Nouveau paragraphe 6.2.2 Relation avec les liaisons et agrégation de liaisons.....	9
14) Paragraphe 6.3 Topologie et découverte .....	11
15) Nouveau paragraphe 6.4 Domaines.....	11
16) Nouveau paragraphe 6.5 Aspects relatifs aux couches multiples.....	14
17) Nouveau paragraphe 6.6 Prise en charge de client intercouches.....	14
18) Paragraphe 7 Architecture du plan de commande .....	15
19) Paragraphe 7.2.1 Modèle général de politique .....	15
20) Paragraphe 7.3 Composants de l'architecture .....	16
21) Paragraphe 7.3.1 Composant "contrôleur de connexion" (CC).....	16
22) Paragraphe 7.3.2 Composant "contrôleur de routage" (RC).....	17
23) Paragraphe 7.3.3 Composant "gestionnaire de ressource de liaison" (LRMA et LRMZ).....	18
24) Paragraphe 7.3.3.1 Gestionnaire LRMA .....	18
25) Paragraphe 7.3.5.1 Contrôleur d'appel de l'appelant/de l'appelé .....	19
26) Paragraphe 7.3.5.2 Contrôleur d'appel réseau .....	20
27) Paragraphe 7.3.5.3 Interactions du contrôleur d'appel.....	23
28) Nouveau paragraphe 7.3.5.4 Modification d'appel.....	24
29) Nouveaux paragraphes 7.3.6, 7.3.7 et 7.3.8.....	24
30) Paragraphe 7.5.1 Routage hiérarchique .....	28
31) Paragraphe 7.5.2 Routage par la source et pas à pas .....	28

	<b>Page</b>
32) Paragraphe 8 Points de référence.....	29
33) Paragraphe 8.1 Interface UNI.....	29
34) Paragraphe 8.3 Interface E-NNI.....	29
35) Nouveau paragraphe 8.4 Architecture côté utilisateur.....	30
36) Paragraphe 9 Gestion réseau des entités du plan de commande.....	31
37) Nouveaux paragraphes 10.1 et 10.2.....	31
38) Nouveaux paragraphes 11.1 et 11.2.....	32
39) Nouveau paragraphe 12 Résilience.....	37
12 Résilience.....	37
40) Bibliographie.....	38
41) Nouvel Appendice II Exemples d'implémentation.....	39
42) Nouvel Appendice III Relations de résilience.....	41
43) Nouvel Appendice IV Exemple de commande d'appel intercouche.....	46

# Recommandation UIT-T G.8080/Y.1304

## Architecture du réseau optique à commutation automatique (ASON)

### Amendement 2

#### 1) Domaine d'application

Le présent amendement contient des informations mises à jour concernant l'architecture du réseau optique à commutation automatique décrite dans la Rec. UIT-T G.8080/Y.1304. Il contient à la fois des informations nouvelles et des informations provenant de l'Amendement 1. En tant que tel, il remplace l'Amendement 1.

#### 2) Paragraphe 2 Références

*Ajouter les nouvelles références suivantes par ordre alphanumérique:*

- Recommandation UIT-T X.25 (1996), *Interface entre équipement terminal de traitement de données et équipement de terminaison de circuit de données pour terminaux fonctionnant en mode paquet et raccordés par circuit spécialisé à des réseaux publics pour données.*
- Recommandation UIT-T Y.1311 (2002), *Réseaux virtuels privés fournis par le réseau – Architecture générique et prescriptions de service.*
- Recommandation UIT-T Y.1312 (2003), *Prescriptions génériques et éléments architecturaux pour les réseaux privés virtuels de couche 1.*
- Recommandation UIT-T Y.1313 (2004), *Architectures de service et de réseau du réseau privé virtuel de couche 1.*

#### 3) Paragraphe 3 Définitions

*Supprimer le § 3.11 (Définition du réseau de connexion):*

*Ajouter ou modifier la définition des termes suivants:*

**3.5 appel:** association entre deux utilisateurs ou plus et un ou plusieurs domaines, prenant en charge une instance d'un service par le biais d'un ou plusieurs domaines. Dans les domaines, l'association est prise en charge par des entités de réseau qui contiennent l'état d'appel. L'appel est constitué d'un ensemble de segments d'appel concaténés, chaque segment d'appel reliant un utilisateur et une entité de commande d'appel de réseau ou deux entités de commande d'appel de réseau.

**3.5a segment d'appel:** association entre deux entités de commande d'appel (selon la Rec. UIT-T Q.2982, elles sont équivalentes aux contrôleurs d'appel G.8080). Chaque segment d'appel est associé à zéro, une ou plusieurs connexions. Les segments d'appel entre les entités de commande d'appel de réseau sont pris en charge par zéro, un ou plusieurs appels de couche serveur.

**3.ab groupe fermé d'utilisateurs:** voir la Rec. UIT-T X.25.

**3.6 composant:** représentation abstraite d'une entité fonctionnelle. Dans la présente Recommandation, les composants ne représentent pas des instances de code d'implémentation. Ils servent à élaborer des scénarios pour expliquer le fonctionnement de l'architecture.

**3.10 plan de commande:** le plan de commande fournit les fonctions de commande d'appel et de commande de connexion. Il utilise la signalisation pour établir et libérer des connexions et, éventuellement, pour rétablir une connexion en cas de défaillance. Il fournit également d'autres

fonctions servant d'appui à la commande d'appel et à la commande de connexion (dissémination des informations de routage par exemple).

**3.14a rattachement multiple:** un utilisateur est considéré comme étant à rattachement multiple lorsque deux liaisons SNPP ou plus raccordent le conteneur de groupe d'accès au réseau. Les liaisons SNPP peuvent être associées à la même interface UNI si, côté réseau, elles relèvent d'un contrôleur d'appel de réseau commun. Par ailleurs, il existe aussi entre l'utilisateur et le réseau un accord de service tel que le réseau offre une certaine fiabilité, une certaine diversité ou d'autres caractéristiques de service entre les connexions sur les différentes liaisons SNPP du rattachement multiple.

**3.16a route:** séquence de noms de points SNP, de noms de pools SNPP, de noms de zones de routage et/ou de noms de ressources de transport qui sont utilisés par le plan de commande pour créer une connexion de réseau.

**3.16b zone de routage:** zone constituée d'un ensemble de sous-réseaux, des liaisons SNPP qui les interconnectent et des pools SNPP représentant les extrémités des liaisons SNPP qui sortent de cette zone de routage. Une zone de routage peut contenir des zones de routage plus petites interconnectées par des liaisons SNPP. La limite de subdivision correspond à une zone de routage contenant un seul sous-réseau.

**3.16c niveau de routage:** relation entre une zone de routage et une zone de routage contenante ou des zones de routage contenues. La hiérarchie de contenance des zones de routage crée des niveaux de routage.

**3.26 réseau privé virtuel:** voir la Rec. UIT-T Y.1311.

#### 4) Paragraphe 4 Abréviations

*Supprimer "logique" et "logiciel" du texte des abréviations E-NNI, I-NNI et UNI et ajouter par ordre alphabétique les abréviations suivantes provenant de l'Amendement 1.*

AGC	conteneur de groupe d'accès ( <i>access group container</i> )
DA	agent de découverte ( <i>discovery agent</i> )
MI	informations de gestion ( <i>management information</i> )
MO	objet géré ( <i>managed object</i> )
TAP	exécuteur de terminaison et d'adaptation ( <i>termination and adaptation performer</i> )

#### 5) Modification du numéro de certaines Figures

*Par le présent amendement, de nouvelles figures sont ajoutées dans la Rec. G.8080/Y.1304. Cela étant, il convient d'apporter les modifications suivantes dans la Recommandation G.8080/Y.1304:*

- La Figure 29/G.8080/Y.1304 devient la Figure 40/G.8080/Y.1304 et toutes les références à la Figure 29 deviennent des références à la Figure 40.*
- La Figure 28/G.8080/Y.1304 devient la Figure 39/G.8080/Y.1304 et toutes les références à la Figure 28 deviennent des références à la Figure 39.*
- La Figure 27/G.8080/Y.1304 devient la Figure 38/G.8080/Y.1304 et toutes les références à la Figure 27 deviennent des références à la Figure 38.*
- La Figure 26/G.8080/Y.1304 devient la Figure 37/G.8080/Y.1304 et toutes les références à la Figure 26 deviennent des références à la Figure 37.*
- La Figure 25/G.8080/Y.1304 devient la Figure 36/G.8080/Y.1304 et toutes les références à la Figure 25 deviennent des références à la Figure 36.*



- *La Figure 24/G.8080/Y.1304 devient la Figure 35/G.8080/Y.1304 et toutes les références à la Figure 24 deviennent des références à la Figure 35.*
- *La Figure 23/G.8080/Y.1304 devient la Figure 34/G.8080/Y.1304 et toutes les références à la Figure 23 deviennent des références à la Figure 34.*
- *La Figure 22/G.8080/Y.1304 devient la Figure 29/G.8080/Y.1304 et toutes les références à la Figure 22 deviennent des références à la Figure 29.*
- *La Figure 21/G.8080/Y.1304 devient la Figure 28/G.8080/Y.1304 et toutes les références à la Figure 21 deviennent des références à la Figure 28.*
- *La Figure 20/G.8080/Y.1304 devient la Figure 27/G.8080/Y.1304 et toutes les références à la Figure 20 deviennent des références à la Figure 27.*
- *La Figure 19/G.8080/Y.1304 devient la Figure 26/G.8080/Y.1304 et toutes les références à la Figure 19 deviennent des références à la Figure 26.*
- *La Figure 18/G.8080/Y.1304 devient la Figure 25/G.8080/Y.1304 et toutes les références à la Figure 18 deviennent des références à la Figure 25.*
- *La Figure 17/G.8080/Y.1304 devient la Figure 24/G.8080/Y.1304 et toutes les références à la Figure 17 deviennent des références à la Figure 24.*
- *La Figure 16/G.8080/Y.1304 devient la Figure 23/G.8080/Y.1304 et toutes les références à la Figure 16 deviennent des références à la Figure 23.*
- *La Figure 15/G.8080/Y.1304 devient la Figure 22/G.8080/Y.1304 et toutes les références à la Figure 15 deviennent des références à la Figure 22.*
- *La Figure 14/G.8080/Y.1304 devient la Figure 21/G.8080/Y.1304 et toutes les références à la Figure 14 deviennent des références à la Figure 21.*
- *La Figure 13/G.8080/Y.1304 devient la Figure 20/G.8080/Y.1304 et toutes les références à la Figure 13 deviennent des références à la Figure 20.*
- *La Figure 12/G.8080/Y.1304 devient la Figure 19/G.8080/Y.1304 et toutes les références à la Figure 12 deviennent des références à la Figure 19.*
- *La Figure 11/G.8080/Y.1304 devient la Figure 18/G.8080/Y.1304 et toutes les références à la Figure 11 deviennent des références à la Figure 18.*
- *La Figure 10/G.8080/Y.1304 devient la Figure 17/G.8080/Y.1304 et toutes les références à la Figure 10 deviennent des références à la Figure 17.*
- *La Figure 9/G.8080/Y.1304 devient la Figure 16/G.8080/Y.1304 et toutes les références à la Figure 9 deviennent des références à la Figure 16.*
- *La Figure 8/G.8080/Y.1304 devient la Figure 15/G.8080/Y.1304 et toutes les références à la Figure 8 deviennent des références à la Figure 15.*
- *La Figure 7/G.8080/Y.1304 devient la Figure 14/G.8080/Y.1304 et toutes les références à la Figure 7 deviennent des références à la Figure 14.*
- *La Figure 6/G.8080/Y.1304 devient la Figure 11/G.8080/Y.1304 et toutes les références à la Figure 6 deviennent des références à la Figure 11.*
- *La Figure 5/G.8080/Y.1304 devient la Figure 6/G.8080/Y.1304 et toutes les références à la Figure 5 deviennent des références à la Figure 6.*
- *La Figure 4/G.8080/Y.1304 devient la Figure 5/G.8080/Y.1304 et toutes les références à la Figure 4 deviennent des références à la Figure 5.*
- *La Figure 3/G.8080/Y.1304 devient la Figure 4/G.8080/Y.1304 et toutes les références à la Figure 3 deviennent des références à la Figure 4.*
- *La Figure 2/G.8080/Y.1304 devient la Figure 3/G.8080/Y.1304 et toutes les références à la Figure 2 deviennent des références à la Figure 3.*

## 6) Paragraphe 5

*Remplacer les alinéas, du sixième au dixième, du § 5 par le texte qui suit:*

Le plan de commande sera mis en œuvre dans le contexte des pratiques d'exploitation des opérateurs commerciaux et de l'hétérogénéité multidimensionnelle des réseaux de transport. Il faut tenir compte de ces considérations commerciales et opérationnelles au niveau de l'architecture et prévoir, par exemple, des barrières logiques solides afin de protéger les pratiques d'exploitation des opérateurs commerciaux, les réseaux de transport étant segmentés en domaines compte tenu de considérations de gestion et/ou de politique, et de l'hétérogénéité intrinsèque de ces réseaux (y compris la commande et la gestion). Le concept de domaine figurant dans la définition G.805 de domaine administratif et le concept de régions administratives de l'Internet (par exemple, systèmes autonomes) ont été généralisés dans l'architecture du plan de commande afin de prendre en considération des responsabilités administratives et/ou de gestion différentes, des relations de confiance différentes, des systèmes d'adressage différents, des capacités d'infrastructure différentes, des techniques de survie différentes, des répartitions de la fonctionnalité de commande différentes, etc. Les domaines sont établis selon les politiques des opérateurs et possèdent un ensemble de critères d'appartenance (voir les exemples ci-dessus).

Le plan de commande prend en charge des services par le biais de la configuration automatique de connexions de transport de bout en bout à travers un ou plusieurs domaines. Pour cela, une perspective service et une perspective connexion entrent en jeu:

- la perspective service (appel) correspond à la prise en charge de la fourniture de services de bout en bout tout en conservant le caractère indépendant des divers opérateurs concernés;
- la perspective connexion correspond à la configuration automatique de connexions de réseau (à l'appui d'un service) qui couvrent un ou plusieurs domaines.

Les informations sur l'état des connexions (par exemple faute et qualité du signal) sont détectées par le plan de transport et fournies au plan de commande.

Le plan de commande achemine (distribue) des informations sur l'état de "liaison" (par exemple adjacence, capacité disponible et défaillance) servant pour l'établissement, la libération et la restauration des connexions.

Les informations détaillées de gestion des fautes ou de supervision des performances sont transportées dans le plan de transport (par le biais des informations de préfixe/OAM) et par le biais du plan de gestion (incluant le réseau RCD).

L'interconnexion interdomaines et l'interconnexion intradomaine sont décrites en termes de points de référence. Comme les domaines sont établis selon les politiques des opérateurs, les points de référence interdomaines sont des points de délimitation de service pour une seule couche de service (c'est-à-dire des points où la commande d'appel est assurée). L'échange d'informations en ces points de référence est décrit par les multiples interfaces abstraites qui existent entre les composants de commande. Une interface physique est réalisée par le mappage d'une ou plusieurs interfaces abstraites vers un protocole. Des interfaces abstraites multiples peuvent être multiplexées sur une interface physique unique. Le point de référence entre le domaine d'un utilisateur et le domaine d'un fournisseur est l'interface UNI. Le point de référence entre domaines est l'interface E-NNI, qui représente un point de délimitation de service prenant en charge l'établissement de connexion multidomaine. Un point de référence intradomaine est une interface I-NNI, qui représente un point de connexion prenant en charge l'établissement de connexion intradomaine. Le § 8 donne une description plus approfondie des flux d'informations en ces points de référence.

## 7) **Paragraphe 5.1 Commandes d'appel et de connexion**

*Ajouter les deux alinéas suivants à la fin du § 5.1:*

La commande d'appel est assurée à l'entrée du réseau (c'est-à-dire au point de référence d'interface UNI). Elle peut également être assurée aux passerelles entre domaines (c'est-à-dire au point de référence d'interface E-NNI). Les fonctions remplies par les contrôleurs d'appel aux frontières des domaines sont définies par les politiques associées aux interactions autorisées entre les domaines. Ces politiques sont établies par l'opérateur. A ce titre, un appel de bout en bout est considéré comme étant composé de multiples segments d'appel, selon les multiples domaines traversés. Cette décomposition offre une certaine souplesse concernant le choix des paradigmes de signalisation, de routage et de rétablissement dans les différents domaines.

Il est à noter que l'appel est la représentation du service offert à l'utilisateur d'une couche Réseau, alors que les connexions constituent l'un des moyens par lesquels les réseaux offrent lesdits services. D'autres entités peuvent être utilisées pour prendre en charge les appels, par exemple les entités contenant des processus propres à un service.

## 8) **Paragraphe 5.1.1 Commande d'appel**

*Modification sans objet pour le texte français.*

## 9) **Nouveau paragraphe 5.2 Interaction entre plans de commande, de transport et de gestion**

*Ajouter le nouveau paragraphe suivant:*

### **5.2 Interaction entre plans de commande, de transport et de gestion**

La Figure 1 illustre les relations générales entre les plans de commande, de gestion et de transport. Chaque plan est autonome, mais il existe des interactions entre les divers plans, qui sont détaillées dans les paragraphes qui suivent.

#### **5.2.1 Interaction gestion-transport**

Le plan de gestion interagit avec les ressources de transport en fonctionnant conformément à un modèle informationnel approprié, qui présente une vue gestion de la ressource sous-jacente. Les objets du modèle informationnel sont physiquement situés au même endroit que la ressource de transport; ils interagissent avec cette ressource par l'intermédiaire des interfaces d'informations de gestion (MI, *management information*) du modèle fonctionnel propre à une couche. Ces interfaces devraient être situées au même endroit que l'objet géré et que le composant de commande.

#### **5.2.2 Interaction commande-transport**

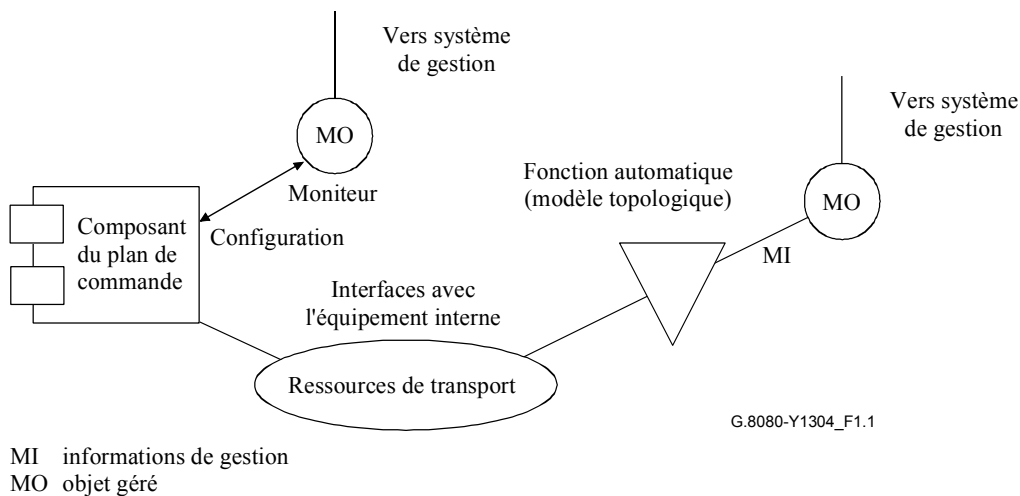
Seuls deux composants architecturaux possèdent une forte relation avec une ressource de transport physique.

