

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2201

(04/2007)

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

Réseaux de prochaine génération – Aspects relatifs aux
services: capacités et architecture des services

Spécifications des réseaux de prochaine génération de version 1

Recommandation UIT-T Y.2201



RECOMMANDATIONS UIT-T DE LA SÉRIE Y
**INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE
 PROCHAINE GÉNÉRATION**

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

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

Recommandation UIT-T Y.2201

Spécifications des réseaux de prochaine génération de version 1

Résumé

La Recommandation UIT-T Y.2201 contient les spécifications de haut niveau relatives aux services et aux capacités des réseaux de prochaine génération (NGN) de version 1.

Source

La Recommandation UIT-T Y.2201 a été approuvée le 27 avril 2007 par la Commission d'études 13 (2005-2008) de l'UIT-T selon la procédure définie dans la Résolution 1 de l'AMNT.

Mots clés

Activateur de service, adressage, authentification, autorisation, capacités, comptabilité, confidentialité, émulation de réseau RTPC/RNIS, environnement de service ouvert, gestion, identification, interfonctionnement, interopérabilité, nommage, numérotage, OAM, politique, profil, qualité de service, réseaux de prochaine génération de version 1, sécurité, simulation de réseau RTPC/RNIS, spécifications de capacités, tarification.

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

© UIT 2008

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

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
2	Références normatives..... 1
3	Définitions 3
3.1	Termes définis ailleurs 3
3.2	Termes définis dans la présente Recommandation 5
4	Abréviations et acronymes 5
5	Conventions 7
6	Spécifications de capacités pour les réseaux NGN de version 1 7
6.1	Connectivité de transport..... 7
6.2	Modes de communication..... 8
6.3	Gestion des ressources de média 8
6.4	Codecs 8
6.5	Réseau d'accès et rattachement au réseau..... 9
6.6	Réseaux d'utilisateur..... 10
6.7	Interconnexion, interopérabilité et interfonctionnement 10
6.8	Routage..... 12
6.9	Qualité de service 12
6.10	Comptabilité et taxation 14
6.11	Numérotage, nommage et adressage 15
6.12	Identification, authentification et autorisation..... 17
6.13	Sécurité..... 21
6.14	Gestion de la mobilité..... 22
6.15	Exploitation, administration et maintenance 22
6.16	Capacité de survie..... 24
6.17	Gestion..... 26
6.18	Environnement de service ouvert 27
6.19	Gestion des profils..... 30
6.20	Gestion des politiques..... 32
6.21	Activateurs de service..... 33
6.22	Emulation et simulation de réseau RTPC/RNIS 39
6.23	Aspects touchant aux intérêts publics..... 40
6.24	Protection d'infrastructure critique 43
6.25	Non-divulgence d'informations à travers des interfaces NNI..... 43
6.26	Echange interfournisseurs d'informations sur les utilisateurs 43
	Appendice I – Mappage entre des services et des activateurs de service 44
	Bibliographie..... 46

Recommandation UIT-T Y.2201

Spécifications des réseaux de prochaine génération de version 1

1 Domaine d'application

La présente Recommandation fournit les spécifications de haut niveau à utiliser pour élaborer un ensemble de Recommandations UIT-T qui définiront les réseaux de prochaine génération de version 1.

Les spécifications de haut niveau et les capacités connexes spécifiées dans la présente Recommandation sont conformes aux buts et objectifs généraux décrits dans [UIT-T Y.2001] et sont fondées sur les objectifs associés aux réseaux NGN de version 1 identifiés dans le [b-UIT-T Y-Sup.1]. Les réseaux NGN doivent proposer au moins un niveau de service offrant des capacités égales ou supérieures à celles fournies par les réseaux à commutation de circuits.

La présente Recommandation ne vise pas à donner des spécifications plus détaillées ou propres aux services considérés. Les spécifications associées aux dispositions d'accès relèvent de la présente Recommandation, contrairement aux spécifications relatives aux équipements d'utilisateur.

Il est admis que l'on peut réaliser de façon spécifique un réseau de prochaine génération à partir d'un ensemble (ou d'un surensemble) de services pris en charge par les réseaux NGN de version 1 et de capacités spécifiées dans la présente Recommandation.

Les administrations peuvent imposer aux fournisseurs de tenir compte des prescriptions en matière de réglementation et de politiques nationales lors de l'implémentation des dispositions de la présente Recommandation.

2 Références normatives

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

- [UIT-T E.106] Recommandation UIT-T E.106 (2003), *Plan international de priorité en période de crise destiné aux opérations de secours en cas de catastrophe.*
- [UIT-T E.107] Recommandation UIT-T E.107 (2007), *Service de télécommunications d'urgence (ETS) et cadre d'interconnexion pour applications nationales du service ETS.*
- [UIT-T E.164] Recommandation UIT-T E.164 (2005), *Plan de numérotage des télécommunications publiques internationales.*
- [UIT-T E.212] Recommandation UIT-T E.212 (2004), *Plan d'identification international pour les terminaux mobiles et les utilisateurs mobiles.*
- [UIT-T G.711] Recommandation UIT-T G.711 (1988), *Modulation par impulsions et codage (MIC) des fréquences vocales.*
- [UIT-T G.780] Recommandation UIT-T G.780/Y.1351 (2004), *Termes et définitions des réseaux à hiérarchie numérique synchrone (SDH).*

- [UIT-T G.808.1] Recommandation UIT-T G.808.1 (2006), *Commutation de protection générique – Protection linéaire des chemins et des sous-réseaux.*
- [UIT-T I.610] Recommandation UIT-T I.610 (1999), *Principes et fonctions d'exploitation et de maintenance du RNIS à large bande.*
- [UIT-T M.3050.0] Recommandation UIT-T M.3050.0 (2007), *Plan amélioré d'exploitation des télécommunications (eTOM) – Introduction.*
- [UIT-T M.3050.1] Recommandation UIT-T M.3050.1 (2007), *Plan amélioré d'exploitation des télécommunications (eTOM) – Schéma des processus d'entreprise.*
- [UIT-T M.3060] Recommandation UIT-T M.3060/Y.2401 (2006), *Principes pour la gestion des réseaux de prochaine génération.*
- [UIT-T Q.825] Recommandation UIT-T Q.825 (1998), *Spécification des applications RGT au niveau de l'interface Q3: enregistrement des données d'appel.*
- [UIT-T Q.1703] Recommandation UIT-T Q.1703 (2004), *Cadre général des capacités de service et de réseau des aspects réseau des systèmes au-delà de l'IMT-2000.*
- [UIT-T Q.1706] Recommandation UIT-T Q.1706/Y.2801 (2006), *Spécifications de gestion de mobilité pour les réseaux de prochaine génération.*
- [UIT-T Q.1741.1] Recommandation UIT-T Q.1741.1 (2002), *Références IMT-2000 à la version 1999 du réseau central UMTS issu du GSM avec réseau d'accès radioélectrique universel de Terre (UTRAN).*
- [UIT-T Q.1741.2] Recommandation UIT-T Q.1741.2 (2002), *Références IMT-2000 à la version 4 du réseau central UMTS issu du GSM avec réseau d'accès radioélectrique universel de Terre (UTRAN).*
- [UIT-T Q.1741.3] Recommandation UIT-T Q.1741.3 (2003), *Références IMT-2000 à la version 5 du réseau central UMTS issu du GSM.*
- [UIT-T Q.1741.4] Recommandation UIT-T Q.1741.4 (2005), *Références IMT-2000 à la version 6 du réseau central UMTS issu du GSM.*
- [UIT-T X.462] Recommandation UIT-T X.462 (1996), *Technologies de l'information – Gestion des systèmes de messagerie: information de journalisation.*
- [UIT-T X.805] Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout.*
- [UIT-T Y.101] Recommandation UIT-T Y.101 (2000), *Infrastructure mondiale de l'information: termes et définitions.*
- [UIT-T Y.110] Recommandation UIT-T Y.110 (1998), *Infrastructure mondiale de l'information: principes et architecture générale.*
- [UIT-T Y.1271] Recommandation UIT-T Y.1271 (2004), *Cadres généraux applicables aux spécifications et aux capacités de réseau pour la prise en charge des télécommunications d'urgence sur les réseaux à commutation de circuits et à commutation de paquets en cours d'évolution.*
- [UIT-T Y.1541] Recommandation UIT-T Y.1541 (2006), *Objectifs de performances de réseau pour les services en mode IP.*
- [UIT-T Y.1710] Recommandation UIT-T Y.1710 (2002), *Prescriptions relatives à la fonctionnalité d'exploitation et de maintenance pour les réseaux MPLS.*

[UIT-T Y.1730]	Recommandation UIT-T Y.1730 (2004), <i>Prescriptions relatives aux fonctions d'exploitation, d'administration et de maintenance dans les réseaux à base Ethernet et les services Ethernet.</i>
[UIT-T Y.2001]	Recommandation UIT-T Y.2001 (2004), <i>Aperçu général des réseaux de prochaine génération.</i>
[UIT-T Y.2012]	Projet de Recommandation UIT-T Y.2012 (2006), <i>Spécifications fonctionnelles et architecture des réseaux de prochaine génération de version 1.</i>
[UIT-T Y.2091]	Recommandation UIT-T Y.2091 (2007), <i>Termes et définitions pour les réseaux de prochaine génération.</i>
[UIT-T Y.2701]	Recommandation UIT-T Y.2701 (2007), <i>Prescriptions de sécurité des réseaux de prochaine génération de version 1.</i>
[UIT-T Z.100]	Recommandation UIT-T Z.100 (2002), <i>SDL: langage de description et de spécification.</i>

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 comptabilité [UIT-T X.462]: action de réunir des informations sur les opérations effectuées au sein d'un système, et les effets de cette action.

