UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T Q.1751

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

(06/2000)

SÉRIE Q: COMMUTATION ET SIGNALISATION

Prescriptions et protocoles de signalisation pour les IMT-2000

Spécifications de signalisation interréseaux pour l'ensemble de capacités 1 des réseaux IMT-2000

Recommandation UIT-T Q.1751

(Antérieurement Recommandation du CCITT)

RECOMMANDATIONS UIT-T DE LA SÉRIE Q

COMMUTATION ET SIGNALISATION

SIGNALISATION DANS LE SERVICE MANUEL INTERNATIONAL	Q.1–Q.3
EXPLOITATION INTERNATIONALE AUTOMATIQUE ET SEMI-AUTOMATIQUE	Q.4–Q.59
FONCTIONS ET FLUX D'INFORMATION DES SERVICES DU RNIS	Q.60–Q.99
CLAUSES APPLICABLES AUX SYSTÈMES NORMALISÉS DE L'UIT-T	Q.100–Q.119
SPÉCIFICATIONS DES SYSTÈMES DE SIGNALISATION N° 4 ET N° 5	Q.120–Q.249
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 6	Q.250–Q.309
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION R1	Q.310–Q.399
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION R2	Q.400–Q.499
COMMUTATEURS NUMÉRIQUES	Q.500–Q.599
INTERFONCTIONNEMENT DES SYSTÈMES DE SIGNALISATION	Q.600–Q.699
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 7	Q.700–Q.849
SYSTÈME DE SIGNALISATION D'ABONNÉ NUMÉRIQUE N° 1	Q.850–Q.999
RÉSEAUX MOBILES TERRESTRES PUBLICS	Q.1000–Q.1099
INTERFONCTIONNEMENT AVEC LES SYSTÈMES MOBILES À SATELLITES	Q.1100–Q.1199
RÉSEAU INTELLIGENT	Q.1200–Q.1699
PRESCRIPTIONS ET PROTOCOLES DE SIGNALISATION POUR LES IMT-2000	**Q.1700–Q.1799**
RNIS À LARGE BANDE	Q.2000–Q.2999

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

Recommandation UIT-T Q.1751

Spécifications de signalisation interréseaux pour l'ensemble de capacités 1 des réseaux IMT-2000

Résumé

La présente Recommandation UIT-T contient les spécifications de signalisation relatives au protocole de l'interface réseau-réseau (NNI, *network-to-network interface*). Ces spécifications ont pour but de prendre en charge les capacités qui sont recommandées dans le document portant sur le cadre général des IMT-2000 et qui sont spécifiées sous la forme de l'ensemble de capacités 1 (CS-1, *capability set 1*). La présente Recommandation UIT-T porte sur les spécifications relatives à quatre groupes de communication de l'interface NNI: commande d'appel et de support; gestion de la mobilité; commande de service de l'environnement de rattachement virtuel (VHE, *virtual home environment*) et commande de services de transmission de données par paquets et de l'accès à l'Internet; des spécifications relatives à la sécurité interréseaux sont décrites à haut niveau et cette fonctionnalité est incorporée aux protocoles de groupes de communication applicables Les spécifications données dans la présente Recommandation UIT-T ne sont pas associées à des flux d'information et elles doivent être considérées comme complémentaires aux flux d'information de la Recommandation UIT-T Q.1721. Elles comprennent des spécifications générales relatives au protocole de l'interface NNI, des modèles fonctionnels de l'interface NNI, des points de référence de l'interface NNI, des modèles d'états pour des entités fonctionnelles sélectives et le choix de diverses séries de protocoles.

Source

La Recommandation Q.1751 de l'UIT-T, élaborée par la Commission d'études 11 (1997-2000) de l'UIT-T, a été approuvée le 15 juin 2000 selon la procédure définie dans la Résolution 1 de la CMNT.

Mots clés

AMF, BICC, CN, CS-1, IMT-2000, INAP, LMFh, LMFv, MT, NNI, RAN, UIM, VHE.

AVANT-PROPOS

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

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

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

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

NOTE

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Recommandation UIT-T Q.1751

Spécifications de signalisation interréseaux pour l'ensemble de capacités 1 des réseaux IMT-2000

1 Domaine d'application

La présente Recommandation UIT-T porte sur l'élaboration de spécifications de signalisation interréseaux à utiliser pour l'établissement d'un protocole d'interface réseau-réseau (NNI) unique et commun. Sur la base des Recommandations UIT-T Q.1701 [1], Q.1711 [2] et Q.1721 [3], la présente Recommandation UIT-T contient des spécifications de signalisation et de protocole, qui ne sont pas de type flux d'information. Elle porte plus particulièrement sur les sujets suivants:

- description des couches de signalisation en fonction des groupes fonctionnels de commande d'appel et de support (CBC, *call and bearer control*), de gestion de la mobilité (MM, *mobility management*), de commande de services de transmission par paquets (PSC, *packet services control*) et de commande de services de l'environnement VHE (VSC, *VHE service control*);
- instances d'interface NNI pour l'itinérance mondiale et leurs points de référence;
- modèles d'états pour diverses entités fonctionnelles;
- spécifications de signalisation relatives au ou aux protocoles d'interface NNI;
- choix de protocoles d'interface NNI.

On peut aussi réaliser l'interfonctionnement entre réseaux centraux (CN-CN) en spécifiant une fonction d'interfonctionnement (IWF, *interworking function*) pour la conversion d'informations de protocole (et de facturation) entre différents membres de la famille. Mais il ne relève pas de la compétence de l'UIT de spécifier en détail la fonction d'interfonctionnement.

L'élaboration d'une description détaillée en langage de description et de spécification (SDL, *specification and description language*), la conception de l'architecture du protocole et le codage du protocole sortent du cadre de la présente Recommandation.

Les aspects d'exploitation, administration et maintenance entre les systèmes membres de la famille sortent également du cadre de la présente Recommandation UIT-T.

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.

[1] Recommandation UIT-T Q.1701 (1999), *Cadre général des réseaux IMT-2000*.

[2] Recommandation UIT-T Q.1711 (1999), *Modèle fonctionnel réseau pour les IMT-2000*.

[3] Recommandation UIT-T Q.1721 (2000), *Flux d'information pour l'ensemble de capacités 1 des IMT-2000*.

[4] Recommandation UIT-T Q.1901 (2000), *Protocole de commande d'appel indépendant du support*.

[5] Recommandation UIT-T Q.2630.1 (1999), *Protocole de signalisation de la couche AAL de type 2 (ensemble de capacités 1)*.

[6] Recommandations UIT-T de la série Q.1238, *Interface pour l'ensemble de capacités 3 du réseau intelligent*.

[7] Recommandation UIT-T Q.1290 (1998), *Glossaire utilisé dans la définition des réseaux intelligents*.

3 Définitions

La présente Recommandation définit les termes suivants:

3.1 réseau central d'ancrage: dans un environnement d'itinérance associé à une session de données, le réseau central d'ancrage est le réseau où la session de données est lancée et où une passerelle de service par paquets est assignée au terminal mobile. Le réseau central d'ancrage peut être le réseau de rattachement ou le réseau visité.

3.2 point de référence: dans un modèle fonctionnel interréseaux ou intraréseau, le point de référence se rapporte à la relation qui existe entre deux entités fonctionnelles pour l'échange de messages de signalisation et de transactions d'opérations.

3.3 application de service: fourniture de services par des capacités de type général, par exemple des capacités de réseau intelligent, telles qu'elles sont appliquées dans le réseau de rattachement ou dans un réseau visité dans le cadre d'un environnement de rattachement virtuel.

3.4 commande de service: fonctions qui fixent ou modifient le contexte dans lequel les appels de base et les supports sont établis, modifiés et libérés.

3.5 modèle d'états: le modèle d'états pour une entité fonctionnelle est une représentation schématique des états de cette entité en relation avec une procédure de signalisation interréseaux. Il inclut l'identification de tous les points de détection (DP) d'entrée et de sortie pour chaque état.

3.6 abonné: utilisateur d'un terminal mobile qui s'est abonné au service considéré.

3.7 application de service complémentaire: fourniture d'un certain service complémentaire, généralement via l'utilisation de capacités propres au service, dans le réseau de rattachement ou dans un réseau visité dans le cadre d'un environnement de rattachement virtuel.

3.8 utilisateur: utilisateur d'un terminal mobile. Les termes "utilisateur" et "abonné" sont utilisés de manière interchangeable dans la présente Recommandation UIT-T.

3.9 environnement de rattachement virtuel: fourniture, à l'abonné visiteur, de services identiques ou aussi semblables que possible à ceux qui lui sont offerts lorsqu'il se trouve dans son réseau de rattachement.

La présente Recommandation UIT-T utilise des termes définis dans la Recommandation UIT-T Q.1701 [1].

– **réseau central**.

La présente Recommandation UIT-T utilise des termes définis dans la Recommandation UIT-T Q.1290 [7].

– **entité fonctionnelle**.

– **point de détection**.

– **déclencheur de service**.

4 Abréviations

La présente Recommandation UIT-T utilise les abréviations suivantes:

AALx couche d'application ATM de type x (*ATM application layer x*)

AC centre d'authentification (*authentication centre*)

ADDS service de livraison de données d'application (*application data delivery service*)

AINI interface ATM entre réseaux (*ATM internetwork interface*)

AMF fonction de gestion d'authentification (*authentication management function*)

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

BICC commande d'appel indépendante du support (*bearer independent call control*)

B-ISUP sous-système ISUP à large bande (*broadband ISUP*)

CBC commande d'appel et de support (*call and bearer control*)

CC commande d'appel (*call control*)

CCAF' fonction d'agent de commande d'appel améliorée (*call control agent function*) (améliorée comme décrit dans la Recommandation UIT-T Q.1711 [2])

CCF fonction de commande d'appel (*call control function*)

CCF' fonction de commande d'appel améliorée (*call control function*) (améliorée comme décrit dans la Recommandation UIT-T Q.1711 [2])

CLI identificateur de la ligne appelante (*calling line ID*)

CN réseau central (*core network*)

CNa réseau central ancré [*core network (anchored)*]

CnCAF fonction d'agent de commande de connexion (*connection control agent function*)

CnCF fonction de commande de connexion (*connection control function*)

CNh réseau central de rattachement [*core network (home)*]

CNpv réseau central précédemment visité [*core network (previous visited)*]

CNsn réseau central de support [*core network (supporting)*]

CNv réseau central visité [*core network (visited)*]

CS-X ensemble de capacités X (*capability set X*)

DFP plan fonctionnel réparti (*distributed functional plane*)

DP point de détection (*detection point*)

FE entité fonctionnelle (*functional entity*)

FT terminal fixe (*fixed terminal*)

GPCF fonction de commande de position géographique (*geographic position control function*)

GPF fonction de position géographique (*geographic position function*)

GTT traduction d'appellations globales (*global title translation*)

ID identité

IF flux d'information (*information flow*)

IMDN numéro de répertoire mobile international IMT-2000 (*IMT-2000 international mobile directory number*)

IMT-2000 Télécommunications mobiles internationales 2000 (*international mobile telecommunications 2000*)

IMUI identité internationale d'usager mobile IMT-2000 (*IMT-2000 international mobile user identity*)

INAP protocole d'application du réseau intelligent (*intelligent network application protocol*)

IP protocole Internet (*Internet protocol*)

ISP fournisseur de service Internet (*Internet service provider*)

ISUP sous-système utilisateur du RNIS (*ISDN user part*)

IWF fonction d'interfonctionnement (*interworking function*)

LAI identité de zone d'emplacement (*location area identity*)

LMF fonction de gestion de l'emplacement (*location management function*)

MCF fonction de commande mobile (*mobile control function*)

MGPF fonction de position géographique mobile (*mobile geographic position function*)

MM gestion de mobilité (*mobility management*)

MRTR réception et émission de radio mobile (*mobile radio transmission and reception*)

MSC centre de commutation de mobile (*mobile switching centre*)

MT terminal mobile (*mobile terminal*)

NAI identificateur d'accès au réseau (*network access identifier*)

N-ISUP sous-système utilisateur du RNIS à bande étroite (*narrow-band ISUP*)

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

Nxx point de référence Nxx

PIAM point dans la gestion de l'authentification (*point in authentication management*)

PIN numéro d'identification personnel (*personal identification number*)

PNNI interface réseau-réseau privée (*private network-to-network interface*)

PSC commande de services par paquets (*packet service control*)

PSCAF fonction d'agent de commande de service par paquets (*packet service control agent function*)

PSCF fonction de commande de service par paquets (*packet service control function*)

PSGCF fonction de commande passerelle de service par paquets (*packet service gateway control function*)

QS qualité de service

RACAF fonction d'agent de commande d'accès radio (*radio access control agent function*)

RAN réseau d'accès radio (*radio access network*)

RDP réseau de données de paquets

RF radiofréquence

RFTR réception et émission par radiofréquence (*radio frequency transmission and reception*)

RI réseau intelligent

RNC contrôleur de réseau radio (*radio network controller*)

RNIS réseau numérique à intégration de services

RTPC réseau téléphonique public commuté

SACF fonction de commande d'accès au service (*service access control function*)

SCF fonction de commande de service (*service control function*)

SCP point de commande de service (*service control point*)

SDF fonction de données du service (*service data function*)

SDP point de données de service (*service data point*)

SIBF fonction de diffusion d'information de système d'accès (*system access information broadcast function*)

SLP programme de logique de service (*service logic program*)

SMF fonction de gestion de service (*service management function*)

SMS service de message court (*short message service*)

SRF fonction de ressource spécialisée (*specialized resource function*)

SSD données secrètes partagées (*shared secret data*)

TMUI identificateur d'utilisateur mobile temporaire (*temporary mobile user identifier*)

TPU télécommunications personnelles universelles

UDP protocole datagramme d'utilisateur (*user datagram protocol*)

UIM module d'identité d'utilisateur (*user identity module*)

UIMF fonction de gestion de l'identification d'usager (*user identification management function*)

VHE environnement de rattachement virtuel (*virtual home environment*)

VSC commande de services VHE (*VHE service control*)

5 Introduction

Les spécifications de signalisation d'interface NNI déterminées dans la présente Recommandation UIT-T visent à aider les concepteurs de protocole à élaborer énoncées des protocoles qui régissent les interactions entre réseaux centraux de la famille des systèmes IMT-2000. Ces spécifications sont subdivisées en deux parties – applications et protocoles – et organisées en 12 paragraphes comme suit. Les paragraphes 1 à 5 sont des considérations générales qui donnent une description du domaine d'application de la présente Recommandation UIT-T, un bref résumé du contenu de la présente Recommandation UIT-T, des références, des abréviations, des définitions et une terminologie ainsi que la présente introduction. Le paragraphe 6 contient toutes les spécifications générales et relatives aux applications, y compris les spécifications des capacités de service, du stockage des données et du profil d'abonné. Il porte aussi sur tous les aspects de modélisation fonctionnelle de l'interface NNI. Le paragraphe 7 identifie et décrit tous les points de référence entre entités fonctionnelles relatifs aux protocoles – 20 points de référence au total. Les paragraphes 8 à 12 portent sur les spécifications de protocole pour cinq catégories de signalisation: commande d'appel et de support, gestion de la mobilité, commande de services VHE et RI, commande de services par paquets et de services Internet, échange de données et d'informations de sécurité entre réseaux centraux.