A la limite inférieure de récurrence, le contrôleur de connexion (CC) fournit une interface de signalisation afin de commander une fonction de connexion. Ce composant est physiquement situé au même endroit que la fonction de connexion et tous les autres détails relatifs au matériel sont masqués. Cependant, comme le flux d'informations est limité, un nouveau protocole peut être utile afin d'optimiser cette communication. L'exécuteur de terminaison et d'adaptation (TAP, *termination and adaptation performer*) est physiquement situé au même endroit que l'équipement qui fournit les fonctions d'adaptation et de terminaison; il offre une vue des connexions de liaison depuis le plan de commande. L'exécuteur TAP masque l'interaction avec le matériel.

### 5.2.3 Interaction gestion-commande

Le paragraphe 7.1 indique que tout composant possède un ensemble d'interfaces spéciales qui permettent la supervision de son fonctionnement, la détermination dynamique des politiques et l'affectation d'un comportement interne. Ces interfaces sont équivalentes à l'interface MI du modèle fonctionnel de transport: elles permettent au composant de présenter une vue à un système de gestion et d'être configuré par ce système. Ceci est discuté plus loin au § 7.1.

Le plan de gestion interagit avec les composants de commande en fonctionnant conformément à un modèle informationnel approprié, qui présente une vue gestion du composant sous-jacent. Les objets du modèle informationnel sont physiquement situés au même endroit qu'un composant de commande; ils interagissent avec ce composant par le biais des interfaces de moniteur et de configuration de ce composant. Ces interfaces devraient être situées au même endroit que l'objet géré et que le composant de commande.



**Figure 2/G.8080/Y.1304 – Interactions du plan de gestion/transport avec les ressources de transport**

Au bas de la figure se trouve un ensemble de ressources physiques de transport, qui représentent la réalité physique de l'équipement. Cette réalité est décrite en termes de fonctions atomiques G.805. Les objets gérés (MO, *managed object*), qui représentent la vue gestion externe de l'équipement, interagissent avec le modèle fonctionnel spécifié dans les Recommandations relatives aux équipements par le biais des points de référence MI, qui sont par ailleurs complètement intégrés dans les équipements. Il est à noter que l'objet géré représente la vue gestion quel que soit le protocole de gestion utilisé. Ces informations sont indépendantes du protocole utilisé.

Du point de vue du plan de commande, les composants de celui-ci opèrent directement sur les ressources de transport, de sorte que le fonctionnement du plan de commande apparaît au plan de gestion comme étant autonome. De même, les opérations du plan de gestion apparaissent au plan de commande comme étant autonomes. C'est exactement la même situation que l'on trouve lorsque de multiples gestionnaires gèrent un équipement. Chaque gestionnaire ignore l'existence de chacun des autres et voit simplement un comportement autonome de l'équipement. Bien que les informations présentées au plan de commande soient semblables à celles qui sont présentées à la gestion, elles ne sont pas identiques aux informations MI. Les informations du plan de commande se superposent aux données MI parce que le plan de commande nécessite une partie mais non la totalité des informations de gestion. Par exemple, un rétablissement est susceptible d'être déclenché par les mêmes conditions que celles qui déclenchent normalement les actions de protection.

Les objets gérés propres à un composant présentent une vue gestion des composants du plan de commande par l'intermédiaire des interfaces de moniteur du composant. Il est essentiel de comprendre que c'est la vue des aspects gérables du composant, et non une vue de la ressource de transport, qui est obtenue par le biais de la vue gestion.

## 10) Paragraphe 6.1 Entités de transport

*Remplacer le cinquième alinéa du § 6.1 par l'alinéa suivant:*

Les états des points SNP et des connexions de liaison entre points SNP qui sont utiles au plan de commande sont décrits respectivement au § 7.3.7 (Exécuteurs de terminaison et d'adaptation) et au § 7.3.3 (Composant "gestionnaire de ressource de liaison" (LRMA et LRMZ)).

*Remplacer les neuvième et dixième alinéas (paragraphe non numéroté: **Ressources de liaisons partagées entre réseaux VPN**) par le texte suivant:*

La Rec. UIT-T Y.1313 définit plusieurs modèles de service de base dans lesquels des réseaux VPN de couche 1 (L1VPN, *layer one VPN*) peuvent être pris en charge par le biais de l'architecture de réseau ASON.

Un VPN est un groupe fermé d'utilisateurs pouvant utiliser un ensemble défini de ressources de réseau. Dans le plan de commande, un pool SNPP peut être public, c'est-à-dire n'être associé à aucun VPN, ou être privé, c'est-à-dire être associé à exactement un VPN. Dans un VPN, le routage de connexion peut uniquement utiliser les pools SNPP associés à ce VPN. Dans le plan de transport, un point de connexion peut être assigné à un point SNP dans plusieurs pools SNPP, publics ou privés. Il est possible de modéliser la connectivité sur une liaison partagée entre VPN en créant un point SNP pour chacun des points de connexion partagés dans chaque VPN. Lorsqu'un point de connexion est attribué à un point SNP donné dans un VPN, les points SNP représentant les mêmes ressources dans les autres VPN passent à l'état occupé. La Figure 5 donne un exemple de deux VPN, possédant chacun deux points SNP dans le plan de commande. Dans le plan de transport, le premier point de connexion est assigné et attribué au deuxième point SNP du VPN 2, le troisième point de connexion est assigné et attribué au deuxième point SNP du VPN 1 et le deuxième point de connexion est assigné à la fois au premier point SNP du VPN 1 et au premier point SNP du VPN 2. Si le deuxième point de connexion est attribué au premier point SNP du VPN 1, ce point SNP passe à l'état disponible tandis que le premier point SNP du VPN 2 passe à l'état occupé.

## 11) Paragraphe 6.2 Zones de routage

*Dans la dernière phrase du premier alinéa, remplacer "contenant deux sous-réseaux et une liaison" par "contenant un sous-réseau".*

*Dans la première phrase du deuxième alinéa, remplacer "utilisent un identificateur de pool SNPP commun pour faire référence à cette liaison SNPP" par "contiennent des liaisons SNPP coïncidentes".*

*Insérer le texte suivant comme nouveau deuxième alinéa:*

Les zones de routage et les sous-réseaux sont très étroitement liés, les deux assurant une fonction identique de partitionnement d'un réseau. La différence fondamentale est qu'à la frontière, les extrémités de liaison sont visibles depuis *l'intérieur* d'une zone de routage, tandis que depuis *l'intérieur* d'un sous-réseau, on ne peut voir que les points de connexion. Vus depuis *l'extérieur*, les sous-réseaux et les zones de routage sont identiques et les termes sous-réseau et zone de routage peuvent quasiment être utilisés l'un pour l'autre. La distinction entre les deux est généralement évidente d'après le contexte, même si le terme *nœud* est souvent utilisé pour désigner soit un sous-réseau soit une zone de routage. Il est par ailleurs à noter que depuis l'extérieur des sous-réseaux et des zones de routage, il est impossible de voir les détails internes, les sous-réseaux

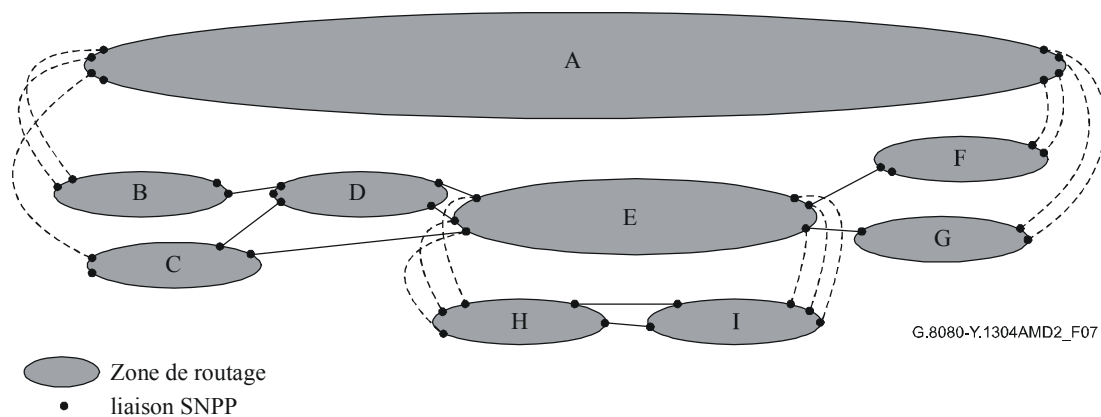
et les zones de routage apparaissant sous la forme de points dans le graphe de la topologie de réseau.

## 12) Nouveau paragraphe 6.2.1 Agrégation de liaisons et de zones de routage

Ajouter le nouveau paragraphe suivant après l'introduction du § 6.2:

### 6.2.1 Agrégation de liaisons et zones de routage

La Figure 7 illustre les relations entre zones de routage et pools de points de sous-réseau (liaisons SNPP). Zones de routage et liaisons SNPP peuvent être associées hiérarchiquement. Dans l'exemple, la zone de routage A est partitionnée de façon à créer un niveau inférieur de zones de routage, B, C, D, E, F, G et de liaisons SNPP d'interconnexion. Cette récurrence peut être répétée autant de fois que nécessaire. Par exemple, la zone de routage E est repartitionnée afin de révéler les zones de routage H et I. Dans l'exemple donné, il y a une seule zone de routage de niveau supérieur absolu. Lors de la création d'une structure hiérarchique de zones de routage fondée sur la "contenance" (hiérarchie dans laquelle les zones de routage de niveau inférieur sont complètement contenues dans une seule zone de routage de niveau supérieur), seuls un sous-ensemble des zones de routage de niveau inférieur et un sous-ensemble de leurs liaisons SNPP sont sur la frontière de la zone de routage de niveau supérieur. La structure interne du niveau inférieur est visible par le niveau supérieur à partir de l'intérieur de la zone A mais non à partir de l'extérieur de A. Par conséquent, seules les liaisons SNPP situées à la frontière entre un niveau supérieur et un niveau inférieur sont visibles par le niveau supérieur à partir de l'extérieur de A. Les liaisons SNPP les plus extérieures des zones B et C et F et G sont donc visibles à partir de l'extérieur de A mais non les liaisons SNPP internes qui sont associées aux zones D et E ni celles qui sont situées entre les zones B et D, C et D, C et E ou entre E et F ou E et G. La même visibilité s'applique entre E et ses zones subordonnées H et I. Cette visibilité de la frontière entre niveaux est récurrente. Les hiérarchies de liaisons SNPP ne sont donc créées qu'aux points où les zones de routage de niveau supérieur sont limitées par des liaisons SNPP situées dans des zones de routage de niveau inférieur.



**Figure 7/G.8080/Y.1304 – Exemple de hiérarchie de zones de routage et de relations avec les liaisons SNPP**

Les points de sous-réseau sont attribués à une liaison SNPP au niveau le plus bas de la hiérarchie de routage. Ils ne peuvent être attribués qu'à un seul pool de points de sous-réseau à ce niveau. Aux frontières de la hiérarchie des zones de routage, le pool de liaisons SNPP de niveau inférieur est entièrement contenu dans une liaison SNPP de niveau supérieur. Un pool de liaisons SNPP de niveau supérieur peut contenir une ou plusieurs liaisons SNPP de niveau inférieur. A tout niveau de cette hiérarchie, une liaison SNPP est associée à une seule zone de routage. En tant que telles, les zones de routage ne se superposent à aucun niveau de la hiérarchie. Les liaisons SNPP qui sont situées à l'intérieur d'un niveau de la hiérarchie des zones de routage mais qui ne sont pas situées à

la frontière d'un niveau supérieur peuvent se trouver à la frontière avec un niveau inférieur, créant à partir de là une hiérarchie de liaisons SNPP (par exemple, zone de routage E). Ce processus permet de créer une hiérarchie de contenance pour des liaisons SNPP.

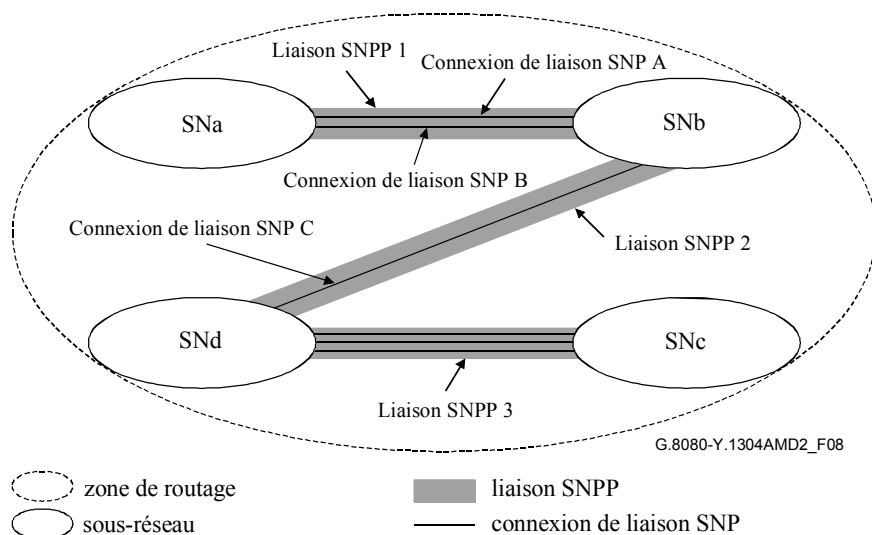
Une zone de routage peut avoir un espace de noms SNPP indépendant de ceux qui sont utilisés dans les autres zones de routage. Il est à noter qu'un nom SNPP est routable dans la zone de routage à l'espace de noms SNPP de laquelle il appartient.

### 13) Nouveau paragraphe 6.2.2 Relation avec les liaisons et agrégation de liaisons

Ajouter le nouveau paragraphe 6.2.2 comme suit:

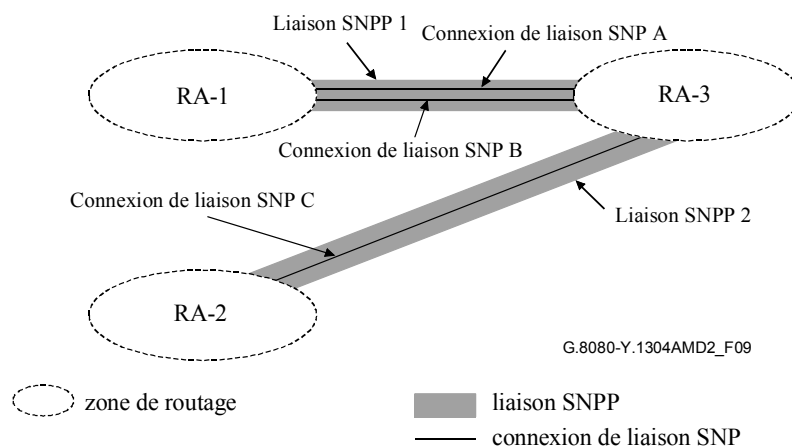
#### 6.2.2 Relation avec les liaisons et agrégation de liaisons

Dans une zone de routage donnée, un certain nombre de connexions de liaison SNP peut être assigné à la même liaison SNPP si et seulement si ces connexions sont établies entre les deux mêmes sous-réseaux. C'est ce qui est illustré sur la Figure 8. Quatre sous-réseaux, SNa, SNb, SNc et SNd, ainsi que les liaisons SNPP 1, 2 et 3, se trouvent dans une même zone de routage. Les connexions de liaison SNP A et B sont dans la liaison SNPP 1. Les connexions de liaison SNP B et C ne peuvent pas être dans la même liaison SNPP parce qu'elles ne connectent pas les deux mêmes sous-réseaux. Un comportement similaire s'applique également au groupement de points SNP entre des zones de routage.



**Figure 8/G.8080/Y.1304 – Relation entre liaisons SNPP et sous-réseaux**

La Figure 9 montre trois zones de routage: RA-1, RA-2 et RA-3 et les liaisons SNPP 1 et 2. Les connexions de liaison SNP A, B et C ne peuvent pas être dans la même liaison SNPP parce que leurs extrémités aboutissent dans plus de deux zones de routage. Les connexions de liaison SNP A et B ne sont pas équivalentes à la connexion de liaison SNP C pour le routage à partir de la zone de routage 3 (RA-3).



**Figure 9/G.8080/Y.1304 – Relations entre liaisons SNPP et zones de routage**

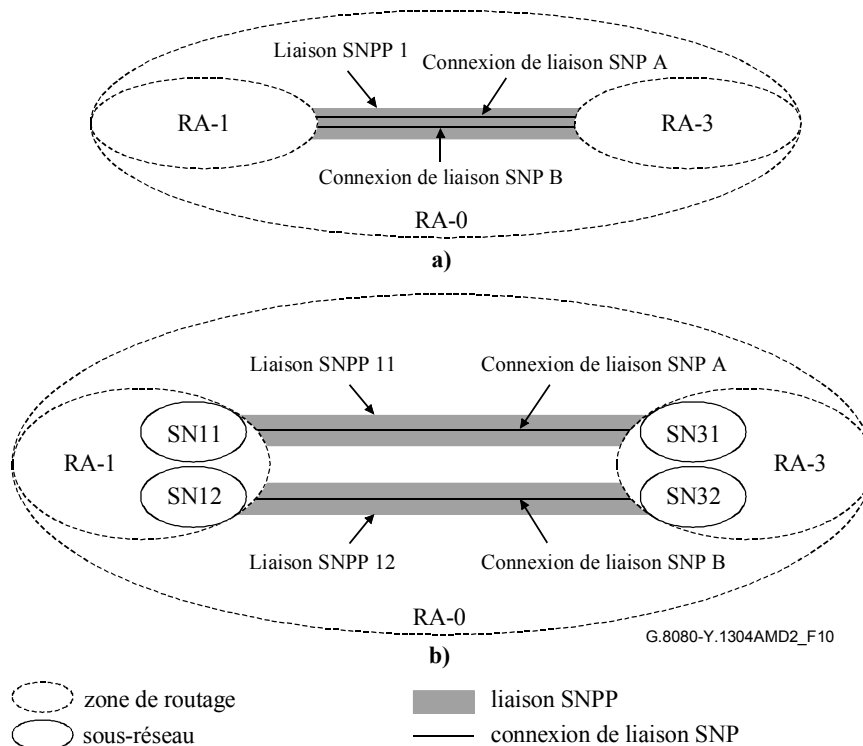
Les connexions de liaison SNP entre deux zones de routage, ou entre deux sous-réseaux, peuvent être groupées en une ou plusieurs liaisons SNPP. Le groupement en de multiples liaisons SNPP peut être requis:

- si ces liaisons ne sont pas équivalentes en termes de routage par rapport aux zones de routage auxquelles ces liaisons sont rattachées, ou par rapport à la zone de routage contenante;
- si de plus petits groupements sont requis à des fins administratives.

Il peut y avoir plusieurs domaines de validité du routage à considérer lors de l'organisation de connexions de liaison SNP dans des liaisons SNPP. Sur la Figure 10, il y a deux connexions de liaison SNP entre les zones de routage 1 et 3. Si ces deux zones de routage sont au sommet de la hiérarchie de routage (et qu'il n'y a donc pas une seule zone de routage de niveau supérieur absolu), alors le domaine de validité du routage des zones RA-1 et RA-3 est utilisé afin de déterminer si les connexions de liaison SNP sont équivalentes en termes de routage.

La situation peut cependant être conforme à la Figure 10, où la zone RA-0 est une zone de routage contenante. Du point de vue de la zone RA-0, les connexions de liaison SNP A et B peuvent se trouver dans une seule vue a) ou dans deux vue b) liaisons SNPP. Un exemple de cas où une seule liaison SNPP est suffisante se présente lorsque la zone RA-0 utilise un paradigme de routage pas à pas. Le calcul de trajet n'établit aucune distinction entre les connexions de liaison SNP A et B en tant que prochaine étape pour passer par exemple de la zone RA-1 à la zone RA-2.