3.1.2 adresse [UIT-T Y.2091]: identificateur d'un point de terminaison spécifique utilisé pour le routage vers ce point.

3.1.3 interface de réseau d'application (ANI, *application network interface*) [UIT-T Y.2012]: interface fournissant une voie pour des interactions et des échanges entre des applications et des éléments de réseau NGN. Elle fournit des capacités et des ressources nécessaires à la réalisation d'applications.

3.1.4 facturation [UIT-T Q.1703]: fonction administrative chargée de préparer les factures pour les clients des services, d'accélérer les paiements, d'obtenir des revenus et de prendre en compte les réclamations des clients.

3.1.5 taxation [UIT-T Q.825]: ensemble de fonctions nécessaires à la détermination du prix affecté à l'utilisation du service.

3.1.6 réseau d'entreprise [UIT-T Y.2701]: réseau privé prenant en charge de multiples utilisateurs et pouvant couvrir plusieurs lieux (par exemple une entreprise, un campus).

3.1.7 client [UIT-T M.3050.1]: le client achète à l'entreprise des produits et des services ou reçoit des offres ou des services gratuits. Il peut s'agir d'une personne ou d'une société.

3.1.8 utilisateur final [UIT-T M.3050.1]: l'utilisateur final est l'utilisateur effectif d'un produit ou d'un service proposé par l'Entreprise. Il est "consommateur" du produit ou du service. Voir également "abonné".

3.1.9 transfert [UIT-T Q.1706]: aptitude à fournir à un objet en déplacement, avant ou après son déplacement, des services avec une certaine incidence sur les accords de niveau de service.

3.1.10 réseau de rattachement [UIT-T E.212]: réseau du fournisseur de services au bénéfice duquel un abonné donné est abonné.

3.1.11 identificateur [UIT-T Y.2091]: série de chiffres, de caractères, de symboles ou toute autre forme de données servant à identifier un abonné, un utilisateur, un élément de réseau, une fonction, une entité de réseau offrant des services ou des applications, ou toute autre entité (par exemple des objets physiques ou logiques). Les identificateurs peuvent être utilisés à des fins d'enregistrement ou d'autorisation. Ils peuvent être publics pour tous les réseaux, partagés entre un nombre limité de réseaux ou propres à un réseau particulier (les identificateurs privés ne sont normalement pas communiqués à de tierces parties).

3.1.12 Internet [UIT-T Y.101]: ensemble de réseaux interconnectés appliquant le protocole Internet pour fonctionner comme un seul grand réseau virtuel.

3.1.13 mobilité [UIT-T Y.2001]: aptitude des utilisateurs et des autres entités mobiles à communiquer et à accéder aux services, indépendamment des changements de lieu et d'environnement technique. Le degré de disponibilité des services peut dépendre de plusieurs facteurs, notamment des capacités du réseau d'accès, des accords de service entre le réseau de rattachement de l'utilisateur et le réseau visité (le cas échéant), etc. La mobilité recouvre l'aptitude à communiquer avec ou sans continuité des services.

NOTE – Dans [UIT-T Y.2001], cette aptitude est appelée "mobilité généralisée".

3.1.14 gestion de la mobilité [UIT-T Q.1706]: ensemble des fonctions utilisées pour assurer la mobilité.

NOTE – Ces fonctions comprennent l'authentification, l'autorisation, la mise à jour de la localisation, la pagination, le téléchargement des informations d'utilisateur, etc.

3.1.15 nomadisme [UIT-T Q.1706]: aptitude de l'utilisateur à changer de point d'accès au réseau. En cas de changement de point d'accès au réseau, la session de service de l'utilisateur est complètement interrompue puis redémarre (aucune continuité au transfert de service n'est donc assurée). On suppose que, en conditions normales d'utilisation, l'utilisateur met fin à la session de service avant de se connecter à un autre point d'accès.

3.1.16 mobilité personnelle [UIT-T Q.1706]: mobilité associée à des scénarios où l'utilisateur change de terminal pour accéder au réseau depuis divers emplacements. Il s'agit de l'aptitude d'un utilisateur à accéder aux services de télécommunication depuis un terminal quelconque, sur la base d'un identificateur personnel, et d'assurer la capacité du réseau à assurer les services définis dans le profil de service de l'utilisateur.

3.1.17 itinérance [UIT-T Q.1706]: aptitude d'un utilisateur à accéder à des services conformément à son profil d'utilisateur lorsqu'il n'est pas dans les limites du réseau auquel il est abonné, par exemple via un point d'accès d'un réseau visité. Il faut pour cela une capacité d'accès au réseau visité, une interface entre le réseau de rattachement et le réseau visité ainsi qu'un accord d'itinérance entre les opérateurs de réseaux concernés.

3.1.18 transfert transparent [UIT-T Q.1706]: Il s'agit d'un cas particulier de mobilité avec continuité de service, car il préserve la possibilité de fournir des services à des objets mobiles pendant ou après leur déplacement sans affecter les accords de niveau de service.

3.1.19 service [UIT-T Z.100]: ensemble de fonctions et de ressources offertes à un utilisateur par un fournisseur de services.

3.1.20 continuité de service [UIT-T Q.1706]: aptitude à continuer à fournir un service à un objet en déplacement en conservant ses paramètres d'état, tels que l'environnement de réseau de l'utilisateur et la session d'un service.

3.1.21 abonné [UIT-T M.3050.1]: personne ou organisation ayant conclu des contrats d'abonnement à des services et les ayant payés.

3.1.22 mobilité de terminal [UIT-T Q.1706]: mobilité pour des scénarios où le même équipement terminal est déplacé ou utilisé en différents lieux. Il s'agit de l'aptitude d'un terminal à

accéder à des services de télécommunications depuis différents lieux ou lors d'un déplacement, ainsi que de la capacité du réseau à identifier et à localiser ce terminal.

3.1.23 réseau utilisateur [UIT-T Y.2701]: réseau privé comportant des équipements terminaux et pouvant desservir de multiples utilisateurs.

3.1.24 réseau visité [UIT-T Q.1706]: réseau local du client dans une configuration d'itinérance.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 classification des priorités: classification des classes de trafic conformément aux différents niveaux de priorité.

3.2.2 mécanismes d'activation des priorités: mécanismes grâce auxquels le traitement approprié du trafic conformément aux classes de priorité peut être activé dans le réseau.

3.2.3 signalisation des priorités: partie des mécanismes d'activation des priorités utilisant la signalisation.

3.2.4 signature unique: aptitude à utiliser une signature unique pour passer d'un opérateur de réseau/fournisseur de services à un autre opérateur/fournisseur dans le cas d'un utilisateur accédant à un service ou en itinérance dans un réseau visité.

3.2.5 identité d'équipement terminal: identificateur unique d'un équipement terminal.

3.2.6 utilisateur: notion couvrant un utilisateur terminal [UIT-T Y.2091], une personne, un abonné, un système, un équipement, un terminal (télécopieur ou ordinateur personnel par exemple), une entité (fonctionnelle), un processus, une application, un fournisseur ou un réseau d'entreprise.

3.2.7 attribut d'utilisateur: caractéristique décrivant l'utilisateur (par exemple la durée de vie de l'identité d'utilisateur, le statut de l'utilisateur ("disponible", "ne doit pas être dérangé", etc.)).

