

UIT-T

G.8080/Y.1304

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(06/2006)

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

Aspects relatifs aux protocoles en mode paquet sur
couche Transport – Aspects relatifs au protocole Ethernet
sur couche Transport

**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)**

Recommandation UIT-T G.8080/Y.1304

RECOMMANDATIONS UIT-T DE LA SÉRIE G
SYSTÈMES ET SUPPORTS DE TRANSMISSION, SYSTÈMES ET RÉSEAUX NUMÉRIQUES

| | |
|---|----------------------|
| CONNEXIONS ET CIRCUITS TÉLÉPHONIQUES INTERNATIONAUX | G.100–G.199 |
| CARACTÉRISTIQUES GÉNÉRALES COMMUNES À TOUS LES SYSTÈMES ANALOGIQUES À COURANTS PORTEURS | G.200–G.299 |
| CARACTÉRISTIQUES INDIVIDUELLES DES SYSTÈMES TÉLÉPHONIQUES INTERNATIONAUX À COURANTS PORTEURS SUR LIGNES MÉTALLIQUES | G.300–G.399 |
| CARACTÉRISTIQUES GÉNÉRALES DES SYSTÈMES TÉLÉPHONIQUES INTERNATIONAUX HERTZIENS OU À SATELLITES ET INTERCONNEXION AVEC LES SYSTÈMES SUR LIGNES MÉTALLIQUES | G.400–G.449 |
| COORDINATION DE LA RADIOTÉLÉPHONIE ET DE LA TÉLÉPHONIE SUR LIGNES | G.450–G.499 |
| CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION ET DES SYSTÈMES OPTIQUES | 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 AUX PROTOCOLES EN MODE PAQUET SUR COUCHE TRANSPORT | G.8000–G.8999 |
| Aspects relatifs au protocole Ethernet sur couche Transport | G.8000–G.8099 |
| Aspects relatifs au protocole MPLS sur couche Transport | G.8100–G.8199 |
| Objectifs de qualité et de disponibilité (suite de la série G.82x) | G.8200–G.8299 |
| Gestion des services | G.8600–G.8699 |
| 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)

Résumé

La présente Recommandation décrit l'architecture de référence pour le plan de commande du réseau optique à commutation automatique, telle qu'elle s'applique pour les réseaux de transfert de la hiérarchie SDH, conformément à la Rec. UIT-T G.803 et pour les réseaux de transport optique, conformément à la Rec. UIT-T G.872. Cette architecture de référence est décrite sous la forme des composants fonctionnels fondamentaux et de leurs interactions mutuelles.

Source

La Recommandation UIT-T G.8080/Y.1304 a été approuvée le 6 juin 2006 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 développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2007

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

| | Page |
|------|---|
| 1 | Domaine d'application 1 |
| 2 | Références normatives..... 1 |
| 3 | Définitions 2 |
| 4 | Abréviations..... 4 |
| 5 | Aperçu général..... 5 |
| 5.1 | Commandes d'appel et de connexion 7 |
| 5.2 | Interaction entre plans de commande, de transport et de gestion..... 9 |
| 6 | Organisation des ressources de transport..... 11 |
| 6.1 | Entités de transport 11 |
| 6.2 | Zones de routage..... 14 |
| 6.3 | Topologie et découverte 19 |
| 6.4 | Domaines 20 |
| 6.5 | Aspects relatifs aux couches multiples 22 |
| 6.6 | Prise en charge de client intercouches 24 |
| 6.7 | Appels pris en charge par des appels dans la même couche 25 |
| 7 | Architecture du plan de commande 26 |
| 7.1 | Notation 26 |
| 7.2 | Politique et fédérations 28 |
| 7.3 | Composants de l'architecture 31 |
| 7.4 | Composants "contrôleur de protocole" (PC) 51 |
| 8 | Points de référence..... 53 |
| 8.1 | Interface UNI..... 54 |
| 8.2 | Interface I-NNI 55 |
| 8.3 | Interface E-NNI 55 |
| 8.4 | Architecture côté utilisateur 55 |
| 8.5 | Interaction des contrôleurs NCC entre couches 56 |
| 9 | Gestion réseau des entités du plan de commande..... 58 |
| 10 | Identificateurs 59 |
| 10.1 | Espaces nominatifs 59 |
| 10.2 | Noms et adresses 59 |
| 10.3 | Relations entre identificateurs 61 |
| 11 | Techniques d'amélioration de la disponibilité des connexions..... 61 |
| 11.1 | Protection..... 62 |
| 11.2 | Rétablissement..... 62 |
| 12 | Résilience..... 66 |
| 12.1 | Principes des interactions entre plan de commande et plan de transport 66 |
| 12.2 | Principes de la communication entre contrôleurs de protocole..... 67 |

| | Page |
|--|-------------|
| 12.3 Interactions entre plan de commande et plan de gestion..... | 67 |
| Annexe A – Services de connexion | 68 |
| Appendice I – Réseaux de couche ASON | 71 |
| Appendice II – Exemples d'implémentation | 72 |
| Appendice III – Relations de résilience | 74 |
| III.1 Relations entre plan de commande et RCD..... | 74 |
| III.2 Relations entre plan de commande et plan de transport | 76 |
| III.3 Relations entre plan de commande et plan de gestion..... | 77 |
| III.4 Relations à l'intérieur du plan de commande..... | 78 |
| Appendice IV – Exemple de commande d'appel intercouche | 80 |
| Appendice V – Interactions de composants pour l'établissement de connexions | 81 |
| V.1 Routage hiérarchique..... | 81 |
| V.2 Routage par la source et pas à pas | 83 |
| V.3 Protection de connexion | 89 |
| V.4 Rétablissement – Reroutage inconditionnel – Reroutage intradomaine – Méthode hiérarchique | 91 |
| V.5 Rétablissement – Méthode de reroutage conditionnel, intradomaine ou par la source..... | 94 |
| V.6 Rétablissement – Méthode de reroutage réversible, intradomaine et par la source..... | 98 |
| V.7 Routage par la source utilisant l'interface de demande de routage..... | 101 |
| BIBLIOGRAPHIE..... | 104 |

Recommandation UIT-T G.8080/Y.1304

Architecture du réseau optique à commutation automatique (ASON)

1 Domaine d'application

La présente Recommandation spécifie l'architecture et les prescriptions pour le réseau de transport commuté automatique, telles qu'elles s'appliquent pour les réseaux de transport de la hiérarchie SDH, conformément à la Rec. UIT-T G.803 et pour les réseaux de transport optique, conformément à la Rec. UIT-T G.872.

La présente Recommandation décrit l'ensemble des composants du plan de commande qui sont utilisés pour piloter les ressources du réseau de transport en vue de la fourniture des fonctionnalités d'établissement, de maintenance et de libération des connexions. L'utilisation de composants permet d'effectuer une séparation entre la commande d'appel et la commande de connexion, ainsi qu'entre le routage et la signalisation.

Les composants sont utilisés aux fins de la présente Recommandation pour représenter des entités abstraites et non des instances de logiciel susceptibles d'être implémentées. La description des composants de l'architecture du réseau optique à commutation automatique utilise une notation comparable au langage UML.

2 Références normatives

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

- Recommandation UIT-T G.705 (2000), *Caractéristiques des blocs fonctionnels des équipements de la hiérarchie numérique plésiochrone.*
- Recommandation UIT-T G.707/Y.1322 (2003), *Interface de nœud de réseau pour la hiérarchie numérique synchrone.*
- Recommandation UIT-T G.709/Y.1331 (2003), *Interfaces pour le réseau de transport optique.*
- Recommandation UIT-T G.783 (2006), *Caractéristiques des blocs fonctionnels des équipements de la hiérarchie numérique synchrone.*
- Recommandation UIT-T G.798 (2004), *Caractéristiques des blocs fonctionnels d'équipements en hiérarchie de réseau de transport optique (OTN).*
- Recommandation UIT-T G.803 (2000), *Architecture des réseaux de transport à hiérarchie numérique synchrone.*
- Recommandation UIT-T G.805 (2000), *Architecture fonctionnelle générique des réseaux de transport.*
- Recommandation UIT-T G.872 (2001), *Architecture des réseaux de transport optiques.*
- Recommandation UIT-T G.8081/Y.1353 (2004), *Termes et définitions des réseaux optiques à commutation automatique (ASON).*

- Recommandation UIT-T M.3000 (2000), *Aperçu général des Recommandations relatives au réseau de gestion des télécommunications.*
- Recommandation UIT-T M.3010 (2000), *Principes des réseaux de gestion des télécommunications.*
- Recommandation UIT-T M.3100 (2005), *Modèle générique d'information de réseau.*
- 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 architectures pour les réseaux privés virtuels de couche I.*
- Recommandation UIT-T Y.1313 ("consentie" en 2004), *Architectures de service et de réseau du réseau privé virtuel de couche I.*

3 Définitions

La présente Recommandation définit les termes suivants:

- 3.1 groupe d'accès (AG, *access group*):** voir la Rec. UIT-T G.805.
- 3.2 adaptation:** voir la Rec. UIT-T G.805.
- 3.3 domaine administratif:** voir la Rec. UIT-T G.805.
- 3.4 chemin:** voir la Rec. UIT-T G.805.
- 3.5 groupe fermé d'utilisateurs:** voir la Rec. UIT-T X.25.
- 3.6 liaison:** voir la Rec. UIT-T G.805.
- 3.7 connexion de liaison:** voir la Rec. UIT-T G.805.
- 3.8 réseau privé virtuel:** voir la Rec. UIT-T Y.1311.
- 3.9 couche de réseau:** voir la Rec. UIT-T G.805.
- 3.10 agent:** Voir Rec. UIT-T G.8081/Y.1353.
- 3.11 appel:** Voir Rec. UIT-T G.8081/Y.1353.
- 3.12 segment d'appel:** voir Rec. UIT-T G.8081/Y.1353.
- 3.13 composant:** voir Rec. UIT-T G.8081/Y.1353.
- 3.14 point de connexion (CP, *connection point*):** voir Rec. UIT-T G.8081/Y.1353.
- 3.15 point de terminaison de connexion (CTP, *connection termination point*):** voir Rec. UIT-T G.8081/Y.1353.
- 3.16 plan de commande:** voir Rec. UIT-T G.8081/Y.1353.
- 3.17 plan de gestion:** voir Rec. UIT-T G.8081/Y.1353.
- 3.18 rattachement multiple:** voir Rec. UIT-T G.8081/Y.1353.
- 3.19 politique:** voir Rec. UIT-T G.8081/Y.1353.
- 3.20 contrôleur de port:** voir Rec. UIT-T G.8081/Y.1353.
- 3.21 route:** voir Rec. UIT-T G.8081/Y.1353.

- 3.22 zone de routage:** voir Rec. UIT-T G.8081/Y.1353.
- 3.23 niveau de routage:** voir Rec. UIT-T G.8081/Y.1353.
- 3.24 sous-réseau:** voir Rec. UIT-T G.8081/Y.1353.
- 3.25 connexion de sous-réseau (SNC, *subnetwork connection*):** voir Rec. UIT-T G.8081/Y.1353.
- 3.26 point de sous-réseau (SNP, *subnetwork point*):** voir Rec. UIT-T G.8081/Y.1353.
- 3.27 pool de points de sous-réseau (SNPP, *subnetwork point pool*):** voir Rec. UIT-T G.8081/Y.1353.
- 3.28 liaison de pool de points de sous-réseau (liaison SNPP):** voir Rec. UIT-T G.8081/Y.1353.
- 3.29 point de connexion de terminaison (TCP, *termination connection point*):** voir Rec. UIT-T G.8081/Y.1353.
- 3.30 point de terminaison de chemin:** voir Rec. UIT-T G.8081/Y.1353.
- 3.31 plan de transport:** voir Rec. UIT-T G.8081/Y.1353.
- 3.32 domaine de commande:** voir Rec. UIT-T G.8081/Y.1353.
- 3.33 domaine de transport:** voir Rec. UIT-T G.8081/Y.1353.
- 3.34 reroutage inconditionnel:** voir Rec. UIT-T G.8081/Y.1353.
- 3.35 protection configurée du plan de commande:** voir Rec. UIT-T G.8081/Y.1353.
- 3.36 domaine de reroutage:** voir Rec. UIT-T G.8081/Y.1353.
- 3.37 rétablissement:** voir Rec. UIT-T G.8081/Y.1353.
- 3.38 domaine de commande de routage:** voir Rec. UIT-T G.8081/Y.1353.
- 3.39 identificateur des ressources de transport:** voir Rec. UIT-T G.8081/Y.1353.
- 3.40 adresse:** voir Rec. UIT-T G.8081/Y.1353.
- 3.41 interface réseau-réseau externe (E-NNI, *external network-to-network interface*):** voir Rec. UIT-T G.8081/Y.1353. Voir également § 8.
- 3.42 interface:** voir Rec. UIT-T G.8081/Y.1353.
- 3.43 I-NNI:** voir Rec. UIT-T G.8081/Y.1353. Voir également § 8.
- 3.44 nom:** voir Rec. UIT-T G.8081/Y.1353.
- 3.45 connexion permanente:** voir Rec. UIT-T G.8081/Y.1353.
- 3.46 connexion commutée (SC, *switched connection*):** voir Rec. UIT-T G.8081/Y.1353.
- 3.47 connexion permanente reconfigurable (SPC, *soft permanent connection*):** voir Rec. UIT-T G.8081/Y.1353.
- 3.48 accord sur le niveau de service:** voir Rec. UIT-T G.8081/Y.1353.
- 3.49 services complémentaires:** voir Rec. UIT-T G.8081/Y.1353.
- 3.50 signalisation par tierce partie:** voir Rec. UIT-T G.8081/Y.1353.
- 3.51 interface utilisateur-réseau (UNI, *user-network interface*) pour le plan de commande:** voir la Rec. UIT-T G.8081/Y.1353.

La présente Recommandation définit les termes suivants:

3.52 connexion: concaténation de connexions de liaison et de connexions de sous-réseau (telles qu'elles sont décrites dans la Rec. UIT-T G.805) assurant le transport des informations utilisateur entre les points d'entrée et de sortie d'un sous-réseau.

3.53 reroutage conditionnel: fonction qui permet de rerouter une connexion à des fins administratives. La connexion initiale n'est pas mise hors service tant que la connexion reroutée n'est pas établie.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

| | |
|-------|--|
| AG | groupe d'accès (<i>access group</i>) |
| AGC | conteneur de groupe d'accès (<i>access group container</i>) |
| CC | contrôleur de connexion (<i>connection controller</i>) |
| CCC | contrôleur d'appel de l'appelant (<i>calling party call controller</i>) |
| CP | point de connexion (<i>connection point</i>) |
| CPS | statut de point de connexion (<i>connection point status</i>) |
| CTP | point de terminaison de connexion (<i>connection termination point</i>) |
| DA | agent de découverte (<i>discovery agent</i>) |
| E-NNI | interface réseau-réseau logique externe (point de référence) (<i>logical external network-network interface</i>) |
| HOVC | conteneur virtuel d'ordre supérieur (<i>higher order virtual container</i>) |
| id | identificateur |
| I-NNI | interface réseau-réseau logique interne (point de référence) (<i>logical internal network-network interface</i>) |
| LOVC | conteneur virtuel d'ordre inférieur (<i>lower order virtual container</i>) |
| LRM | gestionnaire de ressource de liaison (<i>link resource manager</i>) |
| MI | informations de gestion (<i>management information</i>) |
| MO | objet géré (<i>managed object</i>) |
| NCC | contrôleur d'appel réseau (<i>network call controller</i>) |
| PC | contrôleur de protocole (<i>protocol controller</i>) |
| RC | contrôleur du routage (<i>routing controller</i>) |
| RCD | réseau de communications de données |
| SNC | connexion de sous-réseau (<i>subnetwork connection</i>) |
| SNP | point de sous-réseau (<i>subnetwork point</i>) |
| SNPP | pool de points de terminaison de sous-réseau (<i>subnetwork point pool</i>) |
| TAP | exécuteur de terminaison et d'adaptation (<i>termination and adaptation performer</i>) |
| TCP | point de connexion de terminaison (<i>termination connection point</i>) |
| TTP | point de terminaison de chemin (<i>trail termination point</i>) |
| UML | langage de modélisation unifié (<i>unified modelling language</i>) |

| | |
|-----|---|
| UNI | interface utilisateur-réseau logique (point de référence) (<i>logical user-network interface</i>) |
| VPN | réseau privé virtuel (<i>virtual private network</i>) |

5 Aperçu général

Les objectifs du plan de commande du réseau optique à commutation automatique (ASON, *automatic switched optical network*) sont les suivants:

- faciliter une configuration rapide et efficace des connexions au sein d'un réseau de couche de transport pour la prise en charge de connexions commutées et de connexions permanentes reconfigurables;
- reconfigurer ou modifier des connexions prenant en charge des appels déjà établis;
- fournir une fonction de restauration.

Une architecture de plan de commande conçue correctement doit permettre aux fournisseurs de services de gérer leur réseau tout en assurant un établissement rapide et fiable des appels. Le plan de commande doit être fiable et efficace d'une manière intrinsèque, avec une possibilité de mise à l'échelle. Il doit avoir un caractère suffisamment générique pour prendre en charge diverses technologies, divers besoins commerciaux et diverses répartitions des fonctions par les fournisseurs (c'est-à-dire, divers regroupements, sous forme de paquetages, des composants du plan de commande).

Le plan de commande du réseau ASON se constitue de composants qui fournissent des fonctions spécifiques incluant la recherche de route et la signalisation. La description des composants du plan de commande n'impose aucune limitation à la combinaison et à l'assemblage de ces fonctions. Les interactions entre les composants et les flux d'information nécessaires à leurs communications mutuelles se font par le biais d'interfaces.

La présente Recommandation traite des composants de l'architecture de plan de commande ainsi que des interactions entre le plan de commande, le plan de gestion et le plan de transport. Le plan de gestion et le plan de transport sont spécifiés dans d'autres Recommandations et sont en dehors du domaine d'application de la présente Recommandation.

La Figure 1 présente une vue à haut niveau des interactions entre les plans de commande, de gestion et de transport pour la prise en charge de connexions commutées d'un réseau de couche. Elle représente également le réseau RCD qui fournit les itinéraires de communication permettant de véhiculer les informations de signalisation et de gestion. Les détails du réseau RCD, du plan de gestion et du plan de transport sont en dehors du domaine d'application de la présente Recommandation. Les fonctions qui dépendent du plan de commande sont décrites dans la présente Recommandation.

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 de connexion (voir Annexe A) 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 "couche de conduit" (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, qui représente un point de délimitation de service utilisateur-fournisseur. 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 paragraphe 8 donne une description plus approfondie des flux d'informations en ces points de référence.

Le plan de commande peut également être cloisonné pour permettre la ségrégation de ressources, par exemple entre des réseaux privés virtuels (VPN, *virtual private network*). Si les ressources sont dédiées à des domaines indépendants, aucun point de référence ne sera alors fourni entre ces domaines. Le cas de partage dynamique d'une partie des ressources appelle une étude ultérieure.

Des descriptions distinctes seront faites pour les interactions entre:

- le plan de commande et les réseaux de couche du plan de transport, et
- le plan de gestion et le plan de transport, résultant de l'ajout du plan de commande pour la configuration de gestion des connexions et de superviseurs de connexion.

La présente Recommandation aborde également la commande des connexions de réseau de la couche transport, y compris les interactions entre couches découlant des demandes de capacité dans les couches serveur.

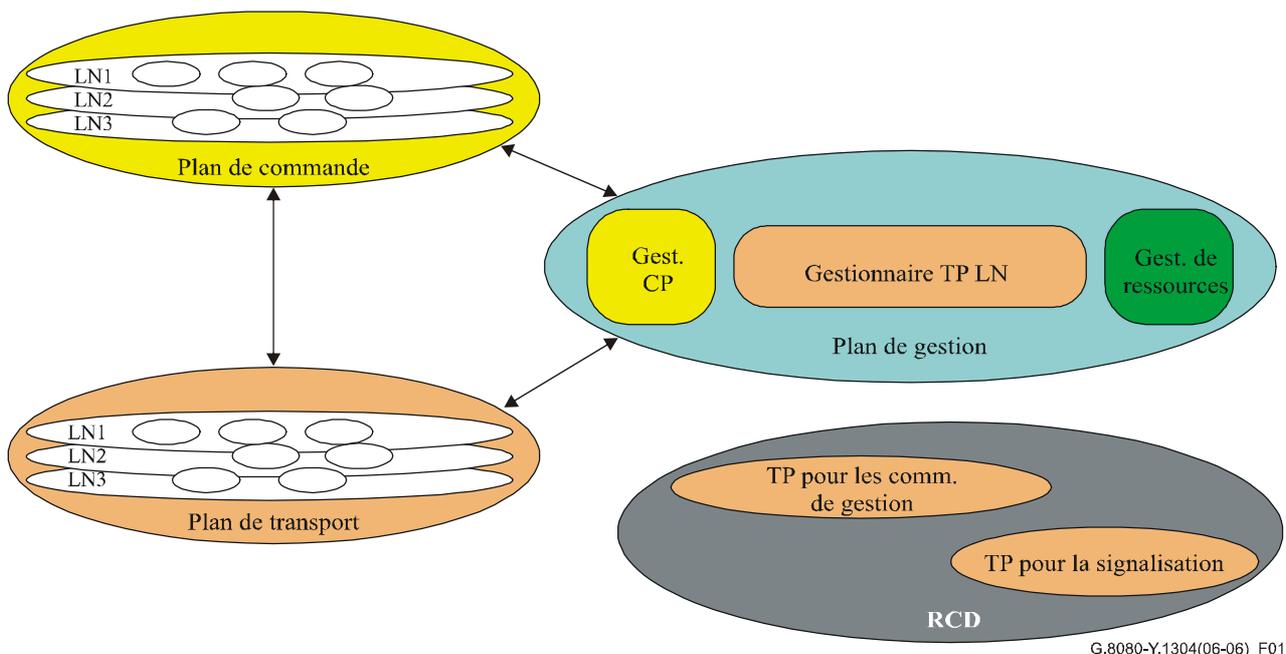


Figure 1/G.8080/Y.1304 – Relations entre les composants de l'architecture

5.1 Commandes d'appel et de connexion

La présente Recommandation traite de manière distincte la commande d'appel et la commande de connexion, étant donné que la commande d'appel n'est nécessaire qu'aux frontières des domaines (interface UNI ou E-NNI, par exemple). Ainsi, au sein d'un domaine (c'est-à-dire à l'interface I-NNI) seules doivent être prises en charge les procédures de commande de connexion. En outre, la commande d'appel est assurée aux frontières des contrôleurs CC intercouches. 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 des processus propres à un service.

5.1.1 Commande d'appel

La commande d'appel est une association de signalisation entre une ou plusieurs applications utilisateur et le réseau permettant la commande de l'établissement, de la libération, de la modification et de la maintenance d'ensembles de connexion. La commande d'appel est utilisée pour la maintenance de l'association ente les participants; un appel peut comprendre à tout instant un nombre quelconque, éventuellement nul, de connexions sous-jacentes.

La réalisation de la commande d'appel peut s'effectuer de l'une des manières suivantes:

- séparation des informations d'appel sous la forme de paramètres véhiculés dans un protocole d'appel/de connexion unique;
- séparation des machines d'état pour la commande d'appel et la commande de connexion, tout en utilisant un seul protocole d'appel/de connexion pour les informations de signalisation;

- séparation des informations et des machines d'état avec utilisation de protocoles de signalisation distincts pour la commande d'appel et la commande de connexion.

La commande d'appel doit assurer la coordination des connexions (pour un appel avec connexions multiples) et la coordination des participants (pour un appel avec participants multiples). La coordination de connexions multiples nécessite les actions suivantes de la part du réseau:

- le routage de toutes les connexions doit se faire de manière à permettre leur supervision par l'une au moins des entités de coordination (de commande d'appel);
- les associations de commande d'appel doivent être réalisées avant l'établissement des connexions. Un appel peut exister en l'absence de toute connexion (ce qui permet de faciliter la réorganisation de connexions complexes).

On peut considérer qu'un appel se déroule selon les trois phases suivantes:

établissement

des messages de signalisation sont échangés durant cette phase entre les utilisateurs et le réseau pour la négociation des caractéristiques de l'appel. L'échange de messages de signalisation entre l'appelant et le réseau constitue un appel de départ. L'échange de messages de signalisation entre le réseau et l'appelé constitue un appel arrivée;

activité

des données peuvent être échangées durant cette phase sur les connexions associées; il est également possible de modifier des paramètres de l'appel (par exemple, d'ajouter de nouveaux participants dans un appel de point à multipoint, lorsque ce type d'appel est pris en charge);

libération

des messages de signalisation sont échangés durant cette phase entre des participants appelants ou appelés et le réseau pour mettre fin à l'appel. Un appel peut être libéré, soit par les terminaux appelants ou appelés, soit par un serveur mandataire ou par la gestion du réseau.

5.1.2 Contrôle d'admission d'appel

Le contrôle d'admission d'appel est une fonction de maintien de l'ordre invoquée par un rôle d'origine dans un réseau et pouvant impliquer une coopération avec le rôle de terminaison du réseau. Il convient de noter que l'autorisation de la progression de l'appel indique uniquement que ce dernier peut demander une ou plusieurs connexions, mais pas que ces demandes de connexion aboutiront. Le contrôle d'admission d'appel peut également être invoqué au niveau d'autres frontières de réseau.

La fonction d'admission d'appel origine est responsable de la vérification de la validité du nom de l'utilisateur appelé et des paramètres fournis. Les paramètres de service sont vérifiés par rapport à une spécification de niveau de service (ensemble de paramètres et de valeurs qui ont fait l'objet d'un accord entre l'opérateur réseau et le client pour un service donné, indiquant le "*domaine d'application*" du service). Ces paramètres peuvent, si nécessaire, être renégociés avec l'appelant. Le domaine d'application de cette négociation est déterminé par des règles découlant de la spécification de niveau de service initiale, elle-même déduite de l'accord de niveau de service (contrat de service entre un opérateur réseau et un client qui définit globalement leurs responsabilités mutuelles).

La fonction d'admission d'appel de terminaison est responsable de la vérification du fait que l'appelé est en droit d'accepter l'appel, compte tenu des contrats de service de l'appelant et de l'appelé. Une adresse appelée peut, par exemple, faire l'objet d'un filtrage.

5.1.3 Commande de connexion

La commande de connexion est responsable de la commande globale des connexions individuelles. On peut également considérer qu'elle est associée à la commande de liaison. La commande globale d'une connexion est assurée par le protocole qui lance les procédures d'établissement et de libération associées à une connexion, ainsi que la maintenance de l'état de la connexion.

5.1.4 Contrôle d'admission de connexion

Le contrôle d'admission de connexion est essentiellement un processus qui détermine si des ressources suffisantes sont disponibles pour admettre une connexion (ou qui renégocie des ressources pendant la durée d'un appel). Ceci se fait en général liaison par liaison, en fonction des conditions et des règles locales. Pour un réseau avec commutation de circuit, il peut s'agir uniquement de déterminer si des ressources libres sont disponibles. Par contre, dans des réseaux avec commutation de paquets tels que l'ATM qui utilisent des paramètres multiples de qualité de service, le contrôle d'admission de connexion implique la garantie que l'admission de nouvelles connexions est compatible avec les accords de qualité de service déjà acceptés pour les connexions existantes. Le contrôle d'admission de connexion peut refuser la demande de connexion.

5.1.5 Relation entre les états d'appel et de connexion

L'état de l'appel dépend de l'état des connexions associées. Cette dépendance est liée au type et à la politique de l'appel. Lorsque, par exemple, une connexion unique subit une défaillance, l'appel peut alors être libéré immédiatement ou il peut, en variante, être libéré après un certain délai si aucune connexion de remplacement ne peut être fournie par des mécanismes de protection ou de restauration. Il convient de noter que les états d'appel et de connexion coïncident aux frontières des domaines.

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.

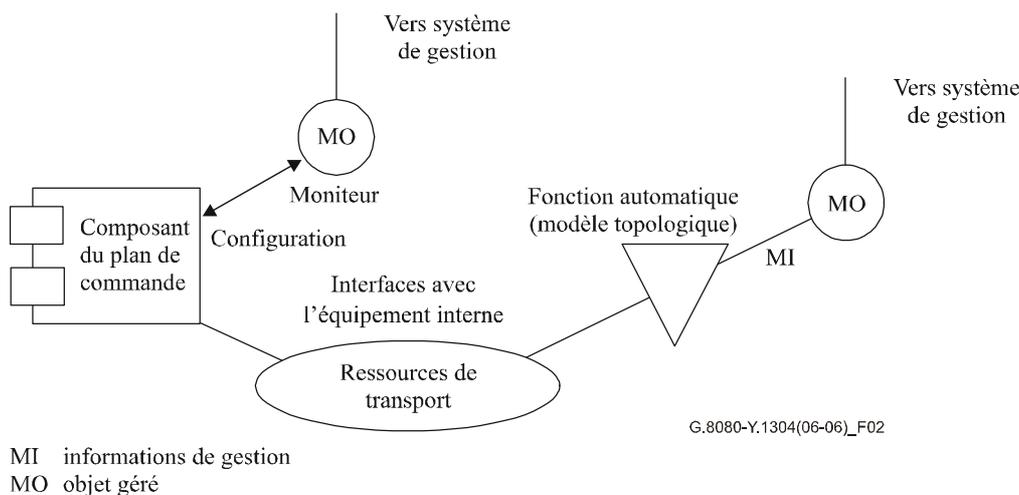


Figure 2/G.8080/Y.1304 – Interactions du plan de gestion/transport avec les ressources de transport

Les ressources physiques de transport, qui représentent la réalité physique de l'équipement, sont décrites 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.

5.2.4 Gestion des ressources

Les ressources du réseau peuvent être réparties entre celles qui sont placées sous l'autorité du plan de gestion et celles qui sont placées sous l'autorité du plan de commande. Celui-ci ne doit pas avoir la possibilité de modifier des ressources qui sont sous l'autorité du plan de gestion, ce qui inclut les ressources de réseau actuellement inutilisées mais réservées pour utilisation future (par exemple, par des planificateurs de réseau). En tant que telle, la gestion des ressources est assurée par le plan de gestion et est hors du domaine d'application de la présente Recommandation.

6 Organisation des ressources de transport

L'architecture fonctionnelle du réseau de transport décrit la manière dont les ressources de transport sont utilisées pour la fourniture des fonctions de transport de base. Toute ressource de transport est représentée, pour les besoins de commande et de gestion, par un agent qui lui est étroitement associé et représente le rôle qu'elle doit jouer. Ces agents interagissent avec d'autres fonctions qui participent à la commande et à la gestion à travers des interfaces et présentent des informations ou effectuent des opérations, en fonction des besoins. Les ressources de transport sont organisées, à des fins de gestion et de commande, sous la forme de zones de routage et de sous-réseaux.

6.1 Entités de transport

Les ressources du plan de transport sous-jacent sont représentées, à des fins de gestion des connexions au sein d'un réseau de couche, par un certain nombre d'entités dans le plan de commande. La Figure 3 illustre la relation entre les ressources de transport (décrites dans la Rec. UIT-T G.805), les entités qui représentent ces ressources à des fins de gestion du réseau (décrites dans la Rec. UIT-T M.3100) et la vue des ressources de transport telle qu'elle est perçue par le plan de commande.

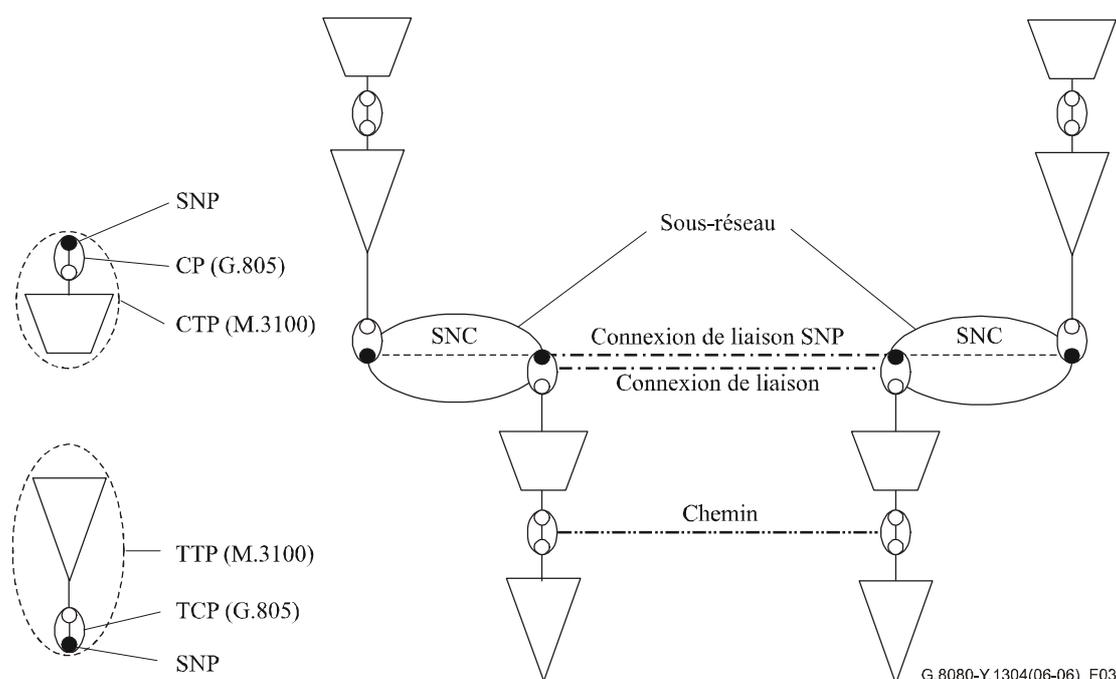


Figure 3/G.8080/Y.1304 – Relation entre les entités d'architecture dans les plans de transport, de gestion et de commande

Un point SNP possède un certain nombre de relations avec d'autres points SNP:

- une relation statique entre deux points SNP situés dans des sous-réseaux différents est appelée connexion de liaison de point SNP;
- une relation dynamique entre deux points de sous-réseau (ou plus dans le cas de connexions de diffusion), situés à la frontière du même sous-réseau est appelée connexion de sous-réseau.

Un point de sous-réseau peut également être regroupé avec d'autres points SNP à des fins de routage. Il s'agit alors d'un pool de points de sous-réseau (SNPP, *subnetwork point pool*) qui est en relation étroite avec les extrémités de liaison (comme défini dans la Rec. UIT-T G.852.2); cette relation est toutefois plus souple que l'extrémité de liaison. Un pool SNPP peut être subdivisé en pools plus petits. Une telle subdivision peut permettre, par exemple, de décrire divers degrés de diversité de routage. A titre d'exemple, tous les points SNP d'un sous-réseau qui ont une relation avec un groupe similaire situé dans un autre sous-réseau peuvent être regroupés dans un pool SNPP unique. Ce dernier peut ensuite être cloisonné pour représenter diverses routes et un cloisonnement supplémentaire, par exemple, des longueurs d'onde individuelles.

L'association entre des pools SNPP situés dans des réseaux différents constitue une liaison de pool SNPP.