6 Spécifications générales

6.1 Spécifications d'interface NNI

L'interface NNI prendra en charge toutes les capacités et fonctionnalités de service/réseau de l'ensemble CS-1 des IMT-2000 pour lesquelles une compatibilité amont est assurée avec les systèmes de la deuxième génération.

L'ensemble suivant de spécifications d'interface NNI numérotées constitue un point de départ pour construire un ensemble complet dans les sections qui suivent. Les spécifications sont intentionnellement associées à un seul objectif pour que la traçabilité puisse être facile et efficace.

1) L'interface NNI doit assurer une "anticipation" ou un routage optimal, par exemple pour éviter l'effet "trombone"[1].
2) L'interface NNI doit prendre en charge le transfert du relevé des données d'appel (CDR, *call detail record*) comme les étiquettes de référence d'appel, les données liées à la taxation, les informations de taxation et d'autres informations de relevé CDR nécessaires à des fins réglementaires.
3) L'interface NNI doit prendre en charge des services de messagerie (par exemple, notification de message vocal et service ADDS).

6.2 Spécifications de commande de services VHE

L'environnement de rattachement virtuel (VHE) doit être fondé sur les scénarios identifiés dans la Recommandation UIT-T Q.1711 [2]. Deux scénarios sont identifiés dans la présente Recommandation UIT-T:

commande directe au réseau de rattachement: dans ce scénario, on invoque la logique de service pour demander des instructions/informations à la fonction SCFsn. Le préarrangement entre le réseau de prise en charge et le réseau de rattachement ou entre le réseau de prise en charge et le réseau visité pourra nécessiter des capacités de filtrage de l'invocation déclenchante;

commande de service via un relais: dans ce scénario, on invoque la logique de service via la fonction SCFh ou SCFv pour demander des instructions/informations à la fonction SCFsn. Le préarrangement entre le réseau de prise en charge et le réseau de rattachement ou entre le réseau de prise en charge et le réseau visité porte aussi bien sur des capacités de relayage et de sécurité/filtrage que sur une logique de service partagée.

6.2.1 Environnement VHE fondé sur une programmation à distance

L'environnement VHE est pris en charge par le téléchargement de la logique de service et des données liées au service, du réseau de rattachement au réseau de desserte et au module UIM.

6.2.2 Capacités de service

taxation: les procédures de taxation servent à fournir des informations concernant l'appel et la durée de l'appel.

gestion de réseau: les procédures de gestion de réseau assurent la protection du réseau de rattachement contre toute surcharge.

---

[1] Dans les systèmes de la deuxième génération, du fait de l'effet trombone, un appel à destination d'un terminal mobile est routé vers le système de rattachement de l'abonné mobile appelé, même si l'appelé se trouve en fait à proximité de l'appelant. Tout particulièrement dans une situation d'itinérance mondiale, il serait très utile d'éviter l'effet trombone, afin d'empêcher que les ressources longue distance soient gaspillées.

interaction de l'appelant et traitement des ressources spécialisées: les procédures permettent de faire des annonces, de lancer des invites et de collecter des informations concernant l'utilisateur après le numérotage (par exemple numéro PIN pour l'appel par carte de crédit).

assistance et transfert: les procédures permettent de demander une assistance à des équipements externes (par exemple IP) pour faire des annonces, lancer des invites et collecter des informations.

6.3 Spécifications de stockage des données dans un réseau central pour le profil (d'utilisateur) d'abonné

Les items d'information suivants sont stockés dans le réseau de rattachement de l'abonné et sont utilisés dans les activités de gestion de profil et d'informations concernant l'abonné:

- numéro de répertoire mobile IMT-2000 (IMDN, *IMT-2000 mobile directory number*), par exemple un numéro pouvant être composé;
- identité d'utilisateur mobile IMT-2000 (IMUI);
- identité d'utilisateur mobile temporaire IMT-2000 (TMUI, *temporary mobile user identifier*);
- état du terminal;
- information de l'emplacement de l'utilisateur/du terminal;
- données sur les services de base (par exemple services supports faisant l'objet d'un abonnement);
- téléservices (par exemple données sur l'abonnement à un appel de groupe et/ou une diffusion);
- données sur les services complémentaires;
- éléments de service/services déterminés par l'exploitant (par exemple données sur l'interdiction d'appels);
- éléments de service/services déterminés par l'abonné (par exemple données sur le filtrage des appels);
- données sur la restriction de l'itinérance;
- données sur l'abonnement régional;
- données sur l'abonnement à un environnement VHE.

6.4 Spécification d'itinérance mondiale

L'interface NNI correspond à un protocole d'interface entre réseaux centraux (CN) commun et unique qui prend en charge la capacité d'itinérance mondiale des IMT-2000 et offre aux utilisateurs se déplaçant dans deux réseaux membres de la famille des IMT-2000 ou davantage l'environnement de services qu'ils ont dans leur réseau de rattachement. La Figure 6-1 montre le rôle que l'interface NNI commune peut jouer, conjointement avec les fonctions IWF de divers membres de la famille, pour assurer l'interopérabilité des réseaux et prendre en charge l'itinérance mondiale en offrant aux utilisateurs itinérants l'environnement de services qu'ils ont dans leur réseau de rattachement. L'implémentation de l'interopérabilité et de la configuration d'itinérance mondiale comme indiqué sur la Figure 6-1 présente les caractéristiques distinctives suivantes par rapport à l'implémentation de fonctions IWF pour chaque couple de réseaux centraux.

- interface ouverte: il n'y aura qu'une seule interface NNI commune et unique (en cours de développement au sein de l'UIT-T);
- efficacité: il faut une seule fonction IWF (par opposition à N-1 fonctions IWF bilatérales) par membre d'une famille IMT-2000 comprenant N membres, permettant à chaque membre d'interfonctionner avec tous les autres membres;

- transparence: des modifications apportées aux spécifications de réseau d'un membre donné de la famille n'auront pas d'incidence sur les fonctions IWF des autres membres;
- évolutivité: facilité d'accueil de nouveaux membres dans la famille.

C'est l'UIT-T qui établit le protocole de l'interface NNI, mais il appartient à chaque membre de la famille de développer la fonction IWF.

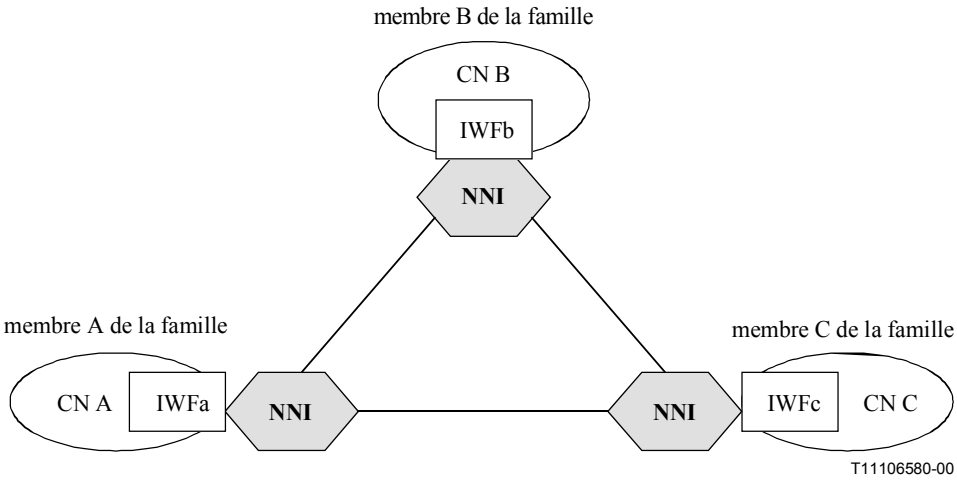


Figure 6-1/Q.1751 – Modèle d'interconnexion des réseaux IMT-2000

6.5 Groupes de communication associés à l'interface NNI

On distingue quatre principaux groupes de communication en ce qui concerne les opérations entre réseaux centraux des IMT-2000. La distinction provient de la nature des opérations que ces groupes prennent en charge dans le cadre d'un protocole d'application d'interface NNI unique et commun. Ces groupes de communication sont les suivants:

- *commande d'appel et de support (CBC, call and bearer control)*

  Ce groupe de communication inclut tous les échanges d'informations entre réseaux centraux se rapportant à la commande de services en mode connexion ou en mode sans connexion (services de base, services supplémentaires normalisés).

- *Gestion de mobilité (MM, mobility management)*

  Ce groupe de communication inclut tous les échanges d'informations entre réseaux centraux se rapportant à la gestion de la mobilité (par exemple enregistrement, authentification et gestion des informations de localisation).

- *Commande de services VHE (VSC)*

  Ce groupe de communication inclut tous les échanges d'informations entre réseaux centraux se rapportant à la commande de services du réseau de rattachement accessibles depuis les réseaux visités.

- *Commande de services par paquets (PSC, packet service control)*

  Ce groupe de communication inclut tous les échanges d'informations entre réseaux centraux se rapportant à la commande de services par paquets (par exemple voix, images et données).

Des spécifications relatives à la sécurité interréseaux sont décrites à haut niveau et cette fonctionnalité est incorporée aux protocoles de groupes de communication applicables.

Dans le contexte d'un protocole d'interface NNI unique et commun décrit au 6.4, ces groupes sont en outre illustrés sur la Figure 6-2 ci-dessous:

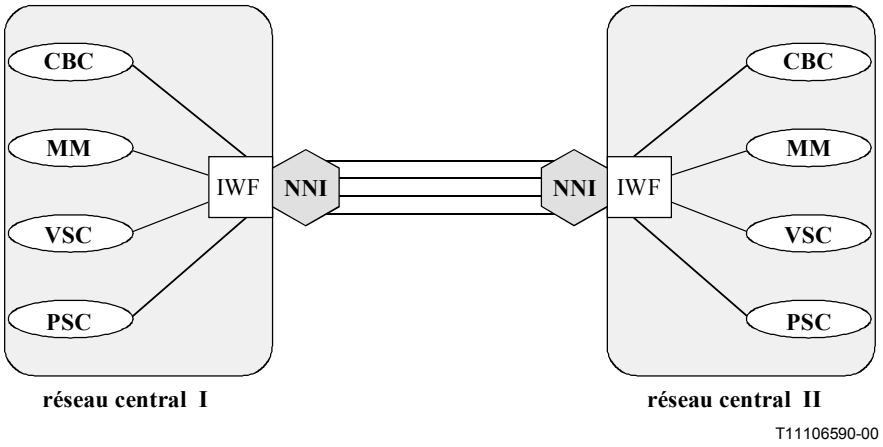


Figure 6-2/Q.1751 – Groupes de communication associés à l'interface NNI

Pour établir un appel et transporter un service à travers un protocole d'interface entre deux réseaux centraux, il faut établir un ou plusieurs de ces groupes de communication soit directement soit indirectement entre deux réseaux centraux ou davantage. Le modèle d'interconnexion pour réaliser les communications requises suit le modèle d'interconnexion des réseaux IMT-2000 du paragraphe 7 (Figure 7-1).

6.6 Services Internet

1) Un utilisateur itinérant abonné à un service de données par paquets doit pouvoir avoir accès à l'Internet public, à un fournisseur ISP de rattachement ou à un réseau privé à partir de plusieurs fournisseurs de services IMT-2000 tout en maintenant une relation officielle client-vendeur avec un seul fournisseur de services IMT-2000.

2) L'abonné doit indiquer explicitement quel service de données d'accès il demande (c'est-à-dire accès à l'Internet public, à un fournisseur ISP de rattachement ou à un réseau privé).

3) L'abonné doit pouvoir établir des sessions de données simultanées avec l'Internet public, un fournisseur ISP de rattachement ou un réseau privé et avoir différentes adresses IP et identificateurs NAI pour les divers services d'accès. Le réseau de données par paquets peut utiliser l'adresse IP de destination ou l'identificateur NAI qui peut être inclus dans la demande d'enregistrement à une session afin de déterminer la destination de la session de données par paquets.

4) L'interface NNI doit pouvoir prendre en charge la qualité de service en assignant le trafic de l'utilisateur à une classe de service différenciée spécifique paquet par paquet en vue du transport sur l'Internet. L'interface NNI doit aussi pouvoir assigner tout le trafic de l'utilisateur à une classe de service spécifique destination par destination.

6.7 Spécifications de sécurité

L'interface NNI est située entre le réseau central d'un système IMT-2000 et les autres réseaux centraux. Elle interagit avec les autres réseaux pour assurer une communication de bout en bout entre utilisateurs (voir Figure 6-1). L'interface NNI transporte des informations concernant les utilisateurs (par exemple emplacement, autorisation, authentification et clés de chiffrement) et les réseaux (par exemple signalisation et commande); ces informations doivent être sécurisées de sorte

qu'aucun intrus ne puisse y accéder. Les aspects liés à la sécurité du transport des informations sont traités dans la présente Recommandation UIT-T.

Les spécifications de sécurité pour l'interface NNI peuvent être subdivisées en trois parties – les spécifications d'authentification (y compris la confidentialité), les spécifications de chiffrement et les spécifications de gestion de clé – décrites en détail dans les paragraphes qui suivent.

6.7.1 Spécifications pour la prise en charge de l'authentification d'utilisateur

- Les normes relatives à l'interface NNI doivent être conçues de manière à ce qu'il soit possible d'introduire de nouveaux algorithmes d'authentification, de nouvelles tailles de clé et de nouvelles méthodes d'authentification facultatives pendant la durée de vie attendue des normes.
- Les mécanismes de sécurité de l'interface NNI doivent être tels que l'incidence sur le trafic de réseau soit minime (par exemple en autorisant facultativement le partage de données secrètes entre l'entité de rattachement et l'entité de desserte).
- Les mécanismes de sécurité de l'interface NNI doivent prendre en charge des mises à l'épreuve uniques de terminaux sur des canaux (supports et de signalisation) spécialisés.
- Les mécanismes de sécurité de l'interface NNI doivent prendre en charge un mécanisme mondial de mise à l'épreuve, avec diffusion sur un canal mondial de signalisation, pour lequel il faut qu'un terminal réagisse correctement à une mise à l'épreuve de réseau avant que des canaux spécialisés soient attribués.
- Les mécanismes de sécurité de l'interface NNI doivent pouvoir détecter et signaler des transgressions de sécurité et doivent comporter des mécanismes de récupération pour ramener le système dans un état protégé.
- La fourniture ou la génération de clés de confidentialité ou de chiffrement peut faire partie de la procédure d'authentification.
- La compromission d'un mobile donné ne doit pas compromettre la sécurité d'ensemble du réseau.