3.2.8 identité d'utilisateur: type de mot de passe, d'image ou de pseudonyme associé à un utilisateur, attribué et échangé entre des opérateurs et des fournisseurs de services pour identifier un utilisateur, authentifier son identité et/ou autoriser l'utilisation d'un service. Il peut par exemple s'agir d'identificateurs tels l'identificateur URI du protocole SIP, etc.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et les acronymes suivants:

ANI	interface de réseau d'application (<i>application network interface</i>)
API	interface de programmation d'application (<i>application programming interface</i>)
ATM	mode de transfert asynchrone (<i>asynchronous transfer mode</i>)
B2B	inter-entreprise (<i>business-to-business</i>)
CC	contenu de communication (<i>content of communication</i>)
CD/DVD	disque compact/vidéodisque numérique (<i>compact disk/digital versatile disk</i>)
DNS	système de noms de domaine (<i>domain name system</i>)
DTMF	multifréquence à deux tonalités (<i>dual tone multi frequency</i>)
ENUM	mappage des numéros téléphoniques (<i>telephone number mapping</i>)
ETS	service de télécommunication d'urgence (<i>emergency telecommunications service</i>)
IEPS	plan international de priorité en période de crise (<i>international emergency preference scheme</i>)

IM	messagerie instantanée (<i>instant messaging</i>)
IMS	sous-système multimédia IP (<i>IP multimedia subsystem</i>)
IN	réseau intelligent (<i>intelligent network</i>)
IP	protocole Internet (<i>Internet protocol</i>)
IP-CAN	réseau d'accès à connectivité IP (<i>IP connectivity access network</i>)
IPv4	protocole Internet-version 4 (<i>Internet protocol version 4</i>)
IPv6	protocole Internet-version 6 (<i>Internet protocol version 6</i>)
IRI	informations liées à l'interception (<i>intercept related information</i>)
IT	technologie de l'information (<i>information technology</i>)
LEA	organisme d'application des lois (<i>law enforcement agencies</i>)
MMS	service de messagerie multimédia (<i>multimedia messaging service</i>)
MPLS	commutation multiprotocole par étiquette (<i>multi-protocol label switching</i>)
NAI	identificateur d'accès au réseau (<i>network access identifier</i>)
NAPT	traduction d'adresse de réseau et de port (<i>network address and port translation</i>)
NAT	traduction d'adresse de réseau (<i>network address translation</i>)
NGN	réseau de prochaine génération (<i>next generation network</i>)
NNI	interface réseau-réseau (<i>network-network interface</i>)
OAM	exploitation, administration et maintenance (<i>operations, administration and maintenance</i>)
OS	système d'exploitation (<i>operating system</i>)
OSA	accès ouvert aux services (<i>open service access</i>)
OTN	réseau de transport optique (<i>optical transport network</i>)
PBX	autocommutateur privé (<i>private branch exchange</i>)
PC	ordinateur personnel (<i>personal computer</i>)
PDA	assistant numérique personnel (<i>personal digital assistant</i>)
QS	qualité de service
RACF	fonctions de contrôle de ressources et d'admission (<i>resource and admission control functions</i>)
RNIS	réseau numérique à intégration de services
RMTP	réseau mobile terrestre public
RTC	réseau téléphonique commuté
RTPC	réseau téléphonique public commuté
SIP	protocole d'ouverture de session (<i>session initiation protocol</i>)
SLA	accord de niveau de service (<i>service level agreement</i>)
SMS	service de messages courts (<i>short message service</i>)
SR	résilience de service (<i>service resiliency</i>)

TDR	télécommunications pour les secours en cas de catastrophe (<i>telecommunications for disaster relief</i>)
TE	équipement terminal (<i>terminal equipment</i>)
UDDI	découverte, description et intégration universelles (<i>universal discovery, description and integration</i>)
UMTS	système universel de télécommunications mobiles (<i>universal mobile telecommunications system</i>)
UNI	interface utilisateur réseau (<i>user to network interface</i>)
URI	identificateur uniforme de ressources (<i>uniform resource identifier</i>)
VPN	réseau privé virtuel (<i>virtual private network</i>)
xDSL	divers types de ligne d'abonné numérique (<i>various types of digital subscriber lines</i>)

5 Conventions

Aucune.

6 Spécifications de capacités pour les réseaux NGN de version 1

Les spécifications de haut niveau et les capacités connexes pour la prise en charge des objectifs de service associés aux réseaux NGN de version 1 (domaine d'application identifié dans [UIT-T Y-Sup.1]) sont données dans les paragraphes qui suivent.

Ces spécifications sont essentiellement données suivant une perspective de haut niveau et n'ont pas pour objet de fournir des spécifications fonctionnelles précises pour les différentes entités NGN.

La présente Recommandation ne vise pas à fournir des spécifications plus détaillées ou propres aux services considérés.

Elle ne traite que des spécifications relatives aux capacités d'un réseau NGN. Les spécifications associées aux dispositions d'accès relèvent de la présente Recommandation, contrairement aux spécifications relatives aux équipements d'utilisateur.

6.1 Connectivité de transport

La strate de transport d'un réseau NGN de version 1 [UIT-T Y.2012] utilisera le protocole IP à des fins de connectivité publique générale, universelle et mondiale. Le protocole IP peut être acheminé à l'aide de différentes technologies de transport sous-jacentes dans les portions d'accès et centrales de la strate de transport (xDSL, ATM, MPLS, relais de trames, OTN), conformément à l'environnement de l'opérateur.

NOTE – Cette connectivité n'empêche pas les opérateurs de fournir des services à technologie spécifique directement aux utilisateurs (ATM, MPLS, relais de trames, OTN par exemple).

La connectivité permettra:

- 1) l'utilisation des protocoles IPv4 et IPv6;
- 2) des communications en temps réel ou non;
- 3) une connectivité point à point;
- 4) une connectivité point à multipoint.

6.2 Modes de communication

Un réseau NGN prendra en charge les modes de communication suivants:

- point à point;
- point à multipoint;
- multipoint à multipoint;
- multipoint à point.

6.3 Gestion des ressources de média

Des mécanismes de gestion de ressources de média sont généralement utilisés parallèlement à des services classiques de traitement de la voix et des interactions d'utilisateur via la voix et la numérotation DTMF. Ils doivent être élargis dans le cas d'un réseau NGN pour prendre en compte des nouveaux services de données, de vidéo et de contenus.

Le réseau NGN prendra en charge diverses ressources de média et diverses capacités de gestion de ressources de média pour assurer la fourniture d'une large gamme d'applications.

- Les capacités de ressources de média comprennent:
- l'enregistrement de données de média (par exemple prise en charge du service de messagerie vocale);
- la lecture de données de média enregistrées (lecture de messages vocaux, tonalités et annonces par exemple);
- la reconnaissance DTMF (prise en charge des services de réponse vocale interactifs par exemple);
- la reconnaissance vocale améliorée (prise en charge des services de réponse vocale interactifs par exemple);
- le transcodage;
- les transitions de vidéo/texte/audio/données (prise en charge des services de conférence par exemple);
- la duplication de données de média (prise en charge d'interception de données de média par exemple);
- l'insertion de données de média.

6.4 Codecs

Les spécifications générales applicables aux codecs sont les suivantes:

- 1) Le transcodage évitera toutes les fois où cela est possible.
- 2) Le réseau NGN prendra en charge la négociation de bout en bout de n'importe quel codec entre des entités NGN (terminaux, éléments de réseau). Il est de la responsabilité des entités situées en bordure du réseau NGN (terminaux et équipements d'utilisateur NGN par exemple) et des équipements de réseau émettant ou recevant des flux de média IP de négocier et de sélectionner un codec commun pour chaque session de média "de bout en bout". Un réseau NGN prendra en charge la négociation de bout en bout des codecs de texte, tels que ceux actuellement spécifiés dans les Recommandations de l'UIT-T.

NOTE 1 – On suggère qu'un équipement d'utilisateur de réseau NGN utilise un codec audio à large bande.

- 3) Afin de permettre son interfonctionnement avec d'autres réseaux (RTPC/RNIS, RMPT ou d'autres réseaux NGN de version 1 par exemple), le réseau NGN pourra recevoir et présenter des données vocales à codage G.711 [UIT-T G.711] lorsqu'il est interconnecté à un autre réseau.

- 4) Lorsque la taille de mise en paquets n'est pas sélectionnée dans le cadre d'une négociation de codec entre des terminaux et/ou des éléments de réseau ou n'est pas définie par un accord bilatéral, une valeur de 10 ms devrait être utilisée pour la mise en paquets des données vocales à codage G.711 [UIT-T G.711]; il s'agit de la valeur optimale préconisée assurant un compromis entre la valeur du temps de propagation de bout en bout et l'utilisation du réseau. On admet qu'en raison de contraintes de réseau, la sélection d'une valeur plus grande devra peut-être être décidée par un accord bilatéral; une valeur de 20 ms est alors recommandée.

NOTE 2 – Lorsque la taille de mise en paquets est sélectionnée dans le cadre d'une négociation de codec entre des terminaux et/ou des éléments de réseau, la présente Recommandation ne donne aucune spécification quant à la valeur à sélectionner.

NOTE 3 – Le transcodage peut être utilisé en tant qu'option de déploiement dans les scénarios où la négociation de bout en bout ne conduit pas à l'utilisation d'un codec commun.

NOTE 4 – Les spécifications susmentionnées n'imposent pas la prise en charge d'un codec par les terminaux ni la prise en charge par le réseau NGN d'un transcodage entre un codec arbitraire et le codage G.711 [UIT-T G.711].