**Figure 10/G.8080/Y.1304 – Domaine de validité du routage**

Du point de vue des zones RA-1 et RA-3, les connexions de liaison SNP peuvent toutefois être tout à fait distinctes en termes de routage s'il est souhaitable, par exemple, de choisir la connexion de liaison SNP A plutôt que la connexion de liaison SNP B pour des raisons de coût, de protection, etc. Dans ce cas, le fait de placer chaque connexion de liaison SNP dans sa propre liaison SNPP répond à l'exigence "d'équivalence aux fins du routage". Il est à noter que, sur la Figure 10, les liaisons SNPP 11, 12 et 1 peuvent toutes coexister.

Le fait de choisir la liaison SNPP 11 (Figure 10 b) plutôt que la liaison SNPP 12 peut également résulter du fait que le coût du franchissement de la zone RA-3 est différent à partir des deux liaisons. Il serait donc utile de prévoir un mécanisme permettant de déterminer le coût relatif de franchissement de la zone RA-3 à partir des deux liaisons. Ce mécanisme pourrait être utilisé de façon récurrente pour déterminer le coût relatif de franchissement de la zone RA-0. Il est à noter que cela n'implique pas que la topologie interne d'une zone de routage soit exposée à l'extérieur du domaine de validité. On pourrait invoquer une fonction d'interrogation, qui renverrait le coût associé à une route particulière. Ce coût serait déterminé en fonction de la politique appliquée à chaque zone de routage. Il conviendrait d'utiliser une politique commune dans toutes les zones de routage, afin de pouvoir comparer les coûts. Ce type de fonction pourrait par ailleurs être généralisé de manière à appliquer des contraintes de routage avant de calculer le coût.

#### 14) **Paragraphe 6.3 Topologie et découverte**

*Modification sans objet pour le texte français.*

#### 15) **Nouveau paragraphe 6.4 Domaines**

*Ajouter le nouveau paragraphe 6.4 comme suit:*

## 6.4 Domaines

Comme indiqué au § 5, nous avons généralisé le concept de domaine figurant dans la définition G.805 des domaines administratif et de gestion ainsi que le concept de régions administratives de l'Internet, afin de prendre en considération des responsabilités administratives et/ou de gestion différentes, des relations de confiance différentes, des systèmes d'adressage différents, des capacités d'infrastructure différentes, des techniques de survie différentes, des répartitions de la fonctionnalité de commande différentes, etc. Un domaine représente donc un ensemble d'entités qui sont groupées pour une fin particulière.

Un domaine de commande comprend un ensemble de composants de plan de commande et constitue une construction architecturale qui encapsule et masque les détails d'une implémentation répartie d'un groupe particulier de composants architecturaux d'un ou de plusieurs types. Il permet de décrire un groupe de composants répartis de telle façon que le groupe puisse être représenté par des interfaces de répartition relatives à une seule entité: le domaine, qui possède des caractéristiques identiques à celles des interfaces d'origine de répartition des composants. Les informations échangées entre domaines de commande utilisent la sémantique commune des informations échangées entre interfaces de répartition de composants, des représentations différentes étant possibles à l'intérieur du domaine.

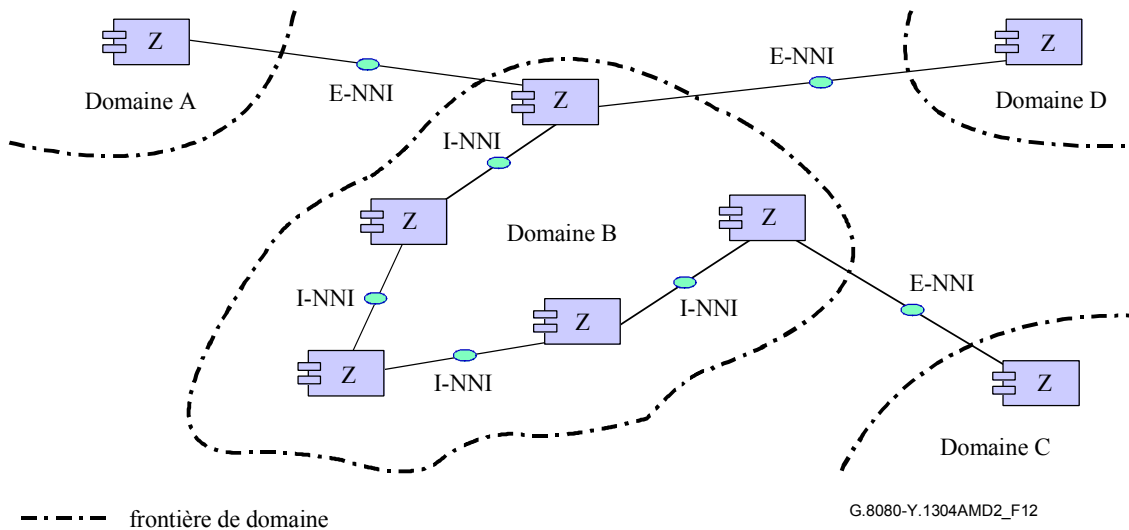
Généralement, un domaine de commande est dérivé d'un ou de plusieurs types particuliers de composants qui interagissent pour une finalité particulière. Par exemple, les domaines (de commande) de routage sont dérivés de contrôleurs de routage tandis qu'un domaine de reroutage est dérivé d'un ensemble de contrôleurs de connexion et de contrôleurs d'appel de réseau qui se partagent la responsabilité du reroutage/rétablissement de connexions/d'appels qui traversent ce domaine. Dans ces deux exemples, l'opération qui se produit (routage ou reroutage) est contenue entièrement dans le domaine. Dans la présente Recommandation, les domaines de commande sont décrits par rapport aux composants associés à un réseau de couche.

Etant donné qu'un domaine est défini en termes de finalité, il est évident que les domaines définis pour une finalité donnée n'ont pas besoin de coïncider avec des domaines définis pour une autre finalité. Les domaines du même type sont restreints en ce sens qu'ils peuvent:

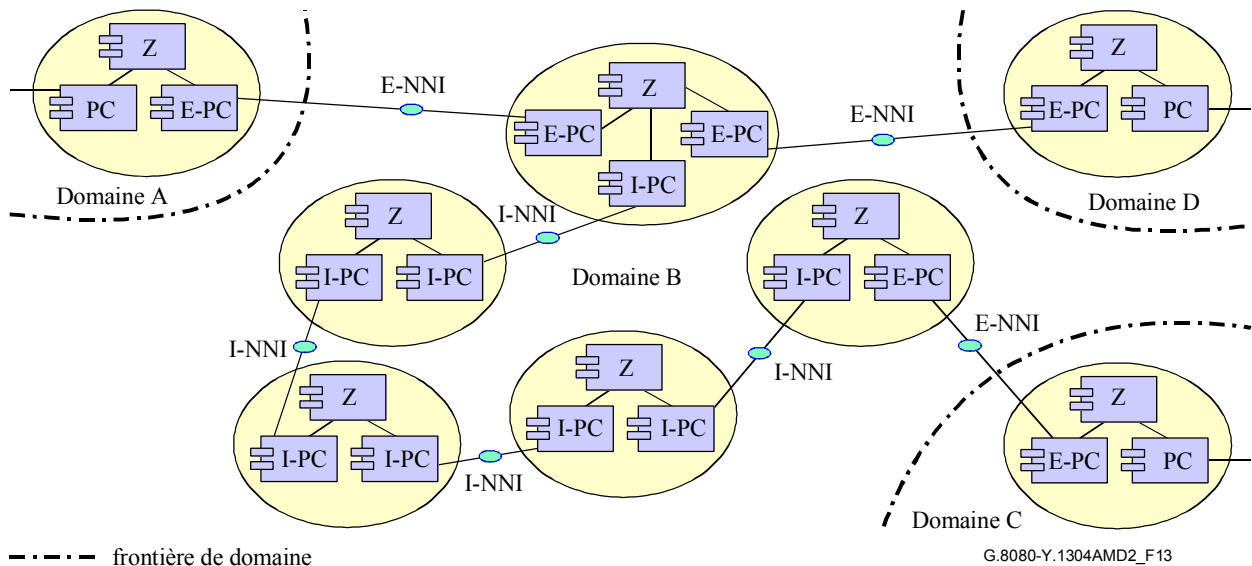
- contenir entièrement d'autres domaines du même type, mais sans superposition;
- être contigus les uns avec les autres;
- être isolés les uns des autres.

Un exemple de relation entre composants, domaines et points de référence est fourni sur la Figure 12, qui montre un domaine, B, et sa relation avec les domaines A, C et D. Chaque domaine est dérivé d'un composant de type Z. La structure interne et les interactions peuvent être différentes dans chaque domaine: elles peuvent par exemple utiliser différents modèles de fédération.

Le même exemple est représenté sur la Figure 13 avec les relations entre composants, domaines et interfaces. Les composants interagissent par l'intermédiaire de leurs contrôleurs de protocole, au moyen du protocole I pour les contrôleurs I-PC et au moyen du protocole E pour les contrôleurs E-PC. Il est également possible que le protocole utilisé en interne dans le domaine A, par exemple, soit différent de celui qui est utilisé dans le domaine B, et que le protocole utilisé entre B et C soit différent de celui qui est utilisé entre A et B. Les interfaces I-NNI sont situées entre des contrôleurs de protocole contenus dans un même domaine tandis que les interfaces E-NNI sont situées entre des contrôleurs de protocole contenus dans des domaines différents.



**Figure 12/G.8080/Y.1304 – Relation entre domaines, contrôleurs de protocole et points de référence**



**Figure 13/G.8080/Y.1304 – Relation entre domaines, contrôleurs de protocole et interfaces**

#### 6.4.1 Relation entre domaines de commande et ressources du plan de commande

Les composants d'un domaine peuvent, selon la finalité, refléter les ressources du réseau de transport sous-jacent. Un domaine de commande de routage peut, par exemple, contenir des composants qui représentent une ou plusieurs zones de routage à un ou à plusieurs niveaux d'agrégation, selon la méthode ou le protocole de routage utilisé dans tout ce domaine.

#### 6.4.2 Relation entre domaines de commande, interfaces et points de référence

Les interfaces I-NNI et E-NNI sont toujours situées entre des contrôleurs de protocole. Les protocoles exécutés entre les contrôleurs de protocole n'utilisent pas nécessairement des liaisons SNPP dans le réseau de transport commandé, de sorte qu'il est incorrect de représenter des interfaces I-NNI et E-NNI sur des liaisons SNPP.

Les points de référence I-NNI et E-NNI sont situés entre des composants du même type, où le type de composant n'est pas un contrôleur de protocole, et permettent de représenter le transfert de primitives (voir le § 7).

Dans un diagramme montrant seulement les domaines et les relations entre eux (sans révéler la structure interne de ces domaines), le transfert d'informations est censé passer par un point de référence.

## **16) Nouveau paragraphe 6.5 Aspects relatifs aux couches multiples**

*Ajouter le nouveau paragraphe 6.5 comme suit:*

### **6.5 Aspects relatifs aux couches multiples**

La description du plan de commande peut être subdivisée entre aspects associés à un seul réseau de couche, comme le routage, la création et la suppression de connexions, etc., et aspects qui se rapportent à des couches multiples. La relation client/serveur entre réseaux de couche est gérée au moyen des exécuteurs de terminaison et d'adaptation (voir § 7.3.7). La topologie et la connexité de toutes les couches serveur sous-jacentes ne sont pas immédiatement visibles par la couche client. Au contraire, ces aspects des couches serveur sont encapsulés et présentés au réseau de couche client comme une liaison SNPP. Lorsque la connexité ne peut pas être réalisée dans la couche client en raison d'une insuffisance de ressources, des ressources complémentaires ne peuvent être créées qu'au moyen de nouvelles connexions dans un ou plusieurs réseaux de couche serveur, créant ainsi de nouvelles connexions de liaison SNP dans le réseau de couche client. Cette création peut être réalisée par modification de points SNP en les faisant passer de l'état potentiel à l'état disponible, ou par adjonction d'une infrastructure supplémentaire en tant que résultat d'un processus de planification. La capacité de créer de nouvelles ressources de couche client au moyen de nouvelles connexions dans un ou plusieurs réseaux de couche serveur est donc un préalable à la fourniture de connexité dans le réseau de couche client. Le modèle fourni dans la présente Recommandation permet de répéter ce processus dans chaque réseau de couche. L'échelle de temps selon laquelle la connexité de couche serveur est fournie pour la création d'une topologie de couche client est soumise à un certain nombre de contraintes externes (comme une prévision de trafic à long terme pour la liaison, la planification du réseau et l'autorité financière) et est propre à chaque opérateur. L'architecture prend en charge la connexité de couche serveur qui est créée en réponse à une demande de nouvelle topologie émise par une couche client au moyen de points SNP potentiels, qui restent à découvrir.

## **17) Nouveau paragraphe 6.6 Prise en charge de client intercouches**

*Ajouter le nouveau paragraphe 6.6 comme suit:*

### **6.6 Prise en charge de client intercouches**

Dans les réseaux de transport, les éléments de réseau peuvent prendre en charge plusieurs couches. Par exemple, en périphérie d'un réseau multicouche, on peut trouver des adaptations vers des largeurs de bande plus petites, alors que de telles adaptations ne sont pas nécessairement prises en charge au milieu du réseau multicouche. Se pose alors, de manière générale, le problème du transfert de l'information caractéristique client (CI, *characteristic information*) en l'absence de réseau de couche client continu/connecté entre deux conteneurs AGC client.

Il existe deux solutions à ce problème. Premièrement, des liaisons de couche client peuvent être créées à partir des connexions de couche serveur. Ces liaisons seraient visibles par le contrôleur de routage de la zone de routage dans laquelle elles apparaissent (voir le § 6.5). Deuxièmement, l'information caractéristique client peut être adaptée, éventuellement plusieurs fois, sur les connexions de couche serveur. Cette information ne serait pas visible par le contrôleur de routage client.

Les interfaces entre contrôleurs NCC situés dans des réseaux de couche différents sont utilisées pour appliquer des fonctions de réseau ASON pour la deuxième solution. Cette interface intercouches permet de procéder à une association entre les appels dans une relation entre couches client/serveur. Cette association peut être faite de façon récurrente afin de refléter un ensemble d'adaptations "empilées". Autrement dit, une récurrence est appliquée parmi les contrôleurs NCC en fonction des couches G.805. Les contrôleurs NCC situés dans des couches différentes peuvent continuer à être instanciés différemment les uns des autres. Par exemple, un contrôleur NCC peut être réparti dans une couche client et centralisé dans une couche serveur. Un contrôleur de connexion de couche serveur crée la ou les connexions. L'information caractéristique client est mappée vers la connexion de couche serveur et cette association est maintenue par la relation entre contrôleurs NCC client/serveur. Dans cette situation, ce mappage entraîne la création d'une connexion de liaison de couche client, mais le contrôleur de connexion de couche client n'intervient pas dans cette création. Une récurrence est appliquée vers le haut, ce qui entraîne la création d'une connexion de liaison dans chacune des couches client affectées.

L'Appendice IV illustre cette capacité avec un exemple.

## **18) Paragraphe 7 Architecture du plan de commande**

*Ajouter le texte suivant à la fin du § 7:*

Des composants spéciaux sont définis dans la présente Recommandation afin d'offrir une souplesse d'implémentation. Ces composants sont les contrôleurs de protocole et les contrôleurs de port. Les détails des interfaces de ces composants et d'autres composants sont fournis dans d'autres Recommandations relatives à une technologie particulière.

Les contrôleurs de protocole ont pour fonction de prendre les interfaces primitives offertes par un ou plusieurs composants architecturaux et de multiplexer ces interfaces en une seule instance d'un protocole. C'est ce qui est décrit au § 7.4 et illustré sur la Figure 35. De cette façon, un contrôleur de protocole absorbe les variations entre divers choix de protocole, tandis que l'architecture reste invariable. Un ou plusieurs contrôleurs de protocole sont chargés de gérer les flux informationnels traversant un point de référence.

Les contrôleurs de port ont pour fonction d'appliquer des règles aux interfaces avec le système. Leur finalité est d'offrir un environnement sécurisé pour le fonctionnement des composants architecturaux, isolant ainsi ceux-ci des considérations relatives à la sécurité. En particulier, ils isolent l'architecture des décisions de répartition prises en matière de sécurité. C'est ce qui est décrit au § 7.2.1 et sur la Figure 16.

## **19) Paragraphe 7.2.1 Modèle général de politique**

*Mettre à jour le premier alinéa du § 7.2.1 comme suit:*

Dans le cadre du présent modèle de politique, les systèmes représentent des ensembles de - composants et une frontière de système fournit un point au niveau duquel il est possible d'appliquer une politique. Une politique est, par définition, l'ensemble des règles s'appliquant aux interfaces au niveau de la frontière de système; elle est implémentée par des contrôleurs de port. On utilise des ports de politique pour simplifier la modélisation des politiques qui sont appliquées à plusieurs ports. Les frontières de système sont imbriquées afin de permettre la modélisation correcte de politiques partagées dans un domaine de validité quelconque (totalité du système, ensemble de composants, composants individuels, etc.). Il convient de noter que l'ordre d'application des politiques correspond à l'ordre d'imbrication.

## 20) Paragraphe 7.3 Composants de l'architecture

Ajouter ce qui suit comme second et dernier alinéa du § 7.3:

Le contrôleur de connexion, le contrôleur de routage, le contrôleur d'appel de l'appelant/de l'appelé et le contrôleur d'appel de réseau sont des composants du plan de commande. Ces composants sont soit publics, auquel cas ils utilisent uniquement des pools SNPP publics, soit privés, auquel cas ils utilisent les pools SNPP associés à un VPN particulier. Le contexte VPN d'un composant du plan de commande est fourni par le contrôleur de protocole associé à ce composant.

## 21) Paragraphe 7.3.1 Composant "contrôleur de connexion" (CC)

Ajouter la Note comme dernière phrase du deuxième alinéa:

NOTE – Le paramètre de route n'est pas applicable dans le cas de l'interface de contrôleur de connexion au point de référence UNI.

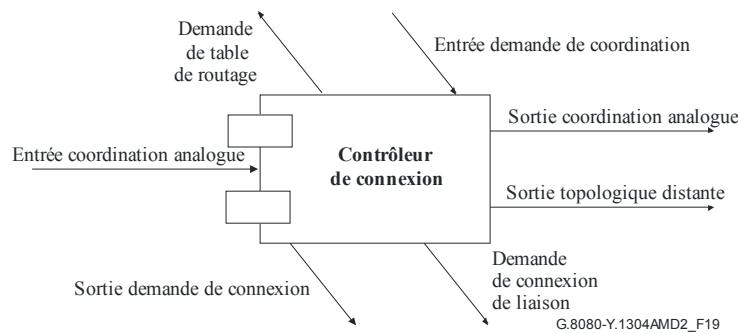
Mettre à jour le Tableau 2 comme suit:

**Tableau 2/G.8080/Y.1304 – Interfaces des composants "contrôleur de connexion"**

Interface d'entrée	Paramètres d'entrée de base	Paramètres de retour de base
Entrée demande de connexion	Paire de noms SNP locaux, et facultativement, route	Connexion de sous-réseau
Entrée coordination homologue	1) paire de noms SNP; 2) SNP et SNPP; 3) paire SNPP; 4) route.	Signal de confirmation

Interface de sortie	Paramètres de sortie de base	Paramètres de retour de base
Demande de table de routage	Fragment de route non résolu	Route
Demande de connexion de liaison	–	Connexion de liaison (paire de points SNP)
Sortie demande de connexion	Paire de noms SNP locaux	Connexion de sous-réseau
Sortie coordination homologue	1) paire de noms SNP; 2) SNP et SNPP; 3) paire SNPP.	Signal de confirmation
Sortie topologie distante	Informations de topologie (liaison et/ou sous-réseau) y compris la disponibilité des ressources	–

Remplacer la Figure 19 (ancienne Figure 12) (ajout d'interfaces selon le nouveau tableau ci-dessus) comme suit:



**Figure 19/G.8080/Y.1304 – Composant "contrôleur de connexion"**

Ajouter ce qui suit juste après la Figure 19:

**Sortie topologie distante:** cette interface est utilisée pour présenter les informations de topologie apprises par le contrôleur de connexion.