6.7.2 Spécifications de chiffrement pour l'interface réseau-réseau

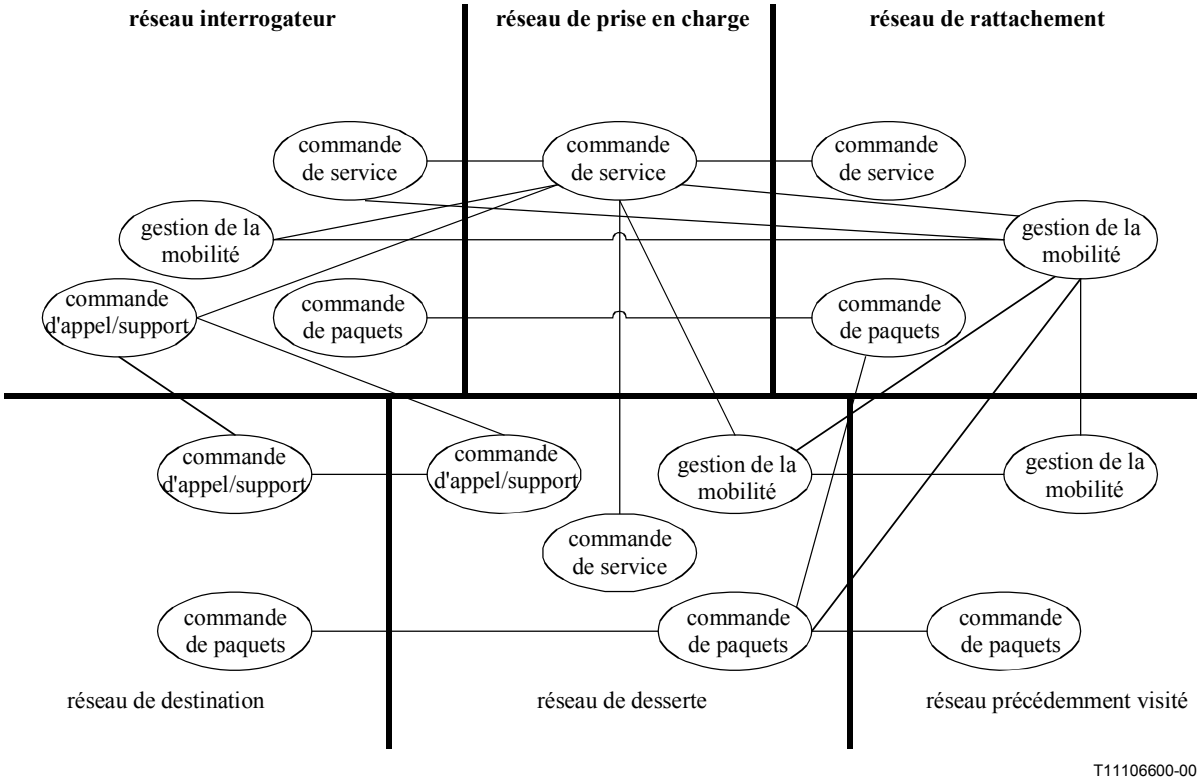
- Les mécanismes de chiffrement de l'interface NNI doivent respecter les dispositions juridiques imposées par les organes de réglementation (par exemple, contrôle des exportations, interception licite).
- Les mécanismes de chiffrement de l'interface NNI doivent pouvoir chiffrer avec un débit de plusieurs mégabits par seconde, sans compromettre la sécurité.
- La sécurité de l'interface NNI doit permettre l'authentification mutuelle entre éléments de réseau.

6.7.3 Spécifications de gestion de clé pour l'interface réseau-réseau

- La compromission d'une clé de confidentialité ne doit pas compromettre l'authentification.
- Les clés pour la confidentialité des données peuvent être fondées sur la même clé racine d'authentification.
- Les mécanismes de chiffrement de l'interface NNI doivent prendre en charge la gestion de clés liées aux appels (par exemple création, distribution, modification ou révocation de clés de chiffrement).
- L'interface NNI ne doit pas prendre en charge la modification de la ou des clés racines d'authentification enregistrées dans un module UIM et dans le centre d'authentification de rattachement (AMFh).

7 Modèle d'interconnexion

La Figure 7-1 qui suit illustre les relations que l'interface NNI doit absolument prendre en charge sur la base de l'ensemble CS-1 des IMT-2000. Toutes les entités fonctionnelles contenues dans chaque réseau ne sont pas nécessairement représentées ici (par exemple le réseau de rattachement peut contenir les fonctions SCF et SDF, le réseau précédemment visité peut contenir la fonction PSGCF). En revanche, la différentiation entre les frontières de l'interface NNI vise à montrer quelles entités fonctionnelles se rapportent à la fonction de réseau donnée pour l'interopérabilité au niveau de l'interface NNI. Pour éviter d'embrouiller la figure, aucune relation intraréseau n'y est représentée.



commande de service	SCF, SDF, SRF
gestion de la mobilité	LMF, AMF, UIMF
commande d'appel et de support	CCF'/SSF, CnCF, SACF
commande de paquets	PSCF, PSGCF

Figure 7-1/Q.1751 – Modèle d'interconnexion des réseaux IMT-2000

8 Interface fonctionnelle NNI

8.1 Modèle fonctionnel

La Figure 8-1 montre le "modèle d'interface fonctionnelle NNI". L'objet de ce modèle est de s'intéresser uniquement aux interfaces qui constituent l'interface NNI au niveau fonctionnel. La Figure 7-1 "Modèle d'interconnexion des réseaux IMT-2000" (NIM, *network interconnection model*) et la Figure 8-1 "Modèle d'interface fonctionnelle NNI" (FIM, *functional interface model*) fournissent ensemble le cadre pour l'identification des relations de signalisation de l'interface NNI et la base pour la définition du protocole.

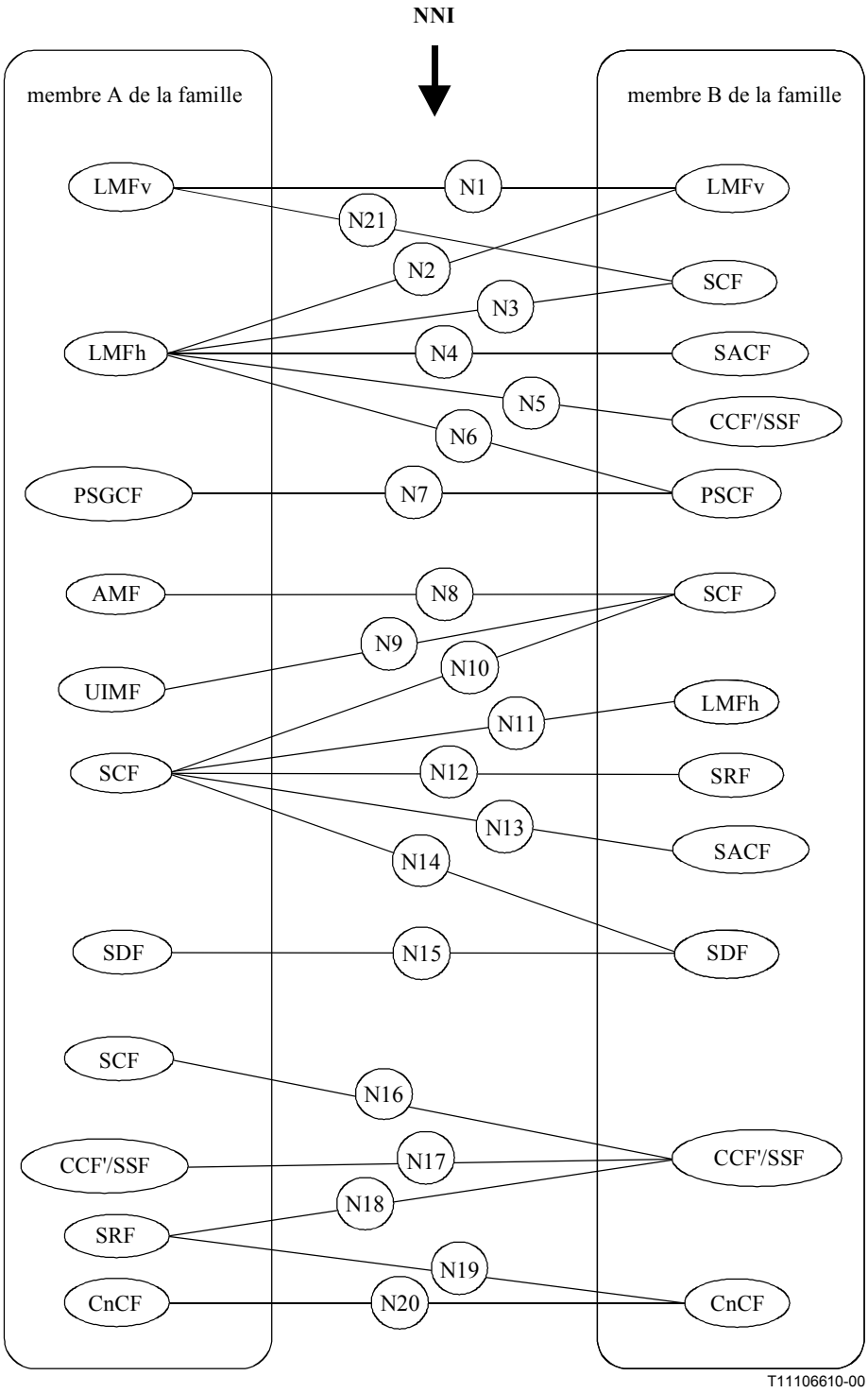


Figure 8-1/Q.1751 – Modèle d'interface fonctionnelle NNI

8.2 Points de référence

Les points de référence (Nxx) montrés sur la Figure 8-1 sont décrits ci-dessous avec des exemples d'illustration relatifs à la messagerie NNI (extraits du paragraphe 5 "Modèles fonctionnels des IMT-2000" de la Recommandation UIT-T Q.1711[2]).

---

[2] Il est possible que certaines relations ne soient pas couvertes au paragraphe 7/Q.1711 [2] "Itinérance mondiale et scénarios d'interfonctionnement", peut-être parce qu'on ne visait pas l'exhaustivité.

Il est à noter que, pour répondre aux besoins de service des IMT-2000, il faut élargir les moyens d'identification des abonnés pour inclure notamment les identités IMUI. C'est une spécification générale, qui est applicable aux interfaces existantes du RI.

8.2.1 Point de référence N01

Le point de référence N01 est l'interface fonctionnelle LMFv – LMFv. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de gérer les informations relatives à l'abonné (par exemple, pour l'extraction d'identités IMUI sur la base d'identificateurs TMUI).

8.2.2 Point de référence N02

Le point de référence N02 est l'interface fonctionnelle LMFh – LMFv. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de faire des enregistrements;
- d'annuler des enregistrements (réseau de rattachement vers réseau précédemment visité);
- de transférer des profils de service;
- de transférer des informations de routage pour l'établissement des appels;
- de gérer les informations relatives à l'abonné;
- d'assurer la commande de services complémentaires.

8.2.3 Point de référence N03

Le point de référence N03 est l'interface fonctionnelle LMFh – SCF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de fournir des services de RI liés à la gestion de la localisation.

8.2.4 Point de référence N04

Le point de référence N04 est l'interface fonctionnelle LMFh – SACF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de transférer des informations de routage pour l'établissement des appels;
- de transférer des demandes liées à l'authentification;
- de gérer des informations de base relatives à la mobilité, par exemple:
  - localisation, statut et identité d'un terminal mobile;
- de partager des informations sur la stratégie de radiorecherche;
- d'assurer la commande de services complémentaires;
- de remettre des messages, par exemple:
  - des messages SMS;
  - des messages ADDS;
- de gérer des activités de mise à l'épreuve aléatoire mondiale;
- de gérer des activités de mise à l'épreuve d'authentification unique.

8.2.5 Point de référence N05

Le point de référence N05 est l'interface fonctionnelle LMFh – CCF'/SSF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de transférer des informations de routage pour l'établissement des appels;

- des transférer des informations de profil y compris la capacité de service, par exemple:
  - des informations concernant le protocole;
  - des informations concernant le support.

8.2.6 Point de référence N06

Le point de référence N06 est l'interface fonctionnelle LMFh – PSCF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- d'accéder à des données liées à l'abonné et de les mettre à jour;
- de mettre à jour les informations liées aux services par paquets;
- de mettre à jour les informations liées au routage de paquets.

8.2.7 Point de référence N07

Le point de référence N07 est l'interface fonctionnelle PSGCF – PSCF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de mettre à jour les informations liées aux services de données par paquets du terminal mobile;
- de mettre à jour l'association de contexte de routage du terminal mobile;
- de transférer des données d'utilisateur entre un terminal mobile et un réseau par paquets.

8.2.8 Point de référence N08

Le point de référence N08 est l'interface fonctionnelle AMF – SCF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de fournir des services de RI liés à l'authentification de l'utilisateur.

8.2.9 Point de référence N09

Le point de référence N09 est l'interface fonctionnelle UIMF – SCF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de transférer des données/une logique de service;
- de modifier le profil de service;
- d'échanger des informations relatives à l'application.

8.2.10 Point de référence N10

Le point de référence N10 est l'interface fonctionnelle SCF – SCF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- d'acquérir et de manipuler des données sécurisées;
- d'assurer une commande de service répartie;
- de faire des notifications de service non sollicité.

8.2.11 Point de référence N11

Le point de référence N11 est l'interface fonctionnelle SCF – LMFh. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- à la fonction LMFh de fournir la localisation du terminal mobile et le statut de l'abonné à la fonction SCF.

8.2.12 Point de référence N12

Le point de référence N12 est l'interface fonctionnelle SCF – SRF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de fournir des ressources spécialisées pour des services de RI.

8.2.13 Point de référence N13

Le point de référence N13 est l'interface fonctionnelle SCF – SACF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de fournir des services de RI fondés sur des événements de gestion de la mobilité, par exemple:
  - gestion de l'emplacement;
  - authentification d'utilisateur;
- de fournir des services de RI non liés à l'appel.

8.2.14 Point de référence N14

Le point de référence N14 est l'interface fonctionnelle SCF – SDF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- à la fonction SDF de fournir à la fonction SCF une vue logique des données d'abonné;
- aux fonctions SCF et SDF de gérer et de mettre à jour les données de service.

8.2.15 Point de référence N15

Le point de référence N15 est l'interface fonctionnelle SDF – SDF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- d'échanger des données de service.

8.2.16 Point de référence N16

Le point de référence N16 est l'interface fonctionnelle SCF – CCF'/SSF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de fournir des services de RI liés à l'appel.

8.2.17 Point de référence N17

Le point de référence N17 est l'interface fonctionnelle CCF'/SSF – CCF'/SSF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de gérer des instances d'appel du point de vue:
  - de l'établissement;
  - du maintien;
  - de la libération;
- de gérer des services fondés sur la fonction CCF', y compris des interactions CCF'-CCF' (par exemple demande de réacheminement).

8.2.18 Point de référence N18

Le point de référence N18 est l'interface fonctionnelle SRF – CCF'/SSF, lorsque la commande d'appel et la commande de connexion sont intégrées. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- d'assurer la commande de supports en ce qui concerne la fonction SRF pour des services de RI, du point de vue:
  - de l'établissement;
  - du maintien;
  - de la libération.

Il est à noter qu'optionnellement, on pourrait aussi utiliser le protocole BICC (commande d'appel indépendante du support) à ce point de référence.