6.5 Réseau d'accès et rattachement au réseau

Un des objectifs liés aux réseaux NGN est la prise en charge de services et d'applications indépendamment des techniques de réseau d'accès. Ainsi:

- 1) Un réseau NGN prendra en charge diverses technologies de fonction de transport d'accès.
- 2) Toutes les fonctions de transport d'accès de réseau NGN devront pouvoir assurer une connectivité IP entre les fonctions d'utilisateur final et les fonctions de transport central.
- 3) Un réseau NGN n'exclura pas la prise en charge d'aucun réseau d'utilisateur présentant un certain niveau de complexité de configuration.
- 4) Un réseau NGN prendra en charge l'enregistrement au niveau du réseau d'accès, l'initialisation des fonctions d'utilisateur final pour l'accès aux services NGN et la gestion de l'espace d'adresses IP du réseau d'accès (existence d'une fonction NAT).
- 5) Le profil d'utilisateur gardera les données d'authentification d'accès de l'utilisateur et les informations relatives à la configuration requise d'accès au réseau.
- 6) Le réseau NGN prendra en charge la reconfiguration des services proposés à l'utilisateur lorsque celui-ci est nomade et accède aux services du réseau à partir d'un emplacement n'appartenant pas à sa zone d'abonnement. Les services fournis peuvent dépendre d'un ou de tous les éléments suivants: le dispositif d'utilisateur, le réseau d'accès et les accords (d'itinérance par exemple) entre le fournisseur de services et le fournisseur du réseau d'accès. Le réseau d'accès attribuera les ressources conformément aux services à fournir.
- 7) Lorsque plusieurs réseaux d'accès sont reliés à un seul réseau central NGN, un réseau d'accès authentifiera/autorisera l'accès d'un utilisateur en itinérance à ce réseau à partir d'un autre réseau d'accès.
- 8) Pour garantir la disponibilité des services d'itinérance, les procédures de rattachement du réseau d'accès NGN prendra en charge l'authentification du réseau d'accès sur la base d'une méthode normalisée d'identification des utilisateurs au niveau du réseau d'accès (utilisation par exemple du mécanisme d'identificateur de rattachement au réseau (NAI, *network attachment identifier*) spécifié dans la norme [b-RFC 2486]).

6.6 Réseaux d'utilisateur

Les spécifications générales d'accès aux NGN version 1 pour les réseaux d'utilisateur sont les suivantes:

- 1) Il ne faudra pas exclure les solutions d'accès d'un réseau NGN via un réseau d'utilisateur à l'aide de fonctions NAT/NAPT et de pare-feu dans l'environnement d'utilisateur où l'attribution d'adresses IP aux équipements d'utilisateur peut être effectuée par le réseau d'utilisateur. Ces adresses n'ont pas besoin d'être acheminables dans le réseau NGN.
- 2) Les solutions d'accès au réseau NGN via un réseau d'utilisateur auront une incidence minimale sur les déploiements de réseaux d'utilisateur existants.
- 3) Les solutions d'accès au réseau NGN via un réseau d'utilisateur prendront en charge les configurations suivantes:
 - connectivité et interaction directes entre les différents terminaux et le réseau NGN;
 - connectivité et interaction indirectes entre les différents terminaux et le réseau NGN (par exemple via des autocommutateurs PBX IP).

Les réseaux NGN de version 1 devraient autoriser l'utilisation simultanée par un seul terminal de plusieurs types de fonctions de transport d'accès, sans qu'il soit toutefois nécessaire de coordonner les communications. Un tel terminal peut donc sembler, du point de vue réseau, revêtir la forme de plusieurs terminaux différents.

NOTE – Bien qu'elles ne portent pas sur les équipements, les spécifications de la présente Recommandation ne visent pas à exclure le rattachement d'un équipement terminal qui serait susceptible de permettre l'adaptation d'une interface à différents besoins d'utilisateur, en particulier ceux de personnes handicapées, utilisant des dispositifs d'interface d'utilisateur couramment fournis.

6.7 Interconnexion, interopérabilité et interfonctionnement

L'interopérabilité et l'interfonctionnement sont deux fonctions distinctes définies respectivement dans [UIT-T Y.101] et dans les Recommandations de la série Y.1400.

6.7.1 Interconnexion

On distingue deux types d'interconnexion entre des réseaux NGN de version 1:

- "L'interconnexion orientée connexion": elle est fondée sur une connectivité IP simple qui ne dépend pas du niveau d'interopérabilité.

NOTE 1 – Une interconnexion de ce type n'a pas connaissance du service de bout en bout spécifique considéré et, par conséquent, de performance de réseau, de qualité de service et de service propres à ce service ne sont pas nécessairement respectées.

- "L'interconnexion orientée service": elle permet aux opérateurs et aux fournisseurs de services d'offrir des services avec des niveaux d'interopérabilité définis.

NOTE 2 – C'est par exemple le cas des services G.711 sur interconnexion IP. Les niveaux d'interopérabilité définis dépendent du service, de la qualité de service ou de la sécurité, etc.

Les prescriptions d'interconnexion sont les suivantes:

- 1) Le type interconnexion orientée connectivité entre des réseaux NGN sera pris en charge.
- 2) Le type interconnexion orientée service entre des réseaux NGN n'est pas exclu.

6.7.2 Interopérabilité

Pour permettre la fourniture de certains services via un conduit de bout en bout traversant un ou plusieurs domaines NGN:

- 1) les composantes de service appropriées au sein d'un même domaine NGN devront interopérer.

- 2) L'interopérabilité de domaines NGN interconnectés déployant des ensembles de capacités de service identiques n'est pas exclue.

6.7.3 Interfonctionnement avec des réseaux non NGN

Les réseaux NGN de version 1 interfonctionneront avec différents types de réseaux pour la fourniture de certains services. Les services identifiés pour l'interfonctionnement opéreront de façon transparente à travers l'infrastructure fournie par un ou plusieurs fournisseurs de services. Les réseaux NGN de version 1 fournissent des capacités, concernant notamment la sécurité, les fonctions OAM, la résilience, la qualité de service et, si nécessaire, le transcodage de média, pour la prise en charge de scénarios d'interconnexion avec d'autres réseaux non NGN en vue d'assurer un fonctionnement de bout en bout transparent.

Pour permettre la fourniture de certains services à travers un conduit de bout en bout faisant intervenir des réseaux NGN et des réseaux non NGN:

- un réseau NGN pourra interfonctionner avec d'autres réseaux non NGN;
- un réseau NGN devrait pouvoir prendre en charge les capacités d'interfonctionnement suivantes:
 - le routage;
 - l'interfonctionnement de signalisation;
 - l'interfonctionnement de numérotage, de nommage et/ou d'adressage;
 - l'échange d'informations relatives à la comptabilité et à la tarification;
 - l'interfonctionnement de sécurité;
 - l'interfonctionnement de qualité de service;
 - l'échange d'informations sur le profil de l'utilisateur ou du terminal;
 - l'interfonctionnement de média;
 - l'interfonctionnement de gestion;
 - la gestion des politiques (par exemple, conformément aux politiques interdomaines, certaines informations internes relatives à un domaine certifié, y compris des informations sur des utilisateurs, peuvent devoir être cachées ou supprimées du flux d'informations échangé à l'interface avec d'autres domaines certifiés ou non), notamment la résolution de différences entre les politiques.

NOTE – Cela ne signifie pas qu'il puisse y avoir interfonctionnement entre tous les services et/ou toutes les caractéristiques de service. Ces spécifications peuvent ne s'appliquer qu'à l'interfonctionnement entre certains services et/ou caractéristiques de service spécifiques (et très vraisemblablement similaires ou identiques).

6.7.3.1 Interfonctionnement avec le réseau RTPC/RNIS

Lorsqu'un réseau NGN est connecté à un RTPC/RNIS, il prendra en charge ce qui suit:

- 1) l'interfonctionnement entre le réseau RTPC/RNIS et des services d'émulation du réseau RTPC/RNIS. Il assurera un haut niveau d'interopérabilité avec les services du RTPC/RNIS émulé. Le degré d'interopérabilité du service relève des opérateurs et, dans certains cas, des régulateurs nationaux;
- 2) l'interfonctionnement entre le réseau RTPC/RNIS et des services de simulation du réseau RTPC/RNIS. Il prendra en charge l'interopérabilité des services de simulation du RTPC/RNIS avec des services complémentaires RTPC/RNIS, bien que cet interfonctionnement puisse conduire à une capacité de service limitée;
- 3) l'interfonctionnement entre le réseau RTPC/RNIS et des services multimédias IP NGN, bien que cet interfonctionnement puisse conduire à une capacité de service limitée.

NOTE 1 – Cela ne signifie pas qu'il puisse y avoir interfonctionnement entre le réseau RTPC/RNIS, d'une part, et tous les services et/ou toutes les caractéristiques de service de réseau NGN, d'autre part. Ces spécifications peuvent ne s'appliquer qu'à l'interfonctionnement entre certains services et/ou caractéristiques de service spécifiques (et très vraisemblablement similaires ou identiques) proposées par le réseau NGN et par le réseau RTPC/RNIS.

NOTE 2 – Les réseaux d'entreprise à commutation de circuits sont pris en charge par les réseaux NGN de version 1 soit par le biais d'une connexion au réseau NGN via un réseau RTPC/RNIS existant soit, lorsqu'une émulation de réseau RTPC/RNIS est déployée, par le biais d'une passerelle d'interfonctionnement.