## 22) Paragraphe 7.3.2 Composant "contrôleur de routage" (RC)

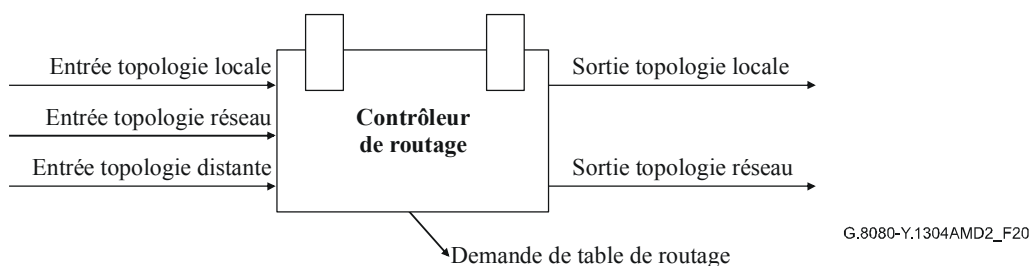
Mettre à jour le Tableau 3 comme suit:

**Tableau 3/G.8080/Y.1304 – Interfaces du contrôleur de routage**

Interface d'entrée	Paramètres d'entrée de base	Paramètres de retour de base
Demande de table de routage	Elément de route non résolu	Liste ordonnée de réserves SNPP
Entrée topologie locale	Mise à jour de la topologie locale	–
Entrée topologie réseau	Mise à jour de la topologie réseau	–
Entrée topologie distante	Informations de topologie (liaison et/ou sous-réseau) y compris la disponibilité des ressources	

Interface de sortie	Paramètres de sortie de base	Paramètres de retour de base
Sortie topologie locale	Mise à jour de la topologie locale	–
Sortie topologie réseau	Mise à jour de la topologie réseau	–

Remplacer la Figure 20 (ancienne Figure 13) (ajout d'interfaces selon le tableau mis à jour ci-dessus) comme suit:



**Figure 20/G.8080/Y.1304 – Composant "contrôleur de routage"**

Ajouter la phrase qui suit comme nouvel alinéa après le point 6 sous "**Interface de demande d'itinéraire**":

Les pools SNPP renvoyés doivent tous être publics ou tous être associés au même VPN.

Ajouter ce qui suit à la fin de l'alinéa décrivant "**l'Interface de topologie locale**":

Les informations de topologie locale sont soit publiques soit associées à un VPN particulier.

Ajouter ce qui suit à la fin de l'alinéa décrivant "**l'Interface de topologie réseau**":

Les informations de topologie réseau sont soit publiques soit associées à un VPN particulier.

**Entrée topologie distante:** cette interface est utilisée pour accepter les informations de topologie provenant d'un contrôleur de connexion.

### **23) Paragraphe 7.3.3 Composant "gestionnaire de ressource de liaison" (LRMA et LRMZ)**

Remplacer le premier alinéa du § 7.3.3 par ce qui suit:

Les composants gestionnaires LRM sont responsables de la gestion d'une liaison SNPP incluant l'allocation des connexions de liaison SNP et le retrait de cette allocation, ainsi que la fourniture des informations de topologie et de statut. Etant donné qu'une liaison SNPP peut être soit publique soit privée, un gestionnaire LRM peut également être soit public soit associé à exactement un VPN.

### **24) Paragraphe 7.3.3.1 Gestionnaire LRMA**

Modification sans objet pour le texte français.



25) **Paragraphe 7.3.5.1 Contrôleur d'appel de l'appelant/de l'appelé**

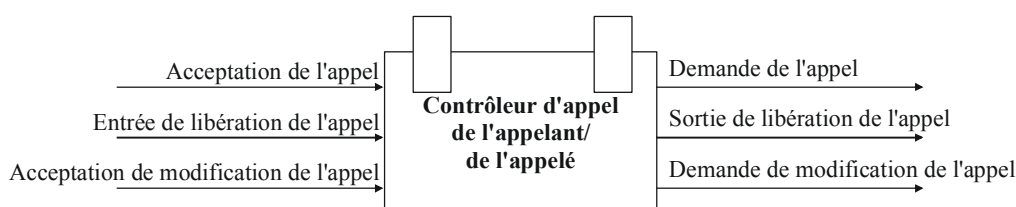
Remplacer le Tableau 6 par le tableau suivant:

**Tableau 6/G.8080/Y.1304 – Interfaces du composant "contrôleur d'appel de l'appelant/de l'appelé"**

Interface d'entrée	Paramètres d'entrée de base	Paramètres de retour de base
Acceptation de l'appel	Nom de ressource de transport ou nom de ressource de transport VPN	Confirmation ou rejet de la demande d'appel
Entrée de libération de l'appel	Nom de ressource de transport ou nom de ressource de transport VPN	Confirmation de la libération de l'appel
Acceptation de modification de l'appel	Nom de l'appel, paramètres à modifier	Confirmation ou rejet de la modification d'appel

Interface de sortie	Paramètres de sortie de base	Paramètres de retour de base
Demande d'appel	Nom de ressource de transport ou nom de ressource de transport VPN; route (facultatif, uniquement pour un VPN)	Confirmation ou rejet de la demande d'appel
Sortie de libération de l'appel	Nom de ressource de transport ou nom de ressource de transport VPN	Confirmation de la libération de l'appel
Demande de modification de l'appel	Nom de l'appel, paramètres à modifier	Confirmation ou rejet de la modification d'appel

Remplacer la Figure 24 (ancienne Figure 17) (ajout d'interfaces selon le tableau ci-dessus) comme suit:



G.8080-Y.1304AMD2\_F24

**Figure 24/G.8080/Y.1304 – Composant "contrôleur d'appel de l'appelant/de l'appelé"**

Dans la description de l'interface de **demande d'appel**, remplacer "fin" par "libération".

Dans la description de l'interface de libération de l'appel, modification sans objet pour le texte français.

Ajouter ce qui suit dans la liste des descriptions d'interface (après "**Libération de l'appel**"): :

**Demande de modification de l'appel:** cette interface est utilisée pour lancer des demandes de modification d'un appel existant. Elle est également utilisée pour recevoir la confirmation ou le rejet des demandes.

**Acceptation de modification de l'appel:** cette interface est utilisée pour accepter des demandes entrantes de modification d'un appel existant. Elle est également utilisée pour confirmer ou pour rejeter les demandes.

**26) Paragraphe 7.3.5.2 Contrôleur d'appel réseau**

*Ajouter le texte suivant comme cinquième alinéa en retrait dans le § 7.3.5.2:*

- traduction des identificateurs de source et de destinations d'appel VPN en noms de ressource de transport.

*Remplacer le Tableau 7 par le tableau suivant:*

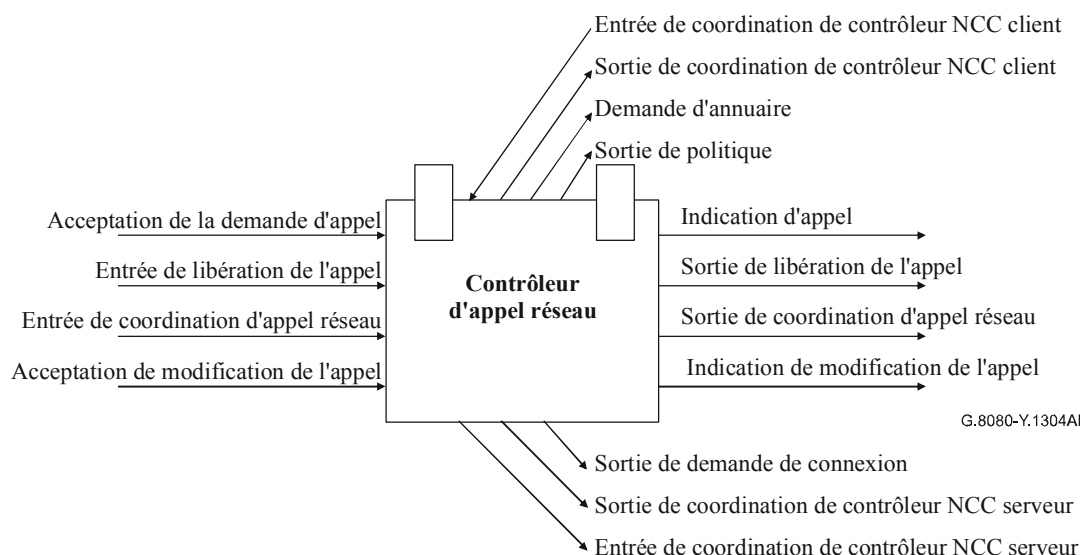
**Tableau 7/G.8080/Y.1304 – Interfaces du composant "contrôleur d'appel réseau"**

<b>Interface d'entrée</b>	<b>Paramètres d'entrée de base</b>	<b>Paramètres de retour de base</b>
Acceptation de la demande d'appel	Nom de ressource de transport UNI ou pseudonyme de ressource de transport UNI	Confirmation ou rejet de la demande d'appel
Entrée de coordination d'appel réseau	Nom de ressource de transport UNI ou pseudonyme de ressource de transport UNI	Confirmation ou rejet
Entrée de libération de l'appel	Nom de ressource de transport UNI ou pseudonyme de ressource de transport UNI	Confirmation de la libération de l'appel
Entrée de coordination de contrôleur NCC client	Paramètres d'appel client facultatifs, identification de couche client facultative, noms de ressource de transport	Paire de points SNP dans la couche client
Entrée de coordination de contrôleur NCC serveur	Paire de points SNP	Confirmation ou rejet de l'utilisation
Acceptation de modification de l'appel	Nom de l'appel, paramètres à modifier	Confirmation ou rejet de la modification d'appel

**Tableau 7/G.8080/Y.1304 – Interfaces du composant "contrôleur d'appel réseau"**

Interface de sortie	Paramètres de sortie de base	Paramètres de retour de base
Indication d'appel	Nom de ressource de transport UNI ou pseudonyme de ressource de transport UNI	Confirmation du rejet de la demande d'appel
Sortie de demande de connexion	Nom de ressource de transport UNI ou pseudonyme de ressource de transport UNI	Paire de points SNP
Sortie de coordination d'appel réseau	Nom de ressource de transport UNI ou pseudonyme de ressource de transport UNI	Confirmation ou rejet de la demande d'appel
Demande d'annuaire	Nom de ressource de transport UNI ou pseudonyme de ressource de transport UNI	Nom local
Sortie de politique	Paramètres d'appel	Acceptation ou rejet de l'appel
Sortie de libération de l'appel	Nom de ressource de transport UNI ou pseudonyme de ressource de transport UNI	Confirmation de la libération de l'appel
Sortie de coordination de contrôleur NCC client	Paire de points SNP dans la couche client	Confirmation ou rejet de l'utilisation
Sortie de coordination de contrôleur NCC serveur	Paramètres d'appel facultatifs, identification de couche, noms de ressource de transport	Paire de points SNP
Demande de modification de l'appel	Nom de l'appel, paramètres à modifier	Confirmation ou rejet de la modification d'appel

Remplacer la Figure 25 (ancienne Figure 18) mise à jour suivante (ajout d'interfaces selon le Tableau 7 mis à jour) comme suit:



**Figure 25/G.8080/Y.1304 – Composant "contrôleur d'appel réseau"**

*Remplacer la description actuelle de l'interface d'**acceptation de la demande d'appel** par ce qui suit:*

**Acceptation de la demande d'appel:** cette interface est utilisée pour accepter une paire d'identificateurs de source et de destination d'appel. Elle est également utilisée pour confirmer ou pour rejeter la demande d'établissement d'appel entrant.

*Remplacer la description actuelle de l'interface de **sortie de demande de connexion** par ce qui suit:*

**Sortie de demande de connexion:** cette interface est utilisée pour lancer, à destination d'un contrôleur de connexion, une demande d'établissement de connexion sous la forme d'une paire de points SNP.

*Remplacer la description actuelle de l'interface de **demande d'annuaire** par ce qui suit:*

**Demande d'annuaire:** cette interface est utilisée pour obtenir un nom de pool SNPP à partir d'un nom ou d'un pseudonyme de ressource de transport UNI. Pour les pseudonymes, si plusieurs pools SNPP sont représentés, le choix du pool SNPP à renvoyer dépend de la politique.

*Ajouter les descriptions d'interface suivantes immédiatement après la description de l'interface de **sortie de politique**:*

**Entrée de coordination de contrôleur NCC client:** cette interface est utilisée pour accepter une demande issue d'un contrôleur NCC de couche client concernant une paire de points SNP. Les identificateurs de source et de destination sont fournis au contrôleur NCC dans sa couche afin que ledit contrôleur puisse fournir une connexion de réseau à utiliser par la couche client. Les points SNP dans la couche client qui sont pris en charge par une adaptation vers la connexion de réseau sont retournés. Cette interface est également utilisée par le client pour procéder à une libération ou pour modifier l'utilisation de la paire de points SNP. Le contrôleur NCC retourne le résultat de l'action.

**Sortie de coordination de contrôleur NCC client:** cette interface est utilisée pour présenter à une couche client une paire de points SNP qui sont pris en charge par une adaptation vers une connexion de réseau. Le contrôleur NCC client indique s'il accepte ou non cette ressource. Cette interface est également utilisée par le serveur pour procéder à une libération ou pour présenter une paire de points SNP modifiée. Le contrôleur NCC client retourne le résultat de l'action.

**Sortie de coordination de contrôleur NCC serveur:** cette interface est utilisée pour demander une paire de points SNP (entrée et sortie) destinée à être utilisée par l'appel pour transférer l'information caractéristique. Cette paire est identique aux paramètres de retour de l'interface de sortie de demande de connexion, sauf qu'aucune connexion de réseau dans cette couche n'est supposée être créée. Cette interface est également utilisée pour procéder à une libération ou pour demander la modification de l'utilisation de la paire de points SNP fournie par la couche serveur. Le contrôleur NCC serveur retourne le résultat de l'action.

**Entrée de coordination de contrôleur NCC serveur:** cette interface est utilisée pour accepter une paire de points SNP (entrée et sortie) présentée par un contrôleur NCC de couche serveur. Cette paire peut être acceptée ou rejetée. Cette interface est également utilisée par le serveur pour procéder à une libération ou pour présenter une paire de points SNP modifiée. Le contrôleur NCC retourne le résultat de l'action.

**Acceptation de modification de l'appel:** cette interface est utilisée pour accepter une demande de modification d'appel. Elle est également utilisée pour confirmer ou pour rejeter la demande de modification d'appel entrant.

**Indication de modification de l'appel:** cette interface est utilisée pour transmettre une demande de modification d'appel à un autre contrôleur NCC. Elle est également utilisée pour recevoir la confirmation ou le rejet de la demande.

## 27) Paragraphe 7.3.5.3 Interactions du contrôleur d'appel

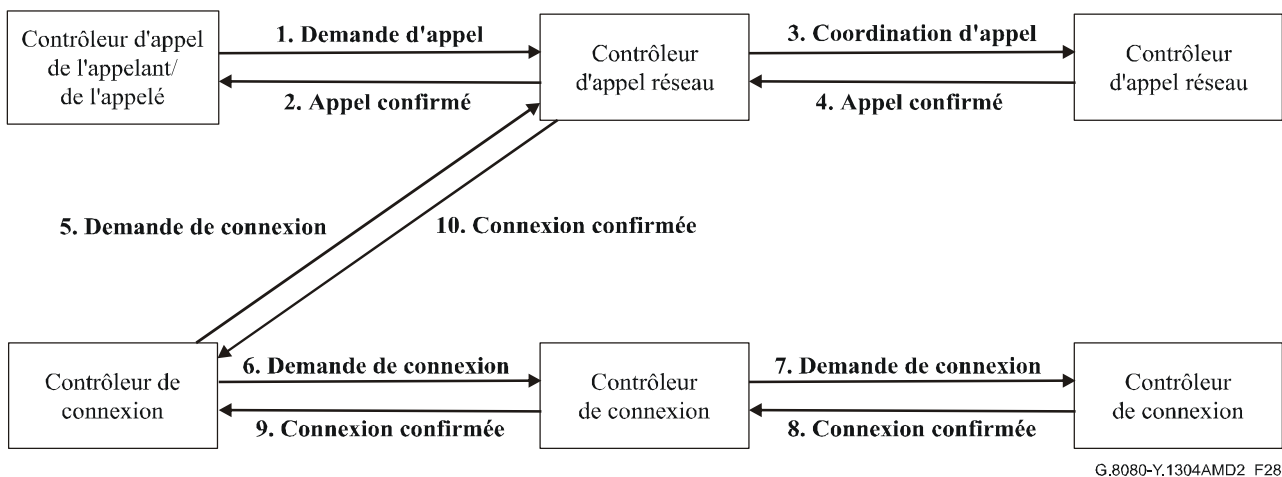
Ajouter ce qui suit dans le texte décrivant les "connexions commutées":

**Connexions commutées:** le contrôleur d'appel de l'appelant (associé à un terminal d'extrémité) interagit avec le contrôleur d'appel réseau pour constituer un appel entrant et le contrôleur d'appel réseau interagit avec le contrôleur d'appel de l'appelé (associé à un terminal d'extrémité) pour constituer un appel sortant. Le contrôleur d'appel réseau interagit avec les contrôleurs de connexion pour fournir l'appel. La Figure 26 donne une illustration de ces interactions. Il convient de noter que les contrôleurs d'appel de l'appelant/de l'appelé n'interagissent pas directement avec le contrôleur de connexion de réseau. Il convient aussi de noter que les contrôleurs d'appel de l'appelant/de l'appelé n'interagissent pas directement avec le contrôleur de connexion associé au contrôleur d'appel réseau correspondant.

Remplacer le texte décrivant les "connexions permanentes reconfigurables" par ce qui suit:

**Connexions permanentes reconfigurables:** on suppose que le système de gestion de réseau contient les contrôleurs d'appel de l'appelant/de l'appelé. Ce système envoie une commande pour configurer le contrôleur d'appel de l'appelant, qui active les contrôleurs d'appel réseau dans le plan de commande lorsque les commandes de configuration d'appel sont envoyées au plan de commande. La réponse à une commande de configuration d'appel issue du plan de commande est considérée comme une confirmation de l'établissement d'appel par le plan de gestion. La commande et la réponse à la commande représentent un appel vide sans aucun service. Les protocoles entre le plan de gestion de réseau et le plan de commande correspondent à une interface de commande et de réponse à la commande.