8.2.19 Point de référence N19

Le point de référence N19 est l'interface fonctionnelle SRF – CnCF, lorsque la commande d'appel et la commande de connexion sont séparées. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- d'assurer la commande de supports en ce qui concerne la fonction SRF pour des services de RI, du point de vue:
  - de l'établissement;
  - du maintien;
  - de la libération.

8.2.20 Point de référence N20

Le point de référence N20 est l'interface fonctionnelle CnCF – CnCF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de gérer des instances de connexion, du point de vue:
  - de l'établissement;
  - du maintien;
  - de la modification;
  - de la libération;
- de gérer des associations de commande de support, du point de vue:
  - de l'établissement;
  - du maintien;
  - de la libération.

8.2.21 Point de référence N21

Le point de référence N21 est l'interface fonctionnelle LMFv – SCF. La messagerie NNI sur cette interface fonctionnelle permet par exemple:

- de fournir des services de RI liés à la gestion de l'emplacement.

9 Spécifications de protocole pour la gestion de la mobilité

9.1 Pilotes de service

Les pilotes de service de RI suivants sont détaillés plus loin dans la présente Recommandation UIT-T et servent d'exemple de services de RI fondés sur des événements de mobilité:

1) **vérification de crédit**: l'abonné peut se voir refuser l'enregistrement lorsqu'il se déplace s'il n'a plus de crédit. De manière analogue, il peut recevoir une notification lorsque son compte

a atteint un seuil prédéterminé. Il peut éventuellement être autorisé à s'enregistrer uniquement pour un ensemble restreint de services si un certain seuil a été atteint;

2) **vérification d'emplacement après authentification**: l'abonné peut se voir refuser l'enregistrement si une fraude a été détectée. On vérifie la cohérence entre les emplacements des enregistrements successifs: par exemple, l'abonné s'est enregistré à Berlin et 15 minutes plus tard à Chicago. La vérification de l'emplacement après authentification facilite la détection de fraudes de ce type;

3) **TPU**: les IMT-2000 sont tenues de prendre en charge les TPU. On suppose ici qu'un utilisateur TPU est autorisé à s'enregistrer sur un terminal mobile à partir de ce terminal: l'enregistrement TPU est fondé sur un numéro IMT-2000, c'est-à-dire qu'il faut qu'un abonné mobile soit enregistré sur le terminal avant qu'un utilisateur TPU puisse procéder à son propre enregistrement. Pour un routage efficace, la fonction SCF TPU a besoin d'avoir une notification lorsque le terminal est éteint ou allumé afin de router l'appel vers la destination appropriée (par exemple vers la messagerie vocale TPU lorsque le terminal est éteint). De manière analogue, le service TPU peut inclure des restrictions lorsque le terminal mobile est en déplacement: la fonction SCF TPU a besoin d'avoir une notification lorsque le terminal s'enregistre dans un réseau visité afin de vérifier l'autorisation d'itinérance pour l'utilisateur TPU et d'appliquer une taxation spécifique pour les appels entrants et pour les appels sortants;

4) **annonces locales**: lorsque l'abonné mobile s'enregistre, certaines annonces peuvent être affichées afin de lui donner certaines informations locales, par exemple les prévisions météorologiques. Cela dépend des éléments de service auxquels l'utilisateur s'est abonné;

5) **filtrage dynamique fondé sur l'emplacement de l'utilisateur**: lorsqu'il se déplace, l'abonné peut souhaiter filtrer les appels entrants, si une taxation partagée est utilisée. Le filtrage dynamique est activé lorsque l'utilisateur s'enregistre dans un réseau visité étranger (utilisateur itinérant) et reste activé tant que le terminal est allumé.

9.2 Modes d'interaction de la logique de service

Parmi les éléments de service détaillés au 9.1, la logique de service de RI commandant le traitement relatif à la gestion de la mobilité peut être subdivisée en deux types:

- **notification**: la fonction SCF est simplement informée par la fonction LMF qu'un événement de mobilité s'est produit. Les annonces locales TPU et le filtrage sont considérés comme étant de ce type. La fonction SCF n'a pas d'influence sur le résultat de la procédure de mobilité, bien que le service de RI soit fourni à l'utilisateur. Dans l'exemple, soit un service de messagerie est fourni, soit un autre service de RI, lié ou non à l'abonné, est notifié;
- **commande**: la fonction SCF est capable de modifier le résultat de la procédure de mobilité, par exemple en refusant ou en annulant l'authentification ou l'enregistrement. La vérification de crédit et la vérification de l'emplacement après authentification sont des exemples de tels services.

9.3 Modèle d'états pour la fonction LMFv

La Figure 9-1 est une présentation schématique du modèle d'états pour la fonction LMFv montrant divers états possibles du terminal mobile dans le réseau visité. Elle identifie tous les points de détection (DP, *detection point*) d'entrée et de sortie pour chaque état. Ces états et les points de détection sont décrits plus en détail ci-dessous.

Les points de détection sans pilote de service identifié sont représentés en gris. Dans l'avenir, ces points de détection pourront être supprimés si aucune justification de service n'est fournie. La

suppression de ces points de détection n'aura aucune incidence sur la validité du modèle (états, événements, transitions d'état et actions).

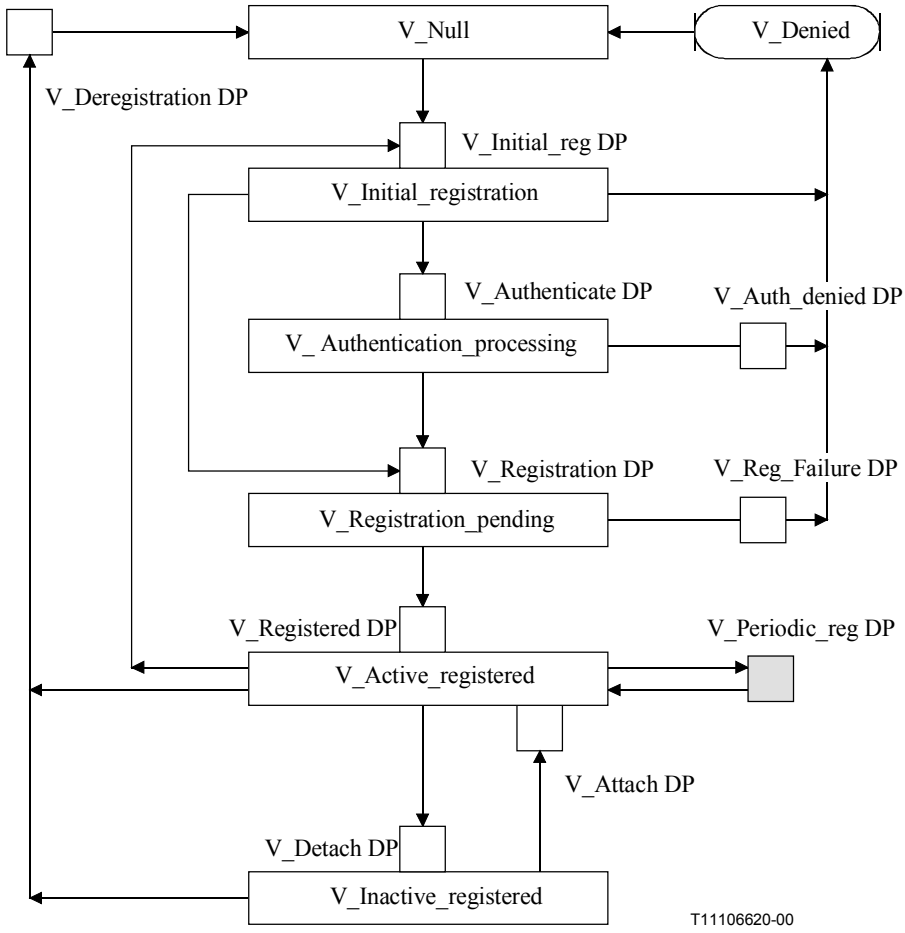


Figure 9-1/Q.1751 – Modèle d'états pour la fonction LMFv

9.3.1 Etat: v_Null (néant)

Description

Etat initial (l'utilisateur mobile n'est pas connu dans la fonction LMFv) et la fonction LMFv attend une demande d'enregistrement.

Evénements d'entrée

- Une annulation d'emplacement pour le terminal mobile a été reçue (DP: v_Deregistration).
- Le traitement d'une authentification ou d'un enregistrement refusé pour le terminal mobile est terminé (transition à partir de v_Denied).

Actions

- Suppression du profil d'abonné s'il est présent et libération de toutes les autres ressources attribuées au terminal mobile.

Evénements de sortie

- Une demande d'enregistrement est reçue pour le terminal mobile (DP: v_Initial_reg).

9.3.2 Etat: v_Initial Registration (enregistrement initial)

Description

L'enregistrement d'utilisateur est lancé et une décision sur le traitement de l'authentification est prise.

Evénements d'entrée[3]

- Une demande d'enregistrement est reçue pour le terminal mobile (DP: v_Initial_reg).
- Une demande d'enregistrement est reçue pour le terminal mobile pour une nouvelle zone d'emplacement (pendant l'état actif) (DP: v_Initial_reg).

Actions

- Lancement de l'enregistrement d'utilisateur et rassemblement d'informations sur l'utilisateur (par exemple informations d'authentification et identité de l'utilisateur à partir du précédent réseau visité).
- Décision d'exécuter ou de ne pas exécuter l'authentification. La façon dont cette décision est prise dépend de l'exploitant.

Evénements de sortie

- L'authentification est à exécuter: authentification (DP: v_Authenticate).
- L'authentification n'est pas à exécuter: pas d'authentification (DP: v_Registration).
- L'enregistrement échoue (transition vers v_Denied).

9.3.3 Etat: V_Authentication Processing (traitement de l'authentification)

Description

L'authentification est traitée.

Evénements d'entrée[3]

- L'authentification est nécessaire (DP: v_Authenticate).

Actions

- Extraction de nouveaux paramètres d'authentification si aucun n'est disponible.
- Traitement de l'authentification.

Evénements de sortie

- L'authentification a abouti (DP: v_Registration).
- L'authentification a échoué (DP: v_Auth_denied).

[3] Si l'on tient compte de spécifications de temps réel dans le réseau, ces points de détection doivent être implémentés pour la notification sans que le traitement de la gestion de l'emplacement ne soit suspendu (équivalents à des points TDP-N).

9.3.4 Etat: V_Registration_pending (enregistrement en instance)

Description

L'enregistrement du terminal mobile est traité.

Evénements d'entrée[3]

- L'authentification du terminal mobile a abouti (DP: v_Registration).
- L'authentification n'était pas à exécuter: pas d'authentification (DP: v_Registration).

Actions

- Traitement de l'enregistrement du terminal mobile.
- Une rubrique concernant l'abonné est remplie ou mise à jour avec, notamment, des informations d'emplacement du terminal mobile et la période d'autorisation.
- Le profil d'abonné est extrait.

Evénements de sortie

- L'enregistrement aboutit (DP: v_Registered).
- L'enregistrement échoue (DP: v_Reg_Failure).

9.3.5 Etat: V_Active_registered (terminal enregistré et actif)

Description

Le terminal mobile est enregistré et on suppose qu'il est atteignable.

Evénements d'entrée

- L'enregistrement a abouti (DP: v_Registered).
- Une demande d'enregistrement est reçue d'un terminal mobile détaché (DP: v_ Attach).
- Une demande d'enregistrement est reçue pour le terminal mobile dans la même zone d'emplacement (DP: v_Periodic_reg).

Actions

- Maintien du pointeur d'emplacement du terminal mobile et mise du statut du terminal mobile à actif.
- Si cela est demandé, fourniture d'une adresse de routage pour l'établissement d'un trajet d'échange d'informations (par exemple remise d'appel, remise de message court). Demande de radiorecherche avant le renvoi d'une adresse de routage [c'est une option du réseau visité].
- Si cela est demandé, fourniture d'une notification que le terminal mobile est bien enregistré et actif.
- Si cela est demandé, fourniture d'informations fondées sur le profil de service de l'abonné.

Evénements de sortie

- Une demande d'enregistrement est reçue pour le terminal mobile dans la même zone d'emplacement (DP: v_Periodic_reg).
- Une demande de détachement est reçue pour le terminal mobile (DP: v_Detach).
- Une demande d'annulation d'enregistrement est reçue pour le terminal mobile (DP: v_Deregistration).
- Une demande d'enregistrement est reçue pour le terminal mobile dans une nouvelle zone d'emplacement (DP: v_Inital_reg).

9.3.6 Etat: v_Inactive_registered (terminal enregistré et inactif)

Description

Le terminal mobile est enregistré, mais n'est pas atteignable. Les données d'utilisateur et le profil de service sont toujours conservés dans le réseau visité.

Evénements d'entrée

- Une demande de détachement est reçue pour le terminal mobile (DP: v_Detach).

Actions

- Maintien du pointeur d'emplacement du terminal mobile et mise du statut du terminal mobile à inactif.
- Si cela est demandé, notification du fait que le terminal mobile est inactif.

Evénements de sortie

- Une demande d'enregistrement est reçue du terminal mobile détaché (DP: v_Attach).
- Une demande d'annulation d'enregistrement est reçue pour le terminal mobile (DP: v_Deregistration).

9.3.7 Etat: v_Denied (refus)

Description

Traitement d'un échec ou d'un refus d'authentification ou d'enregistrement.

Evénements d'entrée

- Refus d'authentification (DP: v_Auth_denied) ou lieu d'enregistrement (DP: v_Reg_failure).

Actions

- Fourniture d'informations sur le refus d'enregistrement ou d'authentification pour le terminal mobile.
- Déclenchement du temporisateur relatif aux anomalies.

Evénements de sortie

- Le temporisateur relatif aux anomalies expire (transition vers v_Null).

9.4 Modèle d'états pour la fonction LMFh

Le présent paragraphe donne une description de haut niveau du modèle d'états de gestion de localisation pour la fonction LMFh (fonction de gestion de localisation), montrant des points dans la gestion de l'emplacement (PILM, *points in location management*) et des points de détection (DP). Toutes les transitions possibles d'un point DP à un point PILM et d'un point PILM à un point DP sont illustrées.

Dans l'avenir, ces points de détection pourront être supprimés si aucune justification de service n'est fournie. La suppression de ces points de détection n'aura aucune incidence sur la validité du modèle (états, événements, transitions d'état et actions).