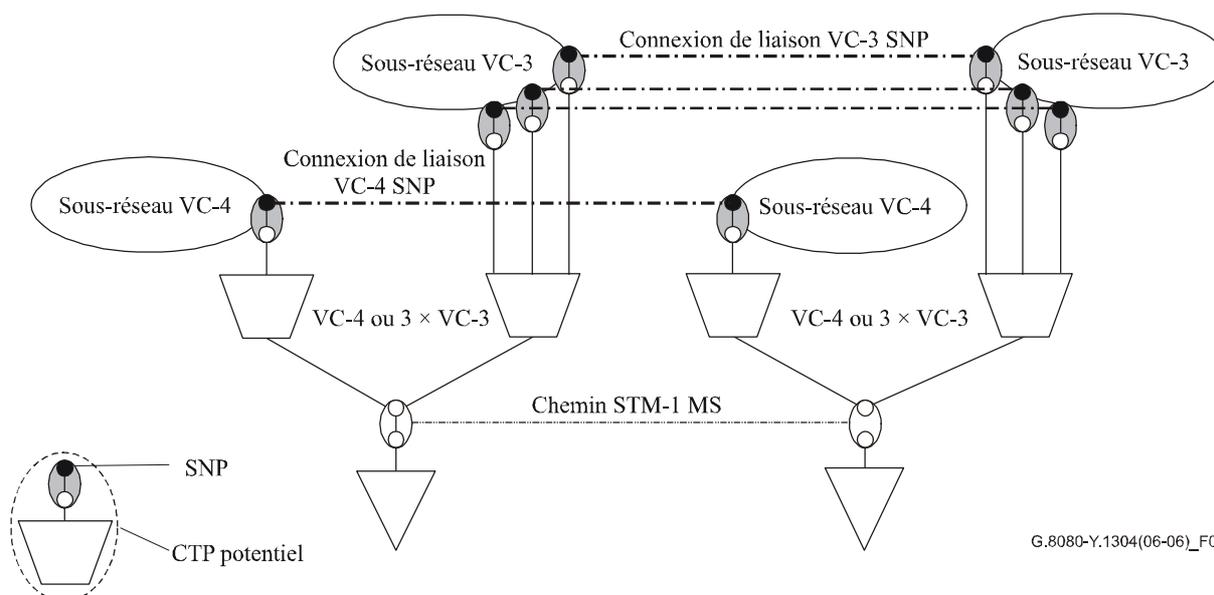
Les états des points SNP et des connexions de liaison entre points SNP qui sont utiles au plan de commande sont décrits respectivement au § 7.3.7 (Exécuteurs de terminaison et d'adaptation) et au § 7.3.3 (Composant "gestionnaire de ressource de liaison").

Fonction d'adaptation variable

Un certain nombre de systèmes de transport mettent en œuvre une adaptation variable, dans laquelle un chemin de couche de serveur unique peut prendre en charge de manière dynamique diverses structures de multiplexage.

On peut modéliser cette situation en associant des points SNP à chaque point CP dans les diverses structures et en plaçant ces points SNP dans leurs sous-réseaux de couche respectifs. Ceci a pour effet, lorsqu'une instance donnée de point SNP est allouée, que le processus spécifique du client adéquat est activé dans la fonction d'adaptation, avec création du point CTP associé. Les points SNP situés dans d'autres réseaux de couche et qui utilisent les mêmes ressources passent dans l'état occupé.

La Figure 4 donne un exemple de chemin STM-1 qui est en mesure de prendre en charge, soit un conteneur VC-4 unique, soit trois conteneurs VC-3.



**Figure 4/G.8080/Y.1304 – Exemple d'adaptation variable
(chemin STM-1 prenant en charge trois conteneurs VC-3 ou un conteneur VC-4)**

Ressources de liaisons partagées entre réseaux VPN

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.

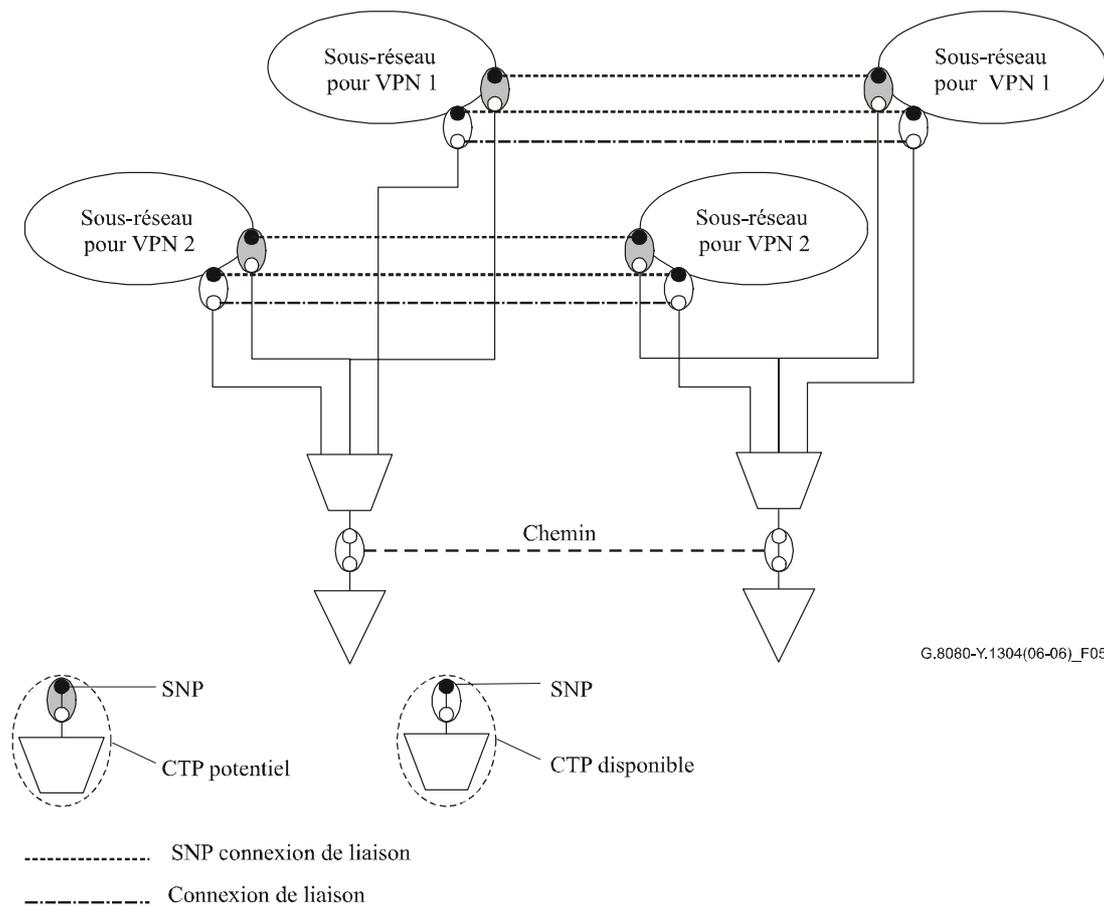


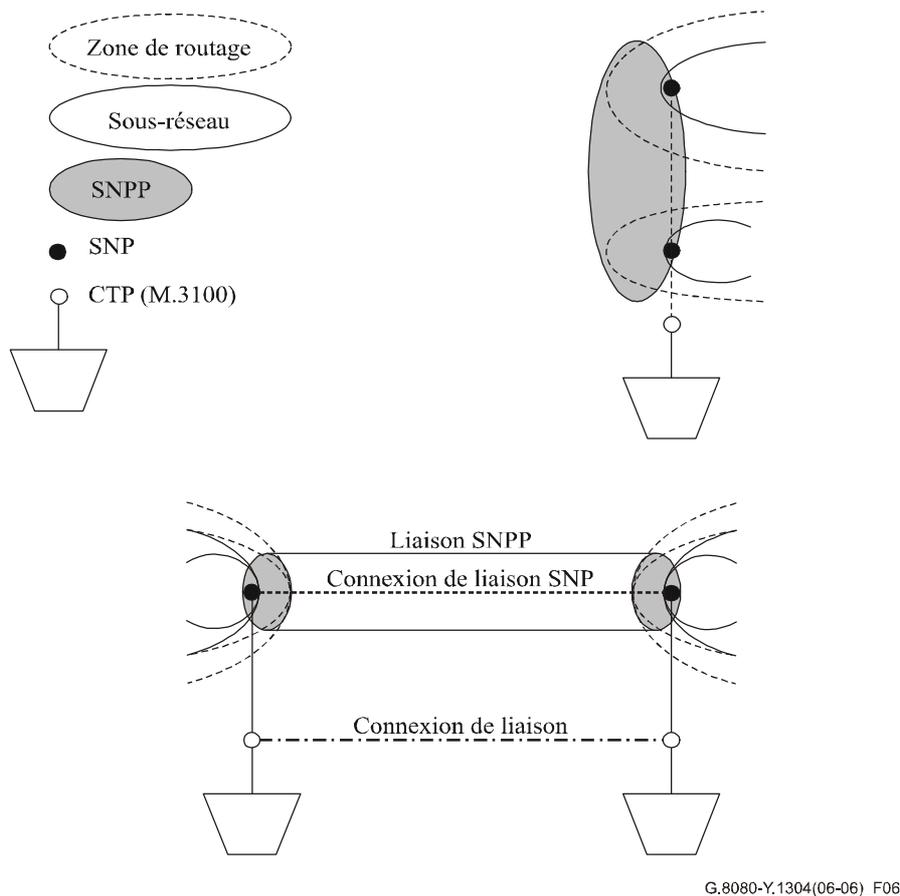
Figure 5/G.8080/Y.1304 – Affectation des ressources de liaisons entre réseaux VPN

6.2 Zones de routage

Une zone de routage est définie, dans le contexte de la présente Recommandation, au sein d'un réseau de couche unique. Elle se constitue d'un ensemble de sous-réseaux, des liaisons SNPP qui les interconnectent et des pools SNPP qui représentent les extrémités des liaisons SNPP présentes dans cette zone de routage. Une zone de routage peut contenir des zones de routage plus petites, interconnectées par des liaisons SNPP. La plus petite subdivision correspond à une zone de routage contenant un sous-réseau.

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.

Lorsqu'une liaison SNPP traverse la frontière d'une zone de routage, toutes les zones de routage qui partagent cette frontière commune contiennent des liaisons SNPP coïncidentes. Ces relations sont illustrées par la Figure 6.



G.8080-Y.1304(06-06)_F06

Figure 6/G.8080/Y.1304 – Relations entre zones de routage, sous-réseaux, points SNP et pools SNPP

6.2.1 Agrégation de liaisons et zones de routage

La Figure 7 illustre les relations entre zones de routage, pools SNPP et 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.

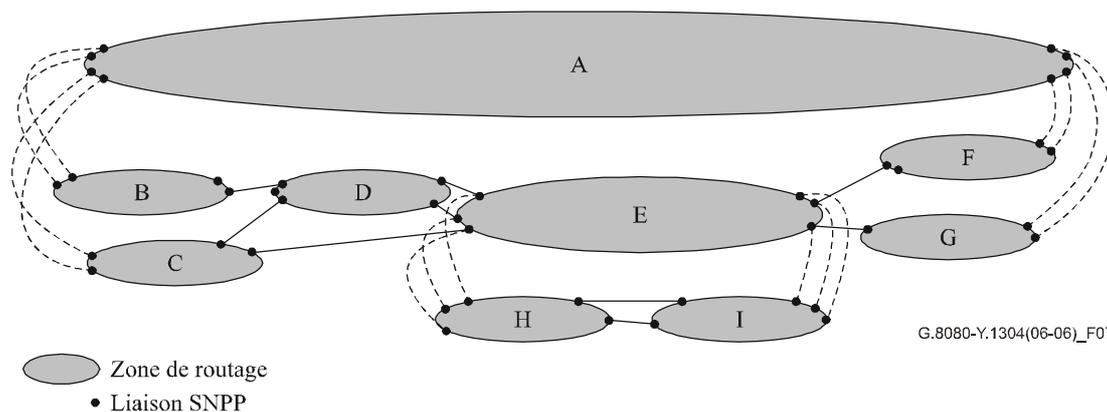


Figure 7/G.8080/Y.1304 – Exemple de hiérarchie de zones de routage et de relations avec les liaisons SNPP

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 à laquelle il appartient.

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.

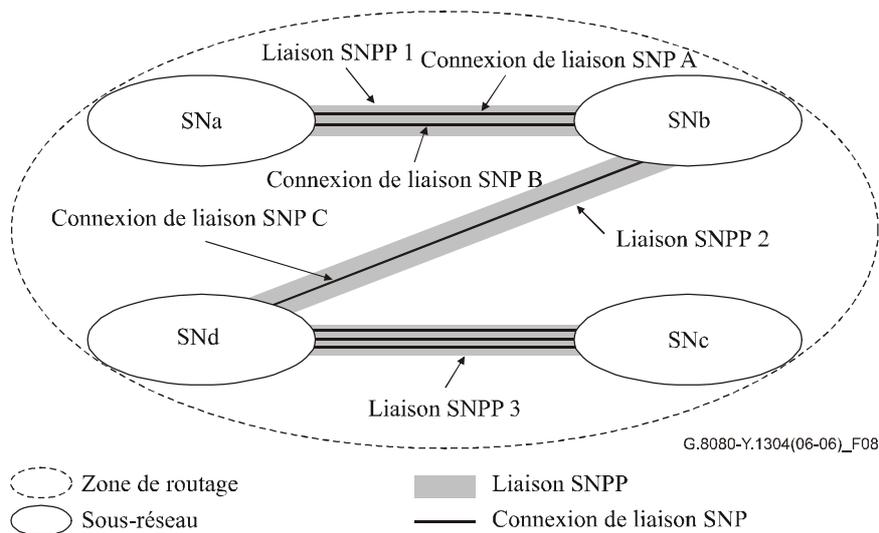


Figure 8/G.8080/Y.1304 – Relation entre liaisons SNPP et sous-réseaux

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).

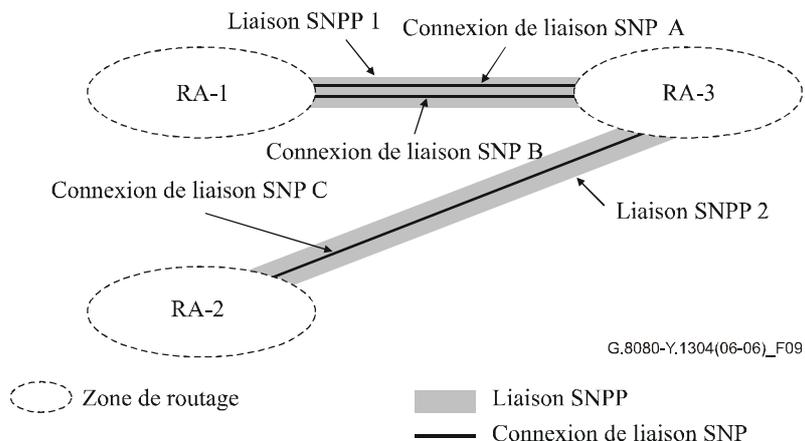


Figure 9/G.8080/Y.1304 – Relations entre liaisons SNPP et zones de routage

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.

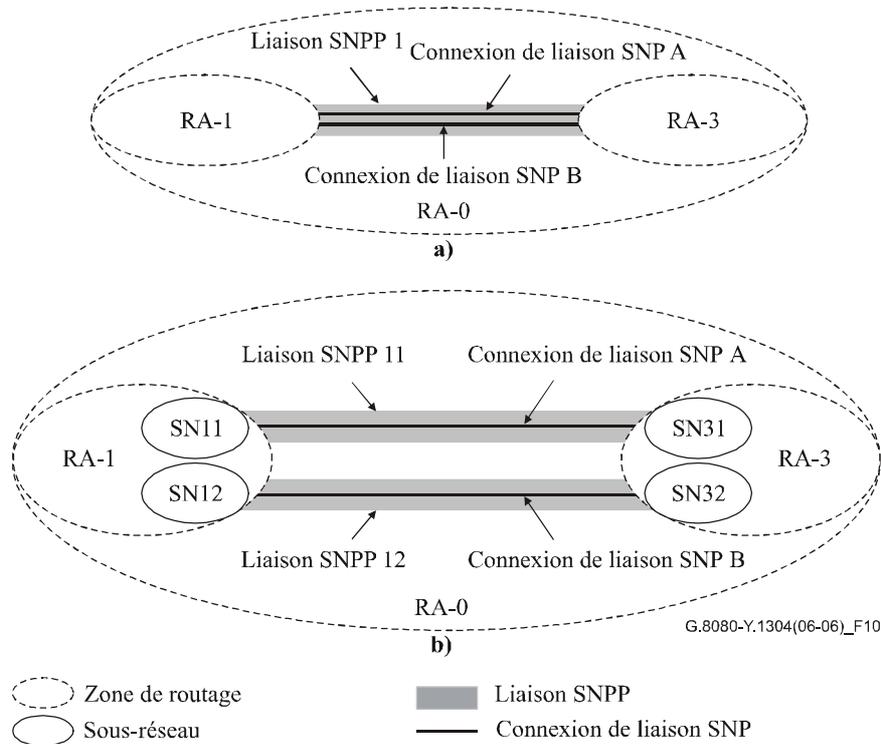


Figure 10/G.8080/Y.1304 – Domaine de validité du routage

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.

6.3 Topologie et découverte

La fonction de routage traite la topologie sous la forme de liaisons SNPP. Avant qu'une telle liaison puisse être créée, il est nécessaire de connaître la topologie de transport sous-jacente, c'est-à-dire les relations de connexion de liaison entre points de connexion (CP, *connection point*) doivent être établies. Ces relations peuvent être découvertes (ou confirmées par rapport à un plan du réseau) en utilisant un certain nombre de mécanismes, par exemple en utilisant un signal d'essai ou en exploitant une trace de chemin dans la couche serveur. Elles peuvent également être fournies par un système de gestion sur la base d'un plan du réseau. Il est également possible de découvrir ou de rendre compte de la capacité de l'équipement de transport en ce qui concerne des fonctions d'adaptation souples (et, de ce fait des connexions de liaison pour des réseaux de couche clients multiples).

Les connexions de liaison qui sont équivalentes du point de vue du routage sont regroupées en liaisons. Ce regroupement se fait sur la base de paramètres tels que le coût de la liaison, la qualité ou la diversité. Certains de ces paramètres peuvent être obtenus à partir de la couche serveur, mais ils seront fournis en général par le plan de gestion.

Il est possible de créer des liaisons distinctes (c'est-à-dire que des connexions de liaison équivalentes du point de vue du routage peuvent être placées dans des liaisons différentes) pour permettre la répartition des ressources entre plusieurs réseaux ASON (par exemple, entre divers réseaux VPN) ou entre des ressources gérées, soit par le réseau ASON, soit par le plan de gestion.

Les informations de liaison (par exemple, les connexions de liaison constitutives et les noms des paires de points de connexion) sont utilisées ensuite pour configurer les instances du gestionnaire LRM (comme décrit dans le § 7.3.3) associées à la liaison SNPP. D'autres caractéristiques de la liaison peuvent également être fournies sur la base de paramètres des connexions de liaison. Les gestionnaires LRM de chaque extrémité de la liaison doivent établir, dans le plan de commande, une relation d'adjacence qui correspond à la liaison SNPP. Les identificateurs d'interface SNPP peuvent être négociés pendant la phase de découverte de l'adjacence ou être fournis dans le cadre de la configuration LRM. Les connexions de liaison et les noms de point de connexion sont ensuite mappés avec les identificateurs de point SNP (et les noms de connexion de liaison SNP). Lorsque les deux extrémités de la liaison appartiennent à une même zone de routage, il se peut que les identificateurs locaux et d'interface SNPP ainsi que les identificateurs locaux et d'interface SNP soient identiques. Dans le cas contraire, l'identificateur d'interface SNPP est mappé avec un identificateur SNPP local et les identificateurs d'interface SNP sont mappés avec des identificateurs SNP locaux aux deux extrémités de la liaison. Ces relations sont représentées par la Figure 11.

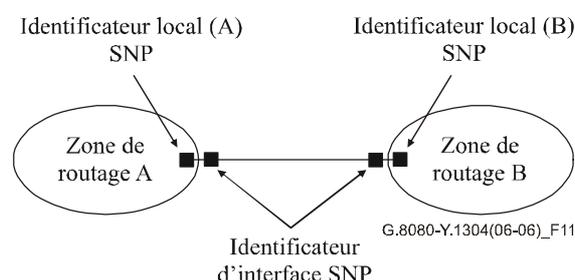


Figure 11/G.8080/Y.1304 – Relation entre les identificateurs locaux et d'interface

Les connexions de liaison SNP résultantes peuvent être validées ensuite par un processus de découverte. L'ampleur de la validation nécessaire à cet instant dépend de l'intégrité des relations de connexion de liaison fournies au départ par le plan de transport ou le plan de gestion ainsi que de l'intégrité du processus utilisé pour le mappage des points de connexion avec les points SNP.

La validation peut être obtenue à partir d'une trace de chemin dans la couche serveur ou en utilisant un signal et des connexions d'essais. Le processus de découverte peut établir et libérer ces connexions en utilisant le plan de gestion ou le plan de commande si on utilise des connexions d'essais. Si on utilise le plan de commande, la liaison doit être fournie temporairement pour le routage et la commande de connexion, mais uniquement pour les connexions d'essai.

Une fois que la liaison SNPP est établie, les gestionnaires LRM fournissent au composant RC (se référer au § 7.3.2) les informations d'adjacence de la liaison SNPP ainsi que les caractéristiques de la liaison, par exemple le coût, les performances, la qualité et la diversité.

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.

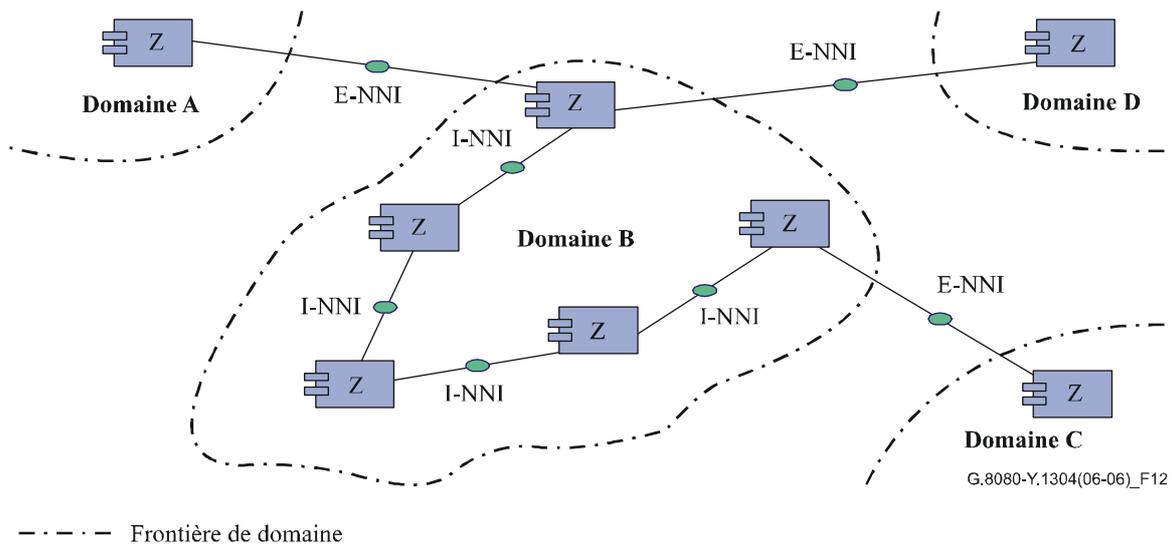


Figure 12/G.8080/Y.1304 – Relation entre domaines, contrôleurs de protocole et points de référence

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.

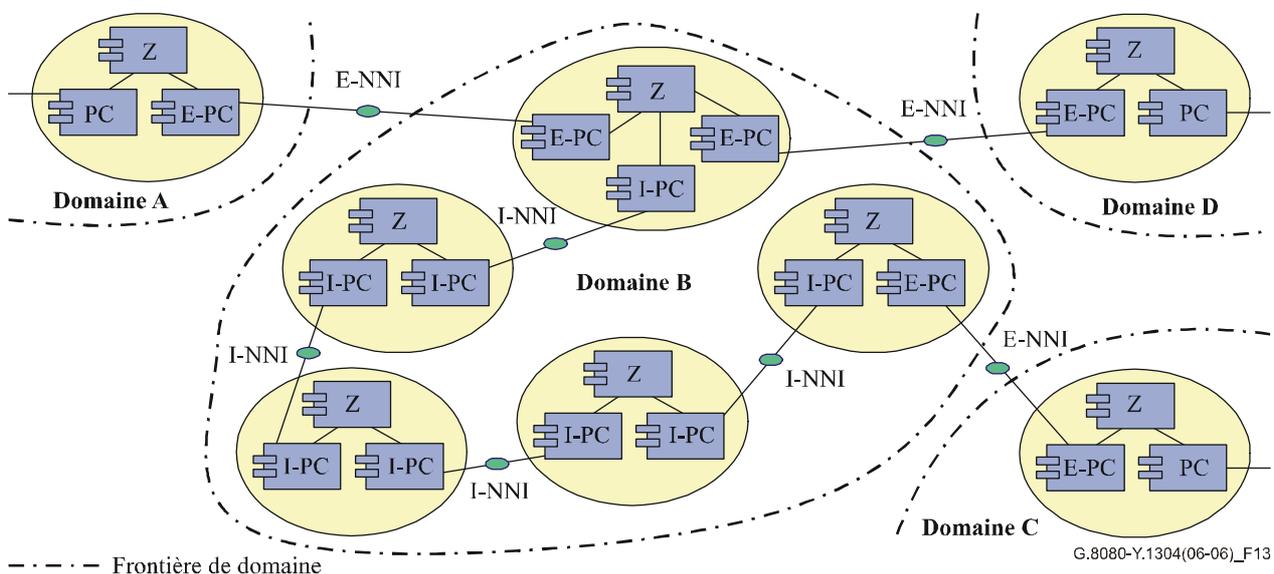


Figure 13/G.8080/Y.1304 – Relation entre domaines, contrôleurs de protocole et interfaces

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.

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 entre les réseaux de couche client et serveur est gérée au moyen des exécuteurs de terminaison et d'adaptation (voir § 7.3.7). La topologie et la connexité de la couche serveur sous-jacente ne sont pas immédiatement visibles par la couche client. Au contraire, certains aspects de la couche serveur sont encapsulés et présentés au réseau de couche client. La couche serveur peut être représentée sous la forme d'une liaison SNPP de couche client, ou de sous-réseaux de couche client interconnectés par des liaisons SNPP. Cette abstraction de la technologie de la couche serveur aux fins du calcul du trajet dans la couche client a des propriétés analogues aux relations hiérarchiques de contenance décrites dans le § 6.2.1. Ainsi, les résultats du calcul du trajet dans la couche client peuvent ne pas déboucher sur une utilisation optimale des ressources de la couche supérieure. Si les ressources mises à la disposition du réseau de couche client sont insuffisantes pour prendre en charge une demande de connexion, des ressources additionnelles peuvent être offertes en activant ou en créant de nouvelles connexions dans un ou plusieurs réseaux de couche serveur. Les politiques des opérateurs régiront la mise à disposition des ressources de la couche serveur sous-jacente à la couche client.

Lorsque la couche serveur est représentée pour la couche client sous la forme d'une liaison SNPP, cette mise à disposition peut être réalisée par modification de points SNP en les faisant passer de l'état potentiel à l'état disponible. Si la couche serveur est représentée sous la forme d'un ensemble de liaisons et de sous-réseaux SNPP, une nouvelle connexion de couche serveur doit alors être demandée directement par le plan de commande en fonction des politiques des opérateurs. Dans le cas où la capacité de la connexion de réseau de couche serveur ainsi obtenue est supérieure à la capacité requise pour prendre en charge la connexion de couche client, cette opération aura pour effet secondaire de créer une nouvelle liaison SNPP. Le mécanisme permettant d'ajouter cette nouvelle liaison SNPP à la topologie de la couche client n'est pas abordé dans la présente Recommandation.

Il peut aussi arriver que la topologie de la couche serveur ne soit pas visible par la couche client. Dans ce cas, la décision d'ajouter de nouvelles connexions de réseau de couche serveur peut être prise dans le cadre d'un processus de planification. Le recours à un système de planification pour invoquer la configuration du réseau de couche serveur afin de fournir des ressources additionnelles au réseau de couche client peut se traduire par une utilisation plus optimale des ressources de couche serveur. Les détails du processus de planification et l'interaction de celui-ci avec les plans de commande client et serveur ne sont pas abordés dans la présente Recommandation. La décision de créer/supprimer les connexions de couche serveur est une décision commerciale qui peut rendre compte de la politique des opérateurs.

Comme indiqué plus haut, il existe deux manières différentes de représenter les ressources de couche serveur dans la couche client. La représentation utilisée dépend de si les ressources de couche serveur ont déjà été sélectionnées pour assurer la connectivité de la couche client. Une instance de plan de commande pour un réseau de couche peut utiliser une de ces méthodes, ou les deux en même temps. Les autres représentations des ressources de couche serveur sont à étudier.

6.5.1 Représentation sous forme de connexions de liaison SNP

Un processus de planification peut avoir pour effet de connecter deux points d'accès dans la couche serveur, ce qui créera une liaison SNPP de couche client contenant de multiples connexions de liaison SNP pour les couches client prises en charge. Il pourrait s'agir, au départ, de connexions de liaison SNP actives ou en puissance, étant donné que la ressource sous-jacente pourra ou non être attribuée à l'usage exclusif de la couche client (voir le § 6.1).

Ce processus peut être appliqué récursivement dans de multiples réseaux de couche client/serveur. La connexion entre les deux points d'accès peut ainsi être prise en charge par des connexions de liaison potentielles. La connexion des points d'accès dans la couche serveur n'est pas activée avant qu'une demande d'utilisation d'une des connexions de liaison SNP de couche client potentielles soit reçue par le plan de commande. A cet instant, la demande de la couche client est "suspendue" le temps que les connexions de la couche serveur soient établies. Une fois que les connexions de la couche serveur sont en place, les connexions de liaison SNP de couche client sont activées, ce qui autorise la reprise de la signalisation de la couche client. Si une connexion dans la couche serveur ne peut pas être établie, les connexions de liaison SNP de couche client ne peuvent pas être activées, ce qui provoque l'échec de la tentative de connexion de couche client faute de ressources.

Lorsqu'une connexion de liaison SNP est supprimée, les ressources sous-jacentes qui prenaient en charge la connexion sont libérées, ce qui leur permet de revenir à l'état potentiel si la politique autorise cette opération. Lorsque toutes les connexions de liaison SNP prises en charge par un chemin de serveur repassent à l'état potentiel, le chemin de serveur peut être modifié pour passer à cet état si la politique autorise cette opération.

Il convient de noter que la liaison SNPP contenant ces connexions de liaison SNP peut être représentée au moyen des composants et états existants décrits dans le § 6.1.

6.5.2 Représentation sous forme d'un ensemble de liaisons et de sous-réseaux SNPP

Un processus de planification peut en outre laisser au plan de commande de couche client plus de latitude dans le choix des ressources de couche serveur pour satisfaire à une demande de connexion. A cet effet, certaines des ressources de couche serveur sont représentées à la couche client sous forme de liaisons et de sous-réseaux SNPP avec les composants du plan de commande de couche client appropriés. Cette représentation est possible si la couche serveur offre une souplesse suffisante pour permettre l'interconnexion des sous-réseaux de couche client. La souplesse de la couche serveur et la souplesse correspondante de la couche client sont représentées dans la Figure 14. Cela permet au contrôleur de routage de savoir qu'un ensemble de points SNP de couche client sont accessibles via une couche serveur commune. En d'autres termes, dans la Figure 14, l'absence de la représentation de la couche serveur ne permettra pas de calculer les trajets entre tous les points SNPP de la couche client.

Les fonctions d'adaptation et de terminaison utilisées pour passer de la couche client à la couche serveur sont représentées sous forme de liaisons SNPP dans la couche client. Dans cette figure, nous avons utilisé des éléments en pointillés pour distinguer cette représentation des ressources de la couche serveur vers la couche client des autres ressources de la couche client. En outre, les points SNP des couches client et serveur sont respectivement représentés sous forme de points noirs et de points blancs (petits cercles évidés). Toutefois, pour le contrôleur du routage de la couche client, il n'y a aucune distinction entre ces éléments représentés et les autres éléments de la couche client.

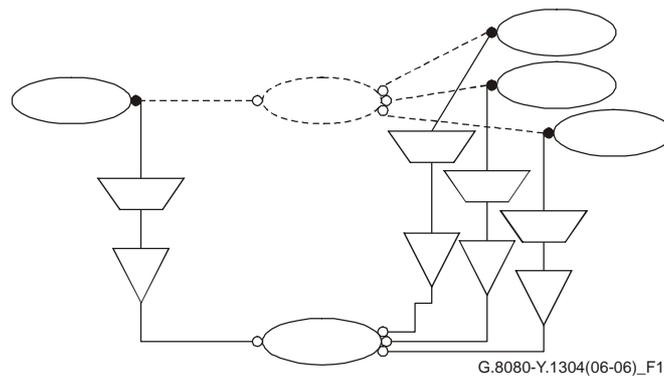


Figure 14/G.8080/Y.1304 – Relation entre éléments architecturaux client et serveur

Comme dans le cas de la représentation de liaison SNPP, les connexions de liaison SNP qui raccordent le sous-réseau de couche client à la couche serveur sont potentielles, du fait que les ressources de la couche serveur n'ont pas été attribuées à l'usage exclusif de la couche client. A la réception d'une demande de connexion qui utilise une ressource potentielle, on calcule un trajet traversant la couche serveur et identifiant les ressources concrètes à utiliser. L'identification de ces ressources permet de créer des connexions de liaison SNP de couche client et de poursuivre le traitement comme indiqué ci-dessus.

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 de transport multicouche, un élément de réseau peut prendre en charge des réseaux de couche client qui sont directement pris en charge au centre d'un réseau de transport multicouche. Par exemple, l'élément de réseau périphérique peut prendre en charge l'adaptation du service dans un conteneur virtuel (VC, *virtual container*) d'ordre inférieur, alors que les éléments de réseau centraux peuvent n'offrir la souplesse voulue que dans la couche VC d'ordre inférieur; ou, l'élément de réseau périphérique peut adapter un service Ethernet dans des VC d'ordre supérieur. 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. Soit une topologie de couche client peut être créée à partir des connexions de couche serveur comme indiqué dans le § 6.5, soit 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 d'appel réseau (NCC, voir le § 7.3.5.1) 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.

La relation entre contrôleurs NCC intercouches peut apparaître en des points autres que celui où les conteneurs de groupe d'accès sont reliés au réseau de couche client. Dans la Figure 14, un appel traverse d'abord un sous-réseau client avant d'être pris en charge par un sous-réseau de couche serveur. Dans la Figure 15, l'appel peut aussi être pris en charge par des connexions dans un sous-réseau de couche client qui n'est pas contigu aux sous-réseaux de couche client à l'entrée ou à la sortie. Dans le cas considéré ici, les relations entre les contrôleurs NCC intercouches apparaissent entre le sous-réseau client C2 et les sous-réseaux serveurs S1 et S2.

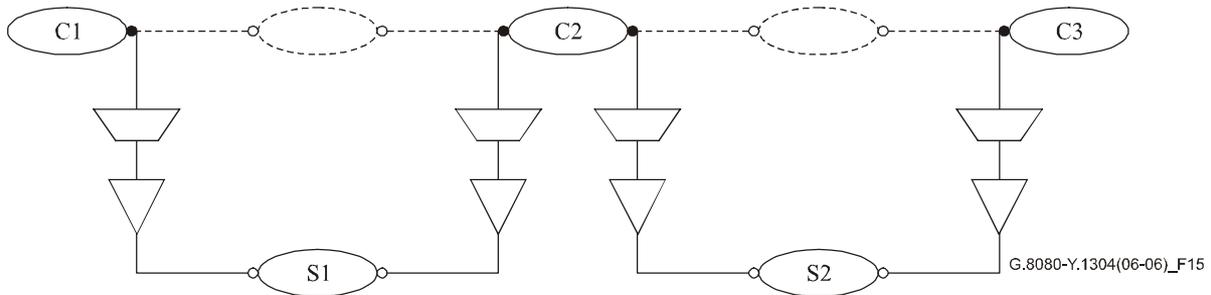


Figure 15/G.8080/Y.1304 – Sous-réseaux de couche client non contigus

6.7 Appels pris en charge par des appels dans la même couche

Comme dans le cas du montage des contrôleurs NCC dans une relation entre couches, un segment d'appel peut être pris en charge par un appel distinct dans la même couche, mais pas sur une interface E-NNI. Dans ce montage, un segment d'appel de contrôleur NCC à contrôleur NCC est pris en charge par un appel complet avec des contrôleurs d'appel appelants/appelés. La Figure 16 illustre cette situation dans le cas d'un scénario d'entreprise entre opérateurs de télécommunications. Dans le cas considéré ici, un appel entre deux clients associés à l'opérateur de télécommunications A est pris en charge dans deux sous-réseaux appartenant à l'opérateur de télécommunications A. Entre ces deux sous-réseaux, l'appel est pris en charge par une connexion SPC distincte interne à l'opérateur de télécommunications B. La connexion retournée par l'opérateur de télécommunications B est associée aux connexions établies dans les sous-réseaux de l'opérateur de télécommunications A.