Remplacer la Figure 28 (ancienne Figure21) comme suit:



G.8080-Y.1304AMD2\_F28

**Figure 28/G.8080/Y.1304 – Interactions des contrôleurs d'appel pour des connexions permanentes reconfigurables**

Ajouter les deux alinéas suivants à la fin du § 7.3.5.3:

**Appels intercouches:** deux contrôleurs NCC dans des couches différentes peuvent coopérer pour permettre la prise en charge de l'information caractéristique client dans une couche serveur. Cette coopération peut être lancée à destination ou en provenance de la couche serveur. Pour un contrôleur NCC, la demande faite à un contrôleur NCC de couche serveur retourne le même résultat que l'interface "sortie de demande de connexion". La différence est qu'une association avec un contrôleur NCC serveur est réalisée. Cette action conduit à l'utilisation ou à la création d'un segment d'appel de couche serveur qui prendra en charge le contrôleur NCC client. Si la couche serveur a

besoin de créer un appel par suite de l'utilisation des interfaces "sortie de coordination de contrôleur NCC serveur" et "entrée de coordination de contrôleur NCC client", les identificateurs de source et de destination sont utilisés comme paramètres d'appel. Une action identique au comportement de l'interface "acceptation de demande d'appel" est alors effectuée si on détermine que l'établissement de connexion au niveau de cette couche serveur est l'action correcte. Autre solution: le contrôleur NCC de couche serveur peut utiliser son interface "sortie de coordination de contrôleur NCC serveur" pour lancer une demande (avec récurrence au niveau des couches) de paire de points SNP à un contrôleur NCC d'une autre couche qui constitue un serveur pour lui.

Un contrôleur NCC peut aussi lancer une action vers une couche client pour présenter une paire de points SNP destinée à être utilisée par la couche client pour transférer l'information caractéristique client. A cette fin, les interfaces "sortie de coordination de contrôleur NCC client" et "entrée de coordination de contrôleur NCC serveur" sont utilisées. Dans ce cas, la paire de points SNP présentée permet de transférer l'information caractéristique client mais aucun appel n'est lancé au niveau de la couche serveur. Cela est utilisé lorsqu'une couche serveur a déjà établi un appel, mais que la présentation à la couche client est opérée ultérieurement. La couche client peut accepter ou rejeter l'utilisation de la paire de points SNP offerte.

## **28) Nouveau paragraphe 7.3.5.4 Modification d'appel**

*Ajouter le nouveau paragraphe 7.3.5.4 comme suit:*

### **7.3.5.4 Modification d'appel**

Le service fourni par un appel peut être modifié par des actions lancées par un contrôleur CCC ou par une application de gestion de réseau se trouvant sur un contrôleur NCC à l'interface UNI. Le degré de modification est fixé par la politique de l'opérateur et cette politique peut ou non être partagée avec l'utilisateur final (par exemple pour indiquer à l'utilisateur quels incréments de largeur de bande sont autorisés). Le degré de modification d'un appel est fonction des règles suivantes:

- l'information caractéristique associée à l'appel à l'interface UNI n'est pas modifiable;
- la connexion de liaison associée à l'appel à l'interface UNI-N n'est pas modifiable.

Les actions peuvent être la modification d'un segment d'appel, auquel cas les contrôleurs NCC restent fixes, ou la création/suppression de segments d'appel dans un appel global, auquel cas des contrôleurs NCC sont créés/supprimés.

A l'interface UNI, on peut par exemple modifier la largeur de bande (par exemple le débit pour un appel Ethernet) et le nombre de contrôleurs CCC impliqués (par exemple appel multiparticipant).

Les opérations suivantes peuvent par exemple se produire dans le réseau par suite de demandes de modification d'appel à l'interface UNI:

- modification du nombre de connexions de couche serveur associées à un appel VCAT prenant en charge un appel Ethernet;
- ajout d'une connexion additionnelle pour créer une configuration 1+1, en réponse à une demande d'augmentation de la disponibilité d'un appel.

## **29) Nouveaux paragraphes 7.3.6, 7.3.7 et 7.3.8**

*Ajouter les nouveaux paragraphes suivants:*

### **7.3.6 Agent de découverte (DA)**

La fédération d'agents de découverte fonctionne dans l'espace nominatif d'un plan de transport. Elle assure la séparation entre cet espace et les noms de plan de commande. La fédération a connaissance des points de connexion (CP, *connection point*) et des points de connexion de terminaison (TCP, *termination connection point*) du réseau, alors qu'un agent DA local n'a

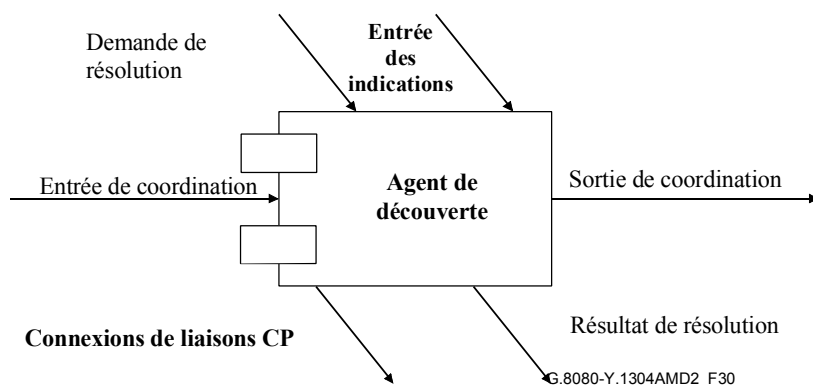
connaissance que des points qui lui sont assignés. La coordination de la découverte implique l'acceptation d'indications éventuelles sur la préexistence de points CP et de connexions de liaison. L'agent DA conserve les connexions de liaison CP-CP afin de permettre à des connexions de liaison SNP-SNP de leur être liées ultérieurement. Les interfaces de résolution de nom facilitent la découverte en assurant la traduction des pointeurs TCP mondiaux en adresse de l'agent DA responsable du point, conjointement avec le nom local du point TCP. Il est à noter que ces indications sont issues d'une coopération avec d'autres composants, ou proviennent de systèmes de configuration externes.

Les agents de découverte ne possèdent pas d'interface avec des équipements privés et peuvent être situés dans toute plate-forme appropriée.

**Tableau 8/G.8080/Y.1304 – Interfaces du composant agent de découverte (DA)**

Interface d'entrée	Paramètres d'entrée de base	Paramètres de retour de base
Entrée de coordination		
Entrée d'indications	Paires de points CP	
Demande de résolution	Nom de point TCP	

Interface de sortie	Paramètres de sortie de base	Paramètres de retour de base
Sortie de coordination		
Connexion de liaison CP	Paire de points CP	
Résultat de résolution		Adresse RCD de l'agent DA, index de point TCP



**Figure 30/G.8080/Y.1304 – Composant agent de découverte**

### 7.3.7 Exécuteurs de terminaison et d'adaptation

L'exécuteur de terminaison et d'adaptation (TAP) est situé au même endroit que la fonction d'adaptation et de terminaison. Il fournit au plan de commande (gestionnaire LRM) une vue de la ressource de connexion de liaison prenant en charge un point SNP et occulte tous les détails propres au matériel et à la technologie de la commande d'adaptation et de terminaison.

L'exécuteur de terminaison et d'adaptation fonctionne à deux moments différents et remplit deux fonctions différentes.

Lorsqu'une ressource est assignée à un plan de commande, l'exécuteur TAP est configuré avec un lien autorisé avec un point SNP, ce qui entraîne la création d'un point SNP (à une extrémité de liaison) relevant d'un gestionnaire LRM. Si la ressource est partagée entre plusieurs plans de

commande (par exemple différents réseaux de couche ou différents VPN de couche 1), l'exécuteur TAP contient une liste de liens autorisés. L'exécuteur TAP commande le lien entre un point CTP et chaque point SNP qui fait référence à l'une quelconque des ressources relevant de cet exécuteur TAP. Les états du lien avec un point SNP sont décrits au Tableau 9 ci-dessous.

**Tableau 9/G.8080/Y.1304 – Etats du lien avec un point SNP**

<b>Etat</b>	<b>Description</b>
Occupé	Lien autorisé, la ressource référencée étant actuellement attribuée à un autre plan de commande ou au plan de gestion
Potentiel	Lien autorisé, la ressource référencée n'étant pas actuellement attribuée à un plan de commande ou au plan de gestion
Attribué	Lien autorisé, la ressource étant configurée pour ce gestionnaire LRM et attribuée à ce gestionnaire
Arrêt	Notification de l'exécuteur TAP indiquant que la ressource doit être retournée dans un délai fixé, par exemple: <ul style="list-style-type: none"> <li>– immédiatement (interrompre l'appel en cours);</li> <li>– rapidement (rerouter l'appel avant l'abandon);</li> <li>– à la prochaine fenêtre de maintenance;</li> <li>– lorsque l'appel est abandonné.</li> </ul>
Libéré	Le gestionnaire LRM n'utilise plus la ressource

Lorsqu'un point SNP est dans l'état attribué, l'exécuteur TAP doit configurer correctement les ressources (par exemple adaptation variable) et mettre l'état de tous les autres points SNP référençant la même ressource à occupé.

Lorsque des connexions de liaison SNP sont liées à leur connexion de liaison CP correspondante, l'exécuteur TAP est chargé du maintien du lien SNP-CP. Un exécuteur TAP local coopère avec un exécuteur TAP distant pour coordonner l'adaptation variable ou toute autre opération requise lors de la formation des connexions de liaison CP.

Si un gestionnaire LRM souhaite utiliser un point SNP dans l'état potentiel pour satisfaire à une demande de connexion, alors, pendant l'établissement de connexion, une paire d'exécuteurs TAP coopèrent avec le gestionnaire LRM pour coordonner l'établissement d'adaptation requis par la connexion de liaison.

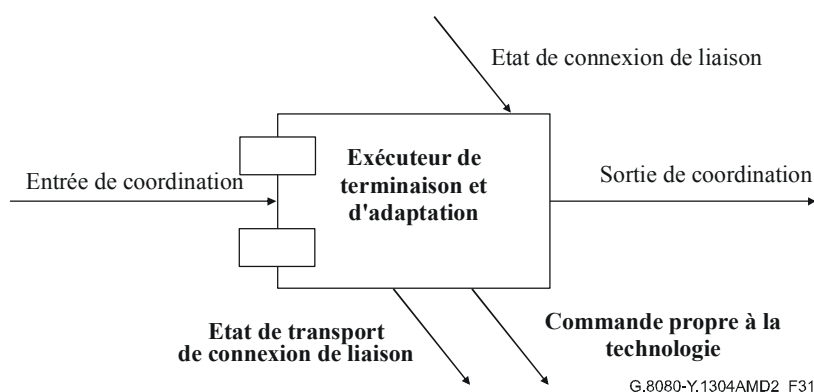
L'exécuteur TAP fournit les informations d'état de transmission de connexion de liaison et accepte les informations d'état de connexion de liaison afin de faire en sorte que les indications du plan de gestion soient cohérentes, et notamment afin de faire en sorte que l'état d'alarme de la connexion de liaison soit cohérent, de manière à éviter qu'une fausse alarme soit générée ou signalée.



**Tableau 10/G.8080/Y.1304 – Interfaces du composant exécuteur de terminaison et d'adaptation (TAP)**

Interface d'entrée	Paramètres d'entrée de base	Paramètres de retour de base
Etat de connexion de liaison (SNP-SNP)	Enum: en service, hors service	
Entrée de coordination	Propre à la technologie	

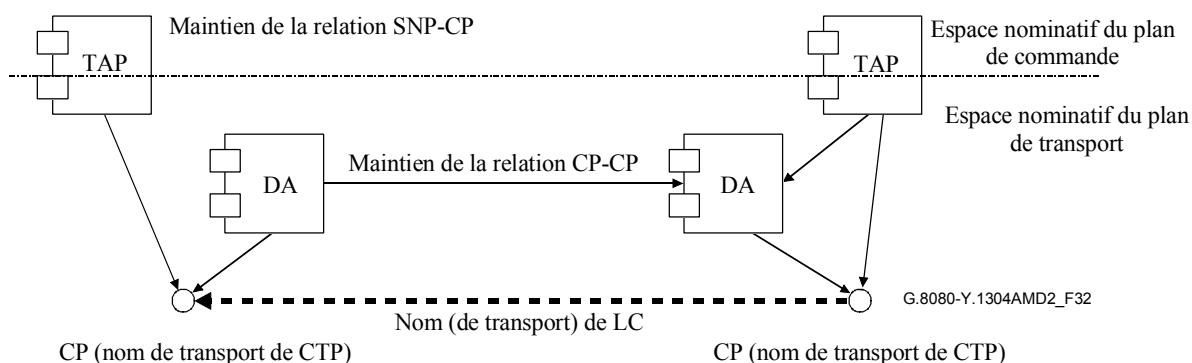
Interface de sortie	Paramètres de sortie de base	Paramètres de retour de base
Etat de transport de connexion de liaison (SNP-SNP)	Enum: vers le haut, vers le bas	
Sortie de coordination	Propre à la technologie	Propre à la technologie
Commande	Propre au matériel	Propre au matériel



**Figure 31/G.8080/Y.1304 – Composant exécuteur de terminaison et d'adaptation**

### 7.3.8 Processus de découverte de liaison

Le processus de découverte générique est subdivisé en deux phases et espaces nominatifs séparés et distincts. La première phase se déroule entièrement dans l'espace nominatif d'un plan de transport (points CP et CTP).



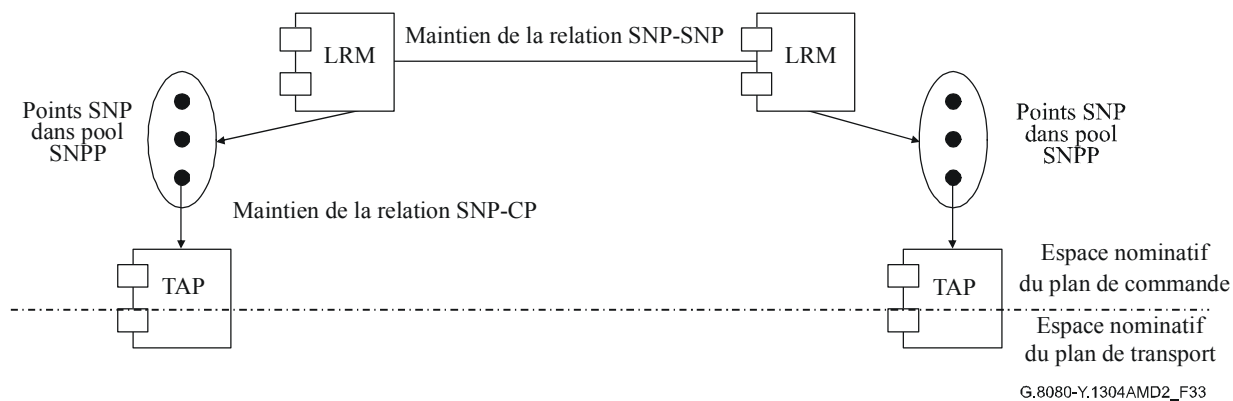
**Figure 32/G.8080/Y.1304 – Découverte des connexions de liaison (LC) du transport**

L'agent DA fonctionne entièrement dans l'espace nominatif du plan de transport et est responsable du maintien du nom de transport de la connexion de liaison (associée à chaque CP). Ces informations peuvent être obtenues: par des mécanismes de transport invisibles à partir de l'espace nominatif du plan de commande, par conservation d'informations relationnelles déjà obtenues ou

par préconfiguration. L'agent DA facilite l'exécution d'un processus sous-jacent de découverte automatique en résolvant des noms de CP de transport en coopération avec tous les agents DA se trouvant dans le réseau, permettant ainsi aux agents DA (ou aux autres composants) chargés de chaque extrémité de la connexion de liaison de transport de communiquer au sujet de cette connexion de liaison.

Un point CP peut être assigné à un ensemble de VPN, y compris l'ensemble vide et le singleton. Cet ensemble de VPN peut être représenté par une étiquette d'appartenance. L'agent DA vérifie que l'étiquette d'appartenance attachée à chaque point CP d'une connexion de liaison est la même.

La seconde phase intervient entièrement dans l'espace nominatif du plan de commande (points SNP).



**Figure 33/G.8080/Y.1304 – Insertion des connexions de liaison du plan de commande**

Le gestionnaire de ressources de liaison (LRM, *link resource manager*) conserve les informations de lien SNP-SNP nécessaires pour le nom dans le plan de commande de la connexion de liaison, alors que l'exécuteur TAP maintient la relation entre le nom dans le plan de commande (SNP) et le nom dans le plan de transport (CP) de la ressource. Cette séparation permet d'isoler complètement les noms dans le plan de commande des noms dans le plan de transport, et de les rendre complètement indépendants de la méthode utilisée pour insérer ces noms de transport dans les agents DA.

Afin d'attribuer une connexion de liaison SNP-SNP à une liaison SNPP, il suffit que le nom de transport concernant la connexion de liaison existe. Il est ainsi possible d'attribuer des connexions de liaison au plan de commande sans que la connexion de liaison soit physiquement connectée. Cette procédure d'attribution peut être vérifiée par les gestionnaires LRM qui échangent le nom de liaison de transport qui correspond au point SNP.

Il est à noter que le nom de liaison SNPP entièrement qualifié est un nom dans le plan de commande qui reflète la structure des ressources du plan de transport.

### 30) Paragraphe 7.5.1 Routage hiérarchique

Remplacer le terme "composant de routage (RC, *routing component*)" par "contrôleur de routage (RC, *routing controller*)" au point 2.

### 31) Paragraphe 7.5.2 Routage par la source et pas à pas

Remplacer le terme "composant de routage (RC)" par "contrôleur de routage (RC)" au point 2.

### 32) Paragraphe 8 Points de référence

Ajouter le nouveau texte suivant et la Figure 41 à la fin du paragraphe:

Un point de référence représente un ensemble de services fourni par l'intermédiaire d'interfaces sur une ou plusieurs paires de composants. L'interface entre composants est indépendante du point de référence, de sorte que la même interface peut être associée à plusieurs points de référence. Du point de vue du point de référence, les composants prenant en charge l'interface ne sont pas visibles, de sorte que la spécification d'interface peut être traitée indépendamment du composant.

Les flux d'informations qui acheminent des services de part et d'autre du point de référence ont pour destination (ou pour origine) des composants. Il n'est pas nécessaire que plusieurs flux aient pour destination le même emplacement physique. Ces flux peuvent traverser différentes séquences de points de référence comme illustré sur la Figure 41.

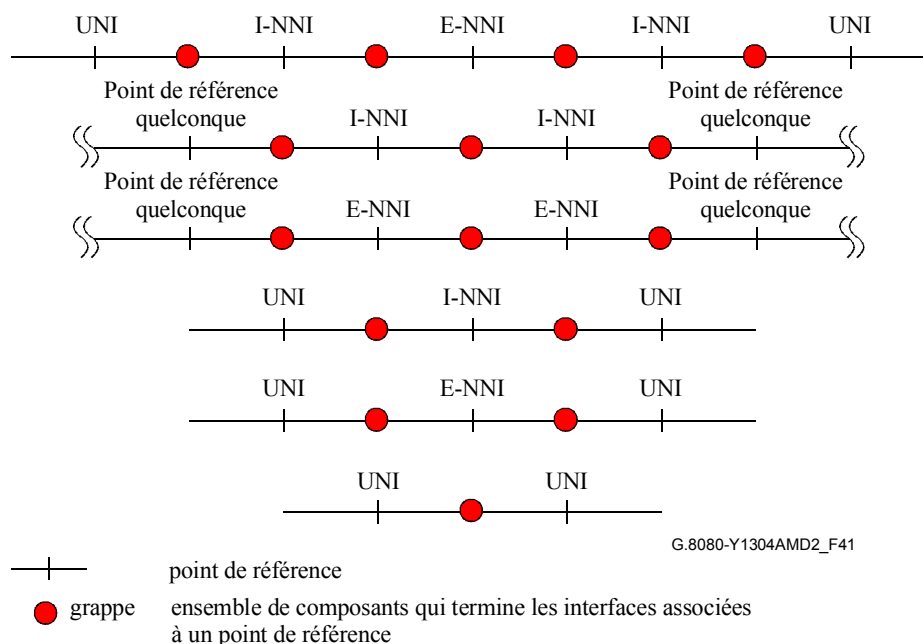


Figure 41/G.8080/Y.1304 – Points de référence

### 33) Paragraphe 8.1 Interface UNI

Ajouter le nouveau texte suivant à la fin du § 8.1:

L'utilisation du point de référence UNI dans les VPN L1 nécessite un complément d'étude.