6.7.3.2 Interfonctionnement avec d'autres réseaux

- 1) Un réseau NGN fournira la capacité d'une interconnexion directe dans le cas de réseaux à circuits commutés, au moins pour les réseaux câblés, les réseaux de radiodiffusion et les réseaux mobiles terrestres publics. Les spécifications d'interfonctionnement avec un réseau à commutation de circuits quelconque sont identiques aux prescriptions d'interfonctionnement avec le réseau RTPC/RNIS.

Un réseau NGN de version 1 fournira la capacité d'une interconnexion orientée connexion avec des réseaux IP non NGN. La capacité d'une interconnexion orientée service avec des réseaux non NGN mais IP ne sera pas exclue.

Si le réseau interconnecté fournit toutes les capacités d'interfonctionnement, comme on l'a identifié au § 6.7.3, de telles interconnexions de réseau peuvent être prises en charge dans un déploiement. Les caractéristiques et les fonctionnalités des réseaux non NGN mais IP sont si diverses et nombreuses qu'il est impossible de fournir des spécifications définitives d'interconnexion avec des réseaux NGN de version 1.

- 2) Un réseau NGN n'exclura pas délibérément l'interconnexion avec des réseaux non NGN mais IP.

NOTE – Les spécifications de sécurité sont données au § 6.13.

6.8 Routage

Un réseau NGN fournira des capacités permettant de sélectionner les conduits de routage appropriés entre le point d'extrémité émetteur du trafic et le point d'extrémité récepteur du trafic.

Un réseau NGN prendra en charge les mécanismes de routage les plus appropriés pour les fournisseurs NGN. Il prendra en charge:

- 1) des mécanismes de routage tant statiques que dynamiques;
- 2) des mécanismes de routage capables de fonctionner avec efficacité dans un domaine NGN;
- 3) des mécanismes de routage pouvant effectivement fonctionner entre domaines NGN, autorisant ainsi l'interopérabilité.

6.9 Qualité de service

Un réseau NGN prendra en charge la qualité de service de bout en bout à travers différents réseaux mettant en œuvre différentes technologies d'infrastructure fournies par divers opérateurs en vue d'assurer le niveau de service requis pour des utilisateurs ou des applications. Il prendra en charge plusieurs niveaux de qualité de service, qui peuvent être négociés entre l'utilisateur et le fournisseur. Cette prise en charge suppose l'utilisation des fonctionnalités suivantes: mécanismes de contrôle de ressources et d'admission, différenciation des classes de trafic, gestion des priorités, mécanismes de signalisation de la qualité de service, mesure et gestion de la performance pour garantir la qualité, et enfin contrôle de la surcharge/de l'encombrement.

6.9.1 Spécifications générales de qualité de service

Un réseau NGN satisfera aux spécifications de qualité de service suivantes:

- 1) permettre l'application de diverses technologies et de divers modèles économiques;
- 2) prendre en charge les différents processus relatifs au cycle de vie d'un service (abonnement/fourniture, invocation, surveillance par exemple);
- 3) prendre en charge différents équipements terminaux (certains équipements terminaux peuvent par exemple, contrairement à d'autres, prendre en charge la signalisation de qualité de service dans la strate de transport);
- 4) contrôler les ressources de transport liées à la qualité de service dans les réseaux à transmission par paquets et en bordure de réseau conformément à ses capacités;
- 5) prendre en charge le contrôle de ressources et d'admission dans un domaine NGN et entre plusieurs domaines NGN;
- 6) prendre en charge le contrôle de la qualité de service relative et celui de la qualité de service absolue;
- 7) prendre en charge les spécifications de qualité de service induites par l'application.

6.9.2 Classes de qualité de service de réseau

- 1) Un réseau NGN devrait prendre en compte la performance du réseau au niveau de la strate de transport.
- 2) Un réseau NGN devrait prendre en charge les classes de qualité de service de réseau NGN fondées sur [UIT-T Y.1541].

6.9.3 Priorité de service/d'application

Pour assurer la priorité de service/d'application, un réseau NGN devrait prendre en charge les fonctionnalités suivantes:

- 1) les mécanismes de classification des priorités pour le contrôle d'admission et le rétablissement;
- 2) les extensions de signalisation indiquant les niveaux de priorité à travers des interfaces UNI et NNI;
- 3) les mécanismes d'activation de priorité déclenchant l'action prioritaire voulue.

6.9.4 Contrôle de la qualité de service

Un réseau NGN devrait prendre en charge:

- 1) une granularité de contrôle de la qualité de service par flux, par session et par classe de service;
- 2) un comportement de qualité de service dynamique (il devrait être possible de modifier des attributs de qualité de service au cours d'une session active);
- 3) un contrôle des ressources de qualité de service fondé sur une approche distribuée, centralisée ou hybride;
- 4) des mécanismes de contrôle d'admission et de contrôle d'encombrement;
- 5) des mécanismes garantissant la fourniture fiable et dans les délais de paquets de signalisation et de paquets de commande;
- 6) des mécanismes permettant de fournir conformément aux niveaux de priorité les télécommunications d'urgence et les télécommunications prioritaires.

6.9.5 Signalisation de la qualité de service

Un réseau NGN devrait utiliser des mécanismes de signalisation pour prendre en charge la qualité de service.

La présente Recommandation ne donne pas de spécifications détaillées relatives à la signalisation de la qualité de service. Celles-ci figurent dans d'autres Recommandations spécifiques.

6.9.6 Mesure et gestion de la performance

Un réseau NGN mesurera et gèrera la performance pour garantir le niveau de qualité de service.

A cette fin, les mesures de performance de réseau et leur gestion permettront:

- 1) de vérifier les garanties du fournisseur quant aux performances (par comparaison avec les dispositions des accords SLA);
- 2) la communication par le fournisseur d'informations de performance aux clients potentiels;
- 3) le diagnostic de pannes par les fournisseurs dans leurs réseaux pour des conduits définis;
- 4) de fournir une indication interne sur l'incidence sur la performance de changements effectués dans ses réseaux;
- 5) la surveillance par chaque fournisseur des performances des réseaux des autres fournisseurs;
- 6) de fournir des informations à d'autres fonctions NGN, par exemple aux fonctions RACF.

La présente Recommandation ne donne pas de spécifications détaillées relatives à la signalisation de la qualité de service. Celles-ci figurent dans d'autres Recommandations spécifiques.

6.9.7 Gestion des surcharges de traitement et de trafic

Pour éviter les surcharges de traitement et de trafic et maintenir des temps de réponse suffisamment faibles en cas de surcharge afin de dissuader les utilisateurs d'abandonner leurs demandes de service, un réseau NGN de version 1 doit proposer des mécanismes de détection et de contrôle des surcharges (notamment des mécanismes de contrôle sophistiqués tels que la répartition de la charge et la réplication des ressources) tant dans la strate de service que dans la strate de transport.

Un réseau NGN doit disposer de mécanismes de contrôle de la surcharge qui:

- 1) indiquent les conditions de surcharge et le degré de surcharge à d'autres réseaux;
- 2) optimisent le débit effectif (par exemple le nombre de demandes de service ou de paquets admis par seconde) en fonction des considérations de priorité de service valables au niveau d'une ressource en surcharge;
- 3) assurent un tel débit pendant la durée de la surcharge, quelle que soit la capacité de la ressource en surcharge ou le nombre de sources de surcharge;
- 4) permettent au réseau recevant l'indication de surcharge de contrôler son trafic.

6.10 Comptabilité et taxation

Un réseau NGN prend en charge des capacités de comptabilité et de taxation afin de fournir à l'opérateur de réseau des données de comptabilité et de taxation relatives à l'utilisation des ressources dans le réseau.

Les spécifications de comptabilité et de taxation associées à un réseau NGN sont résumées ci-après:

- 1) Les capacités de comptabilité et de taxation prendront en charge la collecte de données en vue d'un traitement ultérieur (taxation hors ligne) ainsi que les interactions quasi-temps réel avec des applications telles que les services prépayés (taxation en ligne).
- 2) Des mécanismes ouverts seront disponibles pour la gestion de la taxation.

- 3) Différentes politiques de taxation seront prises en charge (taxation à taux fixe et taxation par session en fonction de l'utilisation par exemple).
- 4) Les capacités de comptabilité et de taxation prendront en charge les services ayant une fonctionnalité de multidiffusion.
- 5) Le réseau NGN acceptera tous les types possibles de dispositions comptables, notamment le transfert d'informations de comptabilité/de taxation entre des fournisseurs. Cette spécification s'applique également aux accords de commerce électronique.

Par exemple, dans un scénario de service de fourniture de contenus faisant intervenir la multidiffusion, un service peut être assuré grâce aux activités conjointes de plusieurs entreprises (par exemple plusieurs fournisseurs de services de contenus et un fournisseur de réseaux): une fonctionnalité de taxation entre les entreprises est nécessaire en plus de la fonctionnalité de taxation des utilisateurs.