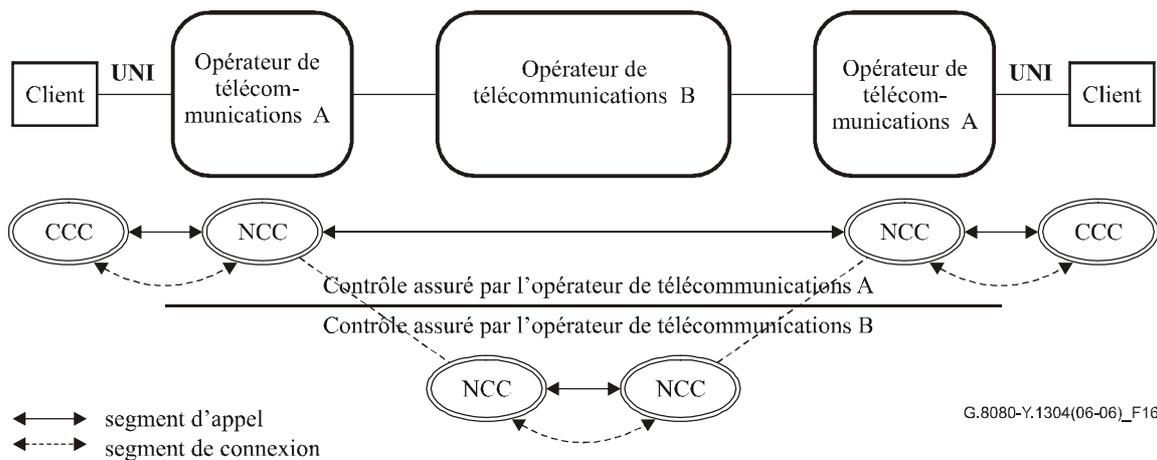


Figure 16/G.8080/Y.1304 – Appels pris en charge par des appels dans la même couche

7 Architecture du plan de commande

Le présent paragraphe décrit une architecture de référence pour le plan de commande prenant en charge les prescriptions de la présente Recommandation; il identifie les composants fonctionnels fondamentaux et leur mode d'interaction. La souplesse de l'architecture de référence est conçue pour permettre aux opérateurs de prendre en charge leurs activités internes et leurs procédures de gestion, ainsi que de facturer l'utilisation des services. Les caractéristiques de l'architecture fonctionnelle sont les suivantes:

- prise en charge de diverses infrastructures de transport, telles que le réseau de transport SONET/SDH, tel qu'il est défini dans la Rec. UIT-T G.803 et le réseau optique de transport (OTN, *optical transport network*), tel qu'il est défini dans la Rec. UIT-T G.872;
- utilisable quel que soit le choix particulier du protocole de commande (c'est-à-dire, l'utilisation d'une démarche neutre par rapport au protocole, indépendante de l'utilisation de protocoles de commande de connexion particuliers);
- utilisable quel que soit le mode de cloisonnement du plan de commande en domaines et zones de routage et des ressources de transport en sous-réseaux;
- utilisable quelle que soit l'implémentation de la commande de connexion, qui peut aller d'une répartition totale à une architecture de commande centralisée.

Cette architecture de référence décrit les points suivants:

- composants fonctionnels du plan de commande, y compris les interfaces abstraites et les primitives;
- interactions entre les composants du contrôleur d'appel;
- interactions entre les composants pendant l'établissement de la connexion;
- composants fonctionnels qui transforment les interfaces du composant abstrait en protocoles sur des interfaces externes.

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 37. 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 18.

7.1 Notation

Le présent paragraphe précise la notation utilisée pour l'architecture de composants; il se base sur un certain nombre de blocs de construction simples, définis par le langage de modélisation unifié (UML, *unified modelling language*).

Interface: une interface prend en charge un ensemble d'opérations qui spécifient le service d'un composant; cette spécification est indépendante des composants qui utilisent ou fournissent ce service. Les opérations spécifient les informations transmises dans les deux sens et l'ensemble des

contraintes qui s'appliquent. Les définitions d'interface se présentent sous la forme de tableaux, dont un exemple est fourni par le Tableau 1. Toute interface possède un nom d'interface qui indique le rôle. Les interfaces en entrée représentent des services fournis par le composant, les paramètres d'entrée de base sont nécessaires pour le rôle spécifique et les paramètres de retour de base (éventuels) contiennent les résultats de l'action faite sur les paramètres d'entrée. Les interfaces de sortie représentent des services utilisés par le composant; les paramètres de sortie de base définissent les informations fournies et les paramètres de retour de base (éventuels) sont ceux qui sont nécessaires en réponse aux paramètres de sortie. Les interfaces de notification représentent des actions de sortie non sollicitées par le composant et sont indiquées par une interface de sortie sans paramètres de retour. Ces trois types d'interface sont décrits de manière distincte dans des spécifications d'interface.

Tableau 1/G.8080/Y.1304 – Format de tableau de description d'interface générique

| Interface d'entrée | Paramètres d'entrée de base | Paramètres de retour de base |
|--------------------|-----------------------------|------------------------------|
| Nom d'interface | Paramètres d'entrée | Paramètres retournés |

| Interface de sortie | Paramètres de sortie de base | Paramètres de retour de base |
|---------------------|------------------------------|------------------------------|
| Nom d'interface | Paramètres de sortie | Paramètres retournés |

On suppose que la sémantique associée à une transaction particulière est traitée de manière transparente et qu'il n'est pas nécessaire de mentionner explicitement à cet effet des paramètres particuliers dans la description d'interface.

Rôle: un rôle définit le comportement d'une entité lorsqu'elle participe à un contexte particulier. Les rôles permettent la participation d'entités diverses à des instants différents; ils sont indiqués en annotant une relation avec le nom d'une interface.

Composant: les composants sont utilisés dans la présente Recommandation pour représenter des entités abstraites et non des instances de code d'implémentation. Ils sont utilisés pour construire des scénarios qui expliquent le fonctionnement d'une architecture. Un composant est représenté sous la forme d'un rectangle avec des onglets, comme représenté par la Figure 17.

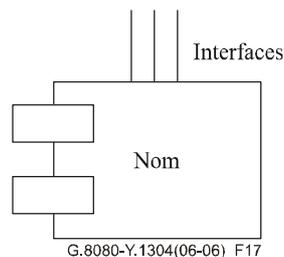


Figure 17/G.8080/Y.1304 – Représentation d'un composant

Tout composant possède, d'une manière générale, un ensemble d'interfaces spéciales qui permettent la supervision de son fonctionnement, le positionnement dynamique des politiques et l'affectation d'un comportement interne. Ces interfaces ne sont pas obligatoires, elles sont fournies si nécessaire pour un composant particulier. Lorsqu'elle s'applique, l'utilisation de l'interface de supervision est précisée dans les descriptions de composant individuel. On ne suppose aucune répartition statique des composants.

On spécifie uniquement les divers types d'interface dans la description éventuelle des interfaces de composants. Tout composant peut prendre en charge simultanément des appelants et des

fournisseurs multiples et le traitement de demandes simultanées n'est pas mentionné de manière explicite.

Les composants sont utilisés d'une manière abstraite, ce qui permet d'étendre cette spécification par des techniques de composition et de sous-classes de composant.

7.2 Politique et fédérations

7.2.1 Modèle général de politique

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.

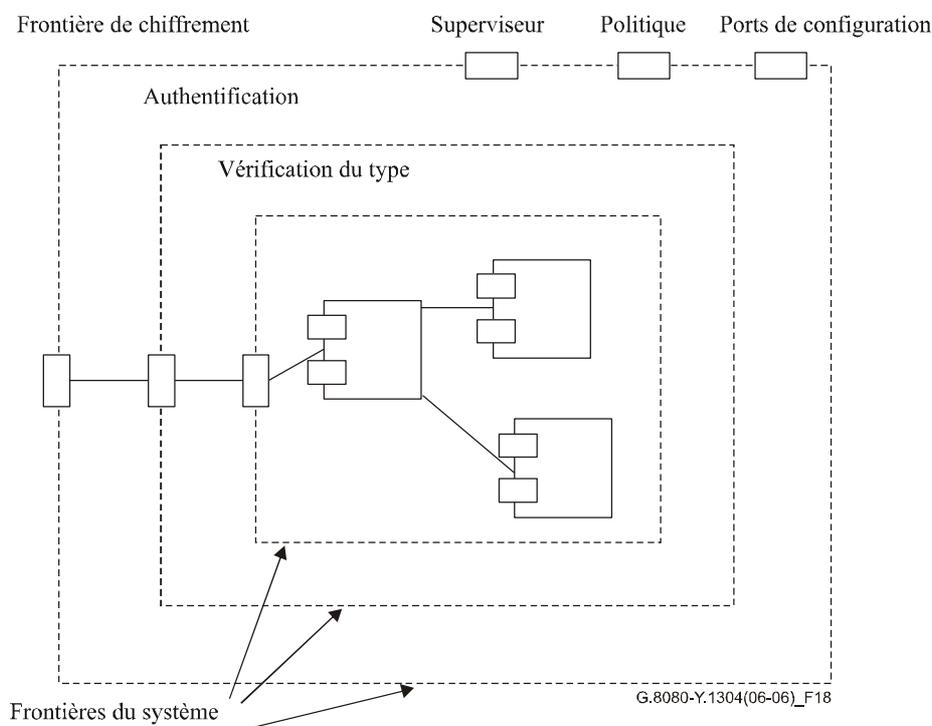


Figure 18/G.8080/Y.1304 – Exemple de frontières de système liées à la gestion de la politique

Dans la Figure 18, les boîtes en trait pointillé représentent des frontières de système et les rectangles en trait plein sur la frontière, appelés ports, représentent des composants "contrôleur de port".

Le superviseur, la politique et les ports de configuration peuvent être disponibles sur tout système (et composant) sans autre spécification de l'architecture. Le port superviseur permet de transférer à travers la frontière des informations de gestion relative à des dégradations des performances, des événements perturbateurs, des défaillances, etc. concernant des composants soumis à des contraintes de la politique. Le port de politique permet la modification des informations de politique relatives aux composants. Le port de configuration permet l'échange d'informations de

configuration, de fourniture et d'administration relatives aux composants (soumis à des contraintes de la politique) afin d'ajuster de manière dynamique le comportement interne du système.

La Figure 18 présente un exemple d'implémentation du chiffrement, de l'authentification et de la vérification du type sous la forme de trois contrôleurs de port imbriqués, dans lequel l'application de la politique correspond à l'ordre des imbrications. Les composants se trouvant à l'intérieur de la frontière d'authentification ne spécifient aucune prescription de chiffrement ou d'authentification car ces dernières sont des propriétés de leur environnement. Des contrôleurs de port sont définis pour chaque aspect indépendant de la politique de port et une politique combinée résulte de la composition des contrôleurs de port. Ceci permet la création de composants réutilisables individualisés par un préfixe descriptif. Les violations de politique font l'objet d'un compte rendu par le biais du port de supervision.

On peut considérer le port de politique comme un filtre qui agit sur les messages entrants et rejette ceux qui ne respectent pas la politique. Il est possible de modifier les politiques de manière dynamique par le biais du port de politique du système et, de ce fait, de décrire des modifications dynamiques du comportement.

Il est d'usage de présenter le mode d'application d'une politique au niveau d'un point de référence, mais cette politique s'applique exclusivement aux interfaces individuelles qui traversent le point de référence. Le paragraphe traitant plus loin des contrôleurs de port décrit une méthode qui permet de combiner plusieurs interfaces sous la forme d'une interface d'implémentation unique.

D'autres caractéristiques de la politique en relation avec le comportement variable des composants (tel que les ordonnancements, les droits d'accès, etc.) sont spécifiées et implémentées par les composants. Il est également possible de modifier de manière dynamique le comportement d'un composant, cette capacité pouvant être gérée par la politique. Ceci permet de déterminer quelles sont les caractéristiques du comportement système qui sont spécifiées en un endroit donné.

Il est possible de répartir la politique de la même manière que d'autres caractéristiques du système. Le modèle de protocole COPS défini par le document RFC 2753 est un exemple de modèle de répartition adéquat. Le point d'exécution de la politique (PEP, *policy enforcement point*) de ce modèle, point au niveau duquel sont mises en application les décisions de la politique, correspond au port du présent modèle. Le point de décision de la politique (PDP, *policy decision point*) est le point au niveau duquel sont prises les décisions de la politique. Ceci peut être fait au sein du port, mais peut également résulter d'une répartition au niveau d'un autre système. La décision de répartition dépend d'un grand nombre de facteurs qui dépendent eux-mêmes de la politique réelle. Des motifs liés aux performances peuvent, par exemple, imposer la délocalisation du point PDP (examen du mot de passe).

Une coopération est nécessaire lorsque les points PEP et PDP ne sont pas situés à un même emplacement.

7.2.2 Modèle général de fédération

La création, la maintenance et la suppression de connexions à travers des domaines est une fonctionnalité indispensable fournie par une coopération entre des contrôleurs appartenant à des domaines différents. Une fédération est considérée, dans le cadre de la présente Recommandation, comme une communauté de domaines qui coopèrent à des fins de gestion de connexion; elle est illustrée par l'utilisation de la coopération entre contrôleurs de connexion (ces derniers sont décrits dans le § 7.3.1).

Il existe deux types de fédération correspondants aux modèles suivants:

- modèle de fédération joint;
- modèle coopératif.

Dans le cas de fédération jointe, un contrôleur de connexion parent exerce une autorité sur des contrôleurs de connexion résidant dans divers domaines. Le contrôleur de connexion de niveau le plus élevé (parent) agit comme coordinateur lorsqu'une demande de connexion implique la traversée de plusieurs domaines. Ce coordinateur a connaissance des contrôleurs de connexion de niveau le plus élevé dans chaque domaine. Le contrôleur de connexion parent répartit la responsabilité pour la connexion réseau entre les contrôleurs de connexion du niveau suivant, chacun de ces derniers étant responsable de sa partie de la connexion. La Figure 19 donne une illustration de cette répartition. Ce modèle est récursif, un contrôleur de connexion parent d'un niveau pouvant être le fils d'un contrôleur d'un niveau plus élevé.

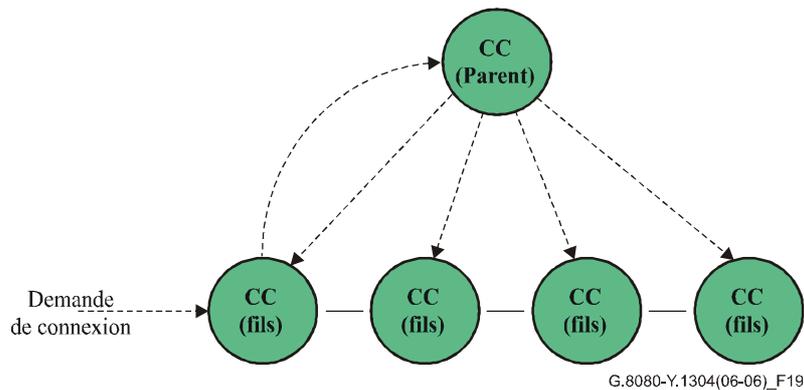


Figure 19/G.8080/Y.1304 – Modèle de fédération joint

Le modèle coopératif n'utilise pas le concept de contrôleur de connexion parent. Lorsqu'une demande de connexion est faite par le contrôleur de connexion d'origine, ce dernier contacte à son initiative chacun des contrôleurs de connexion associés à des domaines, sans intervention d'une coordination d'ensemble. Dans le modèle le plus simple, le contrôleur de connexion d'origine contacte à cet effet le contrôleur de connexion suivant dans la chaîne. La Figure 20 donne une illustration de ce processus, dans lequel chaque contrôleur de connexion détermine quelle est la portion de connexion qu'il peut établir et quel sera le contrôleur de connexion suivant. Le processus se poursuit jusqu'à la fourniture de la connexion complète.

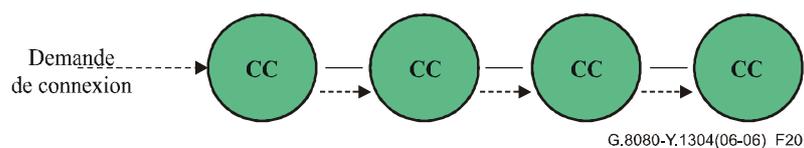


Figure 20/G.8080/Y.1304 – Modèle de fédération coopératif

La fédération entre domaines administratifs se fait au moyen du modèle coopératif. Ce cas prévoit que tous les domaines administratifs disposent de la capacité d'établir une fédération avec d'autres domaines administratifs. Les contrôleurs de connexion parents au sein d'un domaine administratif peuvent se fédérer avec des contrôleurs de connexion parents d'autres domaines administratifs en utilisant le modèle coopératif. Un domaine administratif peut également être cloisonné et le choix du modèle de fédération utilisé entre les domaines au sein d'un domaine administratif peut différer de celui qui est fait pour un autre domaine administratif. Il est possible, de ce fait, de combiner les deux modèles de fédération pour édifier de vastes réseaux, tels que celui illustré par la Figure 21. Les principes décrits ci-dessus peuvent également s'appliquer à des fédérations de contrôleurs d'appel.

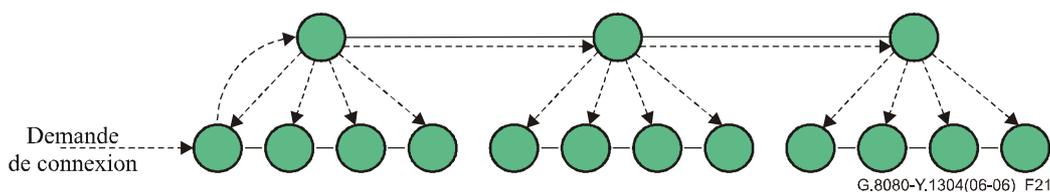


Figure 21/G.8080/Y.1304 – Modèle de fédération combiné

7.3 Composants de l'architecture

Le présent paragraphe décrit les composants de l'architecture du plan de commande. Ces composants peuvent être combinés de diverses manières selon la fonctionnalité nécessaire. L'Appendice V donne des exemples d'interactions des composants à utiliser pour l'établissement des connexions. Chaque composant fait l'objet d'une brève description concernant sa fonction principale au sein de cette architecture de référence. Les interfaces de composant sont fournies ensuite et une description plus détaillée est faite pour les opérations.

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.

7.3.1 Composant "contrôleur de connexion" (CC)

Le contrôleur de connexion est responsable de la coordination entre le gestionnaire de ressource de liaison, le contrôleur de routage et les contrôleurs de connexion homologues ou subordonnés, à des fins de gestion et de supervision de l'établissement et de la suppression des connexions; il est également responsable de la modification des paramètres des connexions existantes. Ce composant est au service d'un sous-réseau unique et fournit les interfaces avec d'autres composants du plan de commande indiqués par le Tableau 2. La Figure 22 décrit le composant "contrôleur de connexion".

NOTE – L'interface de demande d'itinéraire n'est pas applicable dans le cas de l'interface de contrôleur de connexion au point de référence UNI.

Le composant CC fournit en outre une interface de contrôleur de connexion (CCI, *connection controller interface*) située entre un sous-réseau du plan de transport et le plan de commande. Il est utilisé par les composants de commande pour diriger la création, la modification et la suppression de connexions SNC. La politique ne s'applique pas au niveau de l'interface CCI.

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 état de topologie distante | Informations de topologie (liaison et/ou sous-réseau) y compris la disponibilité des ressources | – |

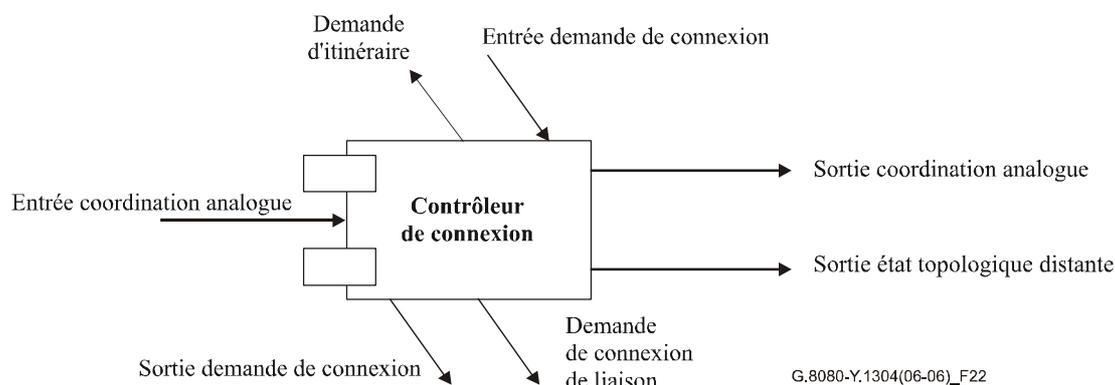


Figure 22/G.8080/Y.1304 – Composant "contrôleur de connexion"

Sortie état de topologie distante: cette interface est utilisée pour présenter les informations d'état de topologie apprises par le contrôleur de connexion. Cet état inclut la capacité de signalisation sur une liaison.

Opération d'établissement de la connexion

L'établissement de la connexion s'effectue en réponse à une demande de connexion émise, soit par un contrôleur de connexion du domaine local, soit par un contrôleur de connexion homologue. L'interface d'entrée/sortie de demande de connexion est utilisée dans le cas d'un routage hiérarchique lorsque le contrôleur de connexion supérieur (c'est-à-dire, parent) choisit les points SNP source et de destination. Dans tous les autres cas, l'interface d'entrée/sortie de coordination d'homologue est utilisée. Le fonctionnement du composant est identique dans les deux cas.

La résolution de la première portion non résolue de l'itinéraire se fait par le biais de l'interface de demande de table de routage; elle fournit comme résultat un ensemble de liaisons devant être traversées qui vient s'ajouter à l'ensemble déjà résolu. Le contrôleur de connexion inspecte le nouvel ensemble de liaisons pour trouver celles qui sont disponibles pour une allocation à la connexion de liaison. Les connexions de liaison sont obtenues et les liaisons qu'elles utilisent sont retirées de l'ensemble de liaisons. Les connexions de sous-réseau correspondantes sont ensuite demandées auprès des contrôleurs de connexion subordonnés (fils) par le biais de l'interface de sortie de demande de connexion. Tout composant non alloué de l'itinéraire est transféré vers le contrôleur de connexion homologue suivant en aval. La succession effective des opérations dépend d'un grand nombre de facteurs, incluant la quantité d'informations de routage disponibles et l'accès à des gestionnaires de ressource de liaison particuliers, mais le fonctionnement du contrôleur de connexion reste identique. L'opération de libération d'une connexion est comparable à l'établissement de la connexion, les opérations étant faites en sens inverse.

7.3.2 Composant "contrôleur de routage" (RC, *routing controller*)

Le contrôleur de routage joue le rôle suivant:

- répondre aux demandes concernant les informations d'itinéraire nécessaires à l'établissement des connexions. Ces informations peuvent aller des caractéristiques détaillées de l'itinéraire de bout en bout jusqu'à un bond suivant. L'itinéraire peut être calculé par un ou plusieurs contrôleurs de routage travaillant en coopération;
- répondre aux demandes d'information de topologie (points SNP et leurs abstractions) à des fins de gestion de réseau.

Comme indiqué dans le § 7.1, le composant "contrôleur de routage" est une entité abstraite qui assure la fonction de routage. Il peut être implémenté sous la forme d'une entité unique, ou d'un ensemble d'entités réparties constituant une fédération coopérative.

Les informations présentes dans le contrôleur de routage lui permettent de rechercher des itinéraires au sein de son domaine de responsabilité. Ces informations concernent la topologie (pools SNPP, connexions de liaison SNP) et les adresses SNP (adresses réseau) correspondant à toutes les adresses de système de terminaison au niveau d'une couche donnée. Les informations d'adressage concernant les autres sous-réseaux de la même couche (sous-réseaux homologues) peuvent également être gérées. Le contrôleur de routage peut également gérer une connaissance de l'état des points SNP pour un routage basé sur des contraintes. L'utilisation de cette vue permet de déterminer une route possible entre un ou plusieurs (ensembles de) points SNP en tenant compte de certaines contraintes de routage. Il existe divers niveaux de détail pour le routage pouvant concerner:

- la portée (par exemple, la vue du vecteur de distance – les adresses et les bonds suivants sont gérés);
- la vue topologique (par exemple, état de la liaison – les adresses et la situation topologique sont gérées).

Le contrôleur de routage utilise les interfaces indiquées dans le Tableau 3 et représentées par la Figure 23.

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 routage | Elément de route non résolu | Route |
| 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 |
|-------------------------|------------------------------------|------------------------------|
| Demande de routage | Elément de route non résolu | Route |
| Sortie topologie locale | Mise à jour de la topologie locale | – |
| Sortie topologie réseau | Mise à jour de la topologie réseau | – |

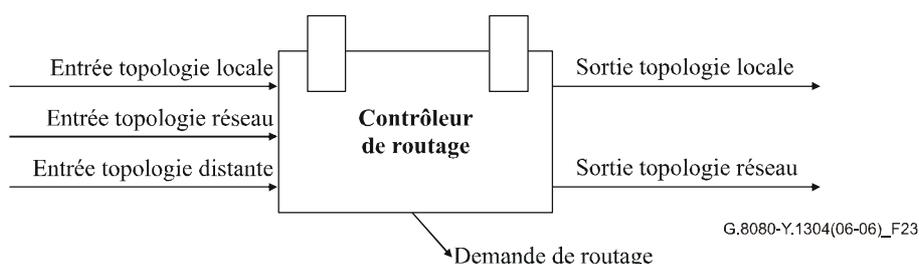


Figure 23/G.8080/Y.1304 – Composant "contrôleur de routage"

Interface de demande d'itinéraire: cette interface accepte un élément d'itinéraire non résolu et renvoie un itinéraire. Un contrôleur de routage (RC) peut demander à un autre RC (ou à plusieurs autres RC) de la zone de routage parent ou fils de l'aider à résoudre l'itinéraire. On peut donner les exemples de résultats de demande suivants:

- 1) renvoi d'un pool SNPP de sortie sur ce sous-ensemble qui se trouve sur le chemin d'un pool SNPP de destination donnée;
- 2) renvoi d'une succession de sous-réseaux qui constituent un chemin entre une paire de pools SNPP de source/de destination données;
- 3) renvoi d'une succession de sous-réseaux qui constituent un chemin entre deux ensembles de pools SNPP;
- 4) renvoi d'une succession de pools SNPP qui constituent un chemin entre une paire de pools SNPP de source/de destination données;
- 5) renvoi d'une succession de pools SNPP qui constituent un chemin entre une paire de pools SNPP de source/de destination données et qui incluent un ou plusieurs pools SNPP spécifiques;

- 6) renvoi d'une succession de pools SNPP qui constituent un chemin entre une paire de pools SNPP de source/de destination données et fournit une diversité par rapport à un chemin donné.

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

Interface de topologie locale: cette interface est utilisée pour configurer les tables de routage au moyen des informations de topologie locale et des informations de mise à jour de la topologie locale. Il s'agit des informations de topologie qui appartiennent au domaine de responsabilité du contrôleur de routage. Les informations de topologie locale sont soit publiques soit associées à un VPN particulier.

Interface de topologie réseau: cette interface est utilisée pour configurer les tables de routage au moyen des informations de topologie réseau et des informations de mise à jour de la topologie réseau. Il s'agit des informations de topologie réduites (par exemple, de la topologie résumée) qui appartiennent au domaine de responsabilité du contrôleur de routage. 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.

7.3.3 Composant "gestionnaire de ressource de liaison" (LRMA et LRMZ)

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.

Deux composants LRM sont utilisés, à savoir le gestionnaire LRMA et le gestionnaire LRMZ. Une liaison SNPP est gérée par un couple de composants gestionnaires LRMA et LRMZ qui traitent chacun une extrémité de la liaison. Les demandes d'allocation de connexions de liaison SNP sont adressées uniquement au gestionnaire LRMA.

La Figure 24 présente deux cas de liaison SNPP.

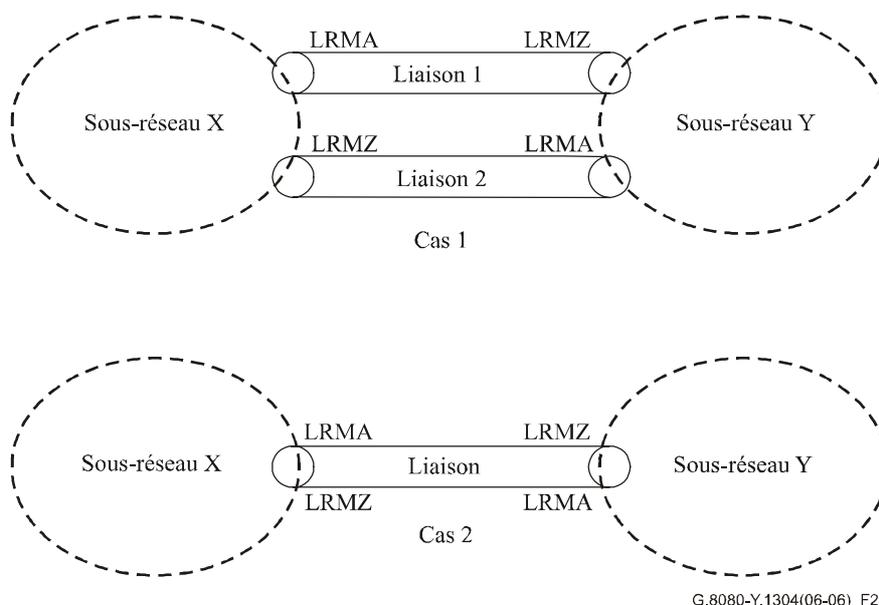


Figure 24/G.8080/Y.1304 – Cas de liaison SNPP

Dans le cas 1, la liaison 1 est dédiée à l'établissement des connexions issues du sous-réseau X. Les demandes de connexions de liaison SNP issues du sous-réseau X sont envoyées au gestionnaire LRMA adjacent pour la liaison 1. Ce dernier peut allouer la connexion de liaison SNP sans négociation de la liaison 1 avec le gestionnaire LRMZ. La liaison 2 est dédiée de même aux demandes d'établissement de connexion issues du sous-réseau Y. Les demandes de connexions de liaison SNP issues du sous-réseau Y sont envoyées au gestionnaire LRMA adjacent pour la liaison 2. Ce gestionnaire LRMA peut allouer la connexion de liaison SNP sans négociation de la liaison 2 avec le gestionnaire LRMZ.

Dans le cas 2, la liaison est partagée entre les sous-réseaux X et Y pour l'établissement des connexions. Les demandes de connexions de liaison SNP issues du sous-réseau X sont envoyées au gestionnaire LRMA adjacent, car un tel composant LRMA situé à l'extrémité distante de la liaison peut également allouer des connexions de liaison SNP; il se peut que le gestionnaire LRMA ait besoin de négocier une allocation avec le gestionnaire LRMZ de l'extrémité distante. Un processus identique est nécessaire pour le traitement des demandes issues du sous-réseau Y à destination de son gestionnaire LRMA adjacent.

7.3.3.1 Gestionnaire LRMA

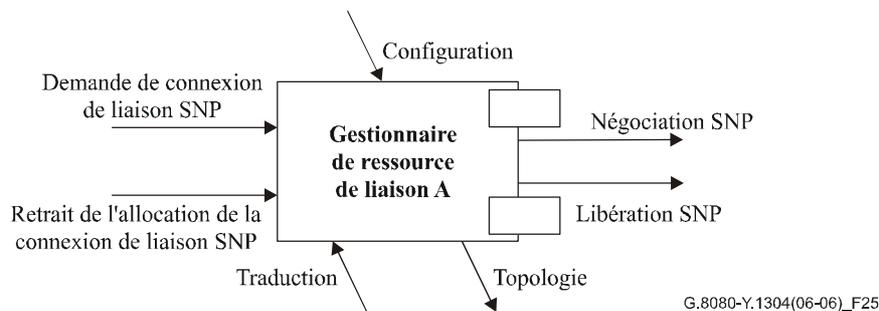
Le gestionnaire LRMA est responsable de la gestion de l'extrémité A de la liaison SNPP, incluant l'allocation des connexions de liaison et le retrait de cette allocation, ainsi que la fourniture des informations de topologie et de statut.

Le composant gestionnaire LRMA utilise les interfaces indiquées dans le Tableau 4 et représentées par la Figure 25.

Tableau 4/G.8080/Y.1304 – Interfaces du composant LRMA

| Interface d'entrée | Paramètres d'entrée de base | Paramètres de retour de base |
|--|---|---|
| Demande de connexion de liaison SNP | Identificateur de demande Identificateur SNP (optionnel) | Identificateur de demande Id. de la paire SNP ou refus |
| Retrait de l'allocation de la connexion de liaison SNP | Identificateur SNP | Confirmation ou refus |
| Configuration | Informations de liaison | – |
| Traduction | Identificateur local | Identificateur d'interface |

| Interface de sortie | Paramètres de sortie de base | Paramètres de retour de base |
|---|--|---|
| Négociation SNP (Cas 2 uniquement) | Identificateur de demande Liste d'identificateurs SNP | Identificateur de demande Identificateur SNP |
| Retrait de l'allocation SNP (Cas 2 uniquement) | Identificateur SNP | Confirmation |
| Topologie | Informations de liaison | – |



G.8080-Y.1304(06-06)_F25

Figure 25/G.8080/Y.1304 – Composant "gestionnaire de ressource de liaison A"

- **Fonctions**

- *Allocation de connexion de liaison*

L'admission de connexion est invoquée lorsqu'une demande d'allocation d'une connexion de liaison est reçue, afin de décider s'il existe suffisamment de ressources libres pour permettre une nouvelle connexion. La décision d'admission de la connexion peut également se faire en fonction de priorités ou d'autres décisions de la politique. Les politiques d'admission de connexion sont en dehors du domaine d'application de la normalisation.

La demande est rejetée s'il n'existe pas de ressources suffisantes.

Si des ressources suffisantes sont disponibles, la demande de connexion peut alors être traitée comme décrit dans les deux cas ci-dessous:

- Cas 1: comme les connexions de liaison SNP sont allouées uniquement à partir de l'une des extrémités de liaison SNPP, le gestionnaire LRMA peut sélectionner la connexion de liaison SNP sans interaction avec le gestionnaire LRMZ situé à l'extrémité distante.
- Cas 2: comme les connexions de liaison SNP peuvent être utilisées par le gestionnaire LRMA de l'une ou l'autre extrémité de la liaison SNPP, le gestionnaire LRMA concerné envoie au gestionnaire LRMZ une liste d'identificateurs de points SNP utilisables. Ce dernier sélectionne l'un des points SNP (en coopération avec son gestionnaire LRMA local) et renvoie au gestionnaire LRMA d'origine l'identificateur correspondant.

- *Retrait de l'allocation d'une connexion de liaison*

Le point SNP concerné est marqué comme étant disponible lorsqu'une demande de retrait de l'allocation est reçue pour une connexion de liaison SNP. Le gestionnaire LRMZ associé est informé dans le cas 2.

- *Traduction de l'identificateur d'interface vers un identificateur local*

Le gestionnaire LRM fournit, si nécessaire, la traduction d'un identificateur d'interface vers un identificateur local. Cette traduction est utilisée, par exemple, si les extrémités de la liaison SNPP se trouvent dans des zones de routage différentes.