### 34) Paragraphe 8.3 Interface E-NNI

Ajouter le nouveau texte suivant à la fin du § 8.3:

D'autres fonctions telles que la sécurité et l'authentification des appels ou des services d'annuaire étendus peuvent éventuellement venir compléter cet ensemble de fonctions de base.

Lorsque le point de référence E-NNI se trouve entre le domaine d'un client VPN et un VPN dans le domaine d'un fournisseur de services, des services complémentaires peuvent être pris en charge (voir la Rec. UIT-T Y.1312), par exemple:

- l'authentification et l'autorisation des utilisateurs VPN;
- la gestion des politiques des utilisateurs VPN, y compris les restrictions de connectivité;
- le transfert transparent d'informations de commande entre utilisateurs VPN;

- la participation du VPN au domaine de routage du client.

La prise en charge de ces services sort du cadre de la présente Recommandation.

### **35) Nouveau paragraphe 8.4 Architecture côté utilisateur**

*Ajouter le nouveau paragraphe 8.4 comme suit:*

#### **8.4 Architecture côté utilisateur**

Le côté utilisateur sera appelé UNI-C (C comme "client"), et le côté réseau sera appelé UNI-N (N comme "network = réseau").

Le nom de ressource de transport de l'interface UNI selon la Rec. UIT-T G.8080/Y.1304 (voir le § 10) définit un ou plusieurs noms globalement uniques pour chaque liaison SNPP qui fait partie d'une interface UNI. Ces noms servent à identifier les destinations d'appel. Etant donné qu'une interface UNI peut contenir de multiples liaisons SNPP, par exemple dans le cas du rattachement multiple, elle peut donc avoir de multiples noms globalement uniques pour ses ressources support. Il est à noter que ces noms ne sont pas des noms d'utilisateur.

Lorsque de multiples liaisons SNPP font partie de la même interface UNI, ces noms peuvent servir à faire un choix entre les liaisons SNPP à utiliser. Des facteurs tels que la diversité ou le coût, pourraient être utilisés par les appelants afin de choisir la liaison SNPP. Les liaisons SNPP entre un conteneur AGC commun et un réseau peuvent appartenir à la même interface UNI si, côté réseau, elles relèvent d'un contrôleur d'appel réseau commun.

Les noms de ressource de transport de l'interface UNI peuvent servir à un utilisateur pour différencier des interfaces UNI. Lorsqu'il y a de multiples interfaces UNI, chacune d'elles possède des noms distincts de ressource de transport de l'interface UNI, qu'elle ne partage pas avec les autres interfaces.

Ce qui suit décrit l'architecture UNI-C:

- 1) il existe une entité de transport appelée conteneur de groupe d'accès (AGC, *access group container*) qui peut terminer de multiples liaisons SNPP. Cette entité peut contenir un ensemble de groupes d'accès G.805;
- 2) un conteneur AGC est une entité monocouche qui contient des groupes d'accès, des gestionnaires LRM et des exécuteurs TAP. Il est semblable aux sous-réseaux G.805 sauf qu'il n'est pas défini par récurrence, qu'il peut être ou ne pas être une matrice (cela n'a pas à être spécifié), et qu'il ne possède pas de connexions de sous-réseau définies. Plusieurs conteneurs AGC issus de différentes couches peuvent coïncider dans le même équipement;
- 3) les fonctions de plan de commande associées au côté UNI-C dans un conteneur AGC sont la commande d'appel (contrôleur d'appel de l'appelant/de l'appelé) et la découverte de ressource (LRM). Une fonction limitée de commande et de sélection de connexion est présente afin d'interagir avec le contrôleur de connexion du côté UNI-N, parce que la commande de connexion du côté UNI-N possède une interface de routage tandis que la commande de connexion du côté UNI-C détecte l'acceptation/la libération de connexion en provenance du côté UNI-N;
- 4) les applications qui utilisent un ou plusieurs chemins relatifs à un conteneur AGC sont appelées "utilisateurs de connexion <nom de l'application>". Elles interagissent directement avec les points d'accès G.805 en présentant et en recevant l'information adaptée. Pour chaque utilisateur de connexion, il peut y avoir un "demandeur de connexion <nom de l'application>". Ces entités interagissent avec les interfaces UNI-C afin de demander/libérer des connexions. Un seul demandeur de connexion peut obtenir des connexions auprès d'une ou de plusieurs interfaces UNI-C pour un utilisateur de connexion associé;

- 5) un utilisateur est considéré comme étant à rattachement multiple lorsque deux liaisons SNPP ou plus raccordent le conteneur AGC au réseau. Par ailleurs, il existe aussi entre l'utilisateur et le réseau un accord de service tel que le réseau offre une certaine fiabilité, une certaine diversité ou d'autres caractéristiques de service entre les connexions sur les différentes liaisons SNPP du rattachement multiple.

### **36) Paragraphe 9 Gestion réseau des entités du plan de commande**

*Remplacer les points 3), 4) et 5) par:*

- 3) assignation de ressources de transport à un client particulier en vue de la création d'un VPN;
- 4) assignation d'identificateurs uniques à des points CTP et assignation de liens autorisés entre le point CTP et les points SNP associés;
- 5) fourniture d'informations de configuration et de politique aux fonctions de filtrage d'adresse et de VPN, si ces fonctions sont présentes dans le plan de commande.

*Ajouter ce qui suit au point 8:*

- identification du VPN auquel les paramètres de qualité de l'appel appartiennent.

*Ajouter un nouveau point 18:*

- 18) transformation d'une connexion permanente (PC) en une connexion permanente reconfigurable (SPC), les ressources de transport associées à la connexion permanente étant assignées au plan de commande sans interruption de service.

### **37) Nouveaux paragraphes 10.1 et 10.2**

*Ajouter les nouveaux paragraphes suivants au § 10:*

#### **10.1 Espaces nominatifs**

Il y a trois espaces nominatifs de transport distincts dans la syntaxe de nommage d'un réseau ASON:

- 1) un espace nominatif de zone de routage;
- 2) un espace nominatif de sous-réseau;
- 3) un espace nominatif de contexte de liaison.

Les deux premiers espaces suivent la structure du sous-réseau de transport et n'ont pas besoin d'être mis en correspondance. Considérés comme un tout, ils définissent le point topologique où se trouve un pool SNPP. L'espace nominatif de contexte de liaison spécifie l'emplacement du point SNP dans le pool SNPP. Il peut servir à refléter la structure d'un sous-pool SNPP et différents types de noms de liaison.

Un nom de pool SNPP est une concaténation:

- d'un ou de plusieurs noms de zone de routage imbriqués;
- d'un nom facultatif de sous-réseau au plus bas niveau de zone de routage. Ce nom ne peut exister que si les noms de zone de routage contenante sont présents;
- un ou plusieurs noms de contexte de ressource imbriqués.

Dans ce modèle, le nom de pool SNPP peut descendre par récurrence dans les zones de routage jusqu'aux plus basses sous-partitions de sous-réseau et de liaison (sous-pools SNPP). Ce procédé permet d'identifier des points SNP à un niveau de routage quelconque.

**Nom de point SNP:** un point SNP reçoit une adresse utilisée pour l'attribution d'une connexion de liaison et, dans certains cas, pour le routage. Le nom de point SNP est dérivé du nom de pool SNPP concaténé avec un index de point SNP de portée locale.

Un pseudonyme de pool SNPP est un autre nom de pool SNPP pour la même liaison SNPP.

NOTE – Il peut être généré à partir du même espace nominatif ou d'un espace nominatif différent. S'il est présent dans une zone de routage, il est disponible pour le contrôleur RC qui est associé à l'agent RA.

*Ajouter le sous-titre suivant pour introduire le texte existant au § 10:*

## **10.2 Noms et adresses**

*Ajouter la description suivante du **nom de ressource de transport de l'interface E-NNI** comme deuxième alinéa du § 10.2:*

**Nom de ressource de transport de l'interface E-NNI:** la liaison SNPP E-NNI peut se voir assigner un nom permettant aux contrôleurs d'appel réseau de spécifier des interfaces E-NNI. Ce type de nom, qui est assigné par le réseau ASON doit être globalement unique. Il est possible d'assigner plusieurs noms à la liaison SNPP. Un pseudonyme peut exister pour un ensemble de noms de ressource de transport de l'interface E-NNI.

Lorsque le point de référence E-NNI se trouve entre le domaine d'un client VPN et un VPN dans le domaine d'un fournisseur de services, le nom de ressource de transport de l'interface E-NNI peut être unique parmi toutes les autres liaisons SNPP E-NNI assignées au VPN et pas nécessairement globalement unique. Il peut être assigné par le client VPN ou par le réseau ASON.

*Ajouter ce qui suit comme dernière phrase de la description de la "**ressource de transport de l'interface UNI**":*

Un pseudonyme peut exister pour un ensemble de noms de ressources de transport de l'interface UNI.

*Supprimer l'avant-dernier alinéa du § 10.2 décrivant le pool SNPP.*

## **38) Nouveaux paragraphes 11.1 et 11.2**

*Ajouter les nouveaux paragraphes suivants après le texte figurant actuellement dans le § 11:*

### **11.1 Protection**

La protection est un mécanisme permettant d'améliorer la disponibilité d'une connexion par l'emploi d'une capacité assignée complémentaire. Dès que cette capacité est assignée aux fins de la protection, il n'y a aucun reroutage et les points SNP attribués à des points intermédiaires afin de prendre en charge la capacité de protection ne changent pas à la suite d'un événement de protection. C'est le plan de commande, plus précisément le composant de commande de connexion, qui est responsable de la création d'une connexion. Cela implique la création d'une connexion de trafic et d'une connexion de protection, ou la fourniture d'informations de configuration propres à la connexion pour un système de protection. En protection dans le plan de transport, la configuration de protection est effectuée sous la direction du plan de gestion. En protection dans le plan de commande, la configuration de protection est placée sous la direction du plan de commande plutôt que du plan de gestion.

La protection dans le plan de commande intervient entre les contrôleurs de connexion d'origine et de destination d'un domaine de protection dans le plan de commande, où l'origine et la destination sont définies par rapport à la connexion. Le fonctionnement du mécanisme de protection est coordonné entre l'origine et la destination. Dans l'éventualité d'une défaillance, la protection n'implique pas le reroutage ou l'établissement d'une connexion supplémentaire dans les contrôleurs

de connexion intermédiaires car seuls les contrôleurs de connexion d'origine et de destination sont mis en jeu. C'est là la principale différence entre protection et rétablissement.

## 11.2 Rétablissement

Le rétablissement d'un appel est le remplacement d'une connexion défaillante par reroutage de l'appel au moyen de la capacité de réserve. Contrairement à la protection, une partie ou la totalité des points SNP utilisés pour prendre en charge la connexion peut être modifiée pendant un événement de rétablissement. Le rétablissement dans le plan de commande se produit par rapport à des domaines de reroutage. Un domaine de reroutage est un groupe de contrôleurs d'appel et de connexion qui se partagent la commande de reroutage domaine par domaine. Les composants situés à la périphérie des domaines de reroutage coordonnent les opérations de reroutage domaine par domaine pour toutes les communications/connexions qui traversent ces domaines de reroutage. Un domaine de reroutage doit toujours être entièrement contenu dans un domaine ou dans une zone de routage. Un domaine de routage peut englober complètement plusieurs domaines de reroutage. Les ressources de réseau associées à un domaine de reroutage doivent donc être contenues entièrement dans une zone de routage. Lorsqu'une communication/connexion est reroutée à l'intérieur d'un domaine de reroutage, l'opération de reroutage domaine par domaine intervient entre les bords du domaine de reroutage et y est entièrement contenue.

L'activation d'un service de reroutage est négociée dans le cadre de la phase d'établissement initial d'un appel. Pour un seul domaine, un service de reroutage intradomaine est négocié dans le domaine de reroutage entre les composants d'origine (contrôleurs de connexion et d'appel) et de destination (contrôleur de connexion et d'appel). Les demandes de service de reroutage intradomaine ne traversent pas la frontière du domaine.

Lorsque de multiples domaines de reroutage sont mis en jeu, les composants périphériques de chaque domaine de reroutage négocient l'activation des services de reroutage à l'intérieur du domaine de reroutage pour chaque appel. Une fois que la communication a été établie, chacun des domaines de reroutage situés dans le trajet de la communication a connaissance des services de reroutage qui sont activés concernant cette communication. Comme dans le cas d'un seul domaine de reroutage, dès que la communication a été établie, les services de reroutage ne peuvent pas être renégociés. Cette négociation permet également aux composants associés aux deux parties – appelant et appelé – de demander un service de reroutage. Dans ce cas, le service est désigné comme un service interdomaines parce que les demandes sont transmises de part et d'autre des frontières de domaine de reroutage. Bien qu'un service de reroutage puisse être demandé en mode de bout en bout, ce service est exécuté domaine de reroutage par domaine de reroutage (c'est-à-dire entre les composants d'origine et de destination dans chaque domaine de reroutage traversé par cette communication).

Pendant la négociation des services de reroutage, les composants périphériques d'un domaine de reroutage échangent leurs capacités de reroutage et la demande d'un service de reroutage ne peut être prise en charge que si le service est disponible aussi bien à l'origine qu'à la destination au bord du domaine de reroutage.

Un service de reroutage inconditionnel offre un mécanisme de rétablissement sur défaillance pour les communications qui est toujours en réponse à un événement de défaillance. Lorsqu'une liaison ou un élément de réseau tombe en panne dans un domaine de reroutage, la communication est libérée aux bords du domaine de reroutage. Dans le cas d'un service de reroutage inconditionnel qui a été activé pour cette communication, l'origine bloque la libération de la communication et essaie de créer un segment de connexion de secours vers la destination à la périphérie du domaine de reroutage. Cette connexion de secours est la connexion de reroutage. La destination située à la périphérie du domaine de reroutage bloque également la libération de la communication et attend que l'origine située à la périphérie du domaine de reroutage crée la connexion de reroutage. En reroutage inconditionnel, le segment de connexion original est libéré avant la création d'un segment

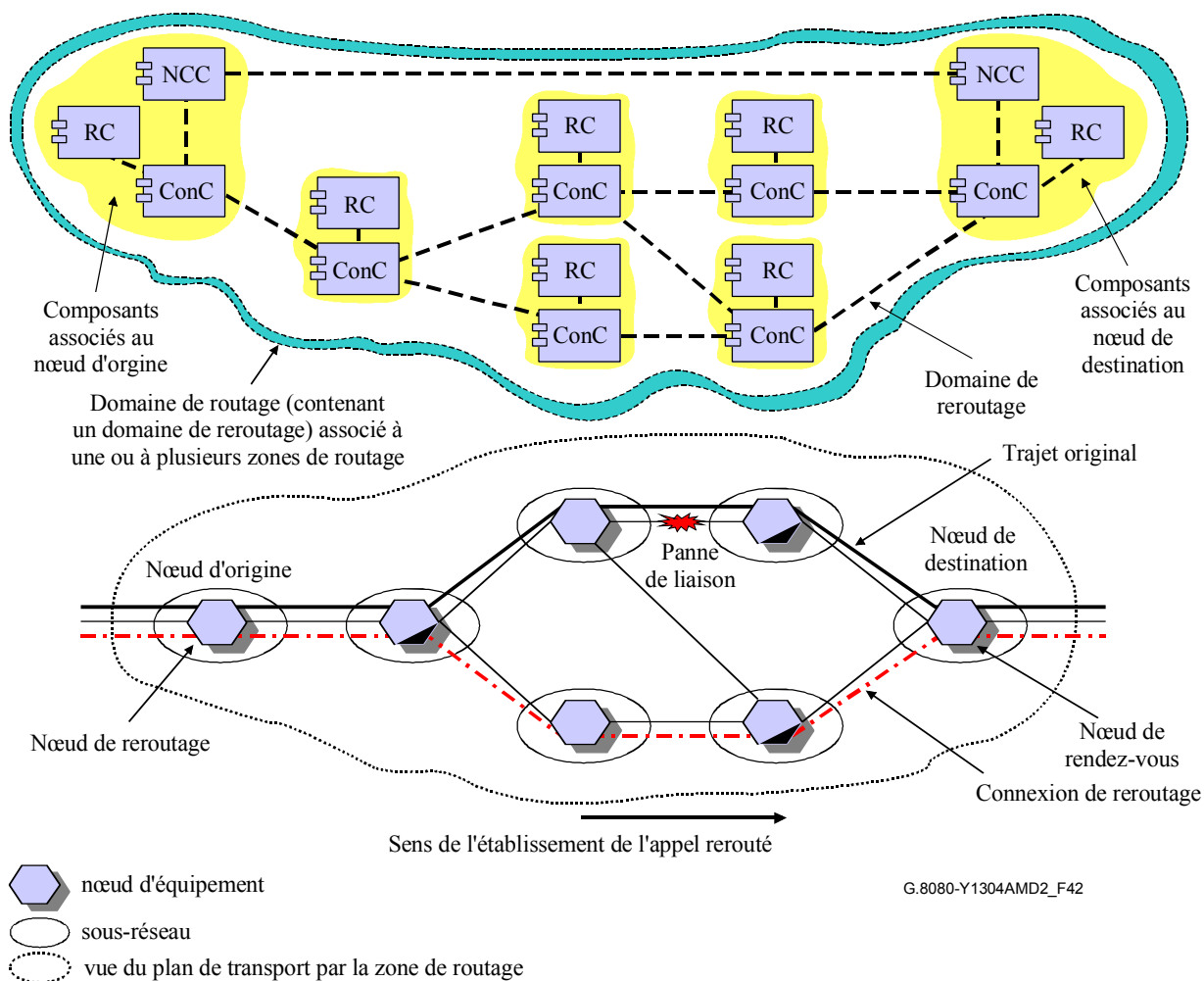
de connexion de secours. C'est ce qu'on appelle coupure avant rétablissement. Un exemple de reroutage inconditionnel est fourni sur la Figure 42. Dans cet exemple, le domaine de routage est associé à une seule zone de routage et à un seul domaine de reroutage. La communication est reroutée entre les nœuds d'origine et de destination et entre les composants qui leur sont associés.

Le service de reroutage conditionnel est un mécanisme permettant de réacheminer un appel à des fins administratives (par exemple, optimisation du trajet, maintenance du réseau, travaux d'ingénierie planifiés). Lorsqu'une opération de reroutage est déclenchée (généralement par l'intermédiaire d'une demande émise du plan de gestion) et envoyée à l'emplacement des composants de reroutage, ceux-ci établissent une connexion de reroutage à l'emplacement des composants de rendez-vous. Dès que la connexion de reroutage est créée, les composants de reroutage l'utilisent et suppriment la connexion initiale. C'est ce qu'on appelle rétablissement avant coupure.

Pendant une procédure de reroutage conditionnel, une défaillance peut se produire sur la connexion initiale. Dans ce cas, l'opération de reroutage inconditionnel prend la priorité sur l'opération de reroutage conditionnel et les composants d'origine et de destination du domaine de reroutage procèdent conformément au processus de reroutage inconditionnel.

Si un comportement réversible est requis (c'est-à-dire que la communication doit toujours être rétablie dans ses connexions originales lorsque la défaillance a été réparée), les contrôleurs d'appel réseau ne doivent pas libérer ces connexions originales (tombées en panne). Les contrôleurs d'appel réseau doivent continuer à surveiller les connexions originales et, lorsque la défaillance est réparée, la communication est rétablie dans ses connexions originales.