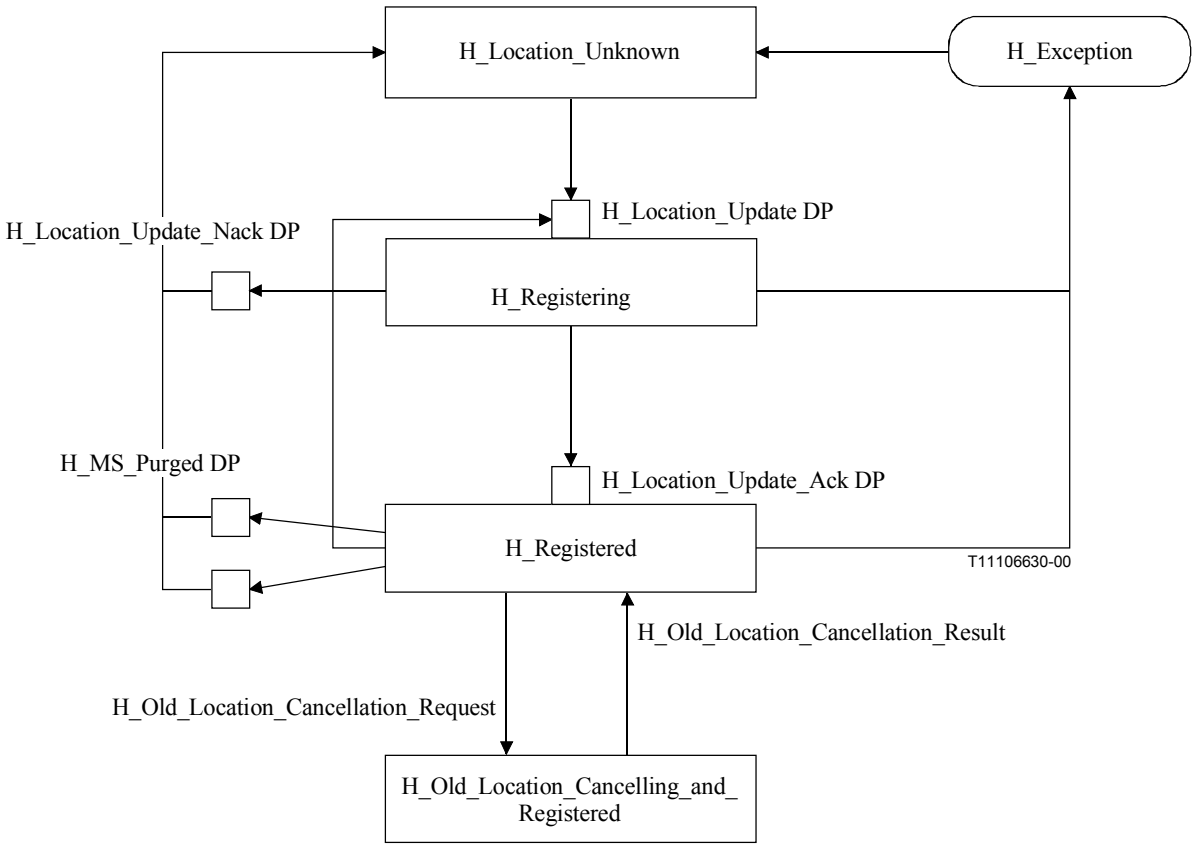


Figure 9-2/Q.1751 – Modèle d'état de gestion de localisation pour la fonction LMFh

9.4.1 Etat H_Location_Unknown (emplacement inconnu)

Description

L'emplacement de l'abonné mobile est inconnu et les services de terminaison (à savoir terminaison d'appel mobile, terminaison de service SMS, etc.) ne peuvent pas être traités.

Evénements d'entrée

- L'abonné mobile est éliminé (DP: H_MS_Purged).
- L'enregistrement de l'abonné mobile dans un domaine visité est annulé par la fonction LMFh (DP: H_present_location_cancelled).
- Une anomalie se produit (PILM: H_Exception).

Actions

- Aucune.

Evénements de sortie

- L'abonné mobile est enregistré dans le réseau mobile (DP: H_Location_Update, prendre note des restrictions décrites dans l'état H_Registering).

9.4.2 Etat H_Registering (enregistrement)

Description

L'abonné mobile qui a changé de zone de service ou s'est rattaché à une zone de service du réseau mobile doit transférer son profil de service dans la zone de service et les informations d'emplacement de l'abonné doivent être mises à jour.

Evénements d'entrée[4]

- L'abonné mobile s'est enregistré dans le réseau mobile (DP: H_Location_Update).
- L'abonné mobile s'est déplacé d'une zone de service à une autre (DP: H_Location_Update).

Actions

- Vérification si l'abonné est connu dans la base de données.
- Autorisation de l'abonné mobile à accéder au réseau.
- Transfert du profil de l'abonné mobile vers la nouvelle zone de service.
- Mise à jour des informations d'emplacement de l'abonné mobile dans la base de données.

Evénements de sortie

- Une réponse négative est faite à la demande de mise à jour d'emplacement (par exemple abonné inconnu, abonné rejeté, etc.) (DP: H_Location_Update_Nack).
- Une réponse positive est faite à la demande de mise à jour d'emplacement (DP: Location_Update_Ack).
- Une anomalie se produit (PILM: H_Exception).

[4] Si l'on tient compte de spécifications de temps réel dans le réseau, ces points de détection doivent être implémentés pour la notification sans que le traitement de la gestion d'emplacement ne soit suspendu (équivalents à des points TDP-N).

9.4.3 Etat H_Registered (enregistré)

Description

L'emplacement de l'abonné mobile est connu et les services de terminaison (à savoir terminaison d'appel mobile, terminaison de service SMS, etc.) peuvent être traités.

Evénements d'entrée

- La mise à jour de l'emplacement a abouti (DP: H_Location_Update_Ack).
- L'annulation de l'emplacement dans l'ancienne fonction LMFv a abouti ou a échoué (PILM: H_old_registration_cancellation_result).

Actions

- Traitement des demandes de l'emplacement pour les services de terminaison.
- Traitement des mises à jour de profil de service dans la fonction LMF visitée. Ces mises à jour de profil n'auront aucune incidence sur l'appel en cours ou sur les autres services en cours.

Evénements de sortie

- Décision d'annuler l'enregistrement (DP: H_present_location_cancelled).
- Décision de supprimer l'abonné dans l'ancienne fonction LMFv (PILM: H_old_location_cancellation_request).
- Indication de la fonction LMFv que l'abonné mobile a été éliminé (DP: H_MS_Purged).
- L'abonné mobile s'est déplacé dans une autre zone de service (DP: Location_Update, prendre note des restrictions décrites dans l'état H_Registering).
- Une anomalie se produit (PILM: exception).

9.4.4 Etat H_Old_Location_Cancelling_and_Registered (annulation de l'ancien emplacement et enregistré)

Description

La rubrique concernant l'abonné dans l'ancienne fonction LMFv est annulée.

Evénements d'entrée

- Décision de la fonction LMFh d'annuler l'emplacement dans l'ancienne fonction LMFv (PILM: H_Old_Location_Cancellation_Request).

Actions

- Interaction avec l'ancienne fonction LMFv pour annuler l'emplacement.
- Mise à jour des informations de l'emplacement de l'abonné mobile dans la base de données.

Evénements de sortie

- L'annulation de l'emplacement aboutit ou échoue (PILM: H_Old_Location_Cancellation_Result).

9.4.5 State_H_Exception

Description

Traitement de la panne et des exceptions.

Evénements d'entrée

- Exceptions HLR survenant pendant le traitement des états H_registered et H_registering.

Actions

- Traitement des exceptions pour un abonné mobile particulier.

Evénements de sortie

- Fin du traitement des exceptions (transition vers l'état H_Location_Unknown).

9.5 Modèle d'états pour la fonction AMF

Le présent paragraphe donne une description de haut niveau du modèle d'états pour la fonction de gestion d'authentification (AMF, *authentication management function*) (voir la Figure 9-3), montrant les points dans la gestion d'authentification (PIAM, *points in authentication management*) et les points de détection (DP). Toutes les transitions possibles d'un point DP à un point PIAM et d'un point PIAM à un point DP sont illustrées. Ce modèle d'états s'applique aussi bien au réseau de rattachement qu'aux réseaux visités. Une instance de modèle d'états d'authentification est créée dans la fonction AMF où l'authentification est traitée. Mais le processus où des paramètres d'authentification sont générés est exclu. Suivant l'implémentation, l'instance est située soit dans le réseau de rattachement soit dans le réseau visité. Il appartient à l'exploitant de décider d'utiliser la fonction AMF du réseau de rattachement ou la fonction AMF du réseau visité.

Dans l'avenir, ces points de détection pourront être supprimés si aucune justification de service n'est fournie. La suppression de ces points de détection n'aura aucune incidence sur la validité du modèle (états, événements, transitions d'état et actions).

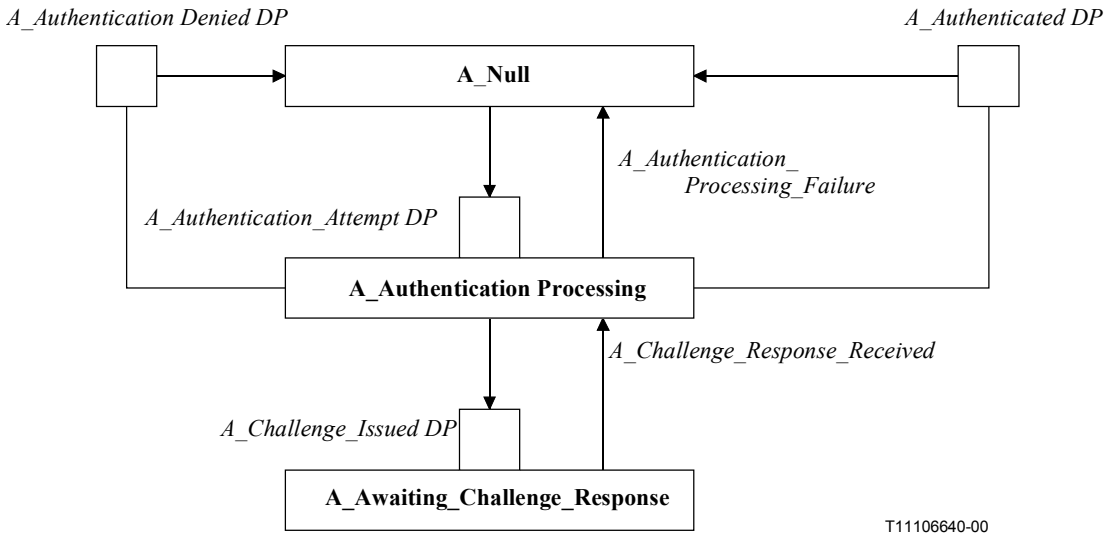


Figure 9-3/Q.1751 – Modèle d'états pour la fonction AMF

9.5.1 Etat: A_Null (néant)

Description

Etat initial (la fonction AMF attend une demande d'authentification de l'utilisateur mobile).

Evénements d'entrée

- Le traitement de l'authentification a échoué (PIAM: A_Authentication_Processing_Failure).
- L'authentification a été refusée (DP: A_Authentication_Denied).
- L'authentification a abouti (DP: A_Authenticated).

Actions

- Aucune.

Evénements de sortie

- Une demande d'authentification est reçue (DP: A_Authentication_Attempt).

9.5.2 Etat: Authentication_Processing (traitement de l'authentification)

Description

Le traitement de l'authentification d'utilisateur a lieu.

Evénements d'entrée

- Une demande d'authentification est reçue (DP: A_Authentication_Attempt).
- Le résultat de Awaiting_Challenge_Response est reçu (PIAM: A_Challenge_Response_Received).

Actions

- Mise à jour du nombre des appels si nécessaire.
- Génération de clés de confidentialité si nécessaire.
- Exécution du traitement de l'authentification et, suivant le résultat de l'état: A_Awaiting_Challenge_Response, l'authentification aboutit ou elle est refusée.

Evénements de sortie

- Le traitement de l'authentification échoue (PIAM: A_Null).
- Une épreuve d'authentification est émise (le traitement par la fonction SCF pourrait avoir lieu à ce moment) (DP: A_Challenge_Issued).
- L'authentification aboutit (DP: A_Authenticated).
- L'authentification est refusée (DP: A_Authentication_Denied).

9.5.3 Etat: Awaiting_Challenge_Response (attente de la réponse à l'épreuve)

Description

La fonction AMF attend une réponse à l'épreuve d'authentification.

Evénements d'entrée

- Une épreuve d'authentification a été émise (DP: A_Challenge_Issued DP).

Actions

- Aucune.

Evénements de sortie

- La fonction AMF reçoit une réponse à l'épreuve d'authentification (PIAM: A_Challenge_Response_Received).
- Le traitement de l'authentification échoue (PIAM: A_Null).

9.6 Communications fonctionnelles de gestion de la mobilité

La Figure 9-4 est extraite de la Recommandation UIT-T Q.1711, avec une extension pour montrer l'interface CN-CN.

Les relations en gras entrent – entièrement ou partiellement – dans le cadre de la gestion de la mobilité.

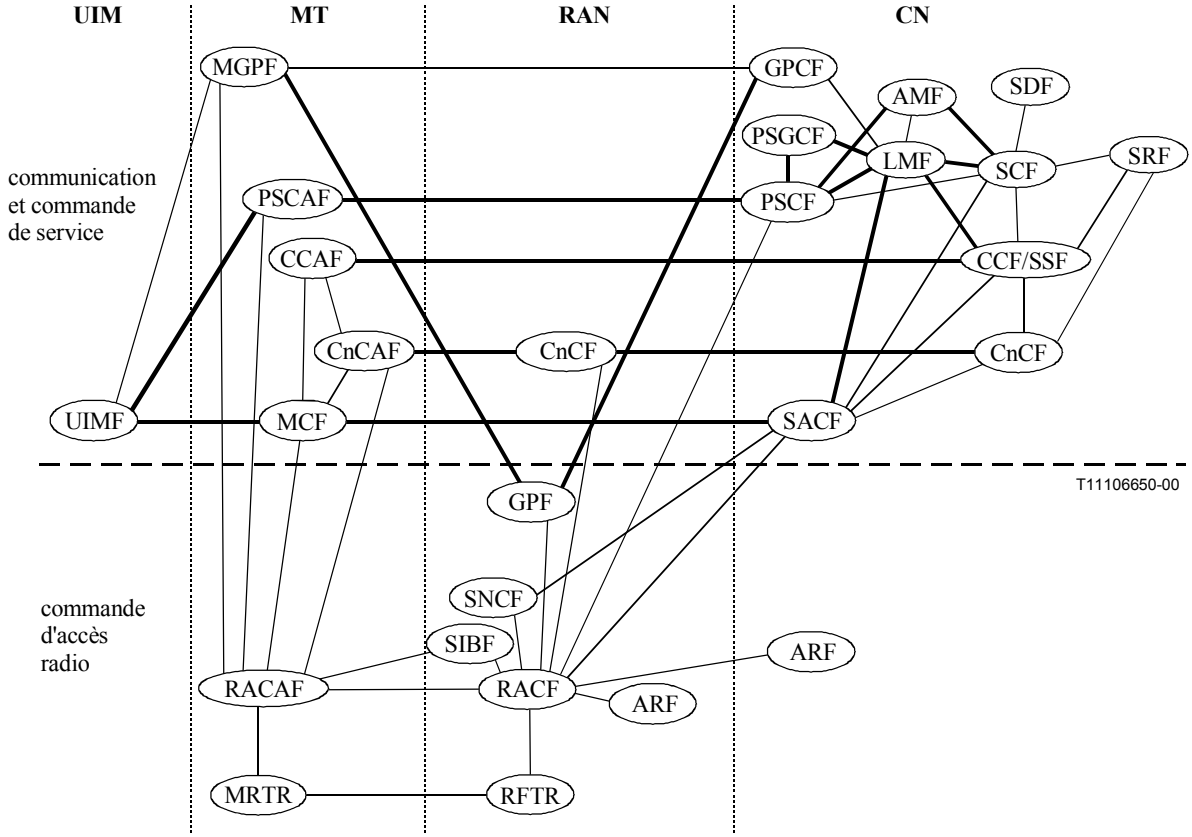


Figure 9-4/Q.1751 – Modèle fonctionnel des IMT-2000 (gestion de la mobilité)

9.7 Choix de la série de protocoles

Il existe déjà divers protocoles sur la mobilité pour les systèmes de la deuxième génération (par exemple GSM MAP et IS-41). Ils ont tous été expressément conçus et optimisés pour ces capacités de service et systèmes de la deuxième génération. Toutefois, le principal inconvénient de ces protocoles est qu'ils ne peuvent pas facilement prendre en charge la communication interfamilles en raison de leur nature et de leur conception spécifiques (c'est-à-dire que la syntaxe et la sémantique des arguments et résultats de ces opérations de gestion de la mobilité sont étroitement couplées avec l'architecture et les services connexes de la deuxième génération).