- **Topologie**

Cette fonction fournit la topologie de liaison utilisant les identificateurs d'interface SNPP et les identificateurs des points SNP contenus.

Elle fournit également des caractéristiques de la liaison, par exemple, son coût, sa qualité ou sa diversité. Certaines des caractéristiques, par exemple le coût, peuvent varier en fonction de l'utilisation de la liaison. Le processus de modification des caractéristiques de la liaison est géré par une politique locale.

7.3.3.2 Gestionnaire LRMZ

Le gestionnaire LRMZ est responsable de la gestion de l'extrémité Z de la liaison SNPP, incluant la fourniture des informations de topologie et de statut.

Le composant gestionnaire LRMZ utilise les interfaces indiquées dans le Tableau 5 et représentées par la Figure 26.

Tableau 5/G.8080/Y.1304 – Interfaces du composant LRMZ

| Interface d'entrée | Paramètres d'entrée de base | Paramètres de retour de base |
|---|--|--|
| Entrée négociation SNP (cas 2 uniquement) | Identificateur de demande Liste d'identificateurs SNP | Identificateur de demande Identificateur SNP ou refus |
| Retrait de l'allocation SNP (cas 2 uniquement) | Identificateur SNP | Confirmation |
| Configuration | Informations de liaison | – |
| Traduction | Identificateur local | Identificateur d'interface |

| Interface de sortie | Paramètres de sortie de base | Paramètres de retour de base |
|---------------------|------------------------------|------------------------------|
| Topologie | Informations de liaison | – |

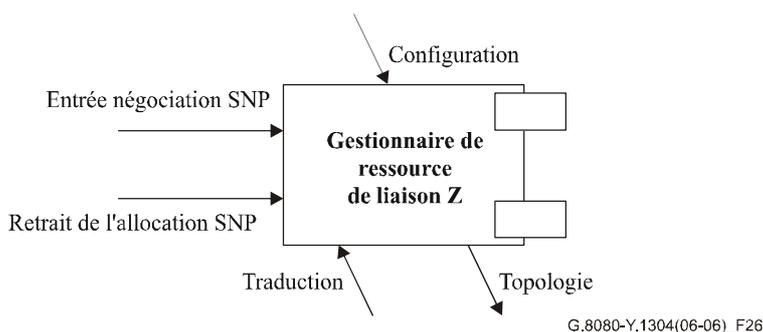


Figure 26/G.8080/Y.1304 – Composant "gestionnaire de ressource de liaison Z"

- **Fonctions**

- *Allocation de point SNP (uniquement pour le cas 2)*

Lorsqu'une liste de points SNP utilisables est reçue, l'une d'elles est sélectionnée et renvoyée.

- *Retrait de l'allocation de point SNP (uniquement pour le cas 2)*

Un point SNP est marqué comme étant disponible lorsque le gestionnaire LRMA associé indique que l'allocation de ce point SNP a été supprimée.

- *Traduction de l'identificateur d'interface vers un identificateur local*

Le gestionnaire LRM doit fournir la traduction d'un identificateur d'interface vers un identificateur local. Cette traduction est utilisée, par exemple, si les extrémités de la liaison SNPP se trouvent dans des zones de routage différentes.

- **Topologie**

Cette fonction fournit la topologie de liaison utilisant les identificateurs d'interface SNPP.

7.3.4 Composant "politique de trafic" (TP, *traffic policing*)

Ce composant est une sous-classe du port de politique, dont le rôle est de vérifier si le trafic arrivé émis sur une connexion utilisateur arrivée émet un trafic conforme aux paramètres qui ont fait l'objet d'un accord. Lorsqu'une connexion viole les paramètres de l'accord, le composant TP prend alors des mesures pour remédier à cette situation.

NOTE – Cette vérification n'est pas nécessaire dans le cas d'un réseau de couche de transport avec un débit binaire constant et n'est pas traitée plus en détail dans la présente Recommandation. De même, la politique de l'interface TP ne sera pas traitée dans la présente Recommandation.

7.3.5 Composants "contrôleur d'appel"

Les appels sont soumis à la commande des contrôleurs d'appel. Les composants "contrôleur d'appel" peuvent être de l'un des types suivants:

- contrôleur d'appel appelant/appelé: ce contrôleur d'appel est associé à une extrémité d'un appel; il peut être situé au même emplacement que le système d'extrémité ou à distance et jouer le rôle de serveur mandataire pour le compte d'un système terminal. Le contrôleur peut jouer l'un des rôles, ou les deux, pour la prise en charge de l'appelant ou de l'appelé;
- contrôleur d'appel réseau: le contrôleur d'appel réseau fournit trois rôles, l'un pour la prise en charge de l'appelant, un autre pour la prise en charge de l'appelé et un troisième pour la prise en charge à travers les frontières des domaines.

Un contrôleur d'appel de l'appelant interagit avec un contrôleur d'appel de l'appelé au moyen d'un ou plusieurs contrôleurs d'appel réseau intermédiaires.

Il convient de noter que la commande d'appel n'est nécessaire que pour les associations de signalisation entre domaines. Dans un appel, la progression de la signalisation et du routage de connexion permet d'établir la connexion, l'appel pouvant ainsi aboutir. En conséquence, lorsque des frontières de domaines sont franchies, il n'est pas utilisé de contrôleurs NCC. L'état d'appel est enregistré dans des contrôleurs NCC.

De plus, les contrôleurs NCC ne sont pas hiérarchiques; le contrôleur NCC qui se trouve à la périphérie d'un ensemble de domaines imbriqués doit appliquer la politique de l'ensemble de ces domaines. Il n'existe pas un contrôleur NCC distinct pour chacun des domaines imbriqués.

7.3.5.1 Contrôleur d'appel de l'appelant/de l'appelé

Ce composant joue le rôle suivant:

- génération des demandes d'appel de départ;
- acceptation ou rejet des demandes d'appel arrivée;
- génération des demandes de terminaison d'appel;
- traitement des demandes de terminaison d'appel arrivée;
- gestion d'état de l'appel.

Ce composant possède les interfaces indiquées dans le Tableau 6. Le contrôleur d'appel de l'appelant/de l'appelé est représenté par la Figure 27.

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 | Identificateur de ressource de transport ou identificateur 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 | Identificateur de ressource de transport ou nom de ressource de transport VPN | Confirmation de la libération de l'appel |
| Demande de modification de l'appel | Identificateur de l'appel, paramètres à modifier | Confirmation ou rejet de la modification d'appel |

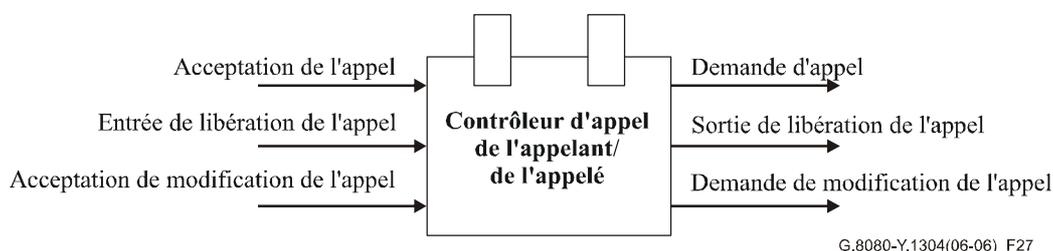


Figure 27/G.8080/Y.1304 – Composant "contrôleur d'appel de l'appelant/de l'appelé"

Demande d'appel: cette interface est utilisée pour effectuer des demandes d'établissement, de maintenance et de libération pour un appel. Elle accepte également la confirmation ou le rejet d'une demande d'appel.

Acceptation de l'appel: cette interface est utilisée pour accepter des demandes d'appel arrivées. Elle effectue également la confirmation ou le rejet de la demande d'appel arrivée.

Libération de l'appel: cette interface est utilisée pour émettre, recevoir et confirmer des demandes de 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.

Il convient de noter qu'un même contrôleur d'appel de l'appelant/de l'appelé peut jouer le rôle d'origine ou de terminaison pour des transactions différentes.

7.3.5.2 Contrôleur d'appel réseau

Les contrôleurs d'appel réseau sont instanciés aux frontières des domaines (c'est-à-dire aux points de référence E-NNI, lorsqu'il y a lieu d'examiner les paramètres de l'appel – administrations différentes, domaines de rétablissement différents, par exemple).

Les contrôleurs d'appel qui sont adjacents (dans le contexte d'un appel) forment un segment d'appel.

Ce composant joue le rôle suivant:

- traitement des demandes d'appel arrivée;
- génération des demandes d'appel de départ;
- génération des demandes de terminaison d'appel;
- traitement des demandes de terminaison d'appel;
- traduction des identificateurs de source et de destinations d'appel VPN en identificateurs de ressource de transport;
- contrôle d'admission d'appel basé sur la validation des paramètres d'appel, des droits de l'utilisateur et de l'accès à la politique des ressources réseau;
- gestion d'état de l'appel.

Ce composant possède les interfaces indiquées dans le Tableau 7 et représentées par la Figure 28.

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

| Interface d'entrée | Paramètres d'entrée de base | Paramètres de retour de base |
|--|---|--|
| Acceptation de la demande d'appel | Identificateur de ressource de transport UNI ou pseudonyme d'identificateur de ressource de transport UNI | Confirmation ou rejet de la demande d'appel |
| Entrée de coordination d'appel réseau | Identificateur de ressource de transport UNI ou pseudonyme d'identificateur de ressource de transport UNI | Confirmation ou rejet |
| Entrée de libération de l'appel | Identificateur de ressource de transport UNI ou pseudonyme d'identificateur 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, identificateurs 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 | Identificateur de ressource de transport UNI ou pseudonyme d'identificateur de ressource de transport UNI | Confirmation du rejet de la demande d'appel |
| Sortie de demande de connexion | Identificateur de ressource de transport UNI ou pseudonyme d'identificateur de ressource de transport UNI | Paire de points SNP |
| Sortie de coordination d'appel réseau | Identificateur de ressource de transport UNI ou pseudonyme d'identificateur de ressource de transport UNI | Confirmation ou rejet de la demande d'appel |
| Demande d'annuaire | Identificateur de ressource de transport UNI ou pseudonyme d'identificateur 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 | Identificateur de ressource de transport UNI ou pseudonyme d'identificateur 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, identificateurs 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 |

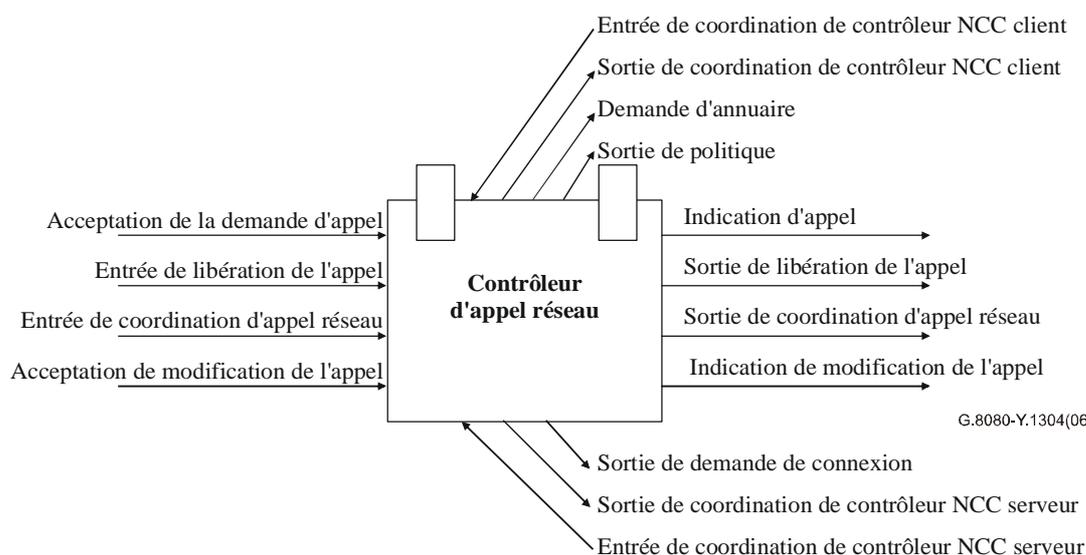


Figure 28/G.8080/Y.1304 – Composant "contrôleur d'appel réseau"

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.

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.

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

Coordination d'appel réseau: cette interface est utilisée pour la coordination de l'appel au niveau réseau.

Libération de l'appel arrivée/de départ: ces interfaces sont utilisées pour émettre, recevoir et confirmer des demandes de libération.

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.

Le rôle du contrôle d'admission dans le contrôleur d'appel réseau de l'appelant consiste à vérifier qu'un nom d'utilisateur appelé et des paramètres valides ont été fournis. Les paramètres de service sont contrôlés par rapport à une spécification de niveau de service. Les paramètres peuvent être renégociés, si nécessaire, avec le contrôleur d'appel de l'appelant. Le domaine de validité de cette négociation est déterminé par les politiques découlant de la spécification de niveau de service, elle-même déduite de l'accord de niveau de service.

Le rôle du contrôle d'admission d'appel arrivée dans le contrôleur d'appel réseau de l'appelé, s'il existe, est de vérifier que l'appelé est habilité à accepter l'appel, compte tenu des contrats de service de l'appelant et de l'appelé. Une adresse d'appelant peut, par exemple, être filtrée, ce qui peut conduire au rejet de l'appel.

L'interface de demande d'annuaire du contrôleur d'appel réseau est utilisée pour accéder à une fonction d'annuaire qui permet de transformer des identificateurs entre ou au sein d'espaces nominatifs. Un identificateur est fourni en entrée à la fonction d'annuaire qui retourne un ou plusieurs identificateurs. Les modalités de mise à jour ou de configuration de l'annuaire ne sont pas abordées dans la présente Recommandation et seront exposées dans d'autres Recommandations. La fonction d'annuaire pourrait notamment assurer le mappage des éléments suivants:

- identificateur de ressource de transport UNI vers identificateur de pool SNPP. Un contrôleur d'appel a besoin d'un pool SNPP pour soumettre une demande à un contrôleur de connexion;
- pseudonyme d'identificateur de ressource ou de transport UNI vers identificateur de ressource ou de transport UNI. Une application de ce mappage est de pouvoir identifier les ressources associées à un conteneur de groupe d'accès (AGC, *access group container*) à rattachement multiple avec un identificateur qui est un pseudonyme d'identificateur de ressource de transport UNI;
- identificateur de pool SNPP vers identificateur de ressource ou de transport UNI. Pour utiliser les interfaces sortie de coordination de contrôleur NCC serveur et entrée de coordination de contrôleur NCC client, les identificateurs de ressource ou de transport UNI nécessaires sont ceux de la couche serveur. Ce mappage est utilisé pour lancer l'appel de couche serveur. Avant que l'appel soit lancé, le client ne dispose pas des identificateurs de ressource de transport UNI de la couche serveur mais uniquement des pools SNPP de la couche client à la périphérie du sous-réseau de couche serveur. Un mappage entre les pools SNPP de couche client et les identificateurs de ressource de transport UNI de couche serveur permet d'invoquer l'appel de couche serveur;
- pseudonyme de pool SNPP vers pool SNPP. Ce mappage est utilisé pour assurer la coordination entre les niveaux de routage.

7.3.5.3 Interactions du contrôleur d'appel

Les interactions entre les composants "contrôleur d'appel" dépendent du type de l'appel et du type de connexion, comme décrit ci-dessous.

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 29 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 associé au contrôleur d'appel réseau correspondant.

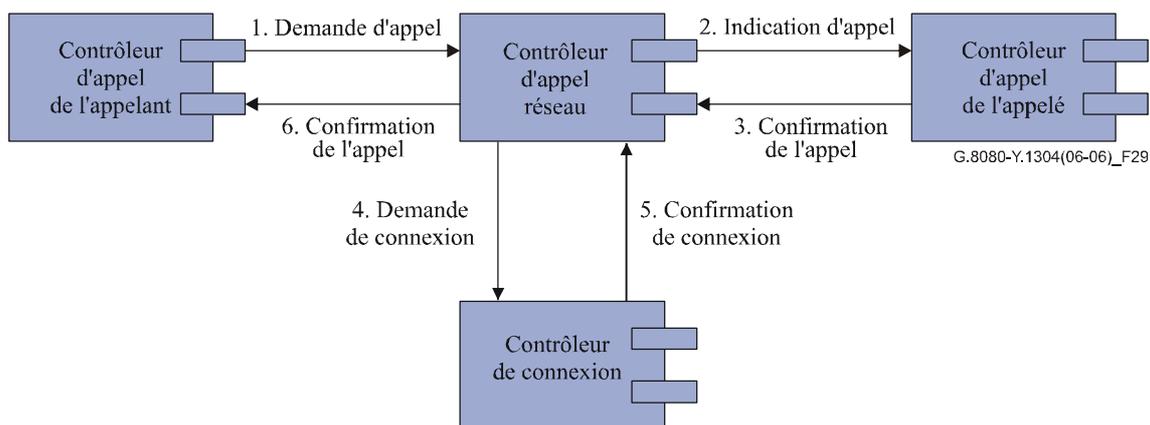


Figure 29/G.8080/Y.1304 – Interactions du contrôleur d'appel de l'appelant/de l'appelé pour des connexions commutées: exemple 1

La Figure 29 présente une situation dans laquelle le contrôleur d'appel de l'appelé accepte l'appel avant que le contrôleur d'appel réseau arrive demande la connexion. Il est également valide de définir une interaction dans laquelle l'établissement de la connexion se fait suite à l'appel, comme illustré dans la Figure 30.

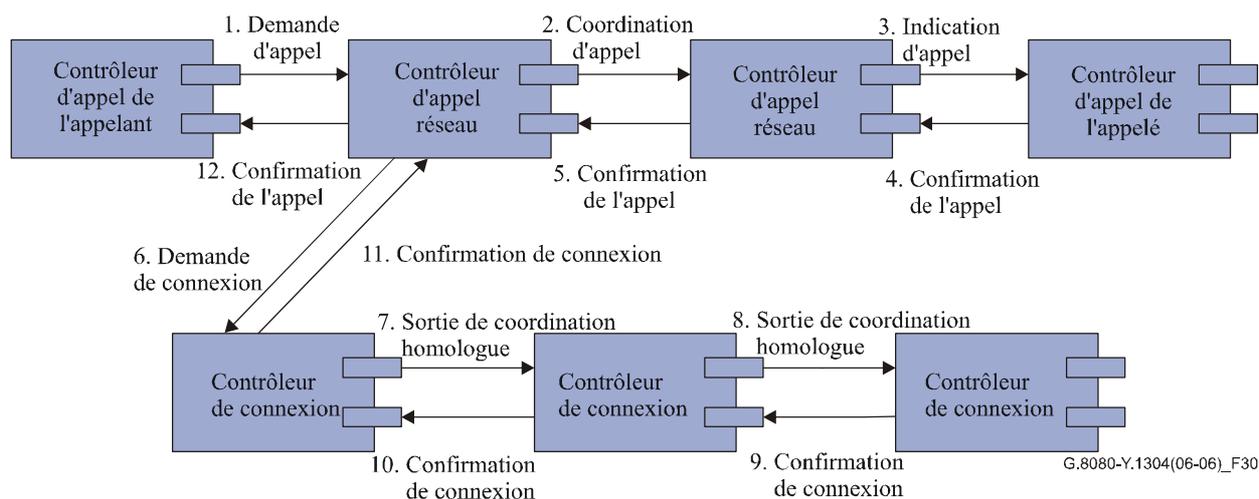


Figure 30/G.8080/Y.1304 – Interaction du contrôleur d'appel de l'appelant/de l'appelé pour des connexion commutées: exemple 2

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. La Figure 31 présente les interactions des contrôleurs d'appel pour des connexions permanentes reconfigurables.

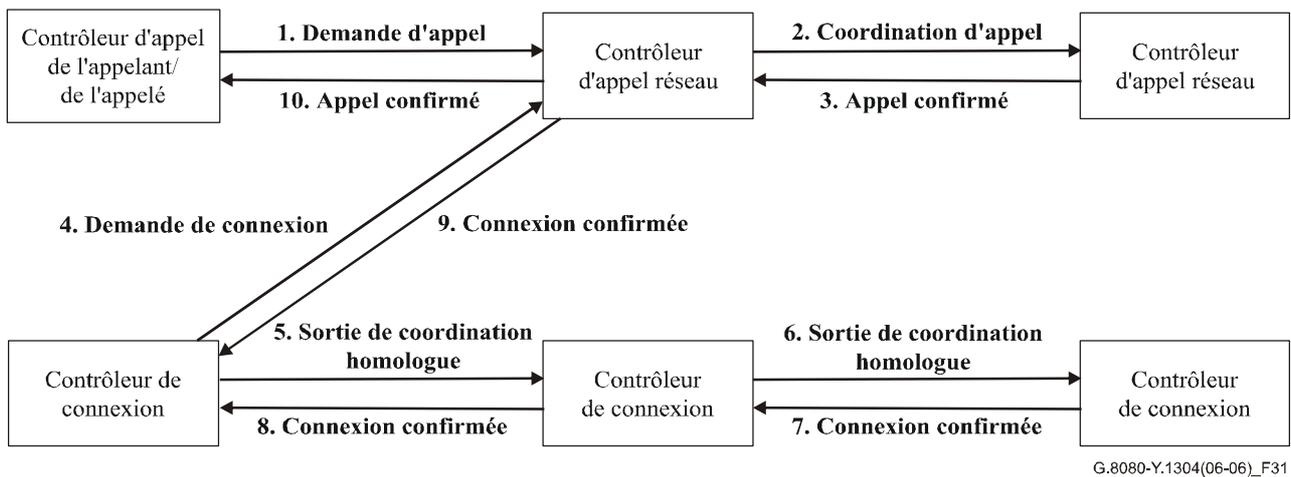
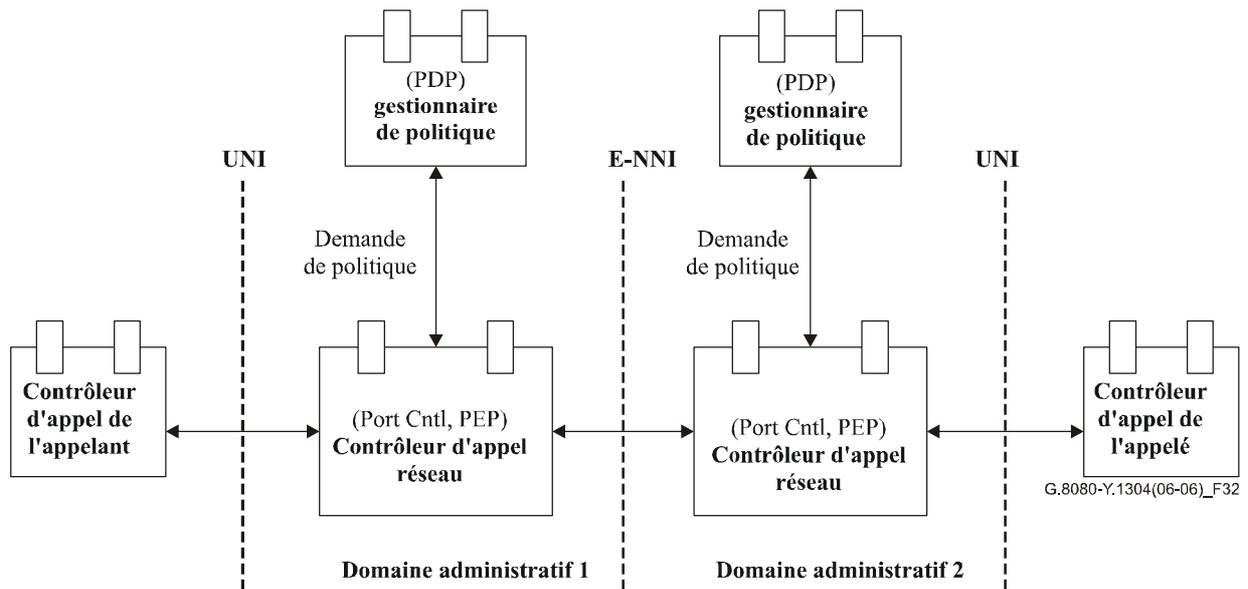


Figure 31/G.8080/Y.1304 – Interactions des contrôleurs d'appel pour des connexions permanentes reconfigurables

Appel avec serveur mandataire: le contrôleur d'appel de l'appelant/de l'appelé interagit avec le contrôleur d'appel réseau par le biais d'un protocole d'appel, mais ne coïncide pas avec l'utilisateur.

La Figure 32 donne un exemple d'interactions nécessaires à la prise en charge de la politique de contrôle d'admission d'appel entre des contrôleurs d'appel réseau.



Port Cntl contrôleur de port
PDP point de décision de politique
PEP point d'exécution de la politique

Figure 32/G.8080/Y.1304 – Exemple d'interactions pour la politique de contrôle d'admission d'appel

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. L'utilisation de ces interfaces intercouches est régie par la politique de l'opérateur. 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.

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;
- les extrémités de la connexion de liaison associée à l'appel à l'interface UNI-N ne sont pas modifiables. Elles peuvent toutefois être ajoutées ou supprimées lorsque des connexions sont ajoutées à un appel ou supprimées de celui-ci.

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.

7.3.5.5 Traitement des appels infructueux

Dans le cas d'une nouvelle demande d'appel, si le réseau n'est pas en mesure d'établir toutes les connexions requises pour satisfaire à cette demande, les connexions ou les connexions partielles qui auront été établies seront libérées (supprimées) et la demande d'appel sera rejetée.

Dans le cas de modifications d'un appel, si le réseau n'est pas en mesure d'ajouter les connexions demandées, la modification de l'appel sera considérée comme ayant échoué. Les connexions ou les connexions partielles seront supprimées et aucune modification ne sera apportée à l'appel en cours.

7.3.6 Agent de découverte (DA, *discovery agent*)

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) et des points de connexion de terminaison (TCP) 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 |

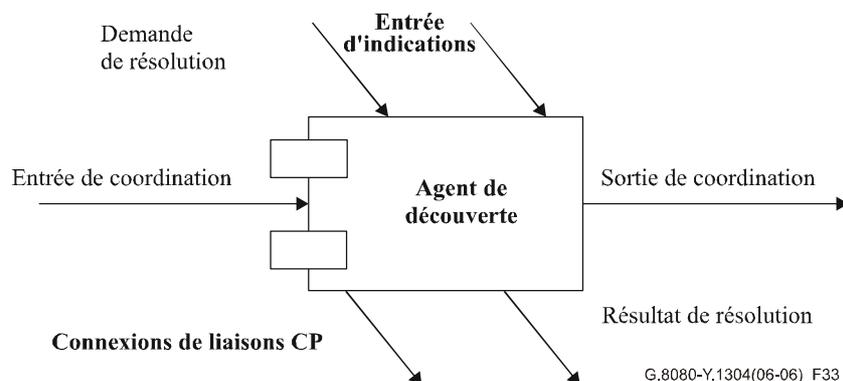


Figure 33/G.8080/Y.1304 – Composant agent de découverte

7.3.7 Exécuteurs de terminaison et d'adaptation

L'exécuteur de terminaison et d'adaptation (TAP, *termination and adaptation performer*) 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 dans le Tableau 9.

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

| Etat | Description |
|-----------|--|
| 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: immédiatement (interrompre l'appel en cours); rapidement (rerouter l'appel avant l'abandon); à la prochaine fenêtre de maintenance; lorsque l'appel est abandonné. |
| 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 |

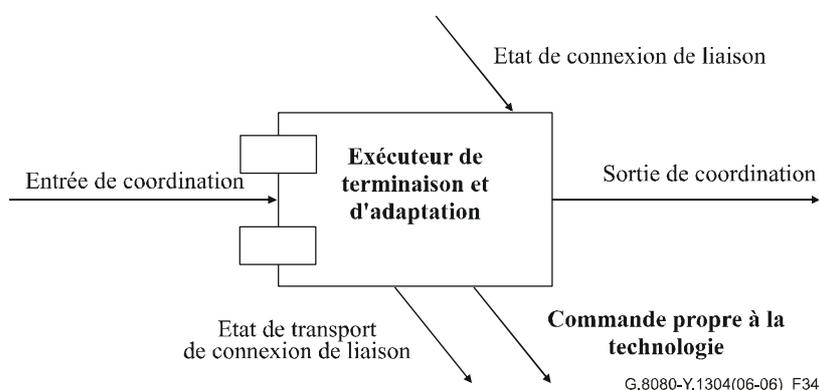


Figure 34/G.8080/Y.1304 – Composant exécuteur de terminaison et d'adaptation

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).

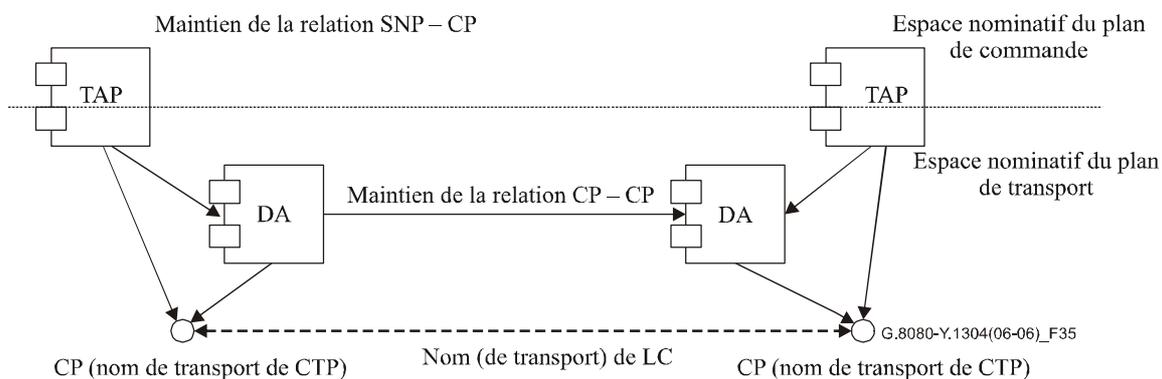


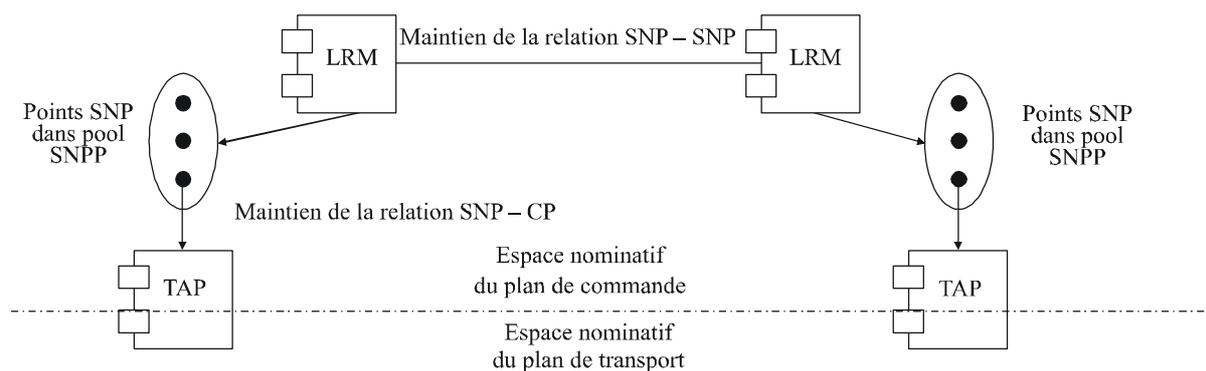
Figure 35/G.8080/Y.1304 – Découverte des connexions de liaison (LC) du transport

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).



G.8080-Y.1304(06-06)_F36

Figure 36/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.

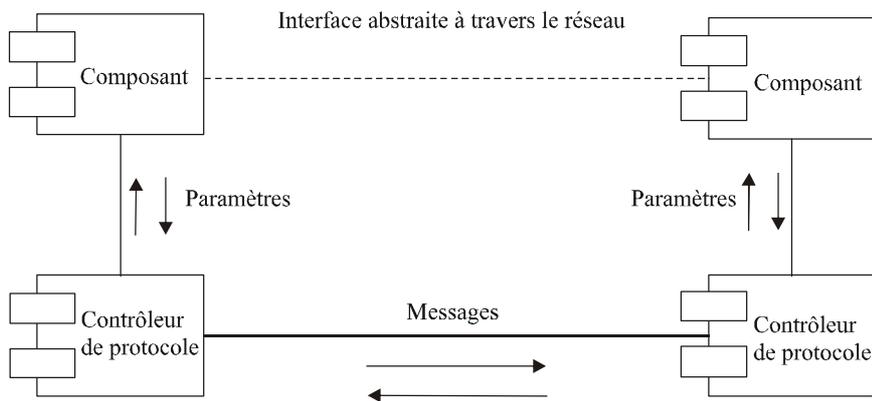
7.4 Composants "contrôleur de protocole" (PC)

Le contrôleur de protocole fournit le mappage des paramètres des interfaces abstraites des composants de commande avec des messages véhiculés par un protocole en vue de la prise en charge de l'interconnexion par le biais d'une interface. Les contrôleurs de protocole sont une sous-classe des contrôleurs de port et fournissent toutes les fonctions associées à ces composants. En particulier, ils rendent compte des violations de protocole à leurs ports de supervision. Ils peuvent également jouer un rôle de multiplexage de plusieurs interfaces abstraites sur une seule instance de protocole, comme indiqué par la Figure 37. Les détails des contrôleurs de protocole

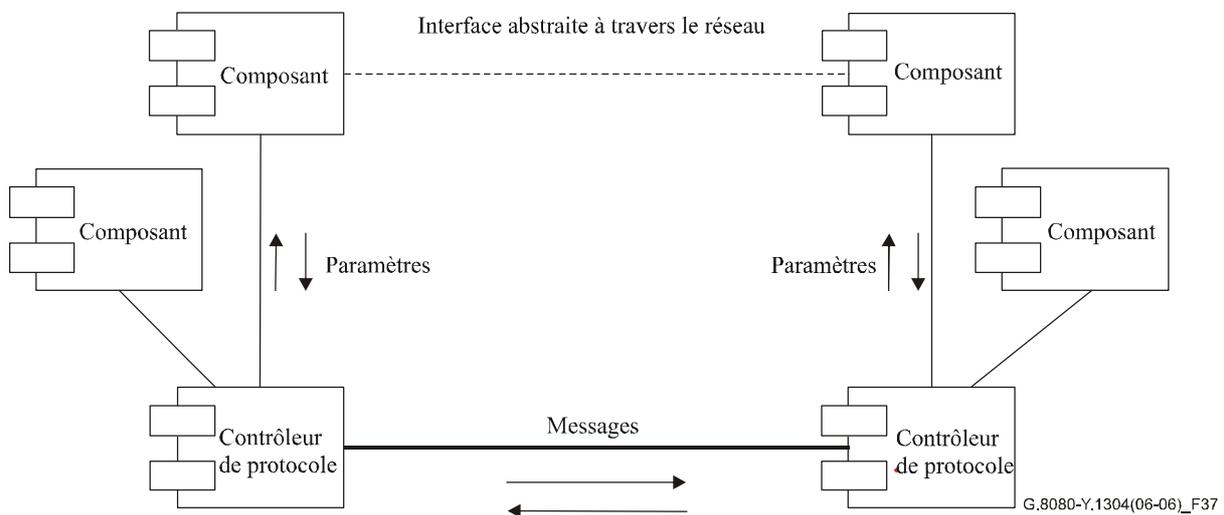
individuels sont des problèmes de conception du protocole, la présente Recommandation en fournit toutefois quelques exemples.

Le rôle d'un contrôleur de protocole de transport consiste à fournir le transfert authentifié, sécurisé et fiable des primitives de commande à travers le réseau par le biais d'une interface définie. Ceci permet de conserver la trace des transactions et de garantir que les réponses attendues sont reçues, ou de rendre compte d'une exception à l'émetteur. Le contrôleur de protocole rendra compte des violations de la sécurité par le biais de son port de supervision lorsque des fonctions de sécurité sont présentes.