**Figure 42/G.8080/Y.1304 – Exemple de reroutage inconditionnel**

## 11.2.1 Reroutage en réponse à une défaillance

### 11.2.1.1 Défaillances intradomaines

D'éventuelles défaillances dans un domaine de reroutage devraient provoquer une action de reroutage (rétablissement) dans ce domaine, telle que tout domaine aval n'observe qu'un signal entrant de défaillance momentanée (ou de défaillance momentanée d'une section précédente). Les connexions prenant en charge la communication doivent continuer à utiliser les mêmes nœuds passerelles d'origine (entrée) et de destination (sortie) dans le domaine de reroutage.

### 11.2.1.2 Défaillances interdomaines

Deux cas de défaillance doivent toujours être considérés: la défaillance d'une liaison entre deux éléments de réseau jouant le rôle de passerelle dans différents domaines de reroutage et la défaillance d'éléments de réseau jouant le rôle de passerelle interdomaines.

### 11.2.1.3 Défaillance de liaison entre éléments de réseau adjacents jouant le rôle de passerelle

Quand une défaillance se produit à l'extérieur des domaines de reroutage (par exemple, la liaison entre éléments de réseau jouant le rôle de passerelle dans différents domaines de reroutage A et B sur la Figure 43-a), aucune opération de reroutage ne peut être exécutée. Dans ce cas, d'autres mécanismes de protection peuvent être employés entre les domaines.

La Figure 43-b montre l'exemple de deux liaisons entre domaine A et domaine B. La fonction de sélection de trajet à l'extrémité A (d'origine) de la communication doit sélectionner une liaison

interdomaines ayant le niveau de protection approprié. La plus simple méthode de protection dans ce scénario consiste à utiliser un mécanisme de protection préétabli (par exemple, dans un réseau de couche serveur. Un tel procédé est transparent aux connexions qui passent au-dessus du sommet de ce réseau). Si la liaison protégée tombe en panne, le système de protection de liaison lancera l'opération de protection. Dans ce cas, la communication continue à être routée sur les mêmes éléments de réseau jouant le rôle de passerelle d'entrée et de sortie dans les domaines adjacents et la reprise sur défaillance est confinée à la liaison interdomaines.

#### 11.2.1.4 Panne d'élément de réseau jouant le rôle de passerelle

Ce cas est représenté sur la Figure 44. Afin de rétablir un appel lorsque B-1 tombe en panne, un autre nœud passerelle, B-3, doit toujours être utilisé pour le domaine B. En général, ce processus nécessitera également l'utilisation d'une autre passerelle dans le domaine A, dans ce cas A-3. En réponse à la défaillance de l'élément de réseau jouant le rôle passerelle B-1 (détectée par l'élément passerelle A-2) le nœud d'origine dans le domaine A, A-1, doit émettre une demande de nouvelle connexion afin de prendre en charge cette communication. L'indication envoyée à ce nœud doit préciser que le reroutage entre les éléments A-1 et A-2 doit être évité dans le domaine A et qu'il faut une nouvelle route et un nouveau trajet vers l'élément B-2. Cette opération peut être considérée comme un reroutage dans un domaine plus grand, C, qui ne se produit que si le reroutage effectué dans A ou B ne peut pas rétablir la connexion.

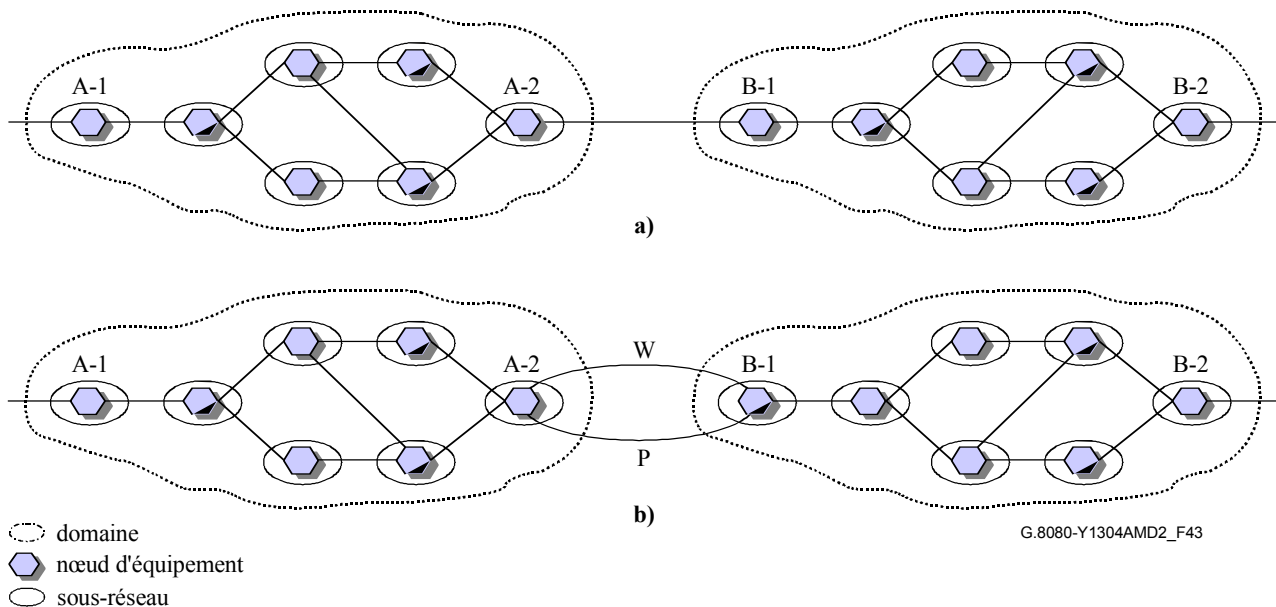
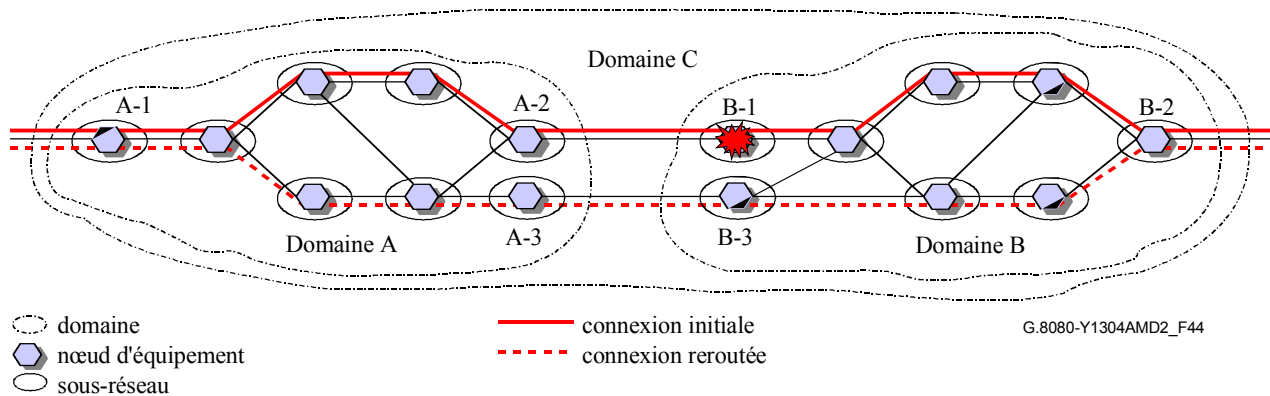


Figure 43/G.8080/Y.1304 – Scénarios de défaillance de liaison



**Figure 44/G.8080/Y.1304 – Reroutage en cas de panne d'élément de réseau jouant le rôle de passerelle**

### 39) Nouveau paragraphe 12 Résilience

*Ajouter les nouveaux paragraphes suivants:*

#### 12 Résilience

La résilience se rapporte à la capacité du plan de commande de continuer à fonctionner en conditions de défaillance. Le fonctionnement du plan de commande dépend d'éléments du réseau de communication de données (RCD), du plan de transport, du plan de gestion et des composants internes du plan de commande proprement dit (voir Figure 1). Des informations complémentaires sont fournies dans l'Appendice II.

##### 12.1 Principes des interactions entre plan de commande et plan de transport

Les principes suivants sont utilisés pour les interactions entre plan de commande et plan de transport lorsque les communications deviennent disponibles entre les deux plans.

- 1) le plan de commande dépend du plan de transport pour les informations sur les ressources de celui-ci;
- 2) la cohérence entre la vue du plan de commande et l'élément correspondant du réseau de transport est établie en premier (cohérence verticale);
- 3) dès que la cohérence locale est établie, la cohérence horizontale est recherchée. Dans ce cas, les composants du plan de commande se synchronisent avec leurs composants adjacents. Cette méthode sert à rétablir une vue cohérente du routage, de la communication et de l'état de la connexion.

Un autre principe d'interaction des plans de commande et de transport est le suivant:

- 4) les connexions qui existent dans le plan de transport ne sont pas altérées si le plan de commande tombe en panne et/ou se rétablit. Les composants du plan de commande sont donc dépendants de l'état de la connexion SNC.

Afin d'assurer la résilience, les informations sur la ressource du plan de transport et sur l'état de connexion SNC devraient être conservées dans une mémoire non volatile. D'autres informations sur l'utilisation de la connexion SNC par le plan de commande devraient être mémorisées. Cela comprend la question de savoir si la connexion SNC a été créée par la gestion de connexion et comment elle a été utilisée. Par exemple, quelle extrémité de la connexion SNC est orientée vers la tête de la connexion complète. A un nœud donné, le plan de commande doit vérifier qu'il possède des informations sur la ressource et sur l'état de la connexion SNC qui sont cohérentes avec les

informations homologues conservées par l'élément du réseau de transport. Si ce n'est pas le cas, les composants de commande chargés de ce nœud doivent toujours:

- annoncer une largeur de bande nulle disponible aux nœuds adjacents afin de garantir qu'il n'y aura pas de demandes du réseau pour acheminer une nouvelle connexion par ce nœud;
- n'effectuer aucun changement de connexion (par exemple, des libérations).

L'état de connexion SNC est la plus importante information à rétablir en premier parce que c'est la base des connexions qui fournissent un service aux utilisateurs ultimes. Cette information suit le principe ci-dessus. Pendant la reprise, le plan de commande reconstruit l'état de la communication et de la connexion correspondant aux connexions existantes. Par exemple, le routage devra disséminer des informations SNP correctes après avoir été synchronisé par les composants locaux du plan de commande (LRM).

Le rétablissement par le plan de commande de la cohérence des informations avec l'élément du réseau de transport devrait s'effectuer dans la séquence suivante:

- le gestionnaire de ressources de liaison se synchronise avec les informations sur l'état de l'élément du réseau de transport;
- le contrôleur de connexion se synchronise ensuite avec le gestionnaire de ressources de liaison;
- le contrôleur d'appel réseau se synchronise ensuite avec le contrôleur de connexion.

Après le rétablissement de la cohérence d'état locale, le plan de commande doit vérifier la cohérence des informations sur l'état des connexions SNC avec les nœuds adjacents, comme examiné dans le principe 3 ci-dessus, avant de participer à des demandes d'établissement ou de libération de connexions dans le plan de commande.

## **12.2 Principes de la communication entre contrôleurs de protocole**

Lorsque la communication entre contrôleurs de protocole est interrompue, les communications existantes et leurs connexions ne sont pas altérées. Le plan de gestion peut être averti si la défaillance persiste et nécessite l'intervention de l'opérateur (par exemple afin de libérer une communication).

Une défaillance du RCD peut affecter une ou plusieurs des sessions de communication entre contrôleurs de protocole. Le contrôleur de protocole associé à chaque voie sémaphore doit détecter et signaler par alarme une défaillance de voie sémaphore.

Quand une session de communication entre contrôleurs de protocole se rétablit, la resynchronisation d'état devrait être exécutée entre les contrôleurs de protocole.

La défaillance d'un contrôleur de protocole est traitée comme une défaillance d'une session de communication entre contrôleurs de protocole.

## **12.3 Interactions entre plan de commande et plan de gestion**

Si les fonctions du plan de gestion deviennent indisponibles, diverses fonctions de commande peuvent être dégradées. Lorsque les fonctions du plan de gestion deviennent disponibles, les composants du plan de commande peuvent avoir besoin de signaler au plan de gestion les actions qu'ils ont entreprises pendant que le plan de gestion était indisponible (par exemple, les relevés d'appel).

## **40) Bibliographie**

*Renommer: "l'Appendice II" devient "l'Appendice V".*

#### 41) **Nouvel Appendice II Exemples d'implémentation**

*Ajouter le nouvel Appendice II suivant:*

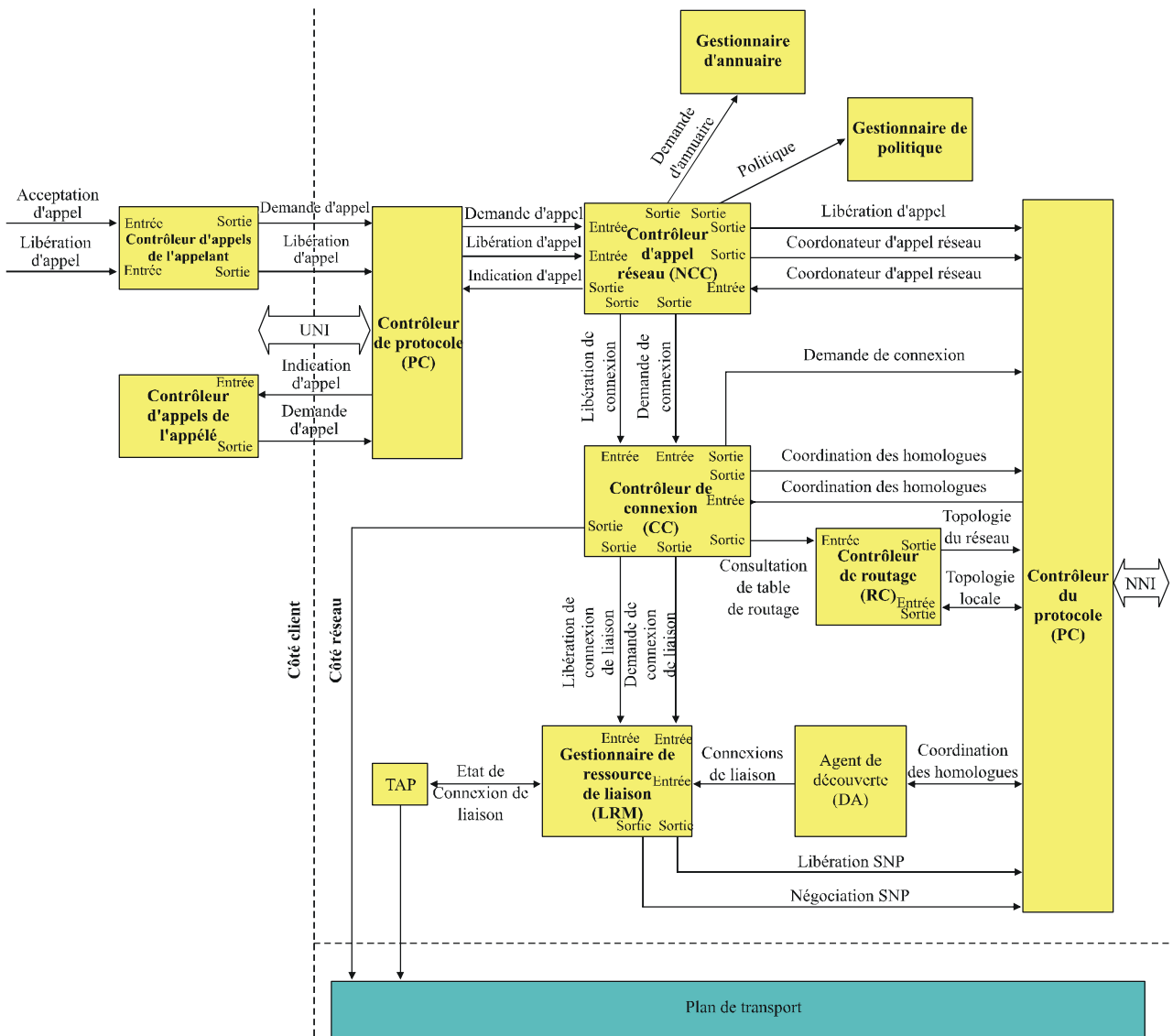
## **Appendice II**

### **Exemples d'implémentation**

L'architecture des réseaux optiques à commutation automatique est définie en termes de diverses fonctions. Celles-ci sont spécifiées dans le § 7 et prennent en charge les exigences spécifiées dans la Rec. UIT-T G.807/Y.1302.

L'architecture spécifiée dans la présente Recommandation assure une certaine souplesse d'implémentation et tient compte du fait que les opérateurs de réseau peuvent avoir des pratiques différentes. L'architecture tient également compte du fait que les fonctions peuvent être implémentées diverses façons. Par ailleurs, selon la fonctionnalité requise, les composants ne sont pas forcément tous nécessaires. Par exemple, l'architecture décrite dans la présente Recommandation assure une certaine souplesse de routage et permet les deux routages, centralisé et réparti. Dans le cas du routage réparti, il y a des interactions entre un certain nombre de fonctions de contrôleur de routage, tandis que dans un système centralisé, le routage peut, à titre d'option, être maintenu par le plan de gestion, ce qui évite la nécessité d'un composant contrôleur de routage. Les demandes de circuits, y compris leurs routes, sont transmises au plan de commande par le plan de gestion.

Bien qu'une certaine souplesse soit assurée dans l'architecture, les interfaces et flux d'informations définis permettent l'interconnexion des divers composants. Un tel exemple est illustré sur la Figure II.1 ci-dessous. Un autre exemple est contenu sur la Figure III.1.



G.8080-Y1304AMD2\_FII.1

Figure II.1/G.8080/Y.1304 – Exemple d'interconnexion de composants

## 42) Nouvel Appendice III Relations de résilience

Ajouter le nouvel Appendice III suivant:

### Appendice III

#### Relations de résilience

La résilience se rapporte à la capacité du plan de commande de continuer à fonctionner en conditions de défaillance. Le fonctionnement du plan de commande dépend d'éléments du réseau de communication de données (RCD), du plan de transport, du plan de gestion et des composants internes du plan de commande proprement dit (voir Figure 1). Les paragraphes suivants indiquent les relations de dépendance du plan de commande. Le degré souhaité de résilience du plan de commande peut ensuite être mis au point par introduction de la redondance appropriée concernant les fonctions dépendantes.

#### III.1 Relations entre plan de commande et RCD

Le plan de commande dépend du RCD concernant le transfert de messages de signalisation sur tout ou partie des interfaces suivantes (voir Figure III.1): UNI, NNI, NMI. L'influence d'une défaillance de voie sémaphore sur le fonctionnement du plan de commande sera examinée pour chacun des contrôleurs de protocole associés à chaque interface.