Les protocoles de la deuxième génération ont besoin d'améliorations pour pouvoir prendre en charge l'itinérance inter-familles entre les différents membres de systèmes IMT-2000. Par conséquent, pour pouvoir établir le protocole commun d'interface NNI pour la gestion de la mobilité en vue de l'itinérance inter-familles, il faut essentiellement créer des éléments de protocole qui ne soient pas restreints à un service mobile particulier et à une technique d'accès radio particulière. Autrement dit, ce protocole doit être suffisamment générique pour s'adapter aux différents membres/systèmes des IMT-2000 du point de vue de l'interface NNI. Pour cela, on peut par exemple définir des opérations génériques fondées sur des paramètres communs des services IMT-2000 qui seront utilisés par ces différents membres. Il faut aussi prendre soin de faire en sorte que l'évolution des systèmes existants de la deuxième génération vers l'interface NNI commune des systèmes de la troisième génération soit aussi lisse que possible.

10 Spécification du protocole pur la commande de services VHE

10.1 Spécifications générales

1) En ce qui concerne les éléments d'information pour l'invocation de service VHE, il est recommandé d'ajouter ce qui suit dans les définitions d'opération applicables du protocole INAP:
   - l'abonné est un abonné mobile;
   - identité de l'abonné mobile (par exemple IMUI);
   - capacités du terminal (par exemple voix, données, etc.);
   - informations d'emplacement (par exemple latitude et longitude, site de cellule, élévation, précision, etc.).
2) Le profil de déclenchement qui est placé dynamiquement et géographiquement doit inclure – en plus de l'identification des déclencheurs, des critères de déclenchement et des adresses de logique de service associées aux déclencheurs – des informations sur la version du protocole destinées au programme de logique de service indiqué. Cette version du protocole est nécessaire pour garantir que la version associée au message envoyé au programme SLP n'est pas supérieure à celle du programme SLP qui peut dans ces conditions reconnaître et traiter le message.
3) En ce qui concerne les flux d'information de service VHE supposant l'utilisation d'une ressource spécialisée, ils doivent être conformes aux spécifications du RI.
4) En ce qui concerne la fourniture de service VHE, les fonctions SCF et SRF du "réseau de prise en charge" pourraient se trouver n'importe où. Des mécanismes d'adressage appropriés sont donc nécessaires. Les capacités d'adressage du protocole INAP pour cet aspect doivent être revues pour vérifier qu'elles sont adéquates.

10.2 Communications fonctionnelles de la commande de service

La Figure 10-1 est extraite de la Recommandation UIT-T Q.1711, et assortie, ici, d'une extension destinée à montrer l'interface CN-CN la capacité de commande de service.

Les relations en gras entrent – entièrement ou partiellement – dans le cadre de la signalisation de commande de service.

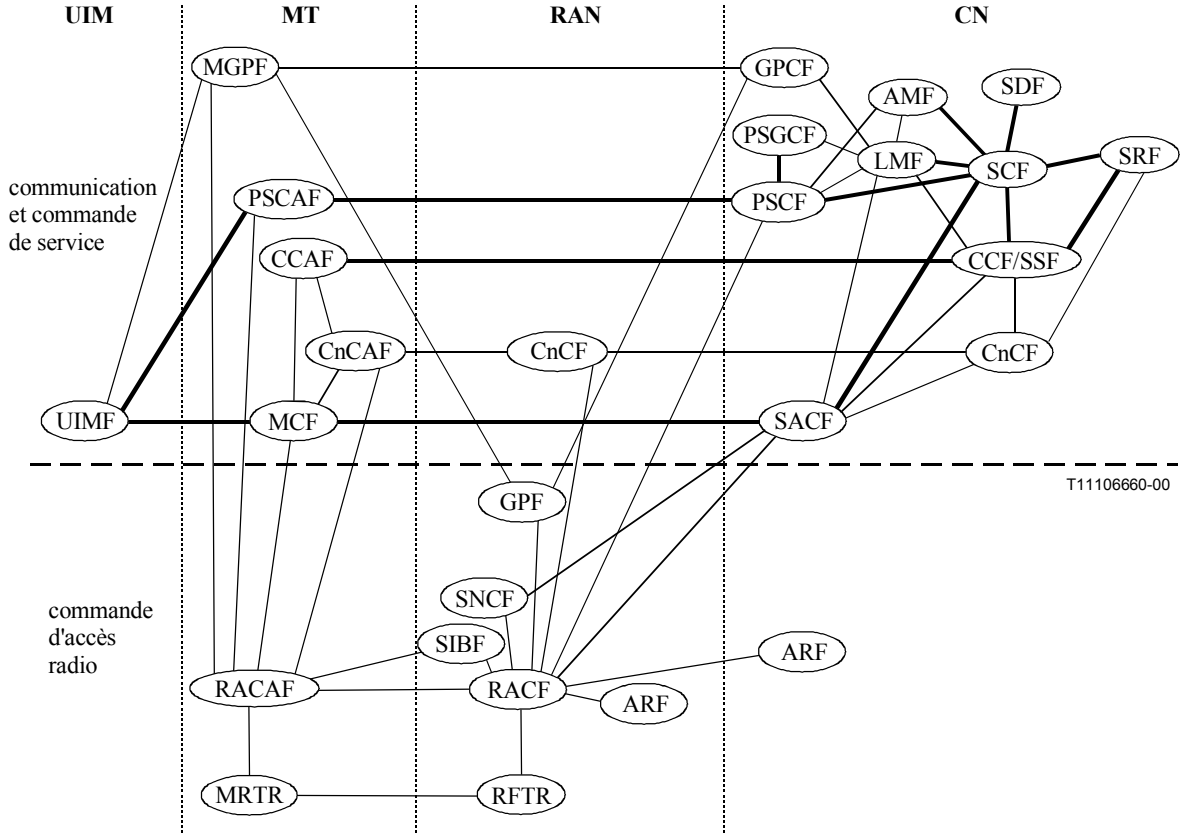


Figure 10-1/Q.1751 – Modèle fonctionnel des IMT-2000 (commande de service)

10.3 Choix de la série de protocoles

Relation	Proposition initiale de protocole
SCF-SDF	INAP + extensions pour la mobilité.
SCF-SRF	INAP + extensions pour la mobilité.
SCF-CCF'/SSF	INAP + extensions pour la mobilité.
SCF-AMF	De type INAP fondé sur le modèle d'états pour la fonction AMF. Voir le paragraphe 9/Q.1721 pour les flux d'information.
SCF-LMF	De type INAP fondé sur le modèle d'états pour la fonction LMF – à définir.
SRF-CCF'/SSF	Protocole approprié de commande de support.
SCF-UIMF (paquet via PSCF, PSCAF)	Le transport sera assuré via le protocole IPv4 avec éventuellement une évolution vers le protocole IPv6.
SCF-UIMF (circuit via SACF, MCF)	Options identifiées: • le service complémentaire USSD du RNIS sera utilisé pour prendre en charge le dialogue service/utilisateur. Voir le paragraphe 11/Q.1721 pour les flux d'information; • la capacité OCCRUI de l'ensemble CS-2 du RI utilise le mécanisme de transport APM de l'ISUP et GAT du DSS1.

11 Spécifications du protocole pour la commande d'appel et de support

11.1 Spécifications générales

Relevé des données d'appel (CDR): cette procédure permet de transférer les données de relevé CDR du réseau de desserte au réseau de rattachement. En outre, un transfert de relevé CDR en temps réel doit être assuré. Toutefois, afin de minimiser le transfert de données, seules les étiquettes de référence d'appel et les données nécessaires au traitement de l'appel doivent être transférées.

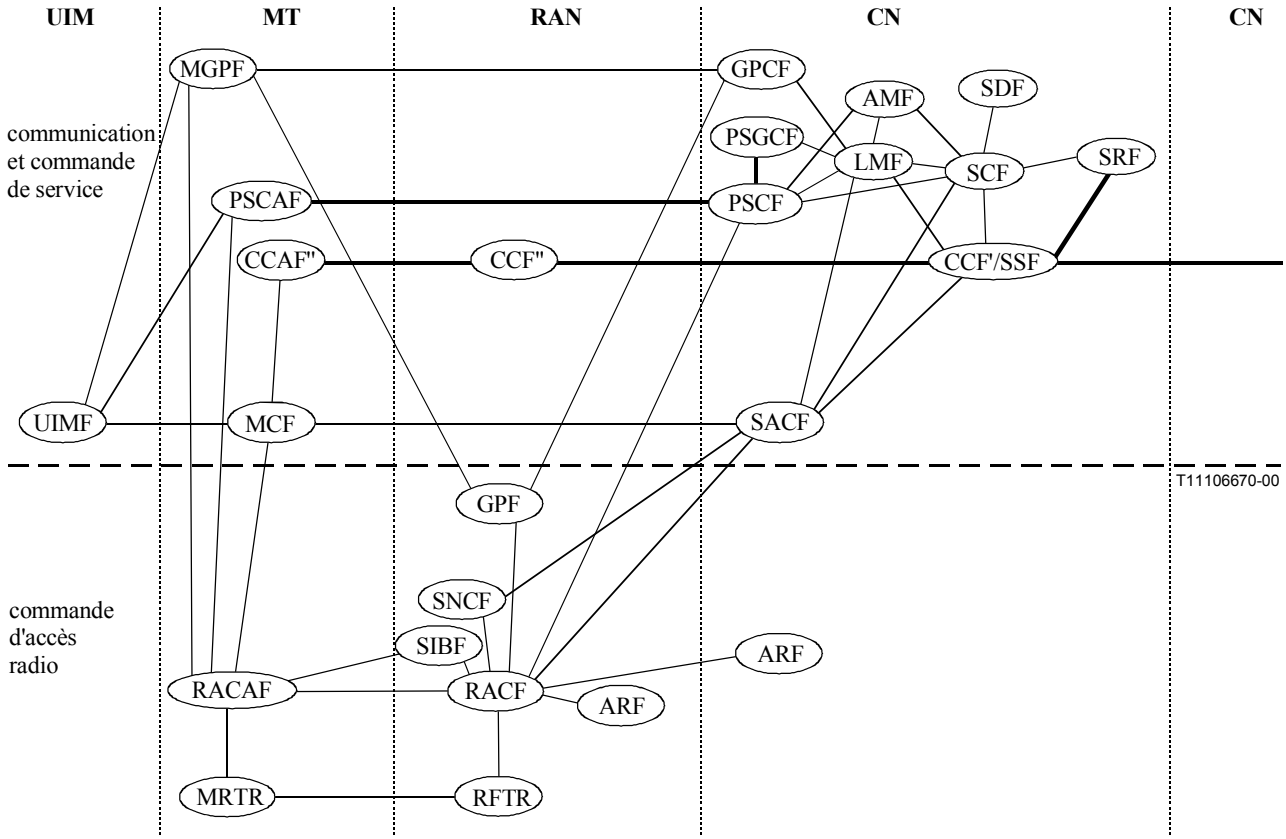
11.2 Choix des principes de commutation

Les techniques de commutation (commutation de circuit, ATM, AAL2, relais de trames, ...) doivent être choisies par l'exploitant ou par le fournisseur de services.

11.3 Communications fonctionnelles de la commande d'appel et de support

Les Figures 11-1 et 11-2 sont extraites de la Recommandation UIT-T Q.1711, avec une extension pour montrer -l'interface CN-CN.

Les relations en gras entrent – entièrement ou partiellement – dans le cadre de la signalisation de commande d'appel et de support.



NOTE – La fonction CCF" est introduite pour tenir compte de la fonctionnalité de conversion de protocole (liée à la commande d'appel et de support) entre les interfaces MT-RAN et RAN-CN.

Figure 11-1/Q.1751 – Modèle fonctionnel des IMT-2000 Variante 1: intégration des entités fonctionnelles de commande d'appel et de commande de connexion

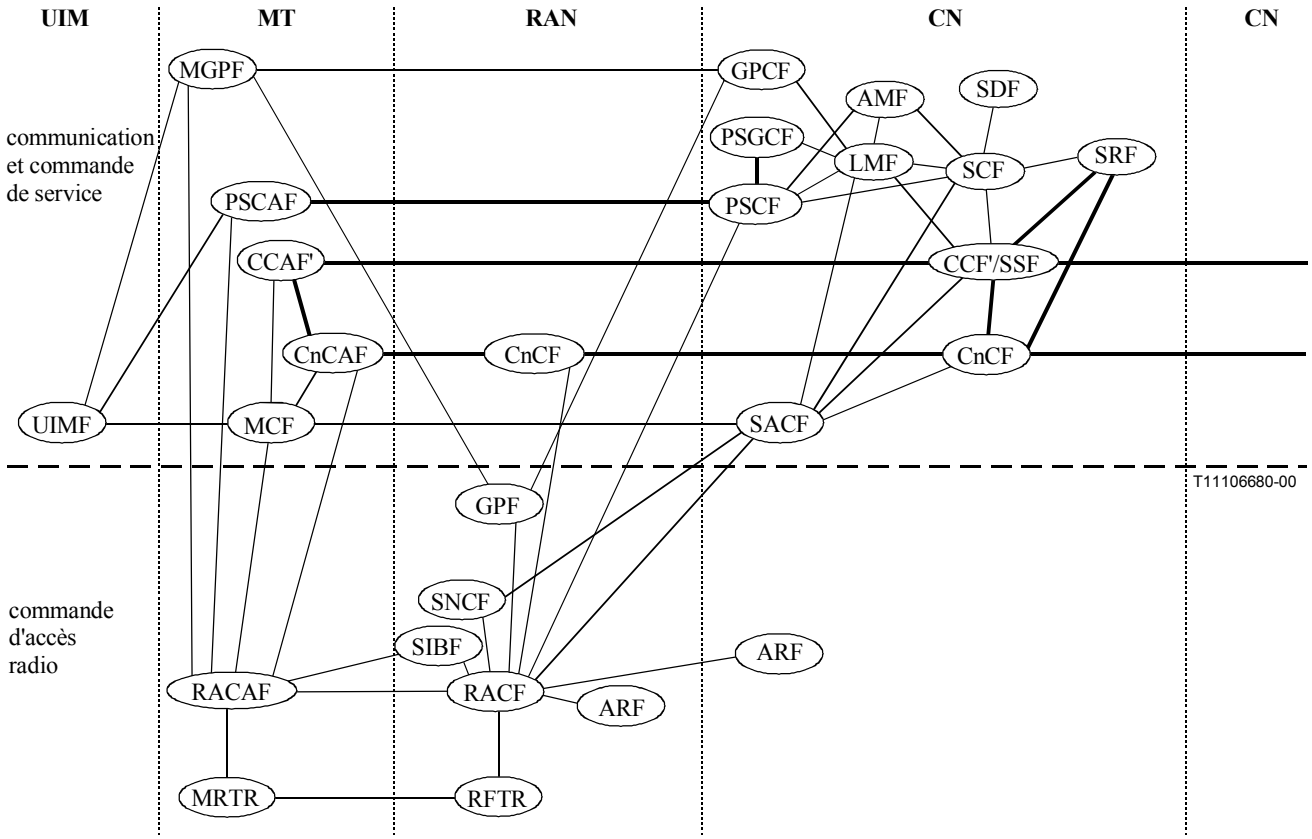


Figure 11-2/Q.1751 – Modèle fonctionnel des IMT-2000 Variante 2: séparation des entités fonctionnelles de commande d'appel et de commande de connexion

11.4 Choix de la série de protocoles

On peut utiliser les protocoles suivants pour l'ensemble CS-1 des IMT-2000:

Relation fonctionnelle	Proposition de protocole
CCF-CCF'	BICC N-ISUP pour STM
CnCF-CnCF	Q.AAL2 pour ATM AAL2 B-ISUP pour ATM AAL1 NOTE – D'autres comme PNNI/ATM ou AINI/ATM ne sont pas exclus.