NOTE – L'utilisation d'informations de taxation recueillies par un réseau NGN pour permettre la facturation ne relève pas de la présente Recommandation.

6.11 Numérotage, nommage et adressage

Un réseau NGN a pour objet de fournir un environnement de numérotage, de nommage et d'adressage efficace, sûr et digne de foi aux utilisateurs, aux opérateurs de réseaux et aux fournisseurs de services. Il sera tenu compte des spécifications de réglementation ainsi que de l'interopérabilité avec le réseau RTPC/RNIS si nécessaire.

Les évolutions des réseaux NGN seront telles que la souveraineté des Etats Membres de l'UIT en matière de plan de numérotage, de plan de nommage et de plan d'adressage sera pleinement respectée, conformément à [UIT-T E.164] et à d'autres Recommandations et Spécifications pertinentes d'autres organismes de normalisation.

Les spécifications données ci-après concernent la prise en charge des capacités de numérotage, de nommage et d'adressage. Sauf mention contraire, elles s'appliquent à la strate de transport et à la strate de service.

6.11.1 Spécifications générales de numérotage, de nommage et d'adressage

- 1) Les modes d'attribution d'adresse fixes et dynamiques seront pris en charge.
- 2) Des capacités de numérotage, d'adressage et de nommage peuvent être implémentées à l'aide d'un mécanisme de mappage propre à chaque service ou d'un mécanisme de mappage commun aux différents services.
- 3) La mise à jour dynamique des bases de données de nommage sera prise en charge (dans le cas d'un terminal mobile par exemple, les adresses au niveau d'une ou plusieurs couches peuvent être modifiées de façon dynamique suivant l'emplacement du terminal).

6.11.2 Numérotage

Les spécifications de numérotage applicables à un réseau NGN sont les suivantes:

- 1) Les mécanismes d'adressage prendront en charge la capacité à différencier le plan de numérotation des plans de numérotage et d'adressage.
- 2) Les mécanismes d'adressage prendront en charge la capacité à traduire une séquence de numérotation en une valeur du plan de numérotage et d'adressage.
- 3) Un réseau NGN prendra en charge le numérotage E.164 (numéros mondiaux).
- 4) Un réseau non NGN devrait permettre l'utilisation d'un numérotage non E.164 (numéros locaux).
- 5) Un réseau NGN devrait permettre l'utilisation de numéros courts dans les plans de numérotation nationaux.

- 6) Un réseau NGN ne devrait pas empêcher l'utilisation de numéros privés et de numéros d'entreprise (voir § 6.6).
- 7) En cas d'utilisation de numéros non E.164 (numéros locaux) ou de séquences de numérotation, le mécanisme d'adressage du réseau NGN déterminera le cadre de validité des numéros locaux.
- 8) Un réseau NGN prendra en charge la capacité à faire la distinction entre, d'une part, des identificateurs alphanumériques composés uniquement de chiffres mais qui ne sont pas des numéros de téléphone et, d'autre part, des identificateurs alphanumériques qui sont des numéros de téléphone et qui devraient être traités comme tels dans les procédures de routage.

6.11.3 Mécanismes de numérotage, de nommage et d'adressage

- 1) Au niveau de la strate de transport, un réseau NGN de version 1 prendra en charge les mécanismes d'adressage IP fondés sur le protocole IPv4, le protocole IPv6 ou sur les deux protocoles.

NOTE 1 – Il convient de reconnaître qu'utiliser les protocoles IPv4 et IPv6 dans un même domaine d'opérateur risque de créer des problèmes de fourniture de service.

- 2) Les opérateurs de réseaux NGN peuvent prendre en charge des équipements d'utilisateur à l'aide du seul protocole IPv4, du seul protocole IPv6 ou des deux protocoles au niveau de l'interface utilisateur-réseau.

NOTE 2 – On suppose qu'un équipement d'utilisateur IPv6 peut également utiliser le protocole IPv4 au niveau de l'interface utilisateur-réseau.

- 3) Un réseau NGN prendra en charge l'établissement de communications multimédias IP (pour l'émission et pour la réception) en utilisant au moins des identificateurs uniformes de ressources de téléphonie E.164 (identificateurs URI de téléphonie, par exemple le numéro de téléphone: +4412345678) et des identificateurs uniformes de ressources du protocole SIP (identificateurs URI du protocole SIP, par exemple sip:my.name@company.org). En ce qui concerne les identificateurs URI de téléphonie:
 - les numéros mondiaux seront pris en charge;
 - les numéros locaux devraient être pris en charge.
- 4) Pour certains scénarios de service (par exemple l'interfonctionnement avec le réseau RTPC/RNIS), un réseau NGN de version 1 prendra en charge l'établissement de communications multimédias IP (pour l'émission et pour la réception) en utilisant le numérotage E.164 avec prise en charge de type ENUM si nécessaire.
- 5) Les mécanismes de numérotage et d'adressage prendront en charge les types de service monodiffusion et multidiffusion.
- 6) Les mécanismes de numérotage et d'adressage devraient prendre en charge les types de service radiodiffusion.
- 7) D'autres mécanismes de numérotage, de nommage et d'adressage peuvent être pris en charge.

6.11.4 Résolution du nom/de l'adresse

[UIT-T Y.2001] donne les spécifications et les principes fondamentaux pour la résolution du nom, du numéro et de l'adresse. La présente Recommandation donne les spécifications suivantes:

- 1) adaptabilité d'échelle: un réseau NGN devrait être adaptable pour pouvoir faire face à une demande accrue de résolution de nom/de numéro/d'adresse;
- 2) fiabilité: les capacités de résolution de nom/de numéro/d'adresse ne seront pas entravées par l'existence d'une défaillance en un point (utilisation par exemple de mécanismes de résolution distribués);

- 3) sécurité: des mesures de sécurité seront associées aux capacités de résolution de nom/de numéro/d'adresse.

NOTE – Ces capacités peuvent faire intervenir des bases de données qui sont internes ou externes au réseau NGN (par exemple une base de données DNS Internet). On peut citer à titre d'exemple les mesures de sécurité suivantes: authentification de l'accès d'utilisateur, sécurité des données, synchronisation des données et rétablissement en cas de panne.

6.11.5 Interfonctionnement de numérotage, de nommage et d'adressage

Les fonctions d'interfonctionnement assurent en cas de nécessité la traduction de numéros, de noms et d'adresses dans des scénarios d'interconnexion de réseau.

- 1) Un réseau NGN prendra en charge plusieurs scénarios d'interfonctionnement d'adresses de la strate de transport sans dégradation du service fourni aux utilisateurs (scénarios d'interfonctionnement entre différents domaines d'adressage, tels que des domaines fondés sur les mécanismes d'adressage IPv4 ou IPv6, et des domaines fondés sur des mécanismes d'adressage public ou privé).
- 2) Lorsque cela est nécessaire, les capacités de traduction d'adresses seront utilisées pour prendre en charge les différences de format d'adresse, tant dans la strate de transport que dans la strate de service, sans dégradation du service fourni aux utilisateurs.

6.12 Identification, authentification et autorisation

Les spécifications du présent paragraphe ne sont pas liées à un ensemble spécifique de services NGN ou d'applications.

NOTE – Les mécanismes d'authentification et d'autorisation spécifiques ne relèvent pas de la présente Recommandation.

6.12.1 Spécifications générales

Des spécifications relatives aux capacités d'identification, d'authentification et d'autorisation réciproques existent pour la strate de transport et pour la strate de service. Pour la strate de transport, on spécifie la façon dont les ressources de transport NGN peuvent être utilisées. Pour la strate de service, on spécifie la façon d'associer un utilisateur et un service ou d'associer deux utilisateurs, notamment lorsqu'ils se trouvent dans des réseaux NGN différents.

NOTE 1 – Parfois l'expression "fournisseur de services" a été utilisée pour faire référence au fournisseur de services de la strate de transport. Dans le présent paragraphe, le fournisseur de réseaux est généralement appelé simplement "réseau NGN" tandis que l'expression "fournisseur de services" désigne précisément le fournisseur de services; celui-ci peut se trouver n'importe où et n'est pas nécessairement le fournisseur de réseaux.

On trouvera ci-après les spécifications générales relatives aux capacités d'identification, d'authentification et d'autorisation.

- 1) Un réseau NGN prendra en charge les fonctions d'authentification et d'autorisation réciproques pour la strate de transport et pour la strate de service. L'authentification dans la strate de transport exige qu'un utilisateur soit identifié par le réseau pour avoir accès au réseau et à des utilisations privilégiées. Une fonction d'authentification peut constituer un facteur important de protection contre une utilisation non autorisée des réseaux, par exemple pour empêcher l'arrivée en masse de télécommunications non sollicitées. La fonction d'autorisation peut mettre en place l'accès aux ressources de réseau et empêcher des violations de l'accès.