Des primitives de signalisation sont transmises entre le contrôleur de connexion et le contrôleur de protocole; ce dernier traite de manière transparente la sémantique des primitives de messagerie comme résultat d'un protocole externe et vice versa. Les messages de signalisation sont transmis entre les deux contrôleurs de protocole, comme indiqué par la Figure 38.



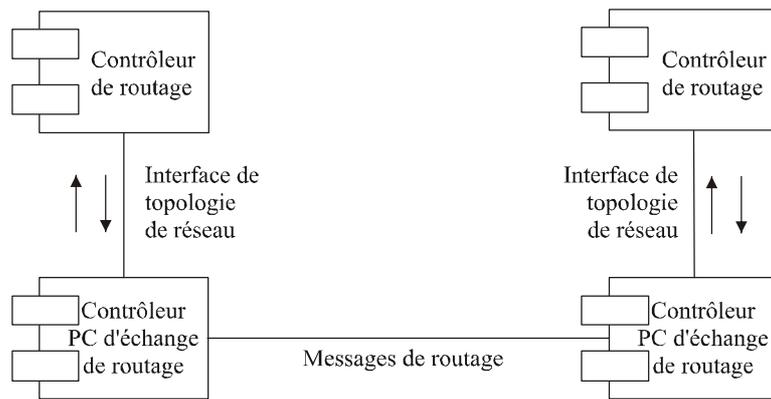
a) utilisation générique du contrôleur de protocole



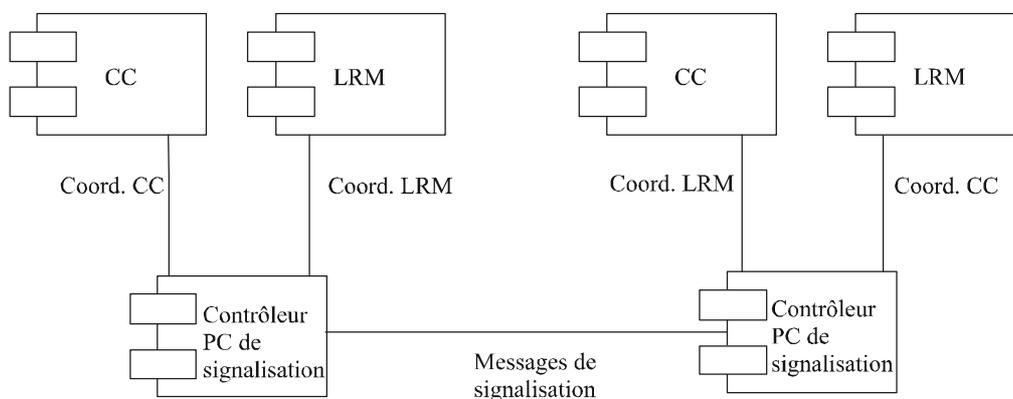
G.8080-Y.1304(06-06)_F37

b) multiplexage générique de plusieurs flux de primitives sur un protocole unique

Figure 37/G.8080/Y.1304 – Contrôleur de protocole



a) échange de table de routage avec un contrôleur PC d'échange de routage



b) multiplexage des coordinations LRM et CC avec un contrôleur PC de signalisation

Figure 38/G.8080/Y.1304 – Exemples d'utilisation de contrôleur de protocole

On peut donner les exemples d'utilisation du contrôleur de protocole pour le transport des informations suivantes:

- messages de mise à jour des tables de routage par le biais d'un contrôleur de protocole d'échange de routage (représenté par la Figure 38-a));
- messages de coordination du gestionnaire de ressource de liaison (lorsque cela est adéquat, comme dans le cas de connexions avec débit binaire disponible) par le biais d'un contrôleur de protocole de gestionnaire de ressource de liaison;
- messages de coordination de commande de connexion par le biais d'un contrôleur de protocole de contrôleur de connexion (représenté par la Figure 38-b)). Il convient de noter que les interfaces de coordination LRM et CC peuvent être multiplexées sur un même contrôleur de protocole.

8 Points de référence

La présente Recommandation définit diverses interfaces logiques (c'est-à-dire, des points de référence) au sein d'un réseau de transport type qui échangent des informations de signalisation et de routage. Les points de référence peuvent être pris en charge par des interfaces multiples, à savoir les interfaces I-NNI et E-NNI. Il est important de noter que plusieurs domaines existeront au sein du réseau ASON et qu'en particulier les interfaces UNI et E-NNI seront utilisées pour la signalisation

de commande entre domaines. Les paragraphes qui suivent décrivent les fonctionnalités particulières qui devront être véhiculées à travers les divers points de référence (UNI, I-NNI et E-NNI) ainsi que leurs différences.

Une politique peut être appliquée au niveau des interfaces prenant en charge un point de référence. Les politiques appliquées dépendent du point de référence et des fonctions prises en charge. Au niveau des points de référence UNI, I-NNI et E-NNI, par exemple, la politique peut s'appliquer à la commande d'appel et de connexion. En outre, pour les points de référence I-NNI et E-NNI, la politique peut s'appliquer également au routage.

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 39.

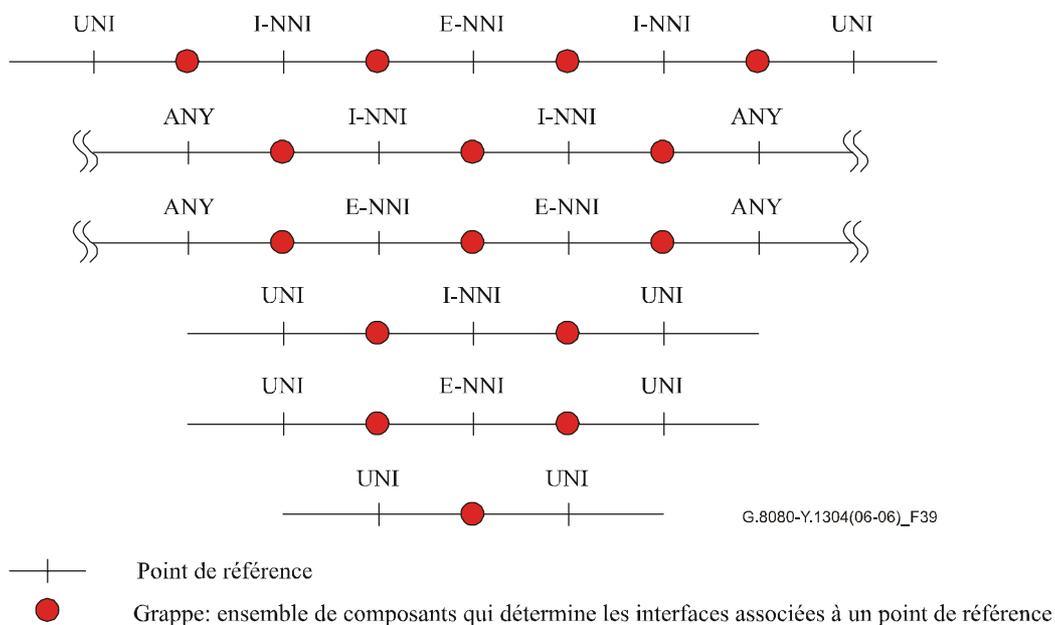


Figure 39/G.8080/Y.1304 – Points de référence

8.1 Interface UNI

Les flux d'informations attendus à travers le point de référence UNI prennent en charge les fonctions suivantes:

- commande d'appel;
- découverte de ressource;
- commande de connexion;
- sélection de connexion.

Il convient de noter qu'aucune fonction de routage n'est associée au point de référence UNI.

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.

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

8.2 Interface I-NNI

Les flux d'informations attendus à travers le point de référence I-NNI prennent en charge les fonctions suivantes:

- découverte de ressource;
- commande de connexion;
- sélection de connexion;
- routage de connexion.

8.3 Interface E-NNI

Les flux d'informations attendus à travers le point de référence E-NNI prennent en charge les fonctions suivantes:

- commande d'appel;
- découverte de ressource;
- commande de connexion;
- sélection de connexion;
- routage de connexion.

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 contrôle de routage du client.

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

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").

L'identificateur 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 supports. 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 identificateurs 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 identificateurs 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 conducteur 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.

8.5 Interaction des contrôleurs NCC entre couches

8.5.1 Appels de contrôleur NCC à contrôleur NCC

Un appel peut exister entre une paire de contrôleurs NCC en l'absence de contrôleurs CCC. Cet appel se trouve dans la même couche. Pour faire en sorte que de tels appels puissent être demandés, un identificateur de ressources de transport est attribué à un ensemble de points SNP indiquant les ressources qui peuvent être utilisées pour prendre en charge un appel. Cet identificateur est analogue à l'identificateur de ressources de transport UNI associé aux ressources de transport à l'interface UNI.

L'appel de contrôleur NCC à contrôleur NCC peut être utilisé dans au moins deux cas. Premièrement, en tant qu'appel invoqué dans un appel entre couches et, deuxièmement en tant qu'autre type de frontière entre domaines dans la même couche.

Lorsqu'il est utilisé dans un appel entre couches, un contrôleur NCC client sert à lancer l'appel entre une autre paire de contrôleurs NCC dans la couche serveur. Au moment où le contrôleur NCC de couche client invoque l'appel de couche serveur, une frontière de domaines est franchie. Cette frontière de domaines est mise en place pour offrir un point de contrôle de politique, ainsi que pour séparer les identificateurs de pool SNPP et de ressource de transport utilisés dans les couches client

et serveur. Les identificateurs de ressource de transport utilisés pour la demande d'appel se trouvent dans la couche serveur. C'est ce que montre la Figure 40.

Une connexion de couche serveur découlant d'un appel de contrôleur NCC à contrôleur NCC utilisée pour prendre en charge une information caractéristique client mappée, comporte une association avec une adaptation. Un tel appel ou une telle connexion peut exister avant que l'adaptation soit effectivement utilisée.

8.5.2 Interaction des espaces nominatifs

Les identificateurs de ressource de transport UNI sont définis pour être uniques sur le plan mondial. Les identificateurs de ressource de transport additionnels ne doivent pas nécessairement faire partie de l'espace d'identificateurs de ressource de transport UNI. Les identificateurs de ressource de transport associés à des appels de contrôleur NCC à contrôleur NCC peuvent provenir d'espaces d'identificateurs distincts.

Un même réseau de couche peut comporter des espaces d'identificateurs SNPP indépendants. Des connexions peuvent être créées à travers ces différents espaces d'identificateurs SNPP du fait que les contrôleurs de routage comprennent le mappage des identificateurs SNPP entre les niveaux de routage.

Lorsque deux espaces d'identificateurs SNPP ne sont pas mappés via le routage, on est autorisé à mapper un espace d'identificateur SNPP dans les identificateurs de ressource de transport associés au deuxième espace d'identificateur SNPP. Cela permettrait notamment d'obtenir une frontière d'entreprise dépourvue d'échanges de routage. Tel est le cas d'une frontière entre couches.

L'accès à ce mappage se fait sous forme d'une fonction de résolution d'adresse qui prend en entrée un identificateur SNPP et qui retourne un identificateur de ressource de transport associé à un pool NPP dans un autre espace d'identificateurs. L'accès à la fonction de résolution d'adresse existante de la présente Recommandation se fait via l'interface de sortie de demande d'annuaire du composant NCC. L'accès à la fonction de résolution d'adresse additionnelle se fera aussi par la même interface de sortie. Pour un appel entre couches, un contrôleur NCC client à la périphérie d'un sous-réseau qui constitue un modèle de souplesse de couche serveur dispose de deux pools SNPP dans la couche client pour laquelle il a besoin d'une connexion. L'obtention de cette connexion est subordonnée à une demande d'itinéraire. La fonction de résolution d'adresse entre couches est utilisée par le contrôleur NCC de couche client pour obtenir la ressource de transport de couche serveur correspondant aux deux pools SNPP de couche client considérés. Les deux identificateurs de ressource de transport sont utilisés pour appeler la couche serveur.

Dans la Figure 40 ci-dessous, SNPP-X dans la couche client est mappé vers l'identificateur de ressource de transport B et SNPP-Y est mappé vers l'identificateur de ressource de transport C. Un appel entre couches peut être invoqué en utilisant l'identificateur de ressources de transport retourné.

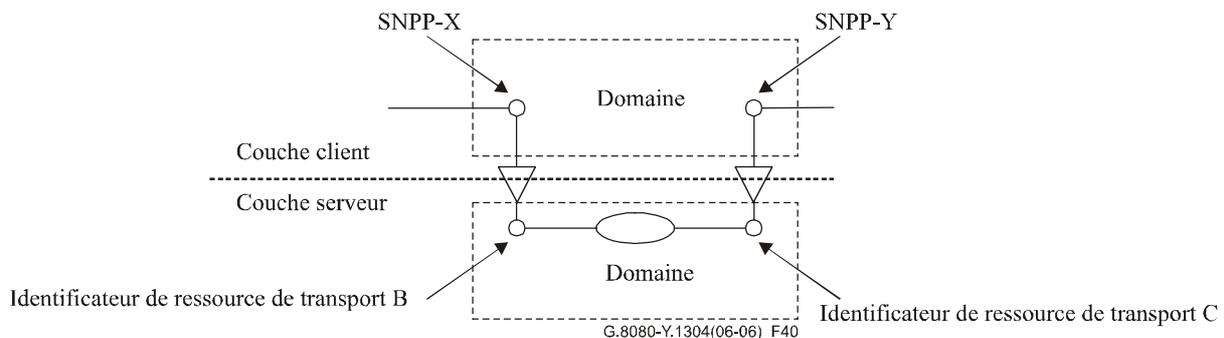


Figure 40/G.8080/Y.1304 – Interaction des espaces nominatifs

9 Gestion réseau des entités du plan de commande

Le paragraphe 5 décrit l'interaction entre le plan de commande et le plan de gestion. Le présent paragraphe identifie certaines capacités de gestion qui peuvent avoir un impact sur les interactions entre ces plans. De telles capacités de gestion peuvent inclure d'une manière spécifique les fonctionnalités suivantes:

- 1) création et suppression d'une connexion;
- 2) séparation des ressources réseau entre celles qui sont visibles par le plan de commande et celles qui sont visibles par le plan de gestion;
- 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;
- 6) positionnement et modification des paramètres du système de signalisation, tels que les temporisations (par exemple, la temporisation d'établissement d'appel), les seuils, les mécanismes de gestion des encombrements, le nombre maximal de connexions autorisées, la charge maximale de signalisation (au-delà de laquelle le processeur de signalisation rejette les demandes d'établissement, etc.);
- 7) lorsque le routage se fait dans le plan de gestion (centralisé):
 - détermination de la route pour les connexions permanentes et utilisation de protocoles de gestion pour la gestion des connexions;
 - détermination de la route pour les connexions permanentes reconfigurables et fourniture d'une route explicite pour le plan de commande;
- 8) mesure des performances d'appel pouvant porter sur les paramètres suivants:
 - taux d'arrivée des demandes d'appel;
 - utilisation des circuits;
 - durée des appels;
 - durées d'occupation (la durée moyenne d'occupation des connexions multipliée par le taux d'arrivée des demandes donne la charge offerte, exprimée en erlangs);
 - moyennes statistiques portant sur le nombre total de demandes de connexion pour une durée donnée;
 - identification du VPN auquel les paramètres de qualité de l'appel appartiennent;
- 9) gestion du contrôle d'admission d'appel;
- 10) détermination du nombre maximal de connexions pouvant être pris en charge par un élément réseau et positionnement éventuel du nombre maximal devant être pris en charge;
- 11) différenciation des changements d'état des connexions entre ceux résultant d'actions du plan de gestion ou de commande et ceux résultant de défaillances; suppression ou génération d'alarmes en fonction des besoins;
- 12) positionnement et modifications des niveaux de priorité de survie ou des niveaux de contrat de qualité de service (QS) pour toutes les connexions appartenant à une "classe de performances" donnée;
- 13) allocation, si nécessaire, de la valeur maximale d'un identificateur de connexion sur une liaison; positionnement des commandes de gestion de trafic, soit de manière manuelle par une entrée spécifique, soit de manière automatique en réponse à une stimulation interne ou

externe. (Dans le cas d'une régulation automatique, le système de gestion positionne les conditions de déclenchement de la régulation et l'amplitude de la réaction);

- 14) activation et désactivation du "routage direct et du routage par débordement";
- 15) prise en charge de procédures de reroutage temporaire;
- 16) gestion du réseau de signalisation permettant d'assurer une configuration cohérente des ressources de signalisation;
- 17) détermination des attributs des liaisons de signalisation, incluant leur statut fonctionnel, les indications d'erreur, les données de trafic ou de largeur de bande maximale;
- 18) transformation d'une connexion permanente (PC, *permanent connection*) en une connexion permanente reconfigurable (SPC, *soft permanent connection*), les ressources de transport associées à la connexion permanente étant assignées au plan de commande sans interruption de service.

10 Identificateurs

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 qui peut être généré à partir d'un autre espace nominatif.

NOTE – Le pseudonyme de pool SNPP 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.

10.2 Noms et adresses

Les noms et les adresses constituent les moyens incontournables d'identification des composants du plan de commande aux fins d'un contrôle concerté des ressources dans un réseau de transport.

Comme indiqué dans la Rec. UIT-T G.8081/Y.1353, les adresses dépendent de l'emplacement, contrairement aux noms. Il importe de noter qu'un identificateur donné peut faire office de nom dans un contexte et d'adresse dans un autre contexte. Considérons par exemple la zone de routage A représentée dans le § 6.3, Figure 11. A l'intérieur de la zone de routage A, l'identificateur de points SNP local est une adresse alors que l'identificateur de points SNP d'interface est un nom. Cependant, à l'extérieur de la zone de routage, l'identificateur de points SNP d'interface peut être une adresse dans le cadre d'une autre zone de routage (non représentée dans la figure).

Diverses entités du plan de commande du réseau ASON ont besoin de noms et d'adresses, comme décrit ci-dessous:

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 d'identificateurs de ressource de transport de l'interface E-NNI, par exemple lorsqu'un appel doit traverser plusieurs domaines et que l'utilisateur peut spécifier un domaine de transit, mais pas une interface E-NNI déterminée.

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, l'identificateur 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.

Ressource de transport de l'interface UNI: la liaison UNI SNPP nécessite un nom pour le contrôleur d'appel de l'appelant et pour le contrôleur d'appel réseau afin de spécifier des destinations. 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. Les identificateurs de ressource de transport de l'interface UNI peuvent être dans une relation 1:N ou N:1 avec les liaisons SNPP. Ceci permet à un appelant ou un appelé d'associer diverses applications à des adresses spécifiques en utilisant une liaison commune. Un pseudonyme peut exister pour un ensemble d'identificateurs de ressources de transport de l'interface UNI.

Contrôleur de protocole de contrôleur de routage: le contrôleur de protocole de contrôleur de routage (RCPC, *routing controller protocol controller*) a besoin d'une adresse RCD pour échanger des messages de protocole de routage avec des contrôleurs RCPC homologues. Le contrôleur de protocole de contrôleur de routage doit en outre avoir un nom qui l'identifie auprès de ses homologues afin d'entretenir des relations protocolaires de routage.

Contrôleur de routage: le contrôleur de routage a besoin d'un nom qui l'identifie comme étant la source des informations de topologie qu'il émet et communique aux autres contrôleurs de routage.

Contrôleur de protocole de commande d'appel réseau: le contrôleur de protocole de commande d'appel réseau a besoin d'une adresse RCD pour échanger des messages de signalisation d'appel. Le contrôleur de protocole de contrôleur d'appel réseau doit aussi avoir un nom qui l'identifie auprès de ses homologues afin d'entretenir des relations de signalisation d'appel.

Contrôleur de protocole de contrôleur de connexion: un contrôleur de protocole de contrôleur de connexion a besoin d'une adresse RCD pour échanger des messages de signalisation de connexion. Ces adresses sont uniques dans le cadre d'un domaine administratif. Le contrôleur de protocole de contrôleur de connexion peut avoir un nom qui l'identifie auprès de ses homologues afin d'entretenir des relations de signalisation de connexion.

Contrôleur de protocole de contrôleur d'appel de l'appelant/de l'appelé: le contrôleur d'appel de l'appelant/de l'appelé nécessite une adresse RCD pour l'échange des messages de signalisation. Le contrôleur de protocole de contrôleur d'appel de l'appelant/de l'appelé doit en outre avoir un nom qui l'identifie auprès de ses homologues afin d'entretenir des relations de signalisation d'appel.

Sous-réseau: un sous-réseau se voit attribuer une adresse qui représente l'ensemble de tous les points SNP de ce sous-réseau et qui est utilisée pour le routage des connexions. Cette adresse est unique au sein d'un domaine administratif.

Zone de routage: une zone de routage se voit attribuer une adresse qui représente l'ensemble de tous les pools SNPP de cette zone de routage et qui est utilisée pour le routage des connexions.

10.3 Relations entre identificateurs

Les composants du plan de commande et ceux du plan de gestion peuvent agir sur les ressources de transport (voir le § 5.2). Par conséquent, les ressources de transport seront désignées par des identificateurs propres au contexte. Pour permettre aux applications utilisées dans ces différents contextes d'échanger des informations relatives à la ressource commune, un mappage est nécessaire entre les identificateurs de ressources de transport utilisés dans le contexte d'un plan de gestion et ceux utilisés dans le contexte d'un plan de commande.

Dans le cadre de l'ensemble des identificateurs utilisés par le plan de commande, pour les ressources du plan de transport, des mappages sont également nécessaires. Par exemple, le mappage d'un identificateur de ressources de transport avec un ou plusieurs pools SNPP.

Les caractéristiques détaillées des éventuels mappages entre identificateurs ne sont pas abordés dans le cadre de la présente Recommandation; elles sont décrites dans les Recommandations UIT-T pertinentes de la série G.771x.x.

11 Techniques d'amélioration de la disponibilité des connexions

Le présent paragraphe décrit les stratégies utilisables pour la maintenance de l'intégrité d'un appel existant en cas de défaillances au sein du réseau de transport.

La Rec. UIT-T G.805 décrit des techniques d'amélioration de la disponibilité du réseau de transport. Elle emploie les termes "protection" (remplacement d'une ressource défaillante par un secours assigné au préalable) et "restauration" (remplacement d'une ressource défaillante avec un reroutage utilisant une capacité de rechange) pour le classement de ces techniques. Les actions de protection s'effectuent en général dans un délai de l'ordre de la dizaine de millisecondes, alors que les actions de restauration prennent normalement un temps allant de la centaine de millisecondes à plusieurs secondes.

Le plan de commande du réseau ASON permet à un opérateur d'offrir à l'utilisateur des appels avec une sélection de la classe de service (CoS, *class of service*) (définissant, par exemple, la disponibilité, la durée des interruptions, les secondes erronées, etc.). Les mécanismes de protection et de restauration (fournis par le réseau) prennent en charge la classe de service sélectionnée par l'utilisateur. Le choix du mécanisme de survie (protection, restauration ou aucun) pour une connexion donnée prenant en charge un appel sera basé sur la politique de l'opérateur réseau, la topologie du réseau et les capacités de l'équipement installé. Il est possible d'utiliser divers mécanismes de survie sur les connexions qui sont concaténées pour la fourniture d'un appel. Si un appel transite par les réseaux de plusieurs opérateurs, chacun de ces réseaux sera alors responsable de la survie des connexions de transit. Les demandes de connexion au niveau des interfaces UNI ou E-NNI contiendront uniquement la classe de service demandée et non un type explicite de protection ou de restauration.

La protection ou la restauration d'une connexion peut être invoquée ou mise hors service de manière temporaire par une commande du plan de gestion. L'utilisation de ces commandes permet également d'effectuer des activités de maintenance programmées à l'avance et de se substituer au fonctionnement automatique dans certaines conditions de défaillance exceptionnelles.

Le mécanisme de protection ou de restauration doit fournir les caractéristiques suivantes:

- prise en charge d'une manière indépendante de tout type de client (par exemple: IP, ATM, SDH, Ethernet);
- fournir une possibilité de reconfiguration permettant une adaptation en cas de défaillance catastrophique dans une couche serveur, par exemple une coupure de câble optique, qui a un impact sur un grand nombre de connexions dans la couche client nécessitant une restauration simultanée et rapide;
- utilisation d'un mécanisme de signalisation robuste et efficace conservant ses fonctionnalités même après une défaillance du réseau de transport ou de signalisation;
- éviter d'utiliser, pour démarrer les actions de protection ou de restauration, des fonctions dont les temps de réponse ne sont pas critiques. Ceci impose de prendre en considération des mécanismes de protection ou de restauration qui ne dépendent pas de la localisation du défaut.

La description de la manière dont les capacités de protection et de restauration sont utilisées par les plans de transport, de contrôle et de gestion d'un réseau ASON appelle une étude ultérieure.

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 contrôle de routage. Un domaine de contrôle 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 41. Dans cet exemple, le domaine de contrôle 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 une connexion 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.

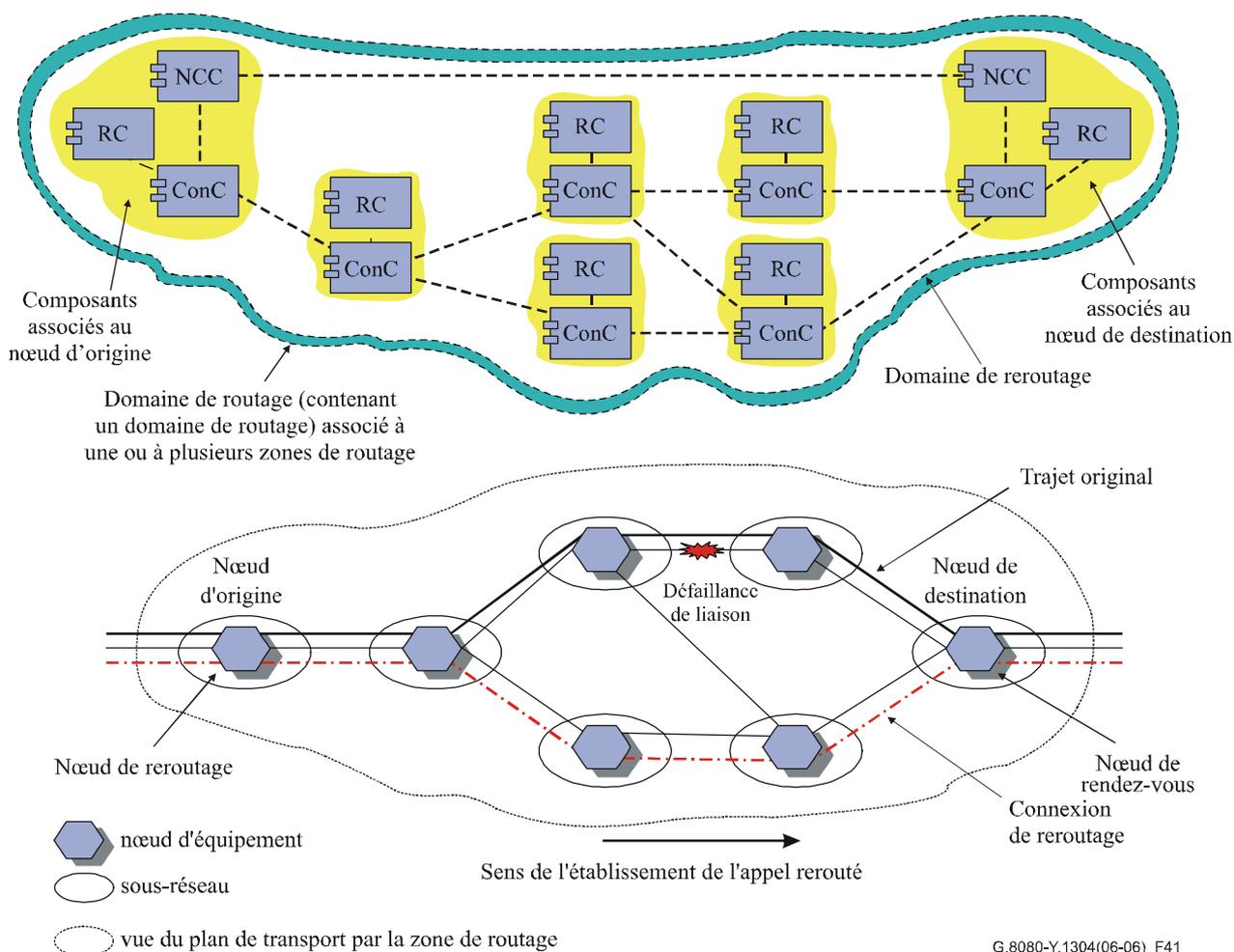


Figure 41/G.8080/Y.1304 – Exemple de reroutage inconditionnel

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.

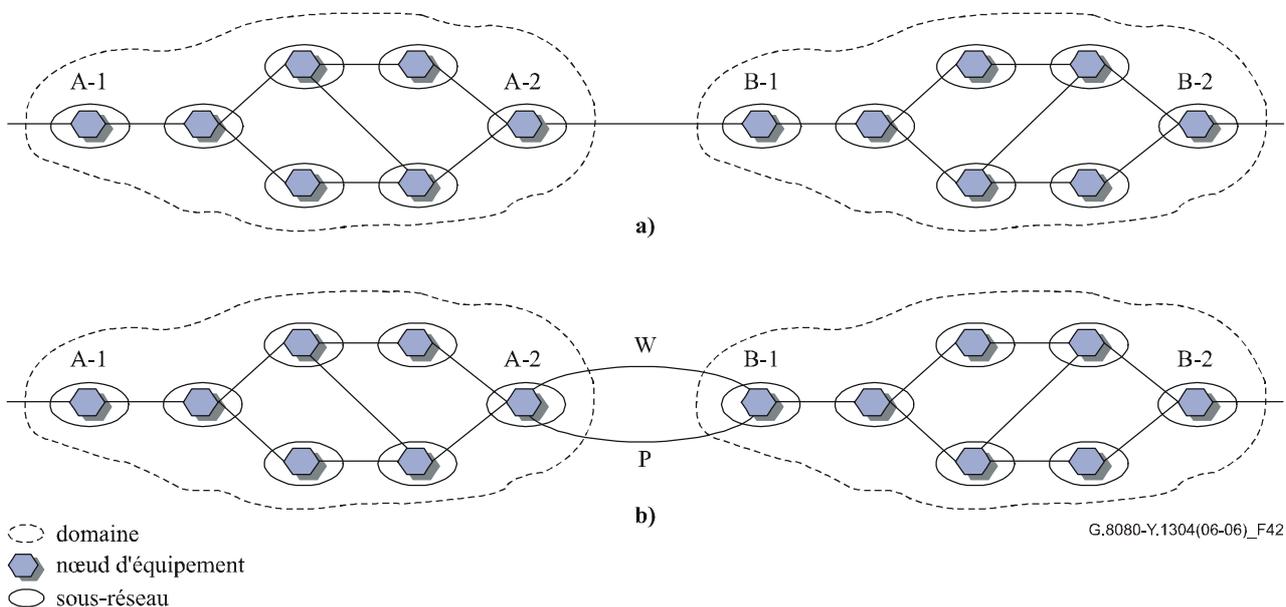
11.2.1.2 Défaillances interdomaines

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 42-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 42-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 43. 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.

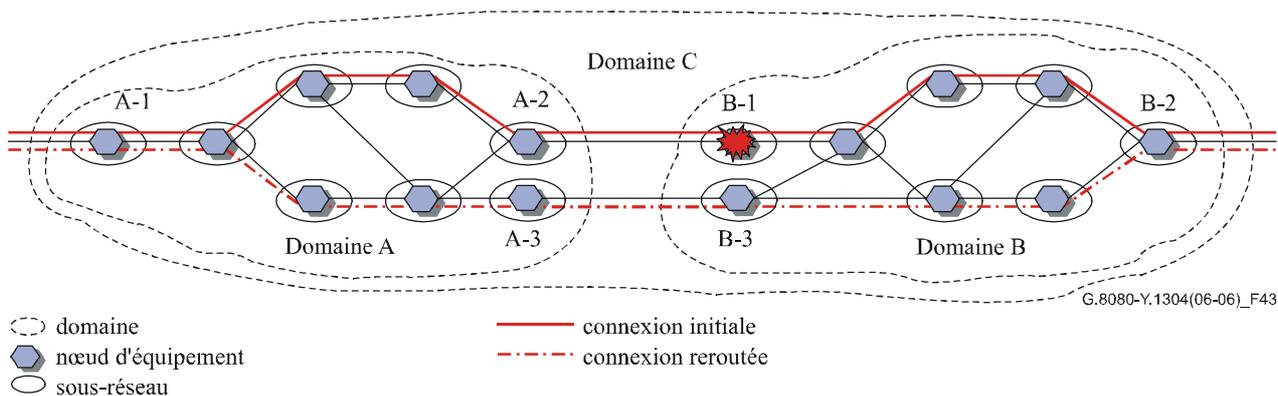


Figure 43/G.8080/Y.1304 – Reroutage en cas de panne d'élément de réseau jouant le rôle de passerelle

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).