En raison de contraintes temporelles, on a attribué aux relations fonctionnelles suivantes un rang de priorité plus bas dans le cadre du calendrier associé à l'ensemble CS-1 des IMT-2000.

Relation fonctionnelle	Proposition de protocole
CCAF'-CCF'	Protocole propre à un membre de la famille dans le cadre du calendrier associé à l'ensemble CS-1 des IMT-2000
CnCAF-CnCF	
CnCF-CnCF	
PSCAF-PSCF	
PSCF-PSGCF	

Deux domaines sont à distinguer, le domaine RTPC/RNIS et le domaine des données par paquets, dans la mesure où ils sont associés aux protocoles suivants:

1) *domaine des services RNIS/RTPC*

   a) commande d'appel: BICC, N-ISUP pour STM;

   b) commande de support: B-ISUP pour ATM AAL1;
   Q.AAL2 pour ATM AAL2.

   Une certaine souplesse est nécessaire en ce qui concerne la technique de transport des IMT-2000 afin de répondre aux besoins d'un marché déréglementé et dynamique;

2) *domaine des services de données par paquets*

   a) commande d'appel: pas nécessaire;

   b) commande de support: support ATM AAL5;

   c) couche Réseau: protocole Internet (IP).

   Une certaine souplesse est nécessaire en ce qui concerne la technique de transport des IMT-2000 afin de répondre aux besoins d'un marché déréglementé et dynamique. Par conséquent, différents types de support doivent être autorisés dans l'ensemble CS-1 des IMT-2000.

11.5 Appels multimédias

Les spécifications pour les appels multimédias des IMT-2000 comprennent la capacité de fusion des flux de médias sur une même connexion. Les médias sont considérés comme étant différents types de trains de données (par exemple voix, données, images, etc.). Ils peuvent être multiplexés sur une même connexion et être commandés (par exemple ajout ou élimination d'un média) sur la base de Recommandations UIT-T existantes (par exemple H.323, H.245, H.248), "dans la bande" dans la connexion support. La spécification dans le cas de l'ensemble CS-2 pour la couche AAL2 est que la largeur de bande de la connexion AAL2 doit être modifiable. Cette spécification est traitée dans le cadre de l'ensemble CS-2 pour la signalisation dans la couche AAL2.

11.6 Appels multiparticipants

Les capacités d'ajout et d'élimination de participant nécessitent uniquement des configurations de communication point à point avec un serveur ou un pont (configuration 6), pouvant simuler les configurations 2, 3, 4 et 5 du point de vue de l'utilisateur. Cette configuration de type 6 est une configuration de communication qui inclut un nœud serveur (par exemple un pont de conférence, MCU, *multipoint communication unit*) dans le réseau, pouvant établir plusieurs connexions point à point. Cela offrira à l'utilisateur final la possibilité d'avoir des communications multipoint à multipoint. Les configurations de communication de type 1 et 6 permettent toujours à la racine, une feuille ou un tiers de lancer l'ajout ou l'élimination de participant (voir TRQ 2001).

En outre, la capacité d'appels multiparticipants inclut uniquement la capacité d'ajout ou d'élimination de participant lancée par la racine ou par une feuille. Aucune capacité d'ajout ou d'élimination d'un participant par un tiers n'est nécessaire pour l'ensemble CS-1 des IMT-2000. Par ailleurs, il est

nécessaire d'inclure une signalisation de notification à la racine, lorsqu'il se produit un événement d'ajout ou d'élimination de participant lancé par une feuille.

12 Spécifications du protocole pour la commande de services par paquets

Les éléments fonctionnels qui prendront en charge des services de données par paquets et leurs relations de part et d'autre des frontières de réseaux centraux sont montrés sur la Figure 12-1. Le présent paragraphe donne un ensemble de spécifications associées à la prise en charge par l'interface NNI des services de données par paquets.

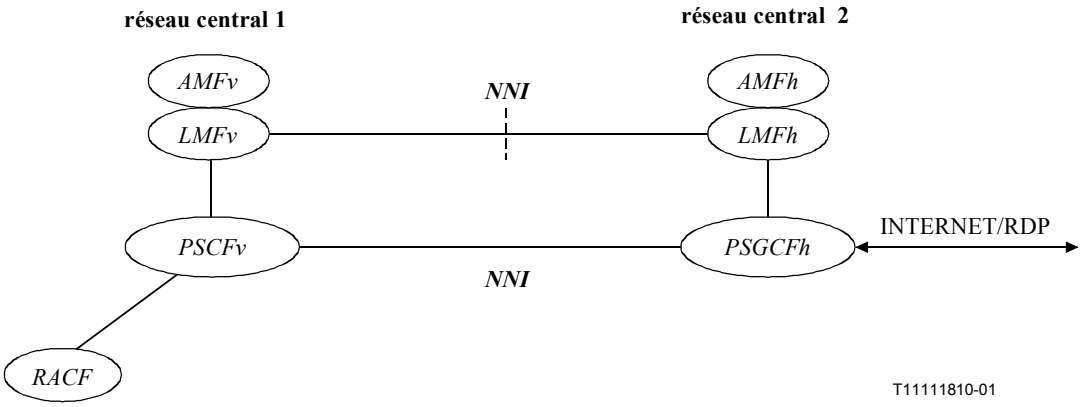


Figure 12-1/Q.1751 – Interfaces entre réseau de données par paquets (RDP) et réseau

12.1 Protocole d'interface PSCF - PSGCF

Les deux capacités fonctionnelles que les fonctions PSCF et PSGCF assureront sont les suivantes:

1) transfert de données d'utilisateur entre ces deux entités;
2) interaction entre ces deux entités pour les mises à jour de contextes de routage et de service par paquets.

Ces deux fonctions et le flux d'information associé appartiennent à deux plans logiques disjoints: le plan d'utilisateur et le plan de commande. La première fonction identifiée ci-dessus appartient au plan d'utilisateur tandis que la seconde appartient au plan de commande.

Les spécifications fonctionnelles énumérées ci-dessous se rapportent aux deux plans (utilisateur et commande) lorsque les fonctions PSCF et PSGCF résident dans deux réseaux centraux (CN, *core network*) différents.

1) Lorsque les fonctions PSCF et PSGCF résident dans deux réseaux centraux différents, ces deux entités doivent être interconnectées sur un réseau IP.
2) Lorsque les fonctions PSCF et PSGCF sont connectées sur l'Internet public, il doit y avoir une association de sécurité entre ces deux fonctions.
3) Lorsque le réseau central de rattachement autorise le terminal mobile à utiliser des services de données dans un réseau central visité, il doit charger le réseau central visité de choisir une fonction PSGCF spécifique ou de proposer l'attribution d'une fonction PSGCF locale dans le réseau central visité pour pouvoir assurer une session de service de données.
4) Lorsque la session de service de données est établie, la fonction PSGCF attribuée doit être fixée pour toute la durée de cette session. Le réseau central visité dans lequel cette fonction PSGCF réside devient le réseau central d'ancrage, CNa, pour la session de données.

5) Lorsque le terminal mobile lance une session de service de données, la fonction PSCF doit être attribuée par le réseau central dans lequel la session de service de données est lancée.

6) Lorsque le terminal mobile se déplace pour entrer dans un réseau central visité au cours d'une session de service établie, le réseau central visité doit attribuer dynamiquement une nouvelle fonction PSCF pour pouvoir assurer cette session. Plusieurs fonctions PSCF successives peuvent être attribuées au terminal mobile au cours de son déplacement dans le réseau central visité (pendant l'itinérance intraréseau central).

7) On peut utiliser l'identificateur IMSI ou NAI comme identificateur de session de service unique dans toutes les transactions de protocole. Si le terminal mobile prend en charge plusieurs sessions de service simultanées, il faut utiliser un numéro de session associé pour identifier de manière univoque chaque session de service.

12.1.1 Spécifications se rapportant au plan d'utilisateur

1) Les fonctions PSCF et PSGCF doivent transférer les informations d'utilisateur sur un réseau IP en employant un tunnel IP bidirectionnel.

2) Le plan d'utilisateur peut incorporer un mécanisme qui prendra en charge l'existence simultanée de plusieurs connexions-tunnel bidirectionnelles à l'intérieur du tunnel IP qui relie les fonctions PSCF et PSGCF.

3) Le plan d'utilisateur doit incorporer un mécanisme optionnel (par exemple un mécanisme d'encapsulation) permettant d'éviter des remises hors séquence d'unités de données de paquet d'utilisateur via la connexion-tunnel.

4) A tout instant, chaque connexion-tunnel entre les fonctions PSCF et PSGCF doit avoir une durée de vie spécifiée, qui doit pouvoir être allongée. Lorsque la durée de vie d'une connexion-tunnel donnée expire, la connexion-tunnel en question doit être libérée.

12.1.2 Spécifications se rapportant au plan de commande

1) Le protocole de commande entre les fonctions PSCF et PSGCF doit être capable d'établir des connexions-tunnel individuelles, d'allonger la durée de vie des connexions-tunnel établies et de libérer les connexions-tunnel établies.

2) Les fonctions PSCF et PSGCF doivent employer le protocole UDP pour échanger des messages de commande. Ces messages peuvent être protégés par un tunnel de sécurité IP.

3) Un port UDP spécialisé et bien connu situé dans la fonction PSGCF doit terminer le canal de commande sur lequel les messages de commande entre les fonctions PSCF et PSGCF doivent être échangés.

4) Les fonctions PSCF et PSGCF doivent employer un protocole bidirectionnel de prise de contact (c'est-à-dire avec deux messages) lors de l'établissement d'une connexion-tunnel ou de l'allongement de la durée de vie d'une connexion-tunnel établie. Le protocole unidirectionnel doit être utilisé pour libérer une connexion-tunnel établie.

5) Les fonctions PSCF et PSGCF doivent être capables d'établir une association de sécurité entre elles et d'exécuter le chiffrement des données et la vérification d'authentification et d'intégrité des messages de commande.

12.2 Protocole d'interface LMFp – LMFp

Pour accéder à des services de données par paquets, le terminal mobile itinérant s'enregistrera auprès du réseau IMT-2000 visité en employant des procédures communes d'authentification et d'enregistrement de terminal et demandera l'accès aux fonctionnalités de données par paquets. On peut conserver un relevé de comptabilité associé pour enregistrer l'utilisation des ressources de données par paquets. L'architecture de réseau central doit permettre de séparer les capacités de la fonction LMF (et de la fonction AMF associée) se rapportant à des fonctionnalités d'accès et les

capacités de la fonction LMFp (et de la fonction AMFp associée) se rapportant aux services de données par paquets. Les spécifications énumérées ci-dessous concernent l'interaction entre les fonctions LMFp du réseau de rattachement et du réseau visité, qui résident dans deux réseaux centraux différents et incorporent uniquement les capacités de données par paquets.

1) Lors de l'échange d'informations se rapportant à des services de données par paquets, la fonction LMFp du réseau visité et une fonction LMFp de réseau de rattachement doivent pouvoir acheminer les informations correspondantes sur un réseau IP.

2) Une association de sécurité entre une fonction LMFp de réseau visité et une fonction LMFp de réseau de rattachement doit exister avant que des informations puissent être échangées entre ces deux entités. L'association de sécurité peut être automatiquement établie, préarrangée, ou la fonction LMFp de réseau visité et la fonction LMFp de réseau de rattachement peuvent communiquer via un tiers de confiance (par exemple un courtier) avec lequel elles ont chacune une association de sécurité.

3) Le protocole entre la fonction LMFp du réseau visité (et la fonction AMFp associée) et la fonction LMFp du réseau de rattachement (et la fonction AMFp associée) doit permettre au réseau central visité d'authentifier le terminal mobile visiteur et de l'autoriser à utiliser les services de données par paquets dans le réseau central visité.

4) Si l'authentification du terminal mobile par la fonction LMFp du réseau de rattachement échoue, le réseau central visité n'autorisera pas de service de données par paquets. Le réseau central visité se fondera sur un accord de taxation si le réseau de rattachement autorise un service.

5) Lorsqu'il utilise des services de données par paquets, le terminal mobile visiteur ne peut s'identifier auprès du réseau de données par paquets qu'avec son identificateur NAI. La fonction LMFp du réseau visité doit pouvoir identifier et localiser la fonction LMFp du réseau de rattachement sur la base de l'identificateur NAI.

6) La fonction LMFp du réseau visité doit pouvoir demander quelle fonction PSGCF le réseau central visité doit utiliser pour la session de données par paquets considérée et la fonction LMFp du réseau de rattachement doit pouvoir identifier cette fonction.

7) La fonction LMFp du réseau visité doit pouvoir demander quelle adresse IP sera utilisée par le terminal mobile au cours de la session de données par paquets considérée et la fonction LMFp du réseau de rattachement doit pouvoir fournir cette adresse.

8) Le protocole entre les fonctions LMFp homologues doit fournir un mécanisme permettant d'acheminer les informations de comptabilité d'un côté à l'autre de l'interface.

9) Les fonctions LMFp homologues doivent utiliser un identificateur de session unique (ID de session) pour chaque session de données par paquets à laquelle elles sont mutuellement associées.

10) Les fonctions LMFp homologues doivent employer un ensemble de codes de réponse qui doit être inclus dans chaque message de réponse. Un code de réponse permet de fournir des informations en réponse à une demande (par exemple service refusé, condition d'erreur, mot de passe incorrect) faite par l'homologue demandeur.