- 2) Le réseau NGN identifiera de façon unique à l'aide d'un ou des deux types suivants d'identificateur d'utilisateur:
 - identificateur d'utilisateur public: il s'agit d'informations généralement utilisées par un utilisateur de réseau NGN pour établir un contact ou une communication avec un autre utilisateur de réseau NGN;
 - identificateur d'utilisateur privé: un identificateur d'utilisateur NGN privé peut être utilisé pour identifier l'utilisateur de réseau NGN aux yeux de son fournisseur de réseaux ou de services NGN. L'identificateur d'utilisateur est un composant utilisé pour l'authentification.
- 3) Un réseau NGN permettra d'effectuer séparément les processus d'identification, d'authentification et d'autorisation pour les utilisateurs et pour les équipements terminaux.
- 4) Un réseau NGN permettra de vérifier l'association entre l'utilisateur et l'équipement terminal de l'utilisateur pour certains services spécifiques.
- 5) Les processus d'authentification, d'autorisation et de comptabilité effectués par le fournisseur de réseaux NGN et par le fournisseur de services devraient être des processus sûrs.
- 6) Un fournisseur de services fournira des mécanismes permettant la présentation de l'identificateur public de l'émetteur de la communication, lorsque cela est approprié et permis.
- 7) Un fournisseur de services fournira des mécanismes masquant l'identificateur public de l'émetteur de la communication, si la présentation de cette information est limitée par l'émetteur ou par le réseau.
- 8) Un fournisseur de services effectuant l'authentification prendra en charge des mécanismes permettant de déterminer l'authenticité d'un identificateur d'utilisateur public présenté pour une communication entrante.
- 9) Un fournisseur de services effectuant l'authentification fournira des mécanismes permettant de présenter l'identificateur d'utilisateur public de la partie connectée à l'émetteur de la communication, le cas échéant, et s'il n'y a pas de restriction émanant de la partie connectée ou du réseau.
- 10) Un réseau NGN doit pouvoir vérifier l'identificateur privé des utilisateurs et des terminaux (le cas échéant). En outre, il devra pouvoir vérifier l'authentification et l'autorisation des utilisateurs et des terminaux pour utiliser les ressources du réseau NGN.
- 11) Un réseau NGN doit pouvoir vérifier l'identificateur privé des utilisateurs des services qu'il fournit. Il prendra en charge les capacités de vérifier l'authentification et l'autorisation des utilisateurs souhaitant utiliser les ressources qu'il gère.
- 12) L'identificateur privé et l'identificateur public d'un utilisateur NGN des ressources de la strate de transport (identificateurs utilisés pour l'authentification et l'autorisation) seront administrés par l'opérateur de réseau approprié.
- 13) L'identificateur privé et l'identificateur public d'un utilisateur NGN des ressources de la couche de service (identificateurs utilisés pour l'authentification, l'autorisation et le routage) seront administrés par le fournisseur de services approprié; l'administration requise doit être telle qu'elle prévienne la modification par l'utilisateur des identificateurs public et privé de manière non autorisée.
- 14) Les identificateurs privés d'utilisateur NGN fournis pour l'authentification et l'autorisation seront masqués pour les autres utilisateurs.
- 15) Les identificateurs publics d'utilisateur NGN d'un utilisateur de services pourront être visibles pour les autres utilisateurs si aucun intermédiaire n'intervient et si l'utilisateur le permet.

- 16) Un fournisseur de services peut autoriser un utilisateur à accéder à un service à partir de plusieurs terminaux en parallèle à l'aide des mêmes identifiants d'utilisateur public et privé.
- 17) Comme un utilisateur donné peut éventuellement utiliser plusieurs identifiants d'utilisateur privés via une seule procédure d'abonnement, le réseau NGN prendra en charge les identifiants privés multiples d'utilisateur par une procédure d'abonnement unique.
- 18) Un réseau NGN peut authentifier et autoriser un même utilisateur pour plusieurs services ("guichet unique").

NOTE 2 – Même lorsque seulement un événement d'authentification est requis, plusieurs événements d'authentification peuvent néanmoins être nécessaires. En outre, étant donné que la fonctionnalité de signature unique peut être mise en œuvre du côté client, l'utilisateur n'a besoin d'établir une relation d'authentification qu'à une seule reprise, même si plusieurs authentifications sont requises. La prise en charge de capacités de signature unique n'est pas obligatoire pour les réseaux NGN de version 1 mais est souhaitée si les technologies actuelles le permettent.

L'authentification de l'identifiant d'un abonné ou de celui d'un utilisateur n'est pas destinée à la validation positive d'une personne.

6.12.2 Spécifications d'identification

Les réseaux NGN de version 1 fournissent des capacités d'identification d'utilisateur, pour permettre aux opérateurs de réseau et aux fournisseurs de services d'identifier les utilisateurs de certains services NGN et d'utiliser ces informations selon les besoins (par exemple pour des procédures d'authentification d'autorisation). Le NGN version 1 offrira à l'utilisateur la capacité d'identifier les fournisseurs NGN (au niveau de chaque couche) lorsqu'une relation directe existe.

Les spécifications relatives à la capacité d'identification sont les suivantes:

- 1) Existence de plusieurs identifiants d'utilisateur
Un utilisateur de réseau NGN pouvant avoir un ou plusieurs identifiants publics et privés, le réseau NGN devra pouvoir les différencier (par exemple à des fins d'utilisation personnelle ou professionnelle).
- 2) Portabilité de l'identifiant
Un réseau NGN fournira des capacités assurant une fonctionnalité équivalente à la portabilité du numéro dans un environnement RTPC.
- 3) Indépendance de l'identifiant
L'identifiant d'utilisateur public devrait être attribuée à l'utilisateur indépendamment de son référentiel, du terminal de l'utilisateur et des technologies de réseau sous-jacentes. Toutefois, la compatibilité avec des dispositifs moins évolués (par exemple un combiné POTS) peut être assurée grâce à des fonctions d'interfonctionnement appropriées.
- 4) Prise en charge des attributs d'identifiant
Des informations d'attribut d'identifiant privé (telles que la durée de vie de cet identifiant pour l'utilisateur, pour l'abonné, pour le réseau utilisé, etc.) peuvent être associées à un identifiant d'utilisateur.
- 5) Prise en charge des conditions d'attribut
Des conditions (déclenchement d'une temporisation pour les conditions de validité par exemple) relatives à un attribut d'utilisateur peuvent être associées à un identifiant d'utilisateur par un fournisseur d'attributs (réseau, utilisateur principal, utilisateur final par exemple).
- 6) Autorisation d'attribut sélective
Un réseau NGN prendra en charge l'autorisation sélective d'informations d'attribut d'identité privée par un fournisseur d'attributs (durée de vie de l'identifiant par exemple).

- 7) **Prise en charge de la programmation par abonné**
Un réseau NGN doit prendre en charge la programmation par l'abonné de différentes permissions relatives à diverses informations d'attribut (par exemple l'accès à des informations d'attribut d'identité privée et l'utilisation de ces informations en fonction de l'attribut considéré).
- 8) **Lien entre l'utilisateur et le terminal**
Un réseau NGN prendra en charge un lien dynamique entre l'identificateur d'utilisateur public et l'identité d'équipement terminal pour certains services.
- 9) **Association à plusieurs terminaux**
Un réseau NGN autorisera l'association d'un identificateur d'utilisateur public ou privé à plusieurs identificateurs d'équipement terminal (mobile ou fixe) pour certains services. L'utilisateur peut être autorisé à utiliser plusieurs terminaux à un instant quelconque.
- 10) **Transfert d'informations d'identificateur**
Un réseau NGN prendra en charge le transfert d'informations d'identification d'utilisateur par des utilisateurs NGN saisissant des données via leur propre terminal ou le terminal de réception pour certains services (par exemple le terminal de point de vente), si la permission leur en est donnée par l'utilisateur.

6.12.3 Spécifications d'authentification

L'authentification est un processus visant à vérifier la validité des identificateurs d'utilisateur et d'équipement terminal ainsi qu'à établir la confiance dans le rattachement au réseau et l'offre de service. Du point de vue des fournisseurs, un réseau NGN peut faire la distinction entre une authentification de réseau et une autorisation de service. Du point de vue des abonnés, un réseau NGN peut faire la distinction entre une authentification d'utilisateur et une authentification d'équipement terminal. L'authentification de réseau est un processus consistant à vérifier les identificateurs d'utilisateur/d'équipement terminal par les seuls fournisseurs de réseaux pour l'accès au réseau de transport. L'authentification de service vise à vérifier les identités d'utilisateur/d'équipement terminal à des fins d'utilisation du service. Du point de vue des abonnés, le NGN doit offrir à un utilisateur la capacité d'authentifier et d'identifier un fournisseur de réseau de transport.

Du point de vue des abonnés, le NGN doit aussi offrir à un utilisateur la capacité d'authentifier et d'identifier un fournisseur de service.

Le NGN doit assurer l'indépendance de ces capacités.

Ces différents concepts d'authentification peuvent être réunis en un seul concept ou être appliqués séparément, suivant la technique de transport ou le modèle économique considéré. Par exemple, un flux d'authentification unique peut être utilisé si le fournisseur de réseaux est également un fournisseur de services.