Annexe A

Services de connexion

La commande de connectivité est essentielle pour l'exploitation d'un réseau de transport, lequel peut être décrit comme un ensemble de réseaux en couches jouant chacun le rôle d'une fonction de connexion par laquelle des associations sont créées et supprimées entre les entrées et les sorties de cette fonction. Ces associations sont appelées connexions. Trois types d'établissement de connexion sont définis:

- 1) **connexion permanente:** ce type de connexion est établi par préconfiguration de chaque élément de réseau sur le trajet avec les informations requises pour établir une connexion de bout en bout. La préconfiguration est assurée soit au moyen de systèmes de gestion soit par intervention manuelle. Lorsqu'un système de gestion de réseau est utilisé, l'accès à un modèle du réseau enregistré dans une base de données est normalement nécessaire pour établir d'abord la route la plus appropriée puis pour envoyer des commandes aux éléments de réseau qui assurent la connexion. Ce type de connexion est appelé connexion permanente physique. Voir Figure A.1. Il convient de noter que les connexions permanentes ne sont pas décrites par l'architecture G.8080/Y.1304;

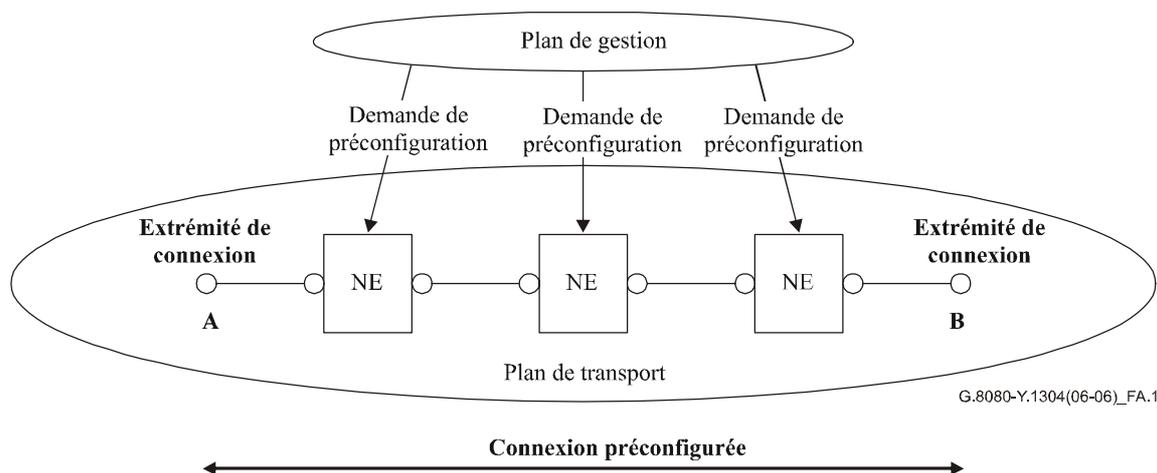


Figure A.1/G.8080/Y.1304 – Exemple d'établissement de connexion de transport de bout en bout par préconfiguration dans le plan de gestion

- 2) **connexion commutée (SC):** ce type de connexion est établi sur demande par les extrémités communicantes dans le plan de commande au moyen d'un échange de messages protocolaires contenus dans des messages de signalisation. Ces messages traversent l'interface I-NNI ou E-NNI contenue dans le plan de commande. Ce type de connexion est appelé connexion commutée. Ces connexions nécessitent des systèmes de nommage et d'adressage ainsi que des protocoles de plan de commande. Voir Figure A.2;

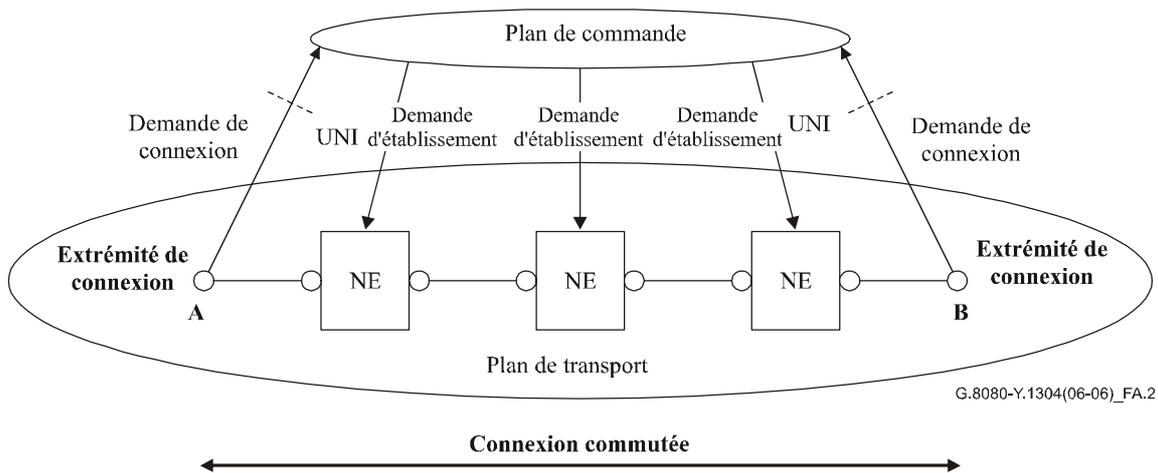


Figure A.2/G.8080/Y.1304 – Exemple d'établissement de connexion de transport de bout en bout au moyen de la signalisation dans le plan de commande (connexion commutée de A à B)

- 3) **connexion permanente reconfigurable (SPC):** dans ce type d'établissement de connexion, un réseau fournit à ses frontières des connexions permanentes et utilise en interne des connexions commutées afin d'établir des connexions de bout en bout entre ces connexions permanentes établies à ses frontières. Les connexions sont établies au moyen de protocoles de signalisation et de routage produits par le réseau. L'établissement de telles connexions dépend de la définition d'une interface NNI. La préconfiguration n'est donc nécessaire que pour les connexions périphériques. Aucune interface UNI n'est définie. Ce type de connexion de réseau est appelé connexion permanente reconfigurable (SPC). Vue par les extrémités, une connexion permanente reconfigurable ne paraît pas différente d'une connexion permanente préconfigurée et commandée par la gestion du réseau. Voir Figure A.3.

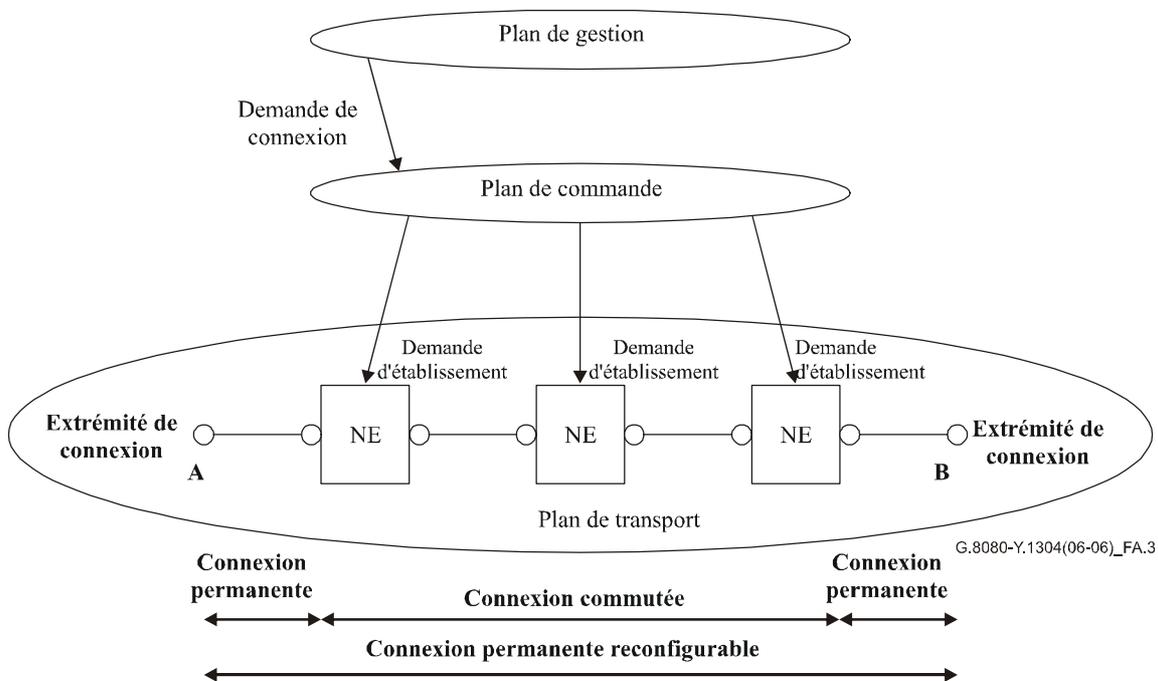


Figure A.3/G.8080/Y.1304 – Exemple d'établissement de connexion de transport de bout en bout sous forme de connexion permanente reconfigurable (SPC)

La différence la plus notable entre les trois méthodes ci-dessus concerne le correspondant qui établit la connexion. Dans le cas de la préconfiguration, l'établissement de la connexion relève de la responsabilité de l'opérateur du réseau alors que dans le cas de la signalisation, l'établissement de la connexion peut également relever de la responsabilité de l'utilisateur final. Par ailleurs, la signalisation par tierce partie devrait être prise en charge de part et d'autre d'une interface UNI.

NOTE 1 – Le type de connexion peut avoir une incidence sur les futurs systèmes de facturation.

Le plan de commande doit prendre en charge soit une connexion commutée (SC) soit une connexion permanente reconfigurable (SPC) selon la capacité du réseau de transport en termes de connexion de base. Les types de capacité de connexion sont les suivants:

- connexion point à point unidirectionnelle;
- connexion point à point bidirectionnelle;
- connexion point à multipoint unidirectionnelle.

NOTE 2 – Un autre type de connexion peut être envisagé: une connexion asymétrique, qui peut être établie sur la base de deux connexions point à point unidirectionnelles ayant des propriétés différentes dans chaque sens, ou en tant que cas particulier d'une connexion bidirectionnelle.

La fonction d'une interface UNI est de transmettre des messages de signalisation directement à l'entité du plan de commande du réseau. En variante, lorsqu'un opérateur de réseau dispose déjà d'importants systèmes de gestion installés qui assurent l'attribution et l'autoconfiguration selon une planification, ces messages de signalisation peuvent être transmis directement aux agents du système de gestion du service et de gestion du réseau afin qu'ils effectuent l'établissement des connexions. Une telle application permettra de fournir des services automatisés en temps quasi réel à partir des plates-formes de gestion existantes.

Appendice I

Réseaux de couche ASON

Le réseau optique à commutation automatique peut être utilisé pour des réseaux de couche. Le Tableau I.1 donne des exemples de réseaux de couche définis dans d'autres Recommandations de l'UIT-T. Le réseau ASON peut également être utilisé pour d'autres réseaux de couche avec prise en charge de charges utiles virtuellement caractérisées.

Tableau I.1/G.8080/Y.1304 – Réseaux de couche SDH, OTN et PDH

| | | | |
|----------------------|-------------------|-----------------------------------|-----------------------------------|
| SDH | Chemin LOVC | VC-11 | |
| | | VC-12 | |
| | | VC-2 | |
| | | VC-3 | |
| | Chemin HOVC | VC-4 | |
| | | VC-4-4c | |
| | | VC-4-16c | |
| | | VC-4-64c | |
| | | VC-4-256c | |
| | Section | MSn, n = 1, 4, 16, 64, 256 | |
| | | RSn, n = 1, 4, 16, 64, 256 | |
| | | ES1 OSn, n = 1, 4, 16, 64, 256 | |
| | | sSTM-1k, k = 1, 2, 4, 8, 16 | |
| sSTM-2n, n = 1, 2, 4 | | | |
| E31/P31s | | | |
| E4/P4s | | | |
| OTN | Chemin numérique | ODU1 | |
| | | ODU2 | |
| | | ODU3 | |
| | Section numérique | OTUk, k = 1, 2, 3 | |
| | Chemin optique | OCh | |
| | Section | OMSn | |
| OTSn | | | |
| OPSn | | | |
| PDH | Chemin | P11x, P11s | |
| | | P12x, P12s | |
| | | P21x | |
| | | P22x, P22e | |
| | | P31x, P31e | |
| | | P32x, P32 | |
| | | P4x, P4e | |
| | | Section | Eq, q = 11, 12, 21, 22, 31, 32, 4 |

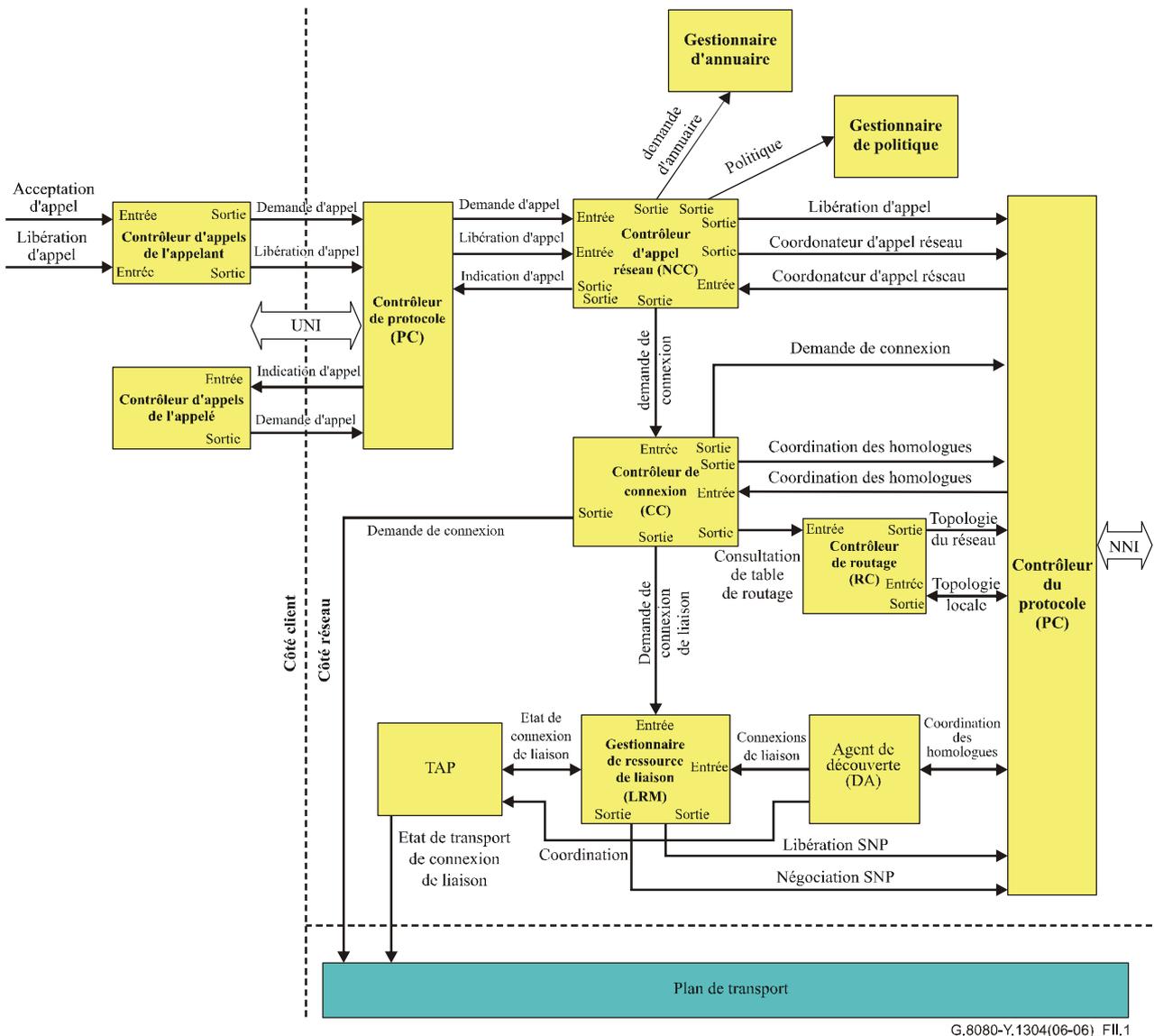
Appendice II

Exemples d'implémentation

L'architecture des réseaux optiques à commutation automatique est définie en termes de diverses fonctions.

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. Un autre exemple est présenté dans la Figure III.1.



G.8080-Y.1304(06-06)_FII.1

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

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.

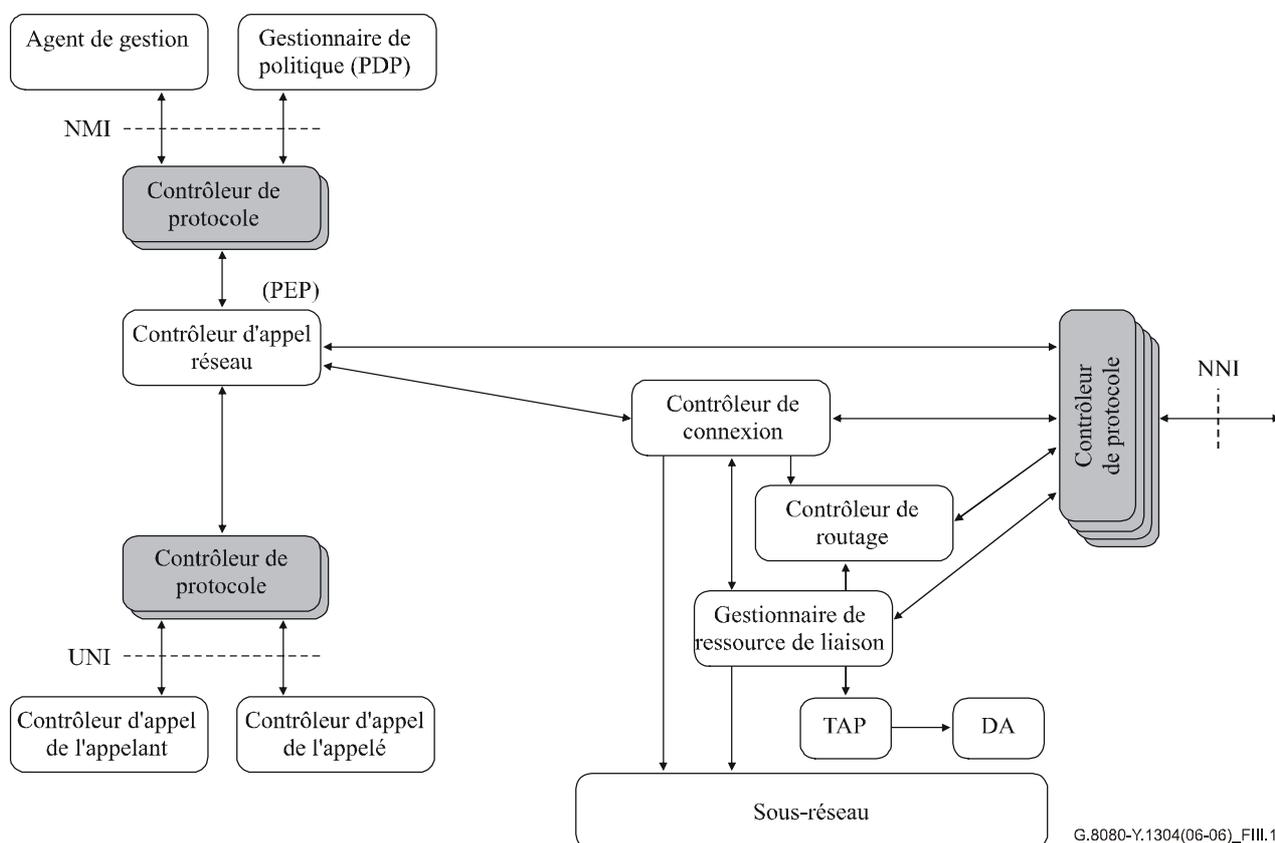


Figure III.1/G.8080/Y.1304 – Composants du plan de commande (interprétation)

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 abordées 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.2.2.1 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.2.3 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 § 12.1, 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.

Appendice IV

Exemple de commande d'appel intercouche

La Figure IV.1 illustre le cas d'un modèle mappé avec 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. La décision du contrôleur NCCMAC d'appeler le contrôleur NCCVC-3 correspondant est dictée par la politique de l'opérateur. 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 NCCMAC commence à exister.

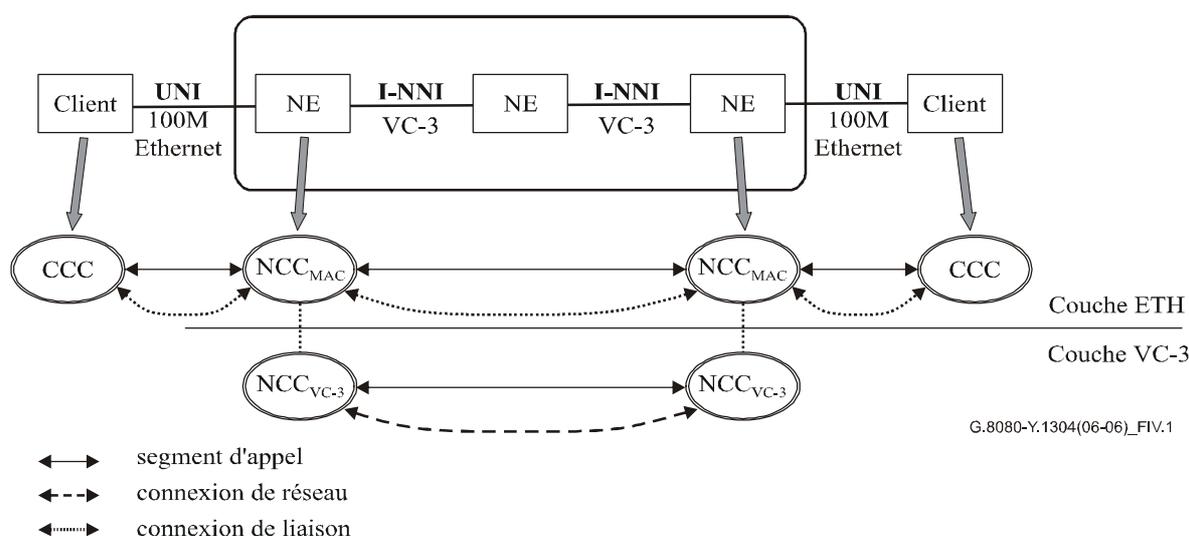


Figure IV.1/G.8080/Y.1304 – Exemple de Ethernet sur VC-3

Dans la séquence d'événements, il n'y a 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. L'association de la connexion VC-3 à l'appel Ethernet demandé est également déclenchée par la politique de l'opérateur.

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

Appendice V

Interactions de composants pour l'établissement de connexions

Le paragraphe 7.1 indique que les composants "contrôleur" sont des entités abstraites qui peuvent être implémentées sous la forme d'une entité unique, ou d'un ensemble d'entités réparties constituant une fédération coopérative. Toutefois, pour la clarté de notre propos, les exemples figurant dans le présent Appendice indiquent des méthodes d'implémentation potentielles dans lesquelles les composants représentés sont, non pas des entités abstraites, mais des instances spécifiques de code d'implémentation. En particulier:

- les contrôleurs d'appel réseau sont représentés sous la forme d'une fédération coopérative répartie;
- les contrôleurs de routage sont représentés dans une fédération coopérative répartie;
- les contrôleurs de connexion sont représentés sous la forme d'une seule entité servant de matrice;
- les gestionnaires LRM sont représentés sous forme d'une seule entité prenant en charge toutes les extrémités de liaison pour une matrice.

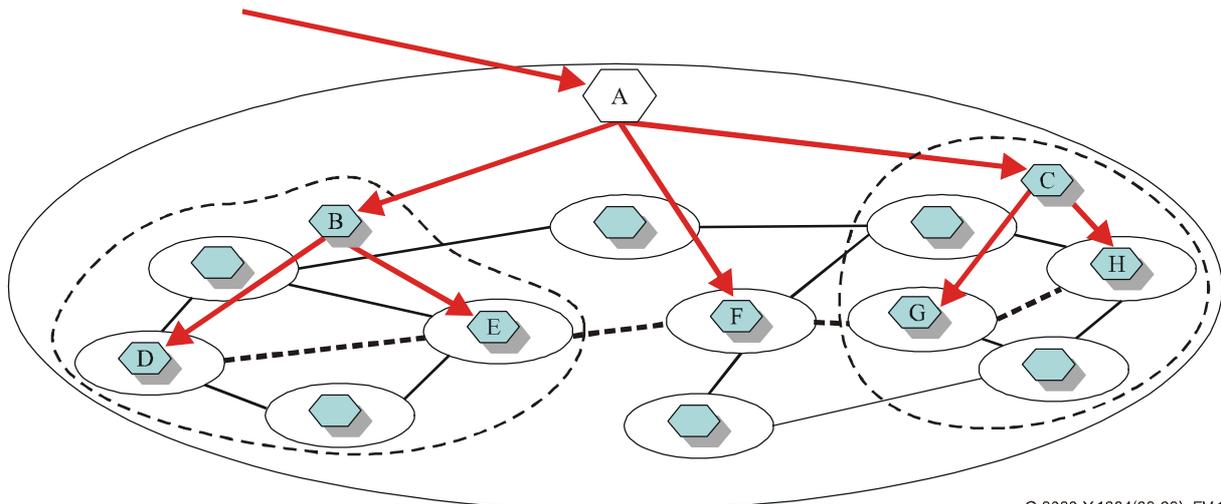
Dans certains exemples, une case ombrée est utilisée pour représenter les frontières de la fédération coopérative répartie qui constituent une entité abstraite.

La commande d'une connexion nécessite l'interaction d'un certain nombre de composants.

On peut distinguer trois formes de base pour les algorithmes de commande d'itinéraire dynamique, à savoir le routage hiérarchique, le routage par la source et le routage pas à pas; ces variantes sont décrites dans les figures qui suivent. Les diverses formes de routage conduisent à des répartitions différentes pour les composants entre les nœuds et pour les relations entre ces contrôleurs de connexion. Dans le cas où un contrôleur de routage ne dispose pas d'informations de routage suffisantes pour indiquer un itinéraire en réponse à une demande de connexion, il peut communiquer avec d'autres contrôleurs de routage en vue de résoudre l'itinéraire en utilisant l'interface de demande d'itinéraire, comme indiqué dans le § 7.3.2.

V.1 Routage hiérarchique

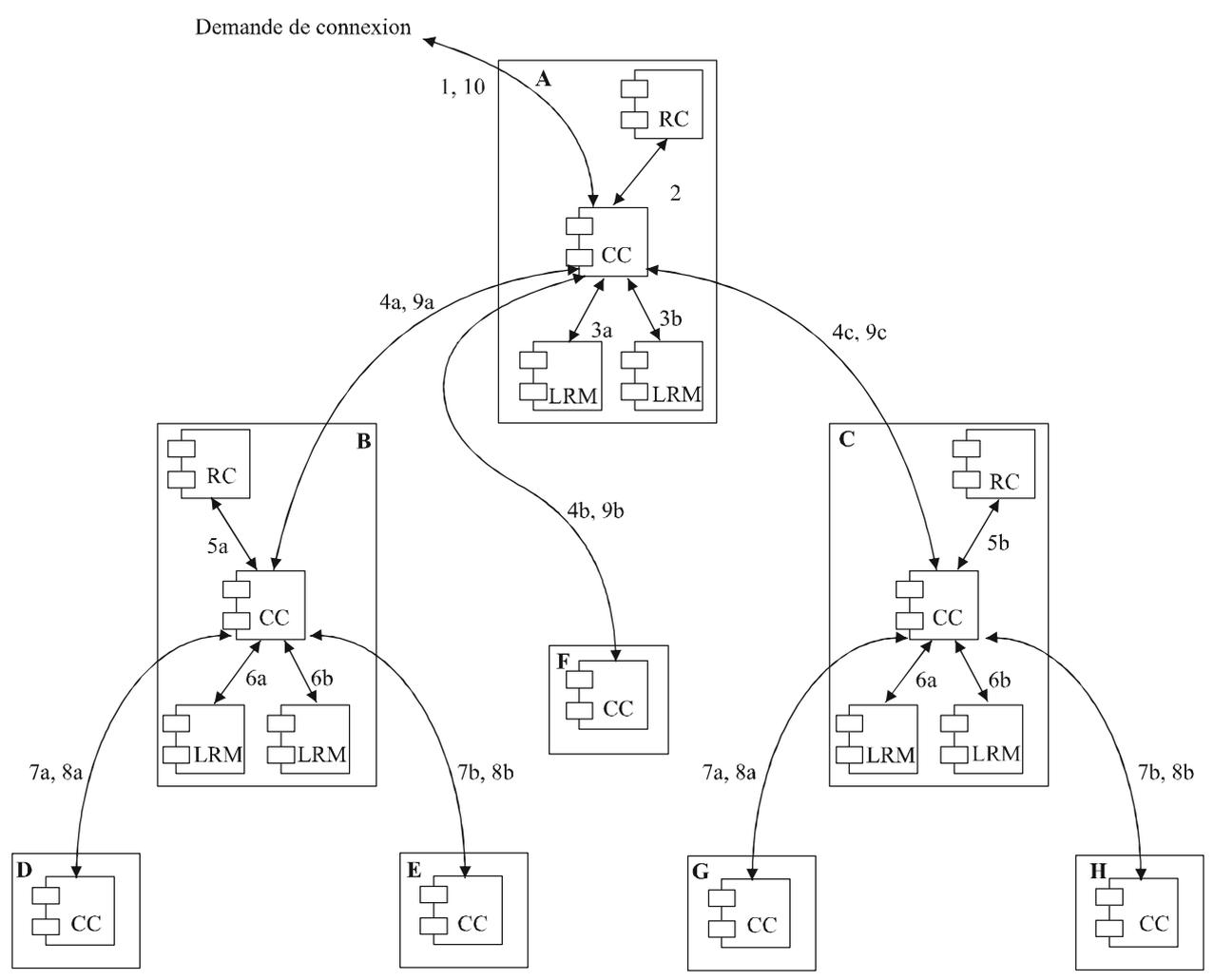
Dans le cas du routage hiérarchique décrit par la Figure V.1, un nœud contient un contrôleur de routage, des contrôleurs de connexion et des gestionnaires de ressource de liaison pour un niveau unique d'une hiérarchie de zone de routage. La décomposition des zones de routage suit la décomposition d'un réseau de couche sous la forme d'une hiérarchie de sous-réseaux (conformément aux concepts décrits par la Rec. UIT-T G.805). Les contrôleurs de connexion ont des relations hiérarchiques mutuelles. Chaque zone de routage possède sa propre commande de connexion dynamique qui connaît la topologie de sa zone de routage mais n'a aucune connaissance de la topologie des zones de routage supérieures ou inférieures dans la hiérarchie, ou d'autres zones de routage au même niveau dans la hiérarchie.



G.8080-Y.1304(06-06)_FV.1

➔ message de demande de connexion
 nœud d'équipement
 zone de routage
 - - - - - connexion établie
 sous-réseau

Figure V.1/G.8080/Y.1304 – Flux de signalisation hiérarchique



G.8080-Y.1304(06-06)_FV.2

Figure V.2/G.8080/Y.1304 – Interactions de routage hiérarchique

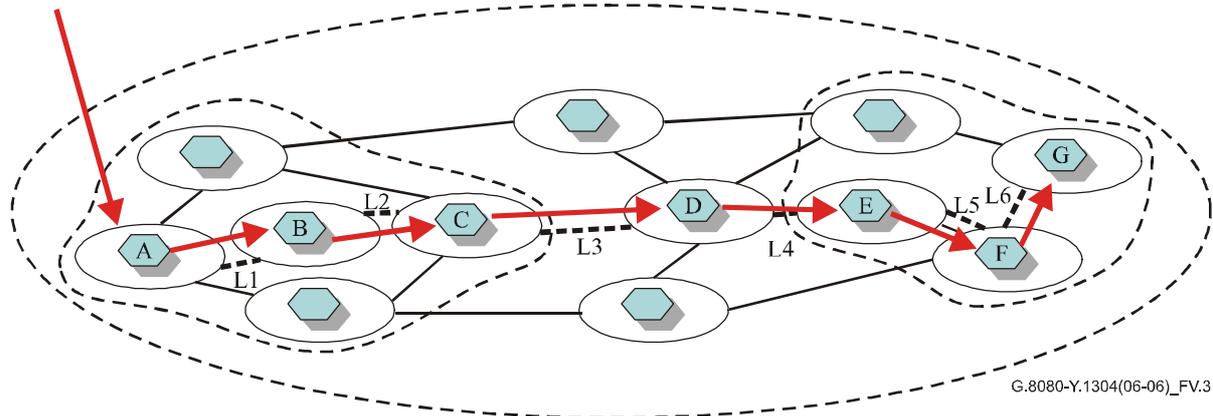
La Figure V.2 donne le détail de la succession des opérations impliquées dans l'établissement d'une connexion utilisant l'acheminement hiérarchique. Ces étapes sont les suivantes:

- 1) une demande de connexion, spécifiée sous la forme d'une paire de points SNP situés à la frontière de la zone de routage de niveau supérieur, est reçue au niveau du contrôleur de connexion (CC) en provenance de l'interface d'entrée de demande de connexion;
- 2) le contrôleur de routage (RC, *routing controller*) est interrogé (en utilisant le point SNP de l'extrémité Z sur l'interface de demande de table de montage) et renvoie l'ensemble des liaisons et des sous-réseaux impliqués;
- 3) les connexions de liaison sont fournies (dans un ordre quelconque, c'est-à-dire, 3a ou 3b dans la Figure V.2) par les gestionnaires de ressource de liaison (LRM) sur l'interface de demande de connexion de liaison;
- 4) une fois que les connexions de liaison (spécifiées sous la forme de paires de points SNP) sont connues, les connexions de sous-réseau peuvent être demandées aux zones de routage filles, en spécifiant une paire de points SNP sur l'interface d'entrée de demande de connexion et en confirmant les connexions de sous-réseau au contrôleur de connexion par le biais de l'interface de sortie de demande de connexion. L'ordre de ces opérations n'est pas déterminé, la seule contrainte étant que les connexions de liaison doivent être obtenues avant que les connexions de sous-réseau puissent être créées. Le processus initial se répète de manière récursive;
- 5) les contrôleurs de routage fils résolvent ensuite une route entre les points SNP spécifiés;
- 6) les connexions de liaison sont fournies (dans un ordre quelconque) par les gestionnaires de ressource de liaison (LRM) sur l'interface de demande de connexion de liaison;
- 7) dans l'étape finale, les commutateurs de niveau inférieur, qui ne contiennent aucun composant de routage ou d'allocation de liaison, fournissent les connexions de sous-réseau nécessaires;
- 8) les étapes restantes traitent le flux de confirmation de l'établissement des connexions, l'étape 10 renvoie la confirmation vers l'utilisateur d'origine.

V.2 Routage par la source et pas à pas

Comme pour le routage hiérarchique, le processus de commande de connexion pour le routage par la source est implémenté par une fédération répartie de contrôleurs de connexion et de routage. La différence significative est que les contrôleurs de connexion invoquent une séquence différente de fonctions de calcul de trajet entre les niveaux de routage pour le montage hiérarchique par opposition au routage par la source. La Figure V.3 présente le flux de signaux pour le routage par la source (ou pas à pas).

Afin de réduire le volume des informations de topologie réseau dont doit disposer chaque contrôleur, seule la partie de la topologie qui s'applique à sa propre zone de routage est mise à la disposition d'un contrôleur.



G.8080-Y.1304(06-06)_FV.3

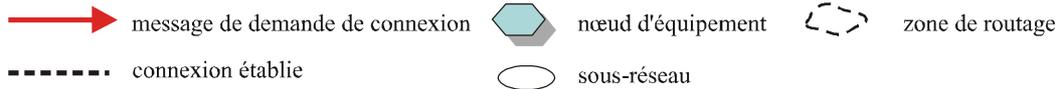
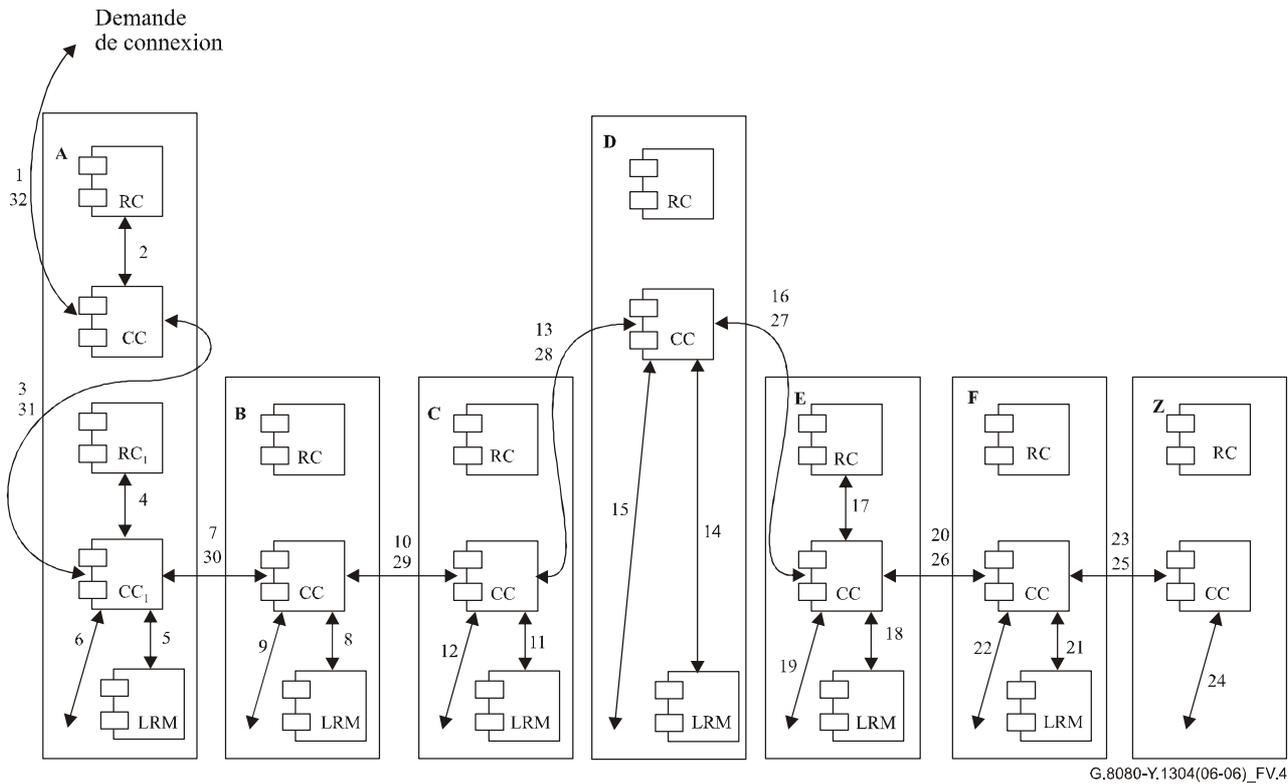


Figure V.3/G.8080/Y.1304 – Flux de signalisation par la source et pas à pas

V.2.1 Routage par la source



G.8080-Y.1304(06-06)_FV.4

Figure V.4/G.8080/Y.1304 – Interactions dans le cas de routage par la source

Les étapes qui suivent décrivent la succession des interactions présentées par la Figure V.4. Les notations suivantes seront utilisées: X_A représente le composant du niveau le plus élevé dans le nœud A et X_{An} le composant situé au niveau supérieur suivant de rang n dans le nœud A.