En ce qui concerne les services de données par paquets, le réseau IMT-2000 fournira deux niveaux de sécurité – la sécurité du réseau d'accès et la sécurité du réseau de données par paquets. La sécurité du réseau d'accès inclut le chiffrement des signaux radio et la gestion de clé d'accès radio pour l'authentification du terminal mobile. La sécurité du réseau de données par paquets inclut le chiffrement et la mise en tunnel de paquets sur l'Internet public et l'authentification du terminal mobile auprès du réseau IMT-2000 au moyen d'une clé secrète. Les spécifications d'interface LMFp – LMFp énumérées ci-dessous se rapportent à la sécurité du réseau de données par paquets.

1) En ce qui concerne l'authentification et l'autorisation de service, il est possible que le réseau central de rattachement puisse fournir au réseau central visité des informations de sécurité concernant le terminal mobile.

2) Il doit exister un mécanisme par lequel la fonction LMFp du réseau visité pourra acheminer à la fonction LMFp du réseau de rattachement la valeur d'épreuve et la valeur de réponse à l'épreuve. La valeur d'épreuve contiendra la valeur que le réseau central visité a transmise au terminal mobile visiteur. La valeur de réponse à l'épreuve contiendra la valeur que le terminal mobile visiteur a générée au moyen de la valeur d'épreuve et du secret que le terminal mobile visiteur partage avec son réseau central de rattachement.

3) Il doit exister un mécanisme par lequel la fonction LMFp du réseau visité et la fonction LMFp du réseau de rattachement pourront échanger des paramètres de sécurité (par exemple un identificateur SPI et des clés de sécurité). Les paramètres de sécurité reçus de la fonction LMFp du réseau de rattachement permettront au réseau central visité d'établir une association de sécurité bidirectionnelle avec le terminal mobile visiteur ainsi qu'entre la fonction PSCF du réseau central visité et la fonction PSGCF du réseau central de rattachement.

APPENDICE I

Indications sur certains concepts liés aux déclencheurs et sur leur utilisation

I.1 Objet

L'objet du présent appendice donné à titre d'information est de fournir des indications sur l'utilisation de déclencheurs au moyen d'un exposé informel sur quelques éléments essentiels relatifs à l'amorçage et au traitement des déclencheurs dans le cadre des IMT-2000. Ces lignes directrices de base seront probablement améliorées et optimisées pour répondre aux besoins spécifiques (par exemple à des besoins opérationnels) des différents membres de la famille des IMT-2000.

I.2 Introduction

Dans le présent appendice, on commence par s'intéresser à certains principes et concepts. Puis on établit des lignes directrices relatives à l'utilisation et à l'application de déclencheurs sur la base de ces principes et concepts. Il est à noter que, bien qu'ils soient fondés sur le modèle BCSM lié à l'appel, les principes et concepts s'appliquent aussi aux modèles d'états de gestion de l'emplacement et d'authentification. Les autres sous-paragraphes du présent appendice, qui portent sur l'amorçage dynamique et la répartition des déclencheurs, nécessitent un examen complémentaire pour déterminer si ces lignes directrices sont appropriées pour le déclenchement de services de gestion de l'emplacement et de gestion de l'authentification.

On trouvera, dans les Recommandations UIT-T Q.1231 et Q.1238 (Parties 1 et 2) relatives au RI, des informations complémentaires sur le déclenchement et les principes de modélisation d'appel du modèle BCSM, servant de base aux sous-paragraphes suivants.

I.3 Principes et concepts

1) Les déclencheurs sont indépendants du service:

   un concept fondamental du déclenchement est que les déclencheurs sont indépendants du service. Cela signifie que lorsqu'on rencontre un déclencheur amorcé dont les critères sont satisfaits, le centre MSC ne sait pas quel ou quels services seront invoqués en résultat du message qu'il envoie au programme de logique de service (SLP, *service logic program*) au niveau de la fonction SCF.

2) Les déclencheurs incluent des informations d'adresse de logique de service:

dans le cas d'abonnés hertziens, le déclencheur de service, qui indique implicitement la fonction SCF qui doit être consultée, se trouve dans la fonction LMFh, tout comme le profil de service d'abonné.

3) Le programme SLP répondra par une instruction exécutable:

le centre MSC attend que la fonction SCF (le programme SLP) réponde par une instruction appropriée sur la façon de traiter l'appel. Il doit vérifier si l'instruction reçue est appropriée compte tenu de la vue qu'il a alors concernant l'appel. Dans certains cas, des événements liés à l'appel ont pu se produire entre la demande faite à la fonction SCF (au programme SLP) et la réponse de la fonction SCF et se traduire par le fait que l'instruction reçue est inappropriée. C'est le cas par exemple de l'abandon par l'appelant.

4) On n'agit en fonction des déclencheurs que lorsqu'ils sont rencontrés dans le modèle BCSM:

dans certains cas, des informations sont fournies avant que le modèle BCSM ne les recherche, par exemple en cas de notification d'abonné occupé en résultat d'une procédure de gestion de la mobilité (par exemple demande d'emplacement). Le modèle O-BCSM ne reconnaît cette condition d'abonné occupé qu'à partir du moment où le traitement d'appel a progressé jusqu'à l'instanciation d'un modèle T-BCSM et où ce dernier a progressé jusqu'à la rencontre du point de détection T_Busy (abonné occupé). Si l'état d'abonné occupé n'est pas utilisé à cet endroit, le modèle T-BCSM le renvoie au modèle O-BCSM où il sera peut-être utilisé.

Il est à noter que le présent exposé décrit la modélisation du RI (se référer aux Recommandations UIT-T de la série Q.1238). Chaque implémentation est libre d'examiner les informations d'abonné occupé dès qu'elles sont disponibles afin d'optimiser la performance, mais elle doit savoir qu'il est possible que d'autres services soient invoqués entre le moment où les informations d'abonné occupé sont reçues et le moment où la modélisation indique qu'elles doivent être examinées.

5) L'ordre de priorité des déclencheurs est le suivant: abonné, groupe, bureau:

cette séquence permet aux fournisseurs de service d'offrir aux abonnés sélectionnés l'utilisation de services qui ne sont pas mis à la disposition de la clientèle générale, par exemple d'offrir l'accès à des services améliorés comme l'appel de conférence, etc. De manière analogue, cet ordre de priorité permet aux fournisseurs de services de refuser aux abonnés sélectionnés des services qui sont mis à la disposition de la clientèle générale, par exemple de restreindre les appelants à certains codes de zone, etc.

6) Chaque déclencheur est examiné entièrement avant de passer au déclencheur suivant:

les déclencheurs sont énumérés dans un certain ordre de priorité. Ce principe indique qu'un type de déclencheur donné est examiné du point de vue de son applicabilité à l'abonné, au groupe et au bureau avant de passer au type de déclencheur suivant dans l'ordre de priorité.

Il est possible d'affiner les points 5) et 6) pour tenir compte de la priorité et du séquencement des critères de déclenchement mais cela dépend du service particulier et des spécifications opérationnelles du membre particulier de la famille des IMT-2000. Par exemple, pour assurer la compatibilité amont avec les systèmes existants de la deuxième génération, un traitement spécifique des déclencheurs de service pourra être nécessaire lors du fonctionnement dans le contexte des systèmes de la troisième génération.

I.4 Amorçage dynamique de déclencheur

Le profil des déclencheurs d'un abonné est enregistré avec d'autres informations relatives aux services dans la fonction LMFh. Ce profil est considéré comme "statique" car il varie lentement, voire pas du tout. En fait, il reste le même sauf si l'abonné ajoute ou supprime, dans le profil, un service avec déclenchement, ou met en fonction ou met hors fonction ou encore modifie l'un des

services auquel il est abonné. C'est ce profil "statique" qui est dynamiquement placé dans un lieu géographique à mesure que l'abonné se déplace et qu'il est desservi par différents centres MSC.

Le profil des déclencheurs d'un abonné peut être modifié pour une instance d'appel donnée sans affecter le profil "statique". Ces modifications du profil ne survivent pas après l'appel en cours. A la libération de l'appel, toutes ces modifications disparaissent. C'est ce qu'on appelle un amorçage "dynamique" de déclencheur.

L'amorçage dynamique de déclencheur est une capacité puissante, mais qui peut aussi être facilement mal utilisée. Il incombe aux fournisseurs de services utilisant cette capacité de comprendre et de traiter les effets secondaires potentiels liés à cette utilisation. Par exemple, lorsque plusieurs points SCP fournissent des services, une utilisation inappropriée de la capacité d'amorçage dynamique de déclencheur peut provoquer des interactions de services non souhaitées ou des pannes du point de vue de l'utilisateur final. En cas de mauvaise coordination, un programme de logique de service au niveau d'un point SCP donné peut écraser des déclencheurs amorcés pour un programme de logique de service au niveau d'un autre point SCP. Les conséquences peuvent être une panne du service, ou une non-exécution ou encore une exécution incorrecte. Lorsque plusieurs fournisseurs de services sont impliqués, il est peu probable qu'ils connaissent l'ensemble complet des services qui font l'objet d'un abonnement et qu'ils aient conscience des effets susceptibles d'être causés aux services qui leur sont inconnus.

I.5 Répartition des déclencheurs

Etant donné que les abonnés sans fil sont par nature mobiles, il faut examiner comment répartir les déclencheurs de leurs services. L'origine ou la destination d'un appel mobile peut se produire n'importe où et l'abonné itinérant peut se trouver n'importe où dans les zones d'itinérance mises à sa disposition, il faut donc répartir le traitement des services de façon optimale. On suppose que lorsqu'un fournisseur de services offre un ensemble de services à un abonné, il doit faire en sorte que cet ensemble contienne des services appropriés, cohérents et homogènes entre eux qui interagiront les uns avec les autres pour l'abonné.

Les options relatives au placement dynamique dans un lieu géographique de déclencheurs d'origine et de destination amorcés statiquement sont les suivantes: centre MSC d'origine, centre MSC de destination ou centre MSC passerelle. Si des profils de déclencheurs identiques sont placés dans les trois centres, certains services risquent d'être exécutés deux fois, ce qui conduira à des résultats indésirables. Etant donné que des profils de déclencheurs identiques ne doivent pas être placés partout, il faut des critères qui permettent de décider où placer les déclencheurs.

On donne les critères suivants pour faciliter le processus de prise de décision quant à la détermination de l'endroit où les déclencheurs de service seront placés.

En ce qui concerne l'optimisation des ressources de réseau, les déclencheurs d'origine d'appel sortant doivent être placés aussi proche que possible de l'appelant. D'une manière générale, cela signifie que les déclencheurs d'origine de l'abonné doivent être placés au niveau du centre MSC d'origine lorsque l'abonné mobile procède à son enregistrement.

En ce qui concerne les appels adressés à un abonné, pour garantir une utilisation optimale des ressources que sont les connexions supports du réseau, il est souhaitable de placer les déclencheurs de services susceptibles d'empêcher la terminaison d'un appel, aussi proche que possible du point d'origine de l'appel. On peut donc placer un ensemble de déclencheurs de destination au niveau du centre MSC d'origine ou du centre MSC passerelle pour être employés dans un modèle BCSM utilisé comme mandataire pour l'appelé. Ces déclencheurs doivent être indiqués dans les informations retournées avec la demande de routage (ou de mise à jour de localisation). Toutefois, il est à noter que le fait de placer des profils de déclencheurs dans des commutateurs locaux (centres MSC) est plus onéreux et rend plus élevés les frais de déploiement du service engagés par les fournisseurs de services de réseau avant que la demande commerciale du service soit confirmée. En règle générale,

sauf si le service nécessite une grande disponibilité (forte utilisation ou temps de réponse courts) ou nécessite un déploiement dans les commutateurs locaux (centres MSC) pour des raisons techniques, il faut examiner les avantages en termes de coût liés au déploiement dans des commutateurs de transit ou dans des passerelles interrogatrices.

Si l'appel est dévié vers une autre destination, cela doit avoir lieu aussi proche que possible de l'origine de l'appel (par exemple dans le centre MSC d'origine ou le centre MSC passerelle). Un exemple en termes de services est le renvoi d'appel vers un service de messagerie vocale.

La sécurité de signalisation peut nécessiter que des déclencheurs soient déployés dans un nœud de transit ou un nœud passerelle. Par conséquent, si la fonction SSF est dans un réseau donné et si le point SCP est dans un autre réseau, des STP et GTT seront nécessaires au niveau du transport de signalisation. L'utilisation de STP et GTT réduira la vitesse de la signalisation et nécessitera une sécurité supplémentaire pour que les fournisseurs de services puissent sécuriser leur contexte de protocole.

Si un service est fortement utilisé, il faut un déploiement dans le centre MSC du réseau visité, d'origine ou de destination.

Si un service nécessite des temps de réponse très courts, il faut un déploiement dans le centre MSC du réseau visité, d'origine ou de destination.

Les réseaux qui emploient un routage optimal peuvent nécessiter que des déclencheurs soient déployés dans le centre MSC du réseau visité, d'origine ou de destination, car le déclenchement au niveau du nœud (de transit) interrogateur peut provoquer un routage complexe, par exemple avec des parties en trombone.

Des temporisateurs de signalisation peuvent nécessiter que les déclencheurs d'origine soient placés dans le centre MSC d'origine et que les déclencheurs de destination soient placés dans le centre MSC de destination. Comme un certain nombre de conditions particulières nécessitent que le centre MSC réinitialise les temporisateurs de courte durée du RNIS au moment de l'accès au réseau pendant que le point SCP traite l'application, cela ne peut se faire à d'autres commutateurs.

L'accès aux informations relatives à la zone d'emplacement peut nécessiter que les déclencheurs d'origine soient placés dans le centre MSC d'origine et que les déclencheurs de destination soient placés dans le centre MSC de destination. Cette exigence pourra être assouplie par les futurs systèmes de signalisation, qui permettront de relayer l'information d'identité LAI dans le trajet de l'appel comme le CLI peut l'être aujourd'hui. Toutefois, le filtrage de ces paramètres aux frontières de réseau peut rendre la signalisation inefficace.

La taxation appliquée par le réseau de rattachement peut nécessiter que des déclencheurs soient déployés dans un nœud de transit ou un nœud passerelle. En effet, si la fonction SSF se trouve dans un réseau donné et si le point SCP se trouve dans un autre réseau, le réseau de rattachement risque de ne jamais recevoir l'appel. En fait, il peut être supprimé du trajet d'appel et ne peut donc pas garantir que la taxation soit appliquée à l'appel. D'autres méthodes de taxation peuvent nécessiter que des déclencheurs de service soient aussi déployés aussi proche que possible de l'appelé. Exemple: les services qui nécessitent que soient connus les paramètres d'interface radioélectrique comme l'identificateur de cellule, le nombre de canaux radioélectriques utilisés etc., pour garantir que les taxes sont calculées précisément. D'autres exemples en termes de services incluent le prépaiement par le mobile de destination et l'information de taxation.

Les services de zone locale nécessiteront que les déclencheurs d'origine soient placés dans le centre MSC d'origine et que les déclencheurs de destination soient placés dans le centre MSC de destination. Exemple: exclusion ou privilèges de l'utilisateur au niveau d'une station de base. Cela peut être équivalent aux services de ligne dans le réseau fixe.

SÉRIES DES RECOMMANDATIONS UIT-T

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

Imprimé en Suisse
Genève, 2001