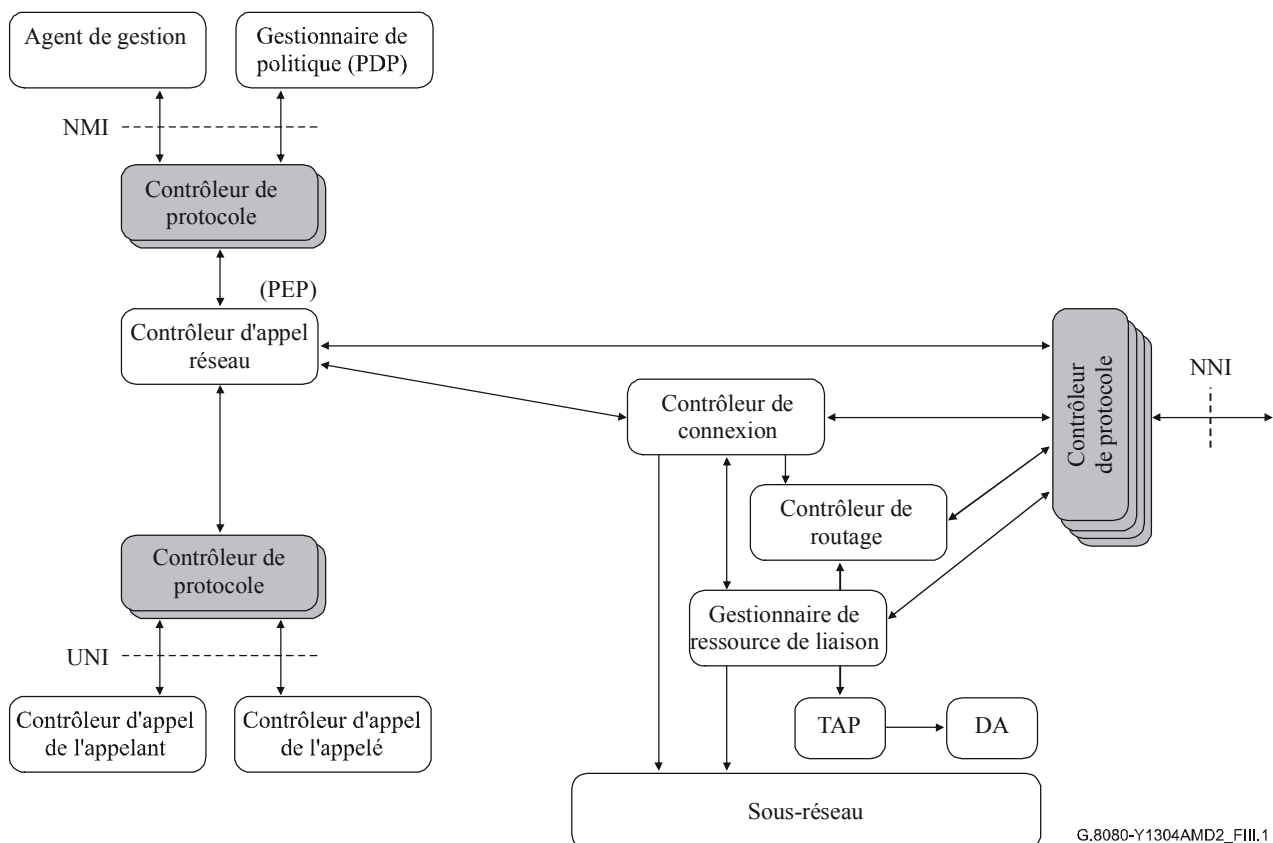


Figure III.1/G.8080/Y.1304 – Composants du plan de commande (interprétation)

### **III.1.1 Interface UNI**

Il peut y avoir deux contrôleurs de protocole distincts, traitant les sessions sémaphores à l'interface UNI: l'un pour la liaison du contrôleur d'appel de l'appelant et l'autre pour la liaison du contrôleur d'appel de l'appelé.

#### **III.1.1.1 Cas d'une défaillance**

Une défaillance de la session de signalisation prenant en charge l'interface UNI pour la liaison du contrôleur d'appel de l'appelant se traduira par la perte des flux de commande de demande d'appel/libération d'appel.

Une défaillance de la session de signalisation prenant en charge l'interface UNI pour la liaison du contrôleur d'appel de l'appelé se traduira par la perte des flux de commande de demande d'appel/indication d'appel.

Une défaillance de l'une de ces deux sessions de signalisation associées à l'interface UNI a une incidence sur la fonction de contrôleur d'appel réseau.

Dans tous les cas ci-dessus, les communications établies et leurs connexions ne sont pas altérées. Le plan de gestion peut être averti si la défaillance persiste et nécessite l'intervention de l'opérateur (par exemple afin de libérer une communication).

#### **III.1.1.2 Cas d'un rétablissement**

Quand la voie sémaphore se rétablit, la resynchronisation des états entre les contrôleurs d'appel clients et le contrôleur d'appel réseau, et le contrôleur de connexions à l'interface UNI, devrait être exécutée.

### **III.1.2 Interface NNI**

Il peut y avoir quatre contrôleurs de protocole distincts traitant les sessions de signalisation à l'interface NNI: un pour la liaison du contrôleur d'appel réseau, un pour la liaison du contrôleur de connexion, un pour la liaison du contrôleur de routage et un pour la liaison du gestionnaire de ressources de liaison.

#### **III.1.2.1 Cas d'une défaillance**

Une défaillance de la session de signalisation prenant en charge l'interface NNI pour la liaison du contrôleur d'appel réseau se traduira par la perte des flux de commande du contrôleur d'appel réseau. Un établissement ou une libération d'appel ne sera pas possible, mais il n'y a pas d'incidence sur l'établissement ou la libération de connexion.

Une défaillance de la session de signalisation prenant en charge l'interface NNI pour la liaison du contrôleur de connexion se traduira par la perte des flux de commande de coordination de contrôleur de connexion et de demande/libération de connexion. L'établissement ou la libération de connexion ne sera pas possible. Par ailleurs, si la commande d'appel est superposée à la commande de connexion, aucune opération d'établissement/de libération d'appel ne sera possible non plus.

Une défaillance de la session de signalisation prenant en charge l'interface NNI pour la liaison du contrôleur de routage se traduira par la perte des flux de commande de topologie locale/réseau.

Une défaillance de la session de signalisation prenant en charge l'interface NNI pour la liaison du gestionnaire de ressources de liaison se traduira par la perte des flux de commande de négociation/libération de point SNP.

Une défaillance de la session de signalisation de gestionnaire de ressources de liaison a une incidence sur la fonction du contrôleur de routage et sur la fonction du contrôleur de connexion. Une défaillance de la session de signalisation du contrôleur de routage a une incidence sur la fonction du contrôleur de connexion. Une défaillance de la session de signalisation du contrôleur de connexion a une incidence sur la fonction du contrôleur d'appel réseau.



Dans tous les cas ci-dessus, les communications existantes et leurs connexions ne sont pas altérées. Le plan de gestion peut être averti si la défaillance persiste et nécessite l'intervention de l'opérateur (par exemple afin de libérer une communication).

Il est à noter qu'une défaillance du RCD peut affecter simultanément une ou plusieurs des sessions de signalisation ci-dessus. Le contrôleur de protocole associé à chaque voie sémaphore doit détecter et signaler par alarme une défaillance de voie sémaphore.

### **III.1.2.2 Cas du rétablissement**

Dès restauration d'une voie sémaphore tombée en panne, le contrôleur de protocole correspondant doit veiller à ce que toute la messagerie reprenne en séquence. Des composants sont chargés de rétablir les informations d'état après rétablissement du contrôleur de protocole.

## **III.2 Relations entre plan de commande et plan de transport**

Le présent paragraphe ne prend en considération que les défaillances du plan de transport qui affectent la capacité du plan de commande à exécuter ses fonctions, par exemple lorsqu'un gestionnaire LRM ne peut pas être informé. Les défaillances du plan de transport, telles que celles des ports, ne sont pas dans le domaine d'application de la présente Recommandation car l'on s'attend que le plan de commande sera informé de cette situation. La cohérence des informations entre les deux plans est traitée dans le § 12.1.

### **III.2.1 Informations du plan de transport – Consultation**

Le plan de commande consultera le plan de transport selon les scénarios suivants:

- lorsqu'une session de signalisation d'un contrôleur de connexion s'active ou se réactive (par exemple après le rétablissement d'un élément NE de liaison de données ou de transport);
- lors des interrogations du plan de commande au sujet des ressources de transport;
- dans le cadre de la synchronisation des informations sur les ressources de transport (par exemple lorsque le plan de commande se rétablit à la suite d'une défaillance).

### **III.2.2 Informations du plan de transport – Déclenchées par un événement**

Le plan de transport informera le plan de commande événement par événement, selon les scénarios suivants:

- défaillance d'une ressource de transport;
- adjonction/suppression d'une ressource de transport.

### **III.2.3 Protection du plan de transport**

Les actions efficaces de protection du plan de transport sont largement transparentes au plan de commande. Le plan de transport est seulement tenu de signaler au plan de commande les changements de disponibilité des ressources de transport.

Les tentatives inefficaces de protection du plan de transport apparaissent au plan de commande comme des défaillances de connexion et peuvent déclencher des actions de rétablissement du plan de commande si une telle fonctionnalité est fournie. Etant donné que le plan de commande prend en charge la fonctionnalité de rétablissement, les relations suivantes existent.

Le contrôleur de routage doit toujours être informé de la défaillance d'une liaison ou d'un nœud du plan de transport et doit mettre à jour en conséquence la base de données relative à la topologie locale/au réseau. Le contrôleur de routage peut informer le contrôleur de connexion local de ces dérangements.

### **III.2.4 Dépendance du plan de transport par rapport au plan de commande**

Si le plan de commande tombe en panne, les nouvelles demandes de connexion qui nécessitent l'utilisation des composants tombés en panne du plan de commande ne peuvent pas être traitées. Il est à noter cependant que le plan de gestion pourrait être utilisé en repli afin de répondre à de nouvelles demandes de connexion. Les connexions établies ne doivent pas être affectées par une panne du plan de commande.

### **III.3 Relations entre plan de commande et plan de gestion**

Le plan de commande peut obtenir des informations relatives à l'annuaire et à la politique à partir du plan de gestion pendant le processus de validation du contrôle d'admission d'appel. Une défaillance des serveurs d'annuaire ou de politique pourrait se traduire par la défaillance de demandes d'établissement de connexion.

Exemples de ces situations:

- dans le contrôleur d'appel réseau (à l'extrémité appelante ou appelée), les demandes d'appel peuvent avoir besoin d'être validées par vérification de la politique;
- lorsque des contrôleurs de connexion demandent un trajet auprès du contrôleur de routage, un serveur de politiques peut devoir être consulté.

Des actions de libération de communication peuvent avoir lieu dans le plan de commande si le plan de gestion n'est pas disponible. Un enregistrement de ces actions doit toujours être conservé par le plan de commande de façon que, lorsque le plan de gestion devient disponible, un journal puisse être envoyé au plan de gestion ou que le plan de commande puisse être interrogé au sujet de ces informations.

#### **III.3.1 Interface NMI**

Tous les composants de commande possèdent des ports moniteur, politique et configuration qui donnent la vue gestion des composants du plan de commande (voir § 7.2.1).

Il peut y avoir deux contrôleurs de protocole distincts ou deux sessions de signalisation distinctes contenant des flux d'informations de gestion: l'un concernant la session de gestionnaire de politiques et l'autre pour une session de gestion de transport. D'autres contrôleurs de protocole pourront être introduits ultérieurement pour d'autres fonctions de gestion.

##### **III.3.1.1 Cas d'une défaillance**

Une défaillance de la session de signalisation prenant en charge la liaison de gestionnaire de politiques se traduira par la perte des flux de commande de sortie de politique.

Une défaillance de la session de signalisation de gestion de transport se traduira par l'interruption des échanges d'informations sur les fautes, la configuration, les comptes, la performance et la sécurité (FCAPS, *fault, configuration, accounting, performance, security*).

Une défaillance de la session de politique a une incidence sur la fonction du contrôleur d'appel réseau. Par exemple, l'éventuelle défaillance de nouvelles demandes d'établissement de connexion lors du processus de validation du contrôle d'admission d'appel nécessite l'accès au gestionnaire de politiques.

##### **III.3.1.2 Cas d'un rétablissement**

Lorsqu'une communication de signalisation de gestion est rétablie, les informations mémorisées dans le plan de commande, qui devraient être envoyées au plan de gestion (par exemple, relevés d'appel) sont envoyées. Les informations en instance d'envoi du plan de gestion au plan de commande devraient être envoyées (par exemple, révision de politique ou de configuration).

### **III.4 Relations à l'intérieur du plan de commande**

L'incidence de défaillances d'un composant du plan de commande sur le fonctionnement de l'ensemble du plan de commande sera examinée conformément à la relation de composants illustrée sur la Figure III.1. Afin d'obtenir un fonctionnement sans interruption du plan de commande en cas de défaillance d'un composant, la capacité de détecter une défaillance de composant et de commuter sur un composant redondant est requise, sans perte de messages ni d'informations d'état.

Si des composants du plan de commande ne sont pas redondants, alors, lorsqu'un composant tombé en panne se rétablit, ce composant doit rétablir une visibilité suffisante des ressources du plan de transport afin d'être opérationnel.

L'on part du principe que les communications entre composants autres que des contrôleurs de protocole (c'est-à-dire les communications non PC) sont très fiables. De telles communications, qui seront probablement internes à un nœud du plan de commande, sont propres à chaque implémentation, de sorte qu'elles sont hors du domaine d'application de la présente Recommandation.

#### **III.4.1 Contrôleur d'appel réseau**

La défaillance d'un contrôleur d'appel réseau se traduira par la perte de nouvelles demandes d'établissement d'appel et de demandes existantes de libération de communication.

#### **III.4.2 Contrôleur de connexion**

La défaillance d'un contrôleur de connexion se traduira par la perte de nouvelles demandes d'établissement de connexion et de demandes existantes de libération de connexion. Comme la signalisation de commande d'appel est souvent implémentée par l'intermédiaire du contrôleur de connexion et de son contrôleur de protocole, une défaillance du contrôleur de connexion peut avoir une incidence sur la fonction du contrôleur d'appel réseau (qui peut, par exemple, ne pas être en mesure de libérer des communications établies).

#### **III.4.3 Contrôleur de routage**

La défaillance d'un contrôleur de routage se traduira par la perte de nouvelles demandes d'établissement de connexion et par la perte de synchronisation de la base de données relative à la topologie. Comme le contrôleur de connexion dépend du contrôleur de routage pour la sélection de trajet, une défaillance du contrôleur de routage a une incidence sur le contrôleur de connexion. Les recherches d'informations de routage par le plan de gestion seront également affectées par une défaillance du contrôleur de routage.

#### **III.4.4 Gestionnaire de ressources de liaison**

La défaillance d'un gestionnaire de ressources de liaison se traduira par la perte de nouvelles demandes d'établissement de connexion, de demandes existantes de libération de connexion et de la synchronisation de la base de données de points SNP. Comme le contrôleur de routage dépend du gestionnaire de ressources de liaison pour les informations sur les ressources de transport, la fonction du contrôleur de routage est affectée par la défaillance d'un gestionnaire de ressources de liaison.

#### **III.4.5 Contrôleurs de protocole**

La défaillance d'un des contrôleurs de protocole a le même effet que celle des sessions de signalisation correspondantes dans le RCD telles que décrites plus haut. La défaillance d'un nœud entier du plan de commande doit toujours être détectée par les contrôleurs de protocole à l'interface NNI avec les nœuds adjacents.

### III.4.6 Cohérence des informations à l'intérieur du plan de commande

Comme examiné au § 12, dans un nœud donné, la cohérence des informations sur les ressources en composants du plan de commande et sur l'état des connexions SNC avec les informations sur les ressources locales en éléments NE de transport et sur leur état doit toujours être établie en premier. Ensuite, les composants du plan de commande doivent vérifier la cohérence des informations sur l'état des connexions SNC avec ses composants adjacents du plan de commande. Les éventuelles différences de connexion doivent toujours être résolues de façon qu'aucun fragment de connexion ne reste ou qu'aucune erreur de connexion ne se produise. A la suite de la contre-vérification de la cohérence des informations dans le plan de commande, les composants du plan de commande sont autorisés à participer aux demandes d'établissement ou de libération de connexions dans le plan de commande.

#### 43) Nouvel Appendice IV Exemple de commande d'appel intercouche

Ajouter le nouvel Appendice IV suivant:

## Appendice IV

### Exemple de commande d'appel intercouche

La Figure IV.1 illustre le modèle d'appel intercouches pour deux clients Ethernet, qui sont attachés à un réseau VC-3 commun ne prenant pas en charge la commutation Ethernet. On suppose qu'un appel à 40 Mbit/s est demandé sur une interface UNI Gigabit Ethernet. Pour acheminer l'information caractéristique Ethernet, une connexion VC-3 est créée. Les deux couches sont représentées mais seule la couche VC-3 possède une connexion de réseau. C'est une fois que la connexion VC-3 est établie que la connexion de liaison FPP ETH entre les deux contrôleurs  $NCC_{MAC}$  commence à exister.

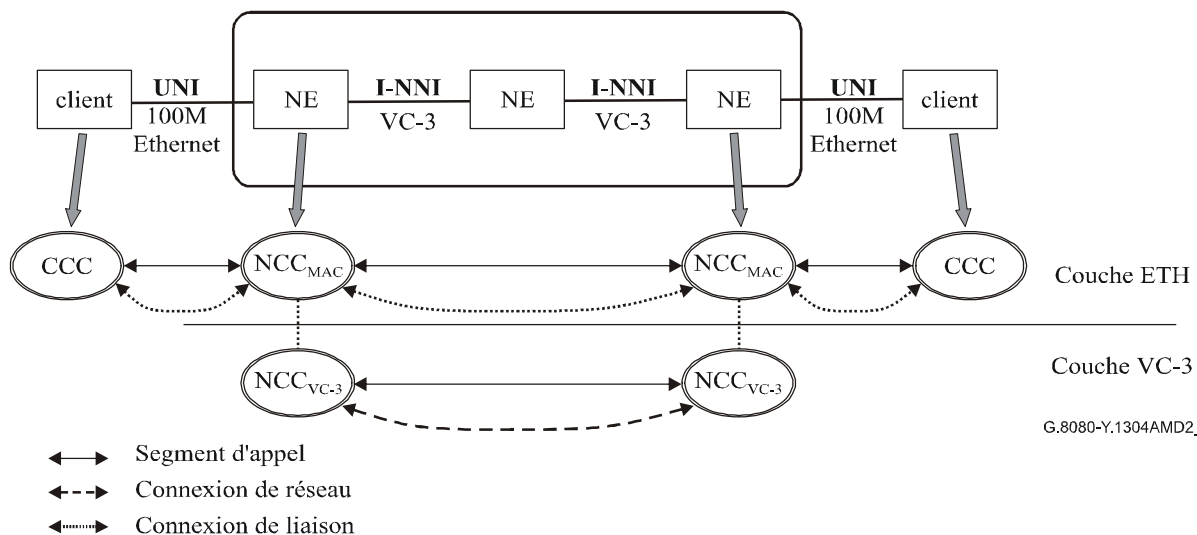


Figure IV.1/G.8080/Y.1304 – Exemple de Ethernet sur VC-3

Dans la séquence d'événements, il n'y pas d'ordre pour l'établissement des appels dans les différentes couches serveur. A titre d'exemple, l'appel Ethernet entrant peut déclencher la connexion VC-3. Autre possibilité: la connexion VC-3 peut déjà exister puis être associée à un appel MAC entrant.

Il existe beaucoup d'autres exemples d'appels intercouches (canal à fibre optique sur SDH/OTN, par exemple).

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

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

<b>INFRASTRUCTURE MONDIALE DE L'INFORMATION</b>	
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
<b>ASPECTS RELATIFS AU PROTOCOLE INTERNET</b>	
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
<b>Transport</b>	<b>Y.1300–Y.1399</b>
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
<b>RÉSEAUX DE PROCHAINE GÉNÉRATION</b>	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Numérotage, nommage et adressage	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899

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

## SÉRIES DES RECOMMANDATIONS UIT-T

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