- 1) Une demande de connexion, spécifiée sous la forme d'une paire de noms (A et Z) situés à la frontière du sous-réseau, est reçue au niveau du contrôleur de connexion (CC_A) en provenance de l'interface d'entrée de demande de connexion.

- 2) Le contrôleur de routage (RC_A) est interrogé (en utilisant le point SNP de l'extrémité Z sur l'interface de demande de table de routage) et renvoie l'itinéraire (A, L3, L4, Z).
- 3) Comme le contrôleur CC_A ne peut pas accéder au gestionnaire de ressource de liaison (LRM_C) adéquat, la demande (A, L3, L4, Z) est transmise à un contrôleur CC_{A1} homologue (sur l'interface de sortie/d'entrée de demande de connexion), qui est en charge de cette zone de routage.
- 4) Le contrôleur CC_{A1} envoie au contrôleur RC_{A1} (sur l'interface de demande d'itinéraire) une demande pour la liaison L3 et obtient une liste de liaisons supplémentaires L1 et L2.
- 5) Une connexion de liaison est obtenue du gestionnaire LRM_A , sur l'interface de demande de connexion de liaison, pour la liaison L1 qui est locale pour ce nœud.
- 6) La connexion SNC est fournie par le commutateur local (le contrôleur n'est pas représenté).
- 7) La demande, qui contient maintenant le restant de la route (L2, L3, L4 et Z) est transmise vers le contrôleur homologue CC_B suivant (sur l'interface de sortie/d'entrée de coordination homologue).
- 8) Le gestionnaire LRM_B est en charge de la liaison L2, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 9) La connexion SNC est fournie par le commutateur local (le contrôleur n'est pas représenté).
- 10) La demande, qui contient maintenant le restant de la route (L3, L4 et Z) est transmise vers le contrôleur homologue suivant CC_C (sur l'interface de sortie/d'entrée de coordination homologue).
- 11) Le gestionnaire LRM_C est en charge de la liaison L3, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 12) La connexion SNC est assurée par le commutateur local (le contrôleur n'est pas représenté).
- 13) La demande, qui contient maintenant le restant de la route (L4, Z) est transmise vers le contrôleur homologue suivant CC_D (sur l'interface de sortie/d'entrée de coordination homologue).
- 14) Le gestionnaire LRM_D est en charge de la liaison L4, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 15) La connexion SNC est assurée par le commutateur local (le contrôleur n'est pas représenté).
- 16) La demande, qui contient maintenant le restant de la route (Z) est transmise au contrôleur homologue suivant CC_E (sur l'interface de sortie/d'entrée de coordination homologue).
- 17) Le contrôleur CC_E demande la destination Z au contrôleur RC_E (sur l'interface de demande de table de routage) et obtient les liaisons L5 et L6.

Le processus de connexion à travers la zone de routage suivante (c'est-à-dire, les étapes 18 à 24 de la Figure V.4) est identique au précédent. Les événements 25 à 32 représentent le flux de signaux de confirmation à destination de l'origine de la connexion.

V.2.2 Routage pas à pas

Cette forme de routage réduit encore plus les informations de routage contenues dans les nœuds, ce qui impose des limitations à la recherche de route à travers le sous-réseau. La Figure V.5 fait référence au diagramme de réseau représenté par la Figure V.3.

Le processus de routage pas à pas est identique à celui du routage par la source avec les variantes suivantes. Le contrôleur de routage RC_{A1} peut fournir uniquement la liaison L1 mais non la liaison L2. Le contrôleur CC_B doit demander ensuite la liaison L2 au contrôleur RC_B (par le biais de l'interface de demande de table de routage). Le même processus de demande d'une liaison à la fois se poursuit à travers la deuxième zone de routage.

- 1) Une demande de connexion, spécifiée sous la forme d'une paire de noms (A et Z) situés à la frontière du sous-réseau, est reçue au niveau du contrôleur de connexion (CC_A) en provenance de l'interface d'entrée de demande de connexion.
- 2) Le contrôleur de routage (RC_A) est interrogé (en utilisant le point SNP de l'extrémité Z sur l'interface de demande de table de routage) et renvoie la liaison de sortie L3.
- 3) Comme le contrôleur CC_A ne peut pas accéder au gestionnaire de ressource de liaison (LRM_C) adéquat, la demande (A, L3, Z) est transmise à un contrôleur CC_{A1} homologue (sur l'interface de sortie/d'entrée de demande de connexion) qui est en charge de cette zone de routage.
- 4) Le contrôleur CC_{A1} envoie au contrôleur RC_{A1} (sur l'interface de demande d'itinéraire) une demande pour la liaison L3 et obtient la liaison L1.
- 5) Une connexion de liaison est obtenue du gestionnaire LRM_A , sur l'interface de demande de connexion de liaison, pour la liaison L1 qui est locale pour ce nœud.
- 6) La connexion SNC est fournie par le commutateur local (le contrôleur n'est pas représenté).
- 7) La demande, qui contient maintenant le restant de la route (L3 et Z) est transmise vers le contrôleur homologue CC_B suivant (sur l'interface de sortie/d'entrée de coordination homologue).
- 8) Le contrôleur CC_{B1} envoie au contrôleur RC_{B1} (sur l'interface de demande d'itinéraire) une demande pour la liaison L3 et obtient la liaison L2.
- 9) Le gestionnaire LRM_B est en charge de la liaison L2, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 10) La connexion SNC est fournie par le commutateur local (le contrôleur n'est pas représenté).
- 11) La demande, qui contient maintenant le restant de la route (L3 et Z) est transmise vers le contrôleur homologue suivant CC_C (sur l'interface de sortie/d'entrée de coordination homologue).
- 12) Le gestionnaire LRM_C est en charge de la liaison L3, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 13) La connexion SNC est assurée par le commutateur local (le contrôleur n'est pas représenté).
- 14) La demande, qui contient maintenant le restant de la route (Z) est transmise vers le contrôleur homologue suivant CC_D (sur l'interface de sortie/d'entrée de coordination homologue).
- 15) Le contrôleur CC_D demande la destination Z au contrôleur RC_D (sur l'interface de demande d'itinéraire) et obtient la liaison L4.
- 16) Le gestionnaire LRM_D est en charge de la liaison L4, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 17) La connexion SNC est assurée par le commutateur local (le contrôleur n'est pas représenté).
- 18) La demande, qui contient maintenant le restant de la route (Z) est transmise au contrôleur homologue suivant CC_E (sur l'interface de sortie/d'entrée de coordination homologue).
- 19) Le contrôleur CC_E demande la destination Z au contrôleur RC_E (sur l'interface de demande d'itinéraire) et obtient la liaison L5.
- 20) Le gestionnaire LRM_E est en charge de la liaison L5, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 21) La connexion SNC est assurée par le commutateur local (le contrôleur n'est pas représenté).

- 22) La demande, qui contient maintenant le restant de la route (Z) est transmise vers le contrôleur homologue suivant CC_F (sur l'interface de sortie/d'entrée de coordination homologue).
- 23) Le contrôleur CC_F demande la destination Z au contrôleur RC_F (sur l'interface de demande d'itinéraire) et obtient la liaison L6.
- 24) Le gestionnaire LRM_F est en charge de la liaison L6, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 25) La connexion SNC est assurée par le commutateur local (le contrôleur n'est pas représenté).

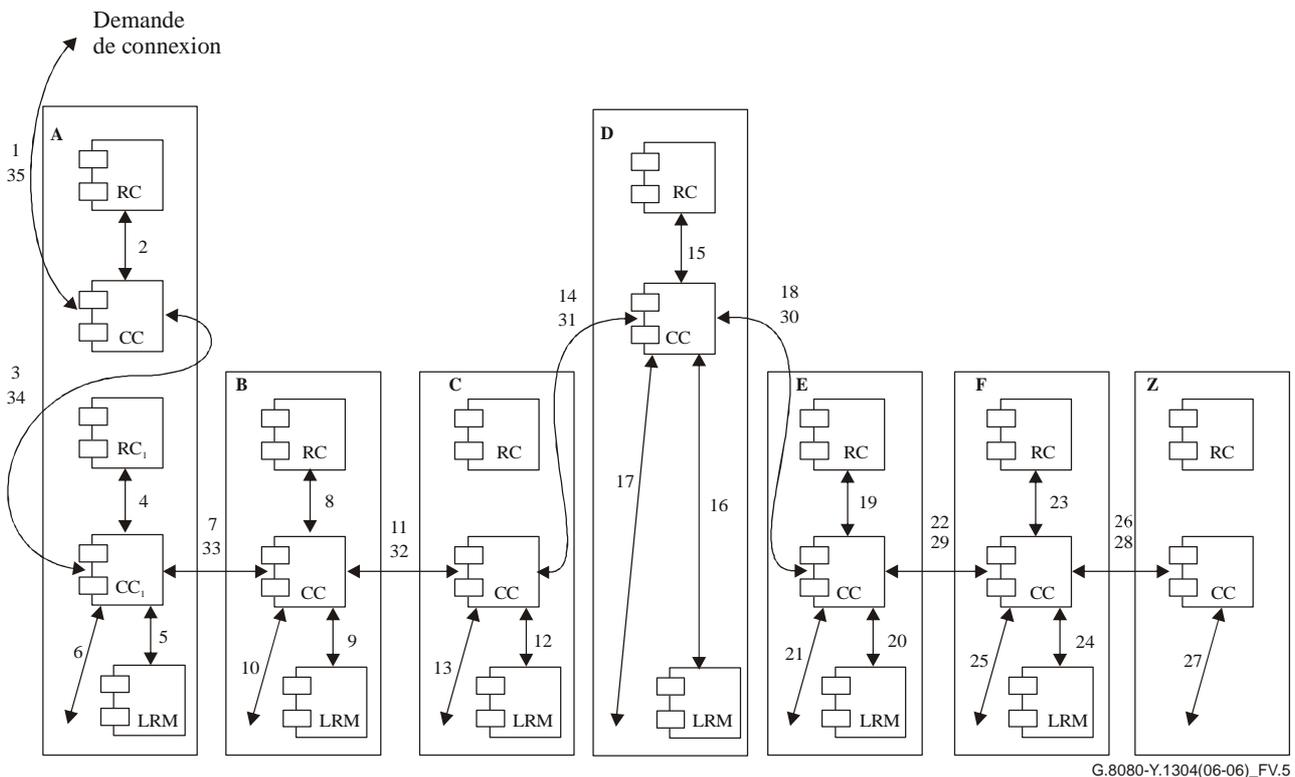
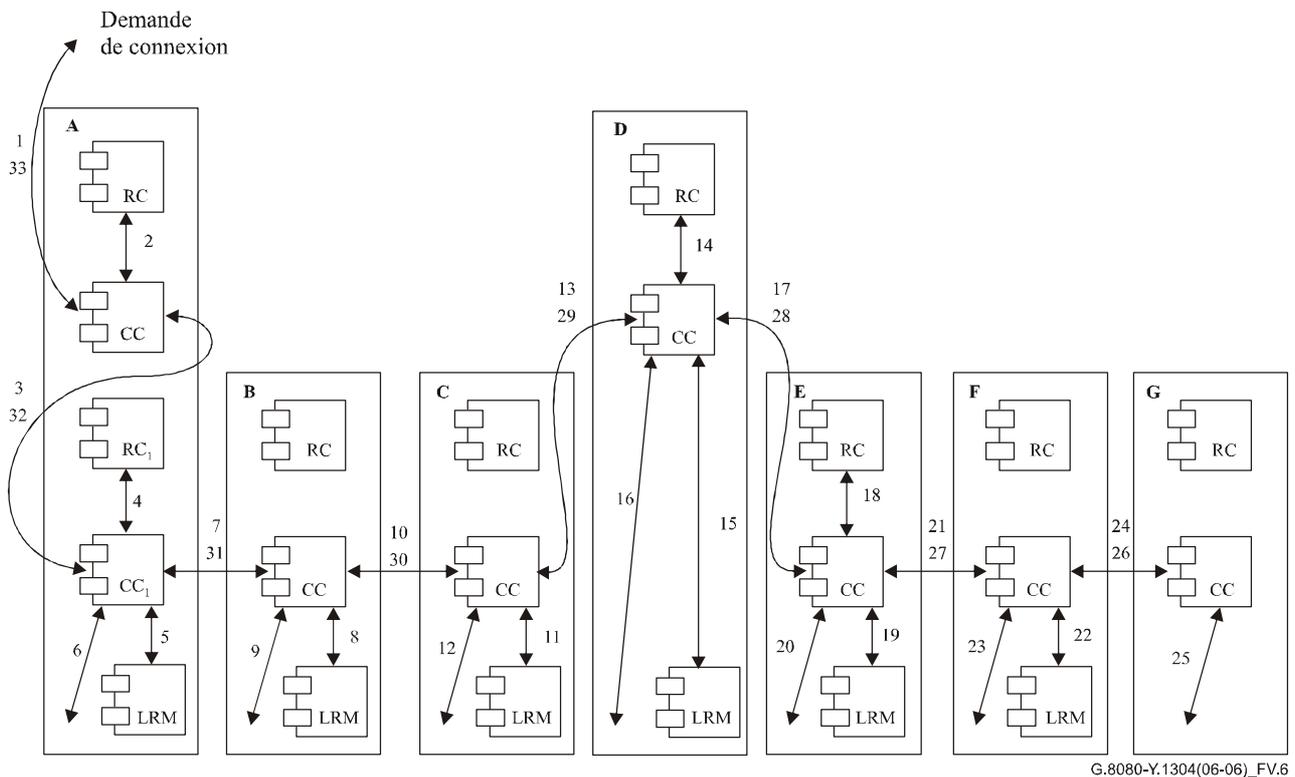


Figure V.5/G.8080/Y.1304 – Routage pas à pas

V.2.3 Utilisation conjuguée du routage par la source et du routage pas à pas

La Figure V.6 illustre un exemple dans lequel le routage par la source et le routage pas à pas peuvent être utilisés ensemble, mais à des niveaux de routage différents, est présenté ci-dessous. Dans cet exemple, le routage de niveau inférieur est le routage par la source, le routage de niveau supérieur étant le routage pas à pas.



G.8080-Y.1304(06-06)_FV.6

Figure V.6/G.8080/Y.1304 – Utilisation conjuguée du routage par la source et du routage pas à pas

- 1) Une demande de connexion, spécifiée sous la forme d'une paire de noms (A et Z) situés à la frontière du sous-réseau, est reçue au niveau du contrôleur de connexion (CC_A) en provenance d'une interface d'entrée de demande de connexion.
- 2) Le contrôleur de routage (RC_A) est interrogé (en utilisant le point SNP de l'extrémité Z sur l'interface de demande de table de routage) et renvoie la liaison de sortie L3.
- 3) Comme le contrôleur CC_A ne peut pas accéder au gestionnaire de ressource de liaison (LRM_C) adéquat, la demande (A, L3, Z) est transmise à un contrôleur CC_{A1} homologue (sur l'interface de sortie/d'entrée de demande de connexion), qui est en charge de cette zone de routage.
- 4) Le contrôleur CC_{A1} envoie au contrôleur RC_{A1} (sur l'interface de demande de table de routage) une demande pour la liaison L3 et obtient une liste de liaisons supplémentaires L1 et L2.
- 5) Une connexion de liaison est obtenue du gestionnaire LRM_A , sur l'interface de demande de connexion de liaison, pour la liaison L1 qui est locale pour ce nœud.
- 6) La connexion SNC est fournie par le commutateur local (le contrôleur n'est pas représenté).
- 7) La demande, qui contient maintenant le restant de la route (L2, L3 et Z) est transmise vers le contrôleur homologue CC_B suivant (sur l'interface de sortie/d'entrée de coordination homologue).
- 8) Le gestionnaire LRM_B est en charge de la liaison L2, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 9) La connexion SNC est fournie par le commutateur local (le contrôleur n'est pas représenté).
- 10) La demande, qui contient maintenant le restant de la route (L3 et Z) est transmise vers le contrôleur homologue suivant CC_C (sur l'interface de sortie/d'entrée de coordination homologue).

- 11) Le gestionnaire LRM_C est en charge de la liaison L3, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 12) La connexion SNC est assurée par le commutateur local (le contrôleur n'est pas représenté).
- 13) La demande, qui contient maintenant le restant de la route (Z) est transmise vers le contrôleur homologue suivant CC_D (sur l'interface d'entrée/de sortie de coordination homologue).
- 14) Le contrôleur CC_D demande la destination Z au contrôleur RC_D (sur l'interface de demande de table de routage) et obtient la liaison L4.
- 15) Le gestionnaire LRM_D est en charge de la liaison L4, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison.
- 16) La connexion SNC est assurée par le commutateur local (le contrôleur n'est pas représenté).
- 17) La demande, qui contient maintenant le restant de la route (Z) est transmise au contrôleur homologue suivant CC_E (sur l'interface d'entrée/de sortie de coordination homologue).
- 18) Le contrôleur CC_E demande la destination Z au contrôleur RC_E (sur l'interface de demande de table de routage) et obtient les liaisons L5 et L6.

V.3 Protection de connexion

Lorsque le plan de commande est utilisé pour assurer la protection, une connexion de protection est établie pour protéger la connexion en service avant l'apparition d'une défaillance. Une fois qu'une défaillance de la connexion en service est détectée, seuls les contrôleurs de connexion d'origine et de destination sont mis en jeu pour mener à bien l'opération de commutation de protection de la connexion en service initiale à la connexion de protection.

La Figure V.7 donne un exemple de protection de connexion utilisant le routage par la source et la signalisation répartie. Le flux de signalisation de protection représenté ici a été obtenu après détection d'une défaillance de la liaison. La relation du trajet en service et du trajet de protection est censée être de 1:1. Autrement dit, le CI n'est pas transféré sur le trajet en service et sur le trajet de protection en même temps. Au lieu de cela, lorsque le trajet en service est interrompu par une défaillance de la liaison, le plan de commande est utilisé pour commuter le CI de l'utilisateur sur le trajet de protection.

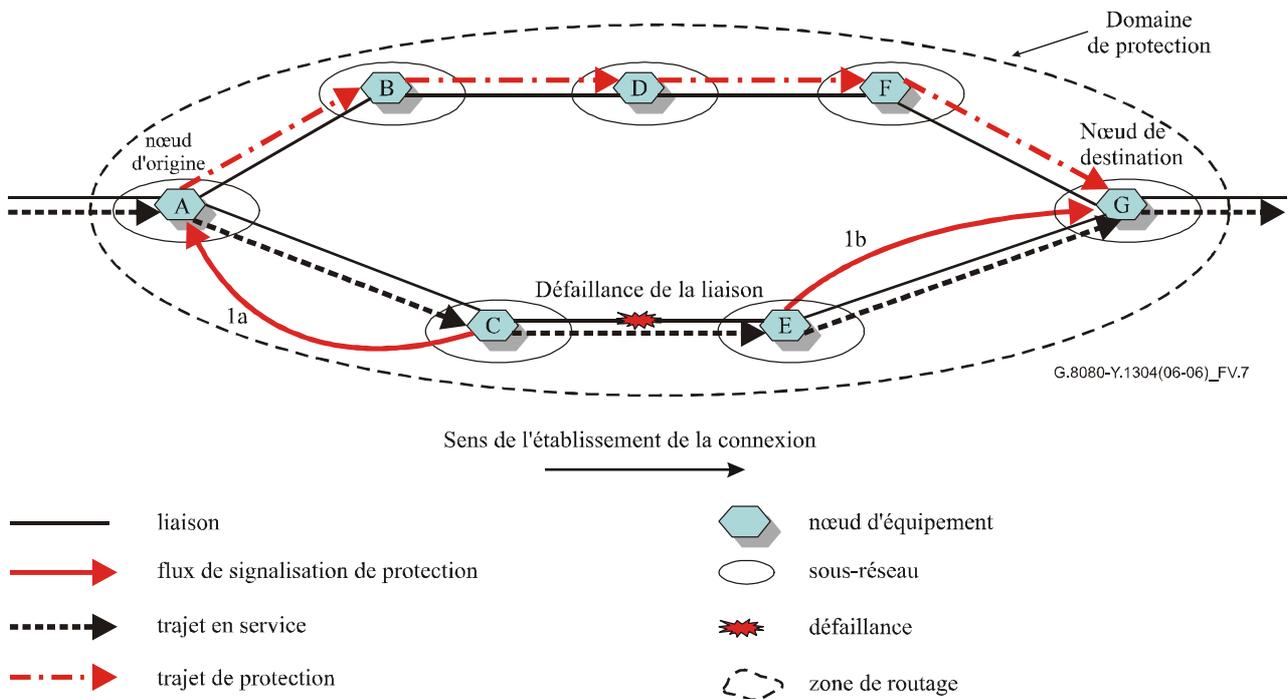


Figure V.7/G.8080/Y.1304 – Flux de signalisation de protection

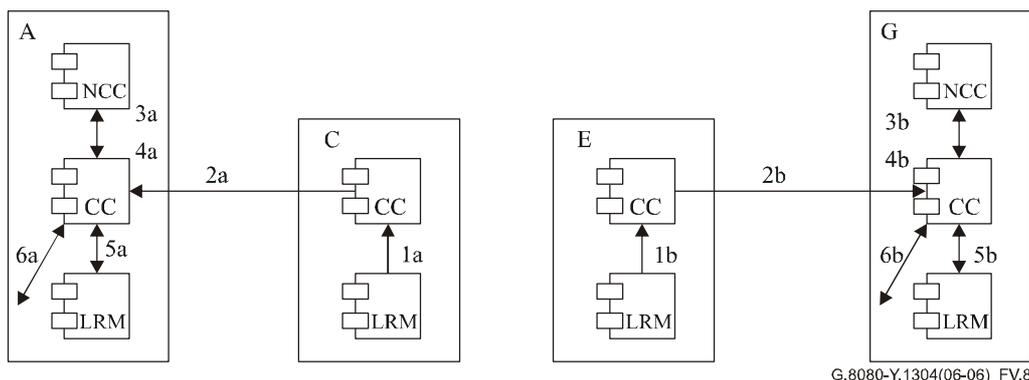


Figure V.8/G.8080/Y.1304 – Interactions de protection

La Figure V.8 donne le détail de la succession des opérations impliquées dans la protection. Ces étapes sont les suivantes:

- 1) le contrôleur de connexion (CC) reçoit une notification de défaillance de la liaison bidirectionnelle, émise par les gestionnaires de ressources de liaison (LRM), l'informant du type de défaillance. Cette notification est reçue dans le nœud E et dans le nœud C;
- 2) la notification de défaillance de la liaison est retransmise au contrôleur CC_A par le contrôleur CC_C et au contrôleur CC_G par le contrôleur CC_E ;
- 3) les contrôleurs CC_A et CC_G avertissent leurs contrôleurs d'appel réseau (NCC) de la défaillance du trajet en service;
- 4) les contrôleurs NCC adressent la demande de commutation de protection à leurs contrôleurs CC, ce qui a pour effet d'établir la connexion de sous-réseau (SNC) par commutation locale de la connexion en service à la connexion de protection.

V.4 Rétablissement – Reroutage inconditionnel – Reroutage intradomaine – Méthode hiérarchique

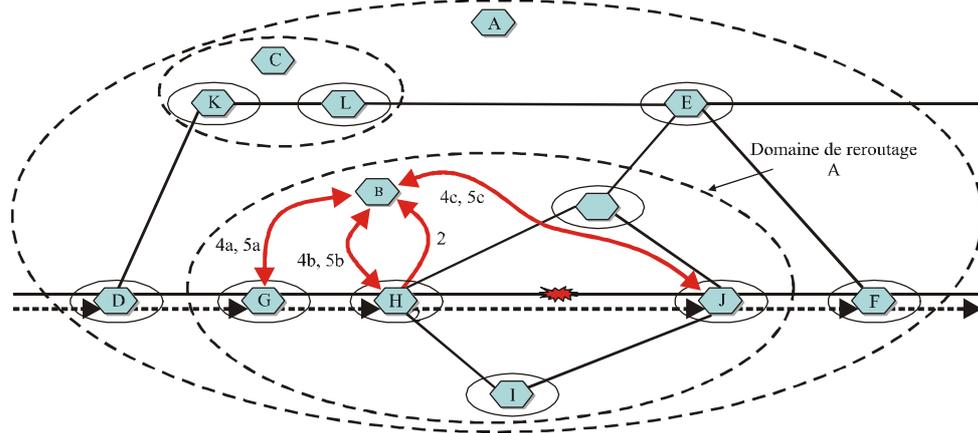
Dans le mode de reroutage inconditionnel, appelé "coupure avant rétablissement", le segment de connexion initial est libéré avant la création d'un segment de connexion de secours.

La Figure V.9 représente le cas d'un flux de signalisation pour un scénario de reroutage inconditionnel avec commande de connexion hiérarchique après détection d'une défaillance de la liaison intradomaine. Dans l'étape de la création de la connexion de reroutage, l'algorithme hiérarchique est adopté.

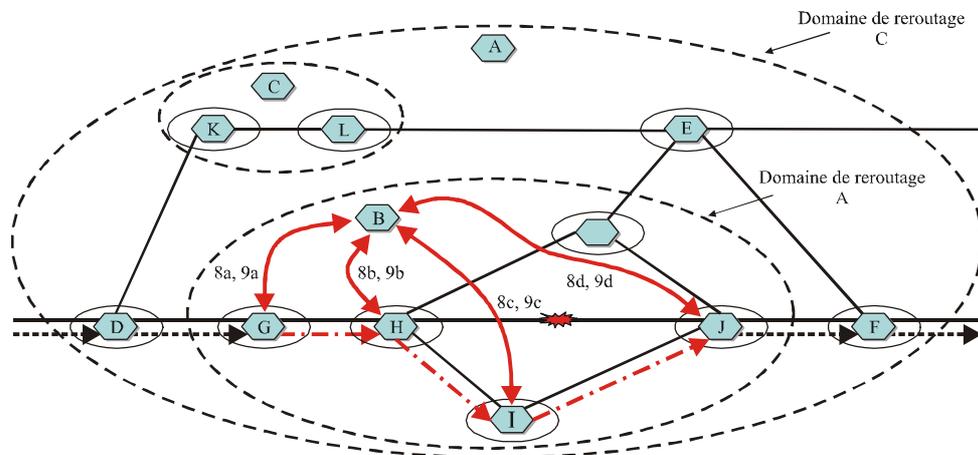
La Figure V.10 donne le détail de la succession des opérations mises en jeu dans la Figure V.9. Ces étapes sont les suivantes:

- 1) le contrôleur de connexion (CC) reçoit une notification de défaillance de la liaison intradomaine émise par les gestionnaires de ressource de liaison (LRM), contenant l'information de routage par retour en arrière qui indique la liaison en dérangement. Cette notification peut être reçue dans le nœud J ou H, ou dans les deux, selon le nœud qui détecte la défaillance de la liaison;
- 2) la notification de la défaillance de la liaison intradomaine est retransmise au contrôleur CC_B ;
- 3) les connexions de liaison sont libérées (dans un ordre quelconque, c'est-à-dire, 3a ou 3b dans la Figure V.10) par le gestionnaire LRM;
- 4) les connexions SNC sont libérées par les commutateurs du niveau le plus faible;
- 5) les confirmations de libération des connexions sont renvoyées au contrôleur CC_B ;
- 6) le contrôleur de routage (RC_B) est interrogé avec l'information de routage par retour en arrière et renvoie l'ensemble des liaisons, exception faite de la liaison en dérangement, et des sous-réseaux impliqués;
- 7)-9) les étapes 7 à 9 décrivent le flux d'établissement des connexions au moyen de l'algorithme hiérarchique, qui est identique à celui qui est décrit au § V.1 – Routage hiérarchique;
- 10) si elle a échoué à établir la connexion dans le domaine de reroutage A, l'information de routage par retour en arrière est retransmise au domaine de reroutage de niveau supérieur C;
- 11) les connexions de liaison restantes sont libérées par le gestionnaire LRM;
- 12) les connexions SNC sont libérées par les commutateurs du niveau le plus faible. Cette opération passe par la libération des nœuds G et J via le contrôleur CC_B , puis le contrôleur CC_G et le contrôleur CC_J ;
- 13) les confirmations de libération des connexions sont renvoyées au contrôleur CC_A . Ces opérations comportent la libération par le contrôleur CC_B ;
- 14) le contrôleur de routage RC_A est interrogé au moyen de l'information de routage par retour en arrière et renvoie l'ensemble des liaisons, exception faite de la liaison en dérangement, et des sous-réseaux impliqués;
- 15)-21) les étapes 15 à 21 décrivent le flux d'établissement des connexions au moyen de l'algorithme hiérarchique, qui est identique à celui qui est décrit dans le § V.1 – Routage hiérarchique;
- 22) si elle a échoué à établir la connexion dans le domaine de reroutage C, l'information de routage par retour en arrière est transmise au domaine de reroutage de niveau supérieur.

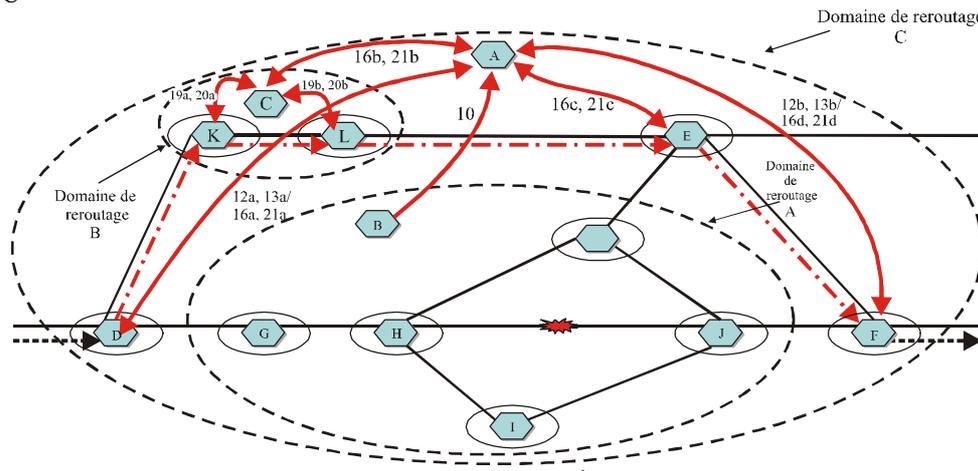
Etape 1: libération du segment de connexion initial dans le domaine de reroutage A



Etape 2: création de la connexion de reroutage dans le domaine de reroutage A



Etape 3: si l'étape 2 a échoué, retransmettre le message de reroutage par retour en arrière au domaine de reroutage de niveau supérieur C

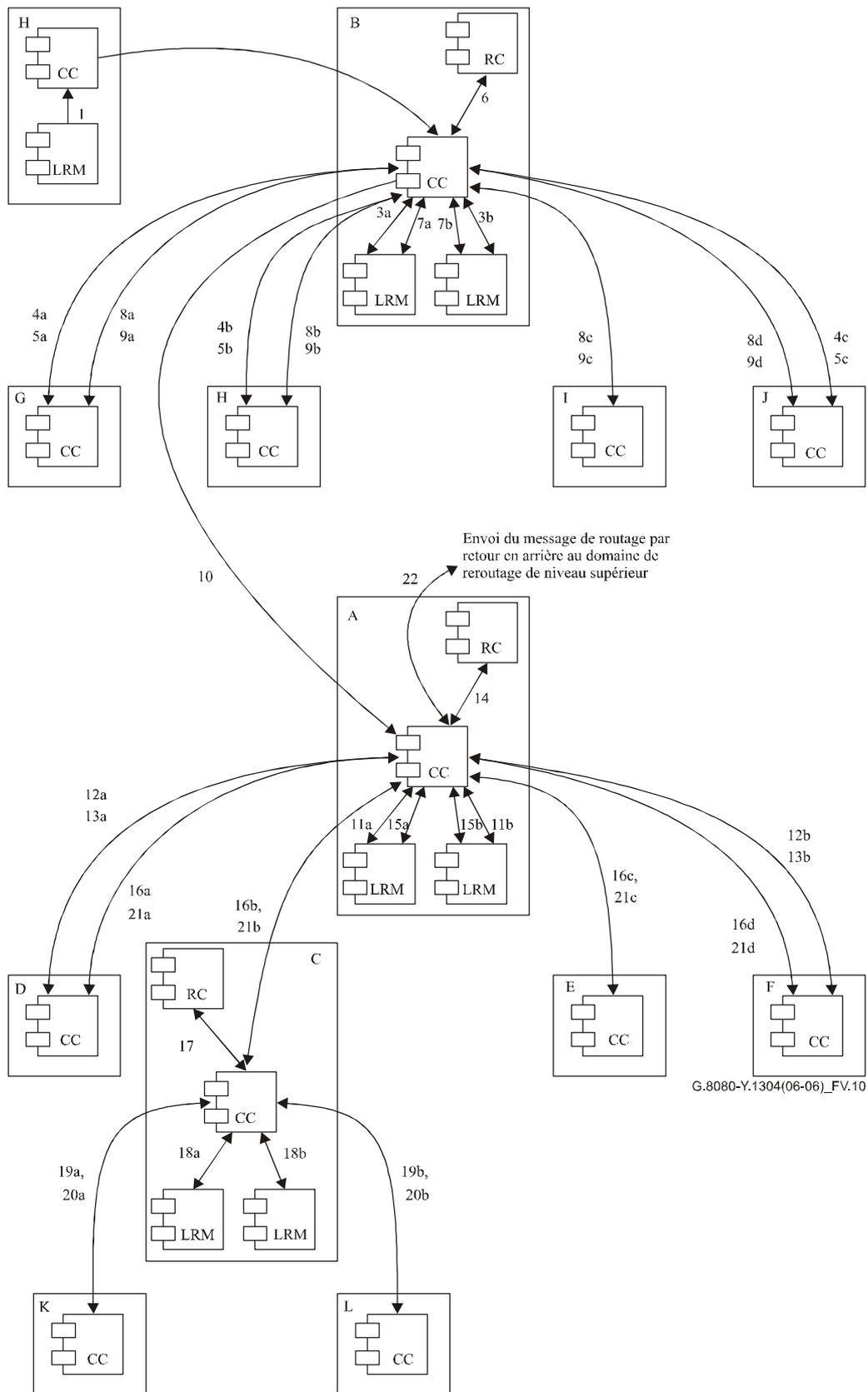


Sens d'établissement de la connexion

| | | | |
|---------------------------------------|------------------------|-------------------|-----------------|
| liaison | trajet en service | nœud d'équipement | défaillance |
| message de signalisation de reroutage | connexion de reroutage | sous-réseau | zone de routage |

G.8080-Y.1304(06-06)_FV.9

Figure V.9/G.8080/Y.1304 – Flux de signalisation du reroutage inconditionnel utilisant l'algorithme hiérarchique après défaillance de la liaison intradomaine



G.8080-Y.1304(06-06)_FV.10

Figure V.10/G.8080/Y.1304 – Interactions des composants du reroutage inconditionnel utilisant l'algorithme hiérarchique après défaillance de la liaison intradomaine

V.5 Rétablissement – Méthode de reroutage conditionnel, intradomaine ou par la source

Le service de reroutage conditionnel est un mécanisme permettant de réacheminer un appel à des fins administratives. Lorsqu'une opération de reroutage est déclenchée (généralement par l'intermédiaire d'une demande émanant du plan de gestion) et envoyée à l'emplacement des composants de reroutage, ceux-ci établissent une connexion de reroutage qui traverse (ou ne traverse pas) l'ensemble de composants désigné conformément aux fins administratives. Dans le reroutage conditionnel, qui est appelé "rétablissement avant coupure", la connexion initiale est supprimée après la création d'une connexion de reroutage.

La Figure V.11 représente le flux de signalisation d'un scénario de reroutage conditionnel avec commande de connexion de routage par la source (ou pas à pas) après réception d'une demande du plan de gestion visant à rerouter une connexion à l'exclusion d'une liaison intradomaine donnée.

La Figure V.12 donne le détail de la succession des opérations utilisant le routage par la source mises en jeu dans la Figure V.11. Ces étapes sont les suivantes:

- 1) le contrôleur de connexion (CC_G) reçoit en provenance du plan de gestion une demande indiquant les contraintes que la connexion de reroutage doit respecter. Par exemple, un itinéraire clairement établi pour la connexion de reroutage. Dans cet exemple, il y a une contrainte d'exclusion qui précise que la liaison L1 ne doit pas être utilisée dans la connexion de reroutage;
- 2a) le contrôleur de routage (RC_G) reçoit une demande d'établissement de la connexion de reroutage émanant du contrôleur de connexion CC_G et contenant la paire de points SNP à la frontière du domaine de reroutage A et la contrainte d'exclusion;
- 2b) le contrôleur RC_G renvoie l'ensemble des liaisons, exception faite de la liaison L1;
- 3-15) les étapes 3 à 15 décrivent le flux d'établissement des connexions utilisant l'algorithme de routage par la source, qui est identique à celui qui est décrit au § V.2.3 – Utilisation conjuguée du routage par la source et du routage pas à pas. La nouvelle connexion vient s'ajouter à la connexion initiale arrivant dans le domaine A aux nœuds G et J.

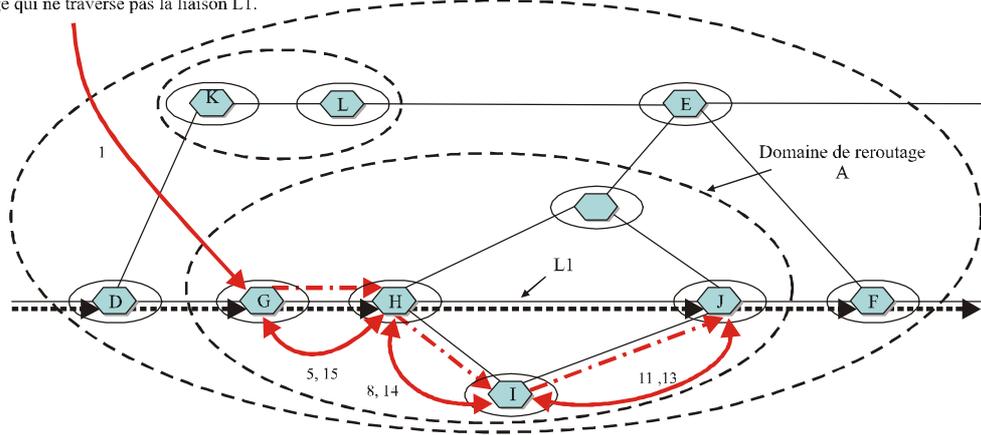
Si la connexion est établie avec succès dans le domaine de reroutage A, on applique ensuite l'étape 16a; sinon, on applique l'étape 16b.

- 16a) La connexion de liaison du trajet initial est libérée par le gestionnaire LRM_G dans l'étape 16a, qui comporte les étapes 16a1 et 16a2;
- 17) la connexion SNC est libérée par le commutateur local;
- 18) la demande de libération de connexion, qui contient l'information de connexion initiale, est retransmise au contrôleur CC_H ;
- 19) la connexion de liaison du trajet initial est libérée par le gestionnaire LRM_H ;
- 20) la connexion SNC est libérée par le commutateur local;
- 21) la demande de libération de connexion, qui contient l'information de connexion initiale, est retransmise au contrôleur CC_J ;
- 22) la connexion SNC est libérée par le commutateur local;
- 23) la confirmation de libération de connexion est renvoyée au contrôleur CC_G d'origine et le processus de reroutage est mené à bien;
- 16b) l'information de reroutage par retour en arrière est retransmise au contrôleur CC_D dans le domaine de reroutage de niveau supérieur C;
- 17a) le contrôleur de routage RC_D reçoit une demande d'établissement de connexion de reroutage émanant du contrôleur CC_D qui contient la paire de points SNP à la frontière du domaine de reroutage C et la contrainte d'exclusion pour éviter le domaine A;

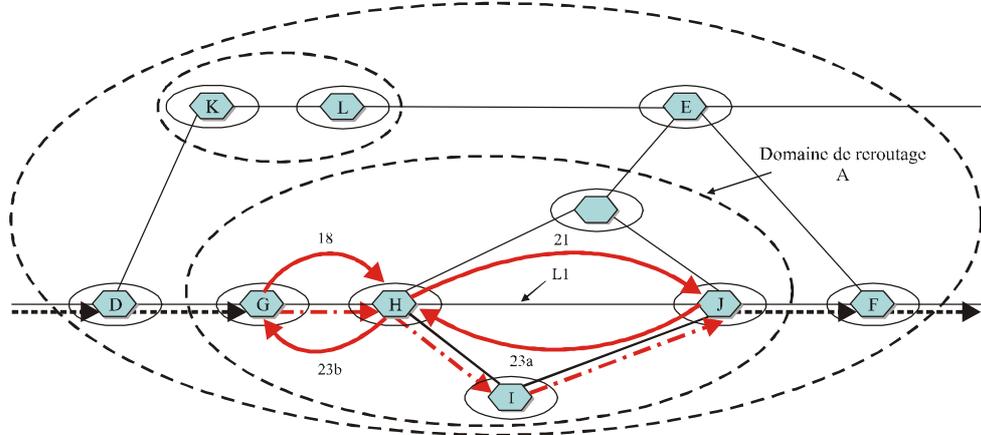
- 17b) le contrôleur de routage RC_D renvoie l'ensemble des liaisons, exception faite de celles du domaine A;
- 18-39) les étapes 18 à 39 décrivent le flux d'établissement des connexions utilisant l'algorithme de routage par la source, qui est identique à celui qui est décrit au § V.2.3 – Utilisation conjuguée du routage par la source et du routage pas à pas;
- 40) la connexion de liaison du trajet initial est libérée par le gestionnaire LRM_D durant l'étape 40 qui comporte les étapes 40a et 40b;
- 41) la connexion SNC est libérée par le commutateur local;
- 42) la demande de libération de connexion, qui contient l'information de connexion initiale, est retransmise au contrôleur CC_G ;
- 43) la connexion de liaison du trajet initial est libérée par le gestionnaire LRM_G ;
- 44) la connexion SNC est libérée par le commutateur local;
- 45) la demande de libération de connexion, qui contient l'information de connexion initiale, est retransmise au contrôleur CC_H ;
- 46) la connexion de liaison du trajet initial est libérée par le gestionnaire LRM_H ;
- 47) la connexion SNC est libérée par le commutateur local;
- 48) la demande de libération de connexion, qui contient l'information de connexion initiale, est retransmise au contrôleur CC_J ;
- 49) la connexion de liaison du trajet initial est libérée par le gestionnaire LRM_J ;
- 50) la connexion SNC est libérée par le commutateur local;
- 51) la demande de libération de connexion, qui contient l'information de connexion initiale, est retransmise au contrôleur CC_F ;
- 52) la connexion SNC est libérée par le commutateur local;
- 53) la confirmation de libération de connexion est renvoyée au contrôleur CC_D d'origine.

Etape 1: création de la connexion de reroutage dans le domaine de reroutage A

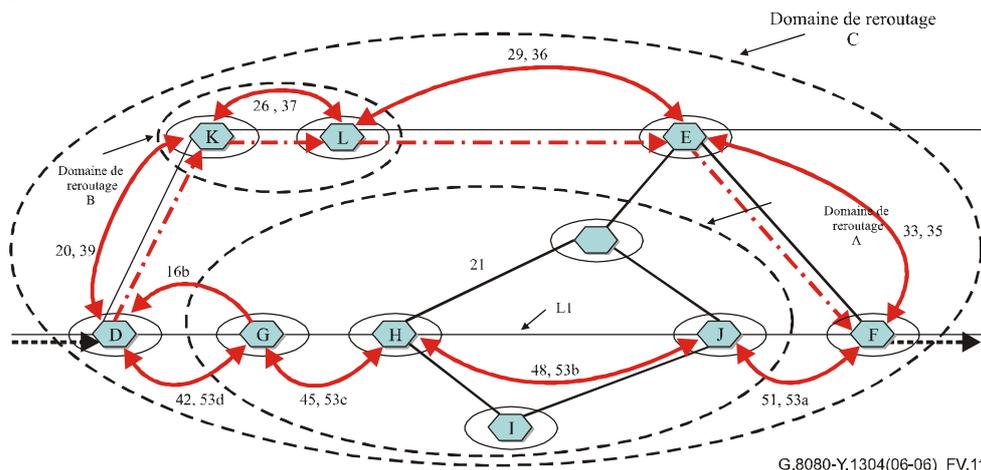
Demande de reroutage émanant du plan de gestion pour créer une connexion reroutage qui ne traverse pas la liaison L1.



Etape 2: libération du segment de connexion initial dans le domaine de reroutage A



Etape 3: si l'étape 1 a échoué, retransmettre le message de routage par retour en arrière au domaine de reroutage de niveau supérieur C



G.8080-Y.1304(06-06)_FV.11

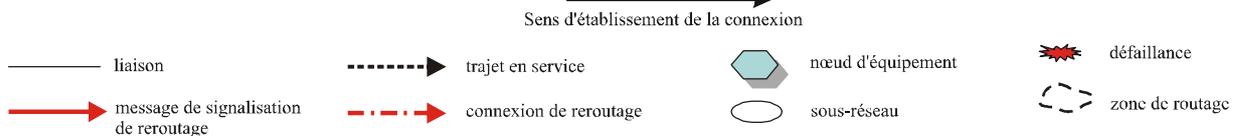
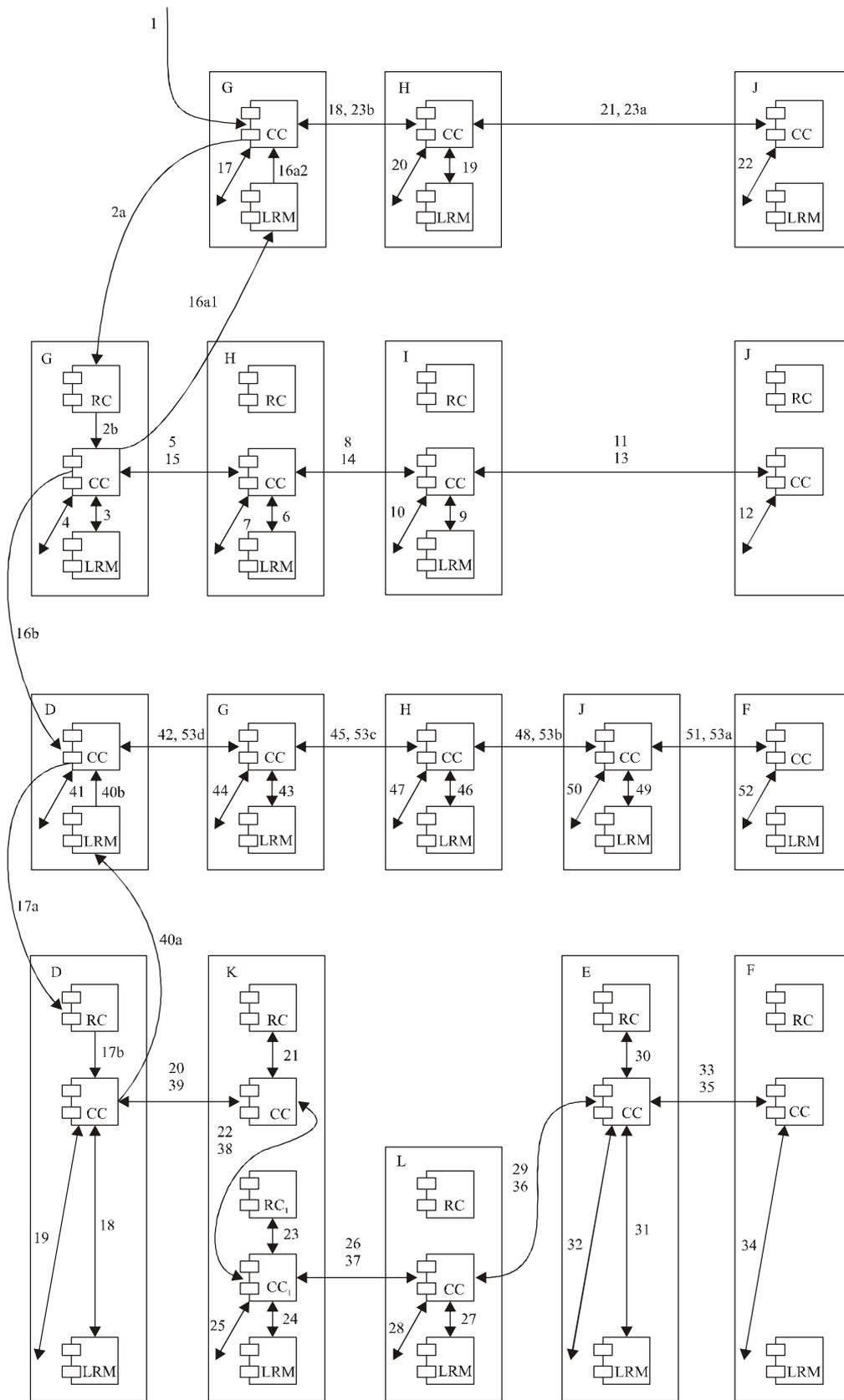


Figure V.11/G.8080/Y.1304 – Flux de signalisation de reroutage conditionnel utilisant l'algorithme de routage par la source (ou pas à pas), à l'exclusion d'une liaison intradomaine

Demande de reroutage émanant du plan de gestion
pour créer une connexion de reroutage qui ne
traverse pas la liaison L1.



G.8080-Y.1304(06-06)_FV.12

Figure V.12/G.8080/Y.1304 – Interactions des composants de reroutage conditionnel utilisant l'algorithme de routage par la source, à l'exclusion d'une liaison intradomaine

V.6 Rétablissement – Méthode de reroutage réversible, intradomaine et par la source

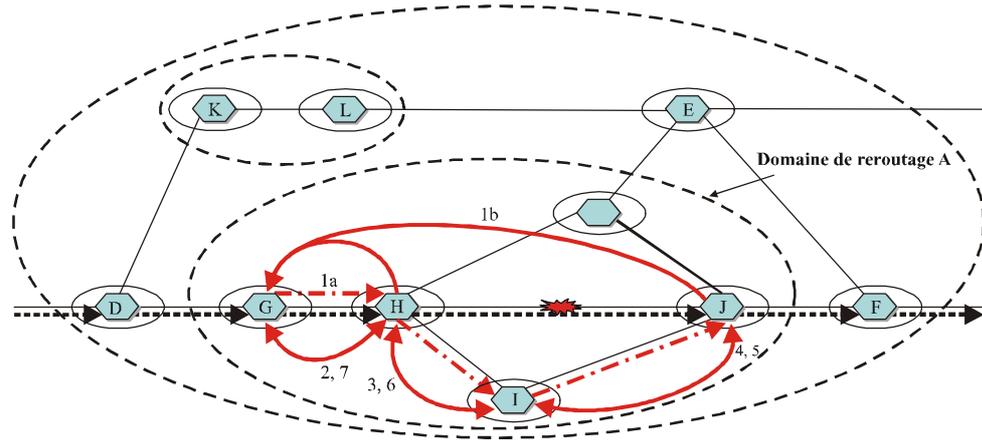
Dans le reroutage à comportement réversible, la connexion initiale ne doit pas être libérée et est surveillée par les contrôleurs d'appel réseau. Lorsque la défaillance est réparée, la communication est rétablie sur sa connexion initiale.

La Figure V.13 représente le flux de signalisation pour un scénario de reroutage à comportement réversible avec commande de connexion de routage par la source (ou pas à pas) après détection d'une défaillance d'une liaison intradomaine.

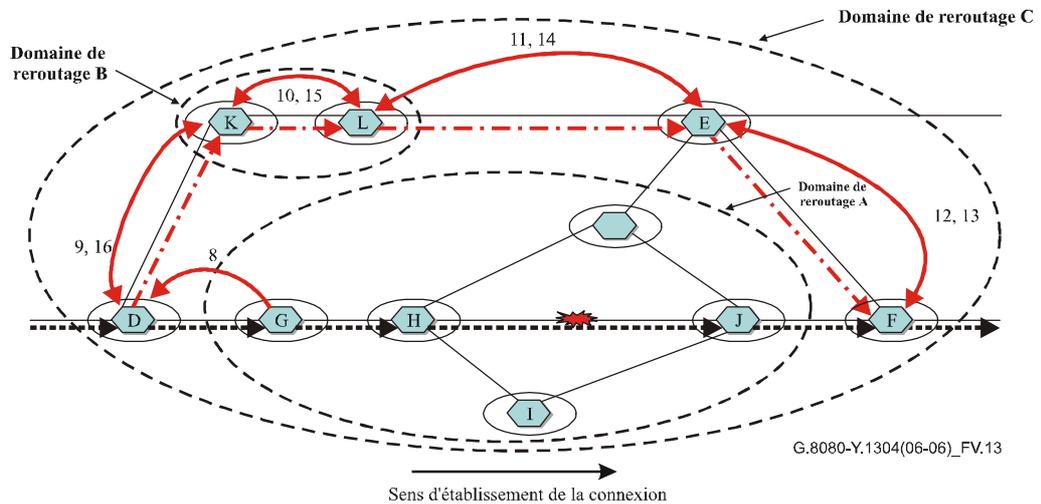
La Figure V.14 donne le détail de la succession des opérations utilisant le routage par la source représentées dans la Figure V.13. Ces étapes sont les suivantes:

- 1) le contrôleur de connexion (CC) reçoit une notification de défaillance d'une liaison intradomaine émise par les gestionnaires de ressource de liaison (LRM) contenant l'information de routage par retour en arrière qui indique la liaison en dérangement. Cette notification peut être reçue dans le nœud J ou H, ou les deux, selon le nœud qui détecte la défaillance de la liaison;
- 2) la notification de défaillance de la liaison intradomaine est retransmise au contrôleur CC_G . Aucune connexion de sous-réseau (SNC) n'est modifiée;
- 3) le contrôleur de routage (RC_G) est interrogé au moyen de l'information de routage par retour en arrière et renvoie l'ensemble des liaisons, à l'exclusion de la liaison en dérangement et des sous-réseaux impliqués;
- 4-16) les étapes 4 à 16 décrivent le flux d'établissement des connexions utilisant l'algorithme de routage par la source, qui est identique à celui qui est décrit dans le § V.2.3 – Utilisation conjuguée du routage par la source et du routage pas à pas;
- 17) si elle n'a pas réussi à établir la connexion dans le domaine de reroutage A, l'information de routage par retour en arrière est retransmise au domaine de reroutage de niveau supérieur C;
- 18) le contrôleur de routage RC_D est interrogé au moyen de l'information de routage par retour en arrière et renvoie l'ensemble des liaisons, à l'exclusion de celles du domaine A;
- 19-40) les étapes 19 à 40 décrivent le flux d'établissement des connexions utilisant l'algorithme de routage par la source, qui est identique à celui qui est décrit dans le § V.2.3 – Utilisation conjuguée du routage par la source et du routage pas à pas.

Etape 1: création de la connexion de reroutage dans le domaine de reroutage A



Etape 2: si l'étape 1 a échoué, renvoyer le message de routage par retour en arrière au domaine de reroutage de niveau supérieur C



G.8080-Y.1304(06-06)_FV.13

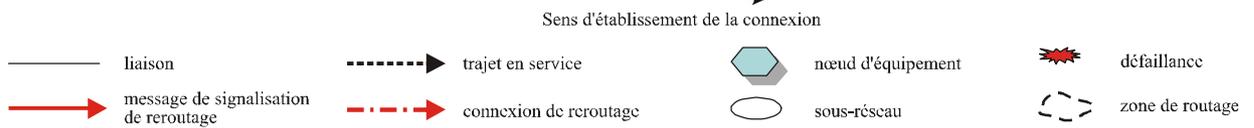
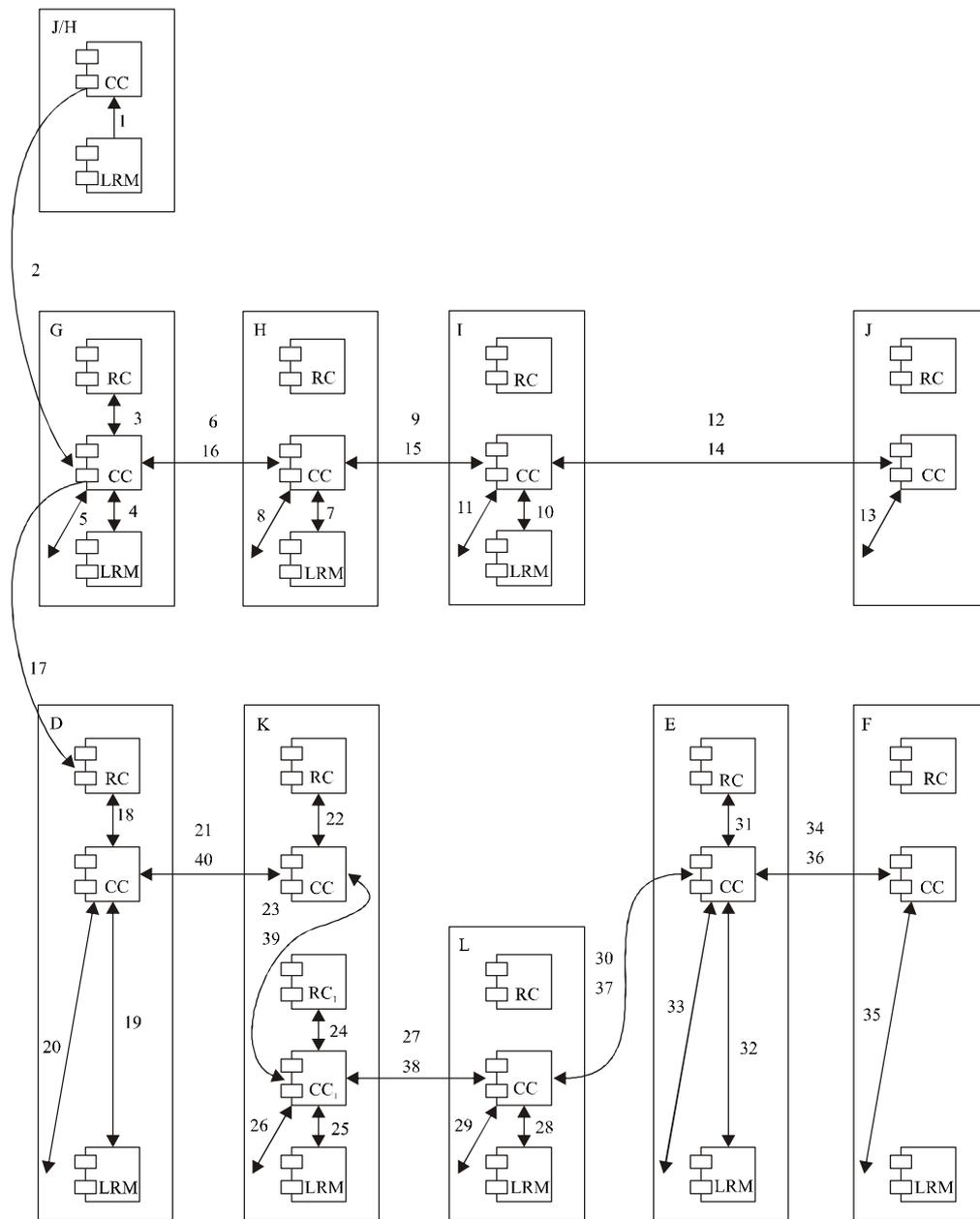


Figure V.13/G.8080/Y.1304 – Flux de signalisation de reroutage à comportement réversible utilisant l'algorithme de routage par la source (ou pas à pas) après défaillance d'une liaison intradomaine



G.8080-Y.1304(06-06)_FV.14

Figure V.14/G.8080/Y.1304 – Interactions des composants du reroutage à comportement réversible utilisant l'algorithme de routage par la source après défaillance d'une liaison intradomaine

V.7 Routage par la source utilisant l'interface de demande de routage

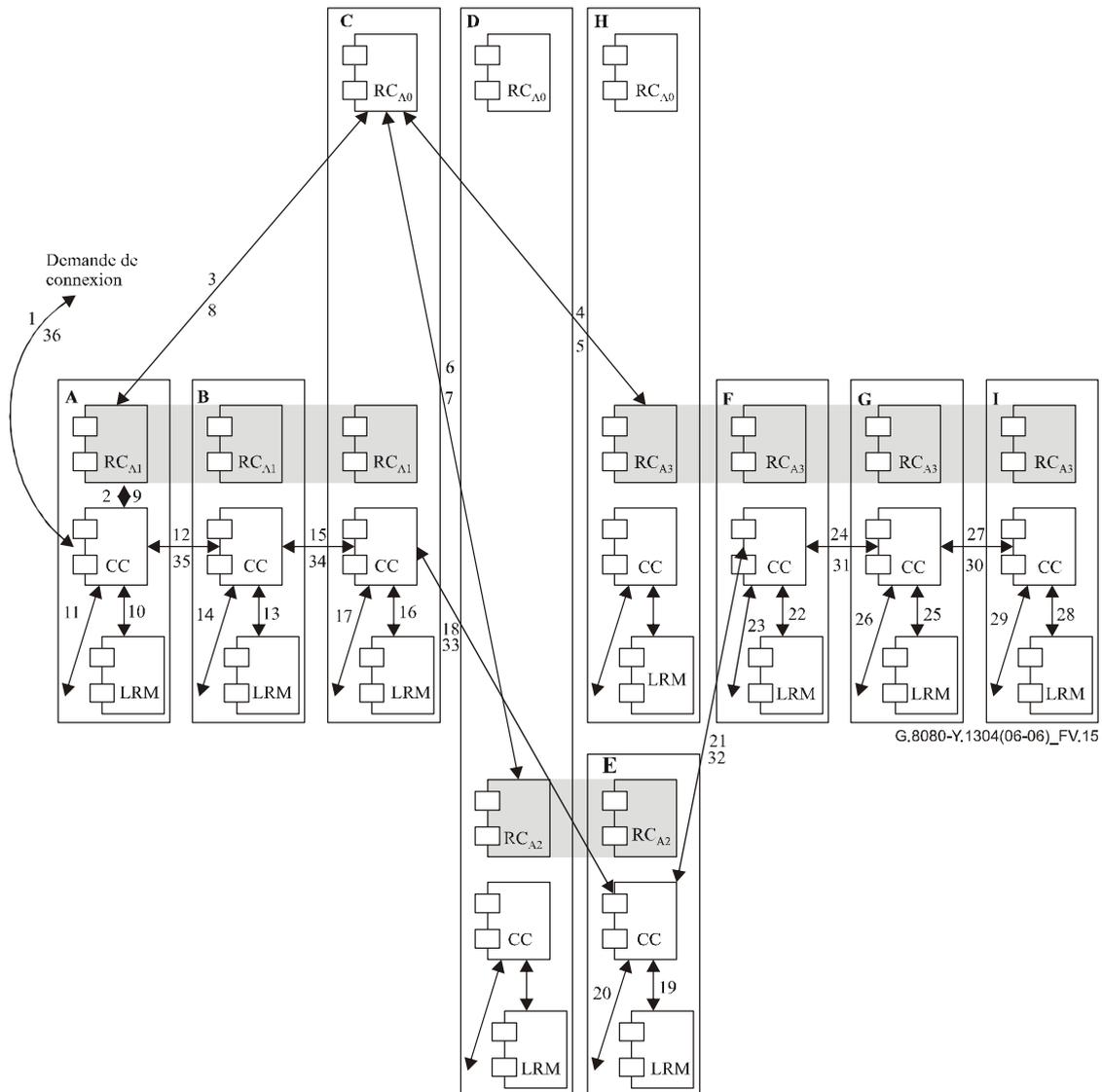


Figure V.15/G.8080/Y.1304 – Interactions des composants pour le routage par la source utilisant l'interface de demande de routage

La Figure V.15 donne le détail de la succession des opérations impliquées dans l'établissement d'une connexion utilisant le routage par la source assisté de la fonction de demande d'itinéraire de RC à RC. La notation RC_{A1} , RC_{A2} , etc., représente le contrôleur de routage de la zone A1, A2, etc. L'obtention des composants de communication effectifs peut être facilitée par d'autres composants intermédiaires – par exemple, la communication entre le contrôleur RC_{A0} du nœud C et le contrôleur RC_{A2} du nœud D peut être assurée en transférant le message par l'intermédiaire du contrôleur RC_{A0} du nœud D.

Ces étapes sont les suivantes:

- 1) le contrôleur de connexion (CC_A) reçoit une demande de connexion émanant de l'interface d'entrée de demande de connexion (`connection_request_in` interface), spécifiée sous la forme d'une paire de noms (A et Z) à la frontière du sous-réseau;
- 2) le contrôleur de routage RC_{A1} du nœud A est interrogé (en utilisant le point SNP de l'extrémité Z sur l'interface de demande d'itinéraire);

- 3) le contrôleur de routage RC_{A1} du nœud A constate que l'adresse de destination n'est pas visible à l'intérieur de la zone A1. En conséquence, il envoie au contrôleur RC_{A0} du nœud C une demande d'itinéraire afin d'obtenir une assistance sur l'interface de demande d'itinéraire. Alors que le contrôleur RC_{A1} du nœud C dispose de la même information de routage que le contrôleur RC_{A1} du nœud A, du fait qu'ils sont situés dans une zone de routage commune, le contrôleur RC_{A0} du nœud C est en mesure de voir la destination, ce qui rend possible le calcul d'un itinéraire;
- 4) en procédant au calcul d'un itinéraire pour se rendre au point de destination, le contrôleur RC_{A0} du nœud C constate que pour parvenir à sa destination il doit se rendre dans la zone A3. Cependant, comme il existe plusieurs itinéraires entre la zone A1 et la zone A3, le contrôleur RC_{A0} doit se faire aider par les contrôleurs RC_{A2} et RC_{A3} pour déterminer le meilleur itinéraire. Le contrôleur RC_{A0} du nœud C envoie donc une demande au contrôleur RC_{A3} du nœud H pour déterminer quelle liaison de A2 à A3 il lui faut utiliser;
- 5) le contrôleur RC_{A3} du nœud H calcule les itinéraires possible à partir des liaisons qui entrent dans la zone A3 en provenance de la zone A2 jusqu'au point de destination dans la zone A3. Cela lui permet de déterminer les coûts de l'utilisation de l'un ou l'autre de ces itinéraires, après quoi il renvoie cette information au contrôleur RC_{A0} du nœud C;
- 6) à l'instar du contrôleur RC_{A3} du nœud H, le contrôleur RC_{A0} du nœud C envoie une demande au contrôleur RC_{A2} du nœud D pour déterminer les itinéraires à utiliser entre les liaisons de sortie qui sortent de la zone A2 et entrent dans la zone A3 et les liaisons d'entrée qui entrent dans la zone A2 après être sorties de la zone A1;
- 7) le contrôleur RC_{A2} du nœud D calcule les itinéraires possibles à travers la zone A2 et renvoie cette information au contrôleur RC_{A0} du nœud C;
- 8) le contrôleur RC_{A0} du nœud C communique au contrôleur RC_{A1} du nœud A la liste des itinéraires établis depuis la frontière de la zone A1 jusqu'au point de destination dans la zone A3 et inclut le coût global de chaque itinéraire ainsi établi;
- 9) le contrôleur RC_{A1} du nœud A dispose à présent des informations nécessaires pour calculer un itinéraire traversant la zone A1 en utilisant les informations de coût qui lui ont été communiquées par le contrôleur RC_{A0} du nœud C pour déterminer l'itinéraire de bout en bout le plus économique. Pour le reste de cet exemple, nous admettons que l'itinéraire choisi va de A, via L1 à B, via L2 à C, via L3 à E, via L4 à F, via L5 à G et via L6 à I. Le contrôleur RC_{A1} du nœud A renvoie alors la réponse au contrôleur CC du nœud A, qui lance le processus d'établissement de la demande de connexion de bout en bout utilisant l'itinéraire (A, L1, L2, L3, L4, L5, L6 et Z);
- 10) la liaison L1 est locale pour le nœud A, et une connexion de liaison pour la liaison L1 est obtenue auprès du gestionnaire LRM_A sur l'interface de demande de connexion de liaison;
- 11) la connexion SNC appropriée est établie sur le commutateur local (le contrôleur n'est pas représenté);
- 12) la demande de connexion (L2, L3, L4, L5, L6 et Z) est ensuite retransmise au contrôleur CC du nœud B suivant (sur l'interface de sortie/d'entrée de coordination homologue (peer coordination_out/in interface));
- 13) le gestionnaire LRM_B est en charge de la liaison L2, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison (link connection_request interface);
- 14) la connexion SNC appropriée est établie sur le commutateur local (le contrôleur n'est pas représenté);
- 15) la demande de connexion (L3, L4, L5, L6, Z) est ensuite retransmise au contrôleur CC du nœud C suivant (sur l'interface de sortie/d'entrée de coordination homologue (peer coordination_out/in interface));

- 16) le gestionnaire LRM_C est en charge de la liaison L3, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison (link connection_request interface);
- 17) la connexion SNC appropriée est établie sur le commutateur local (le contrôleur n'est pas représenté);
- 18) la demande de connexion (L4, L5, L6, Z) est ensuite retransmise au contrôleur CC du nœud E suivant (sur l'interface de sortie/d'entrée de coordination homologue (peer coordination_out/in interface));
- 19) le gestionnaire LRM_E est en charge de la liaison L4, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison (link connection_request interface);
- 20) la connexion SNC appropriée est établie sur le commutateur local (le contrôleur n'est pas représenté);
- 21) la demande de connexion (L5, L6 et Z) est ensuite retransmise au contrôleur CC du nœud F suivant (sur l'interface de sortie/d'entrée de coordination homologue (peer coordination_out/in interface));
- 22) le gestionnaire LRM_F est en charge de la liaison L5, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison (link connection_request interface);
- 23) la connexion SNC appropriée est établie sur le commutateur local (le contrôleur n'est pas représenté);
- 24) la demande de connexion (L6 et Z) est ensuite retransmise au contrôleur homologue suivant CC du nœud G (sur l'interface de sortie/d'entrée de coordination homologue (peer coordination_out/in interface));
- 25) le gestionnaire LRM_G est en charge de la liaison L6, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison (link connection_request interface);
- 26) la connexion SNC appropriée est établie sur le commutateur local (le contrôleur n'est pas représenté);
- 27) la demande de connexion (Z) est ensuite retransmise au contrôleur CC du nœud I suivant;
- 28) le gestionnaire LRM_I est en charge de la liaison de sortie en direction du nœud de destination, de sorte qu'une connexion de liaison est obtenue à partir de cette liaison sur l'interface de demande de connexion de liaison (link connection_request interface);
- 29) la connexion SNC appropriée est établie sur le commutateur local (le contrôleur n'est pas représenté);
- 30) le contrôleur CC du nœud I renvoie ensuite une confirmation au contrôleur CC du nœud G. L'échange des réponses se répète ensuite entre paires de contrôleurs CC en remontant en arrière jusqu'au contrôleur CC du nœud A à l'origine de la connexion.

BIBLIOGRAPHIE

- IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control (Cadre général de contrôle d'admission basé sur une politique)*.
- Unified Modelling Language (UML) (OMG UML Specification v. 1.3:OMG document ad/99-06-08) (*Langage unifié de modélisation*).

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

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

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

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

SÉRIES DES RECOMMANDATIONS UIT-T

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