Les spécifications relatives à la capacité d'authentification sont les suivantes:

- 1) un réseau NGN permettra l'utilisation de divers mécanismes d'authentification de réseau adaptés aux technologies de réseau d'accès sous-jacentes.
- 2) Il faudrait que le mécanisme d'authentification de service soit indépendant des technologies de réseau d'accès NGN et reste cohérent.
- 3) Un réseau NGN demandera à un utilisateur/un équipement terminal de fournir des informations d'authentification d'une manière explicite ou implicite.
- 4) Un réseau NGN devrait prendre en charge des mécanismes d'authentification fondés sur le logiciel utilisé et des mécanismes d'authentification fondés sur le matériel utilisé.

- 5) L'authentification d'équipement terminal utilisant des informations de profil de dispositif sera prise en charge.
- 6) Un réseau NGN devrait fournir des capacités d'authentification réciproque entre un fournisseur de services et un utilisateur.
- 7) Un réseau NGN doit fournir des capacités d'authentification réciproque entre le fournisseur de réseau de transport et l'utilisateur.

6.12.4 Spécifications d'autorisation

Les spécifications relatives à la capacité d'autorisation sont les suivantes:

- 1) Un réseau NGN fournira l'accès à des services à des utilisateurs et/ou à des dispositifs authentifiés en fonction de leurs droits d'accès, des profils d'utilisateur et de la politique de réseau appliquée.
- 2) L'autorisation d'accès aux services devrait être indépendante des technologies de réseau d'accès NGN.
- 3) La capacité d'autorisation devrait prendre en charge les scénarios de mobilité des réseaux NGN de version 1 lorsque cela est possible.

6.13 Sécurité

Les réseaux NGN de version 1 prendront en charge les caractéristiques de sécurité mises en œuvre dans les réseaux existants et permettre une interconnexion sûre à d'autres réseaux NGN ou non NGN. Ces spécifications découlent de l'application de [UIT-T X.805] aux réseaux NGN et concernent donc les aspects suivants de la sécurité des réseaux NGN: contrôle d'accès, authentification, non-répudiation, confidentialité des données, sécurité des communications, intégrité, disponibilité et confidentialité des données.

Un réseau NGN respectera les points suivants:

- 1) protection contre une utilisation non autorisée des ressources de réseau et contre un accès non autorisé à des flux d'informations et à des applications;
- 2) authentification de l'identificateur des entités de communication si cela est conforme aux politiques appliquées;
- 3) existence de mécanismes assurant la confidentialité des données;
- 4) existence de mécanismes assurant l'intégrité des données;
- 5) existence d'un mécanisme de responsabilité au travers duquel les individus sont tenus responsables des conséquences de l'ensemble de leurs actions;
- 6) disponibilité du réseau et accessibilité au réseau, en cas de demande d'une entité autorisée;
- 7) existence de mécanismes de non-répudiation empêchant l'une des entités ou des parties intervenant dans une communication de nier à tort d'avoir participé à la totalité ou à une partie de la communication;
- 8) confidentialité des données d'utilisateur (préférences, profils, informations de présence, de disponibilité ou de localisation par exemple). On la garantira en ne révélant des informations que lorsqu'une autorisation valable est fournie;
- 9) protection pour réduire au minimum les attaques contre le réseau, de l'intérieur ou de l'extérieur;
- 10) protection contre la cybercriminalité en permettant à l'utilisateur d'identifier le fournisseur du réseau de transport et le fournisseur de service.

6.14 Gestion de la mobilité

La gestion de la mobilité a trait à la capacité d'itinérance d'objets mobiles (utilisateurs, terminaux ou réseaux par exemple) entre différents réseaux (NGN ou non NGN). Dans les réseaux NGN de version 1, on distingue deux types de mobilité: la mobilité personnelle et la mobilité du terminal [UIT-T Q.1706].

Dans un réseau NGN de version 1, la mobilité personnelle existe lorsqu'un utilisateur peut utiliser les mécanismes d'enregistrement pour s'associer à un terminal que le réseau peut associer à cet utilisateur. On suppose que, lorsqu'elles existent, les interfaces entre les utilisateurs et les terminaux ou entre les utilisateurs et les réseaux servant à l'enregistrement d'utilisateur seront utilisées par les réseaux NGN de version 1.

Dans un réseau NGN de version 1, la mobilité du terminal existe dans et entre les réseaux pour lesquels des mécanismes d'enregistrement sont utilisés pour associer le terminal au réseau. La prise en charge de la mobilité du terminal avec continuité de service devrait, lorsqu'elle existe, également être mise en œuvre dans les réseaux NGN de version 1.

On trouvera ci-après des spécifications générales de gestion de la mobilité axées sur la prise en charge des besoins des clients.

Les réseaux NGN de version 1 doivent, pour les services pour lesquels la mobilité est appropriée, assurer le respect des points suivants:

- 1) le nomadisme pour la mobilité personnelle et la mobilité du terminal;
- 2) la prise en charge de la mobilité pour les technologies d'accès existantes, les capacités de qualité de service existantes et les capacités de sécurité existantes;
- 3) la prise en charge de la gestion de l'emplacement pour l'enregistrement, la mise à jour de l'emplacement et la traduction d'adresse pour permettre la mobilité à travers les limites de réseaux des fournisseurs;
- 4) la prise en charge de la gestion de l'abonnement itinérant et de l'authentification;
- 5) la prise en charge de la sécurité pour empêcher l'accès non autorisé et assurer la confidentialité des données d'utilisateur, compte tenu de la continuité ou du transfert de service le cas échéant;
- 6) la prise en charge de la confidentialité de l'emplacement pour cacher des informations sur l'emplacement à des entités qui ne sont pas dignes de confiance;
- 7) la prise en charge de capacité de pagination pour l'établissement des appels entrants afin d'économiser de l'énergie dans les terminaux mobiles et diminuer la signalisation dans le réseau.

6.15 Exploitation, administration et maintenance

Il est reconnu que les capacités OAM sont importantes dans les réseaux publics pour faciliter leur exploitation, vérifier leur performance et diminuer les coûts opérationnels en réduisant autant que faire se peut les interruptions de service, les dégradations de service et les pannes de fonctionnement. Les capacités OAM sont particulièrement importantes dans le cas de réseaux qui sont tenus de respecter un niveau de performance et des objectifs de disponibilité (et qui peuvent donc être évalués en conséquence) [UIT-T Y.1710] [UIT-T Y.1730].

Les réseaux NGN de version 1 assureront des fonctions OAM dans la strate de service et dans la strate de transport.

Les services de réseau NGN disposeront de leurs propres capacités OAM pour être fiables et respecter les prescriptions des accords SLA.

NOTE – Les capacités OAM décrites dans le présent paragraphe complètent les capacités de gestion décrites au § 6.17.

6.15.1 Spécifications générales d'exploitation, d'administration et de maintenance

Les spécifications OAM d'un réseau NGN sont les suivantes:

- 1) La capacité du fournisseur de services ou de réseaux à choisir les fonctions OAM souhaitées sera prise en charge.
- 2) Les fonctions OAM seront utilisées pour des applications point à point, point à multipoint et multipoint à multipoint.
- 3) Les fonctions OAM seront efficacement adaptables à des réseaux de grande taille.
- 4) La capacité à détecter des dérangements, des défauts et des défaillances sera prise en charge.
- 5) La capacité de diagnostic, de localisation et de notification aux entités de gestion de réseau et d'application des mesures correctrices appropriées sera prise en charge.
- 6) La capacité à permettre au réseau NGN d'empêcher le client de déclencher une fonction OAM de fournisseur de services/de réseaux sera prise en charge.
- 7) La capacité à permettre au réseau NGN d'empêcher le client de détecter ou de localiser des défaillances (puisque cela relève de la responsabilité du fournisseur de services ou du fournisseur de réseaux) sera prise en charge.
- 8) Le trafic OAM sera acheminé dans le même conduit que le trafic d'utilisateur.
- 9) Les anomalies suivantes seront automatiquement détectées:
 - la perte de données;
 - la perte de connectivité;
 - les données erronées;
 - les données involontairement autorépliquées;
 - les données mal insérées [UIT-T Y.1730].
- 10) Les fonctions OAM seront compatibles avec les versions antérieures. Un réseau NGN sera capable d'activer des fonctions OAM de façon transparente sans perturber le trafic d'utilisateur ou provoquer des actions inutiles.
- 11) Les fonctions OAM seront fiables même dans des cas de conditions de transmission dégradées (apparition d'erreurs par exemple).
- 12) L'évaluation de l'état de la connectivité ne doit pas dépendre du comportement dynamique du trafic d'utilisateur [UIT-T Y.1710], [UIT-T Y.1730].
- 13) Des relations OAM de couches serveur-client entre les couches inférieures et les couches supérieures (défaillance/dégradation du signal par exemple) seront prises en charge dans un réseau multicouche.
- 14) Dans le cas d'un réseau multicouche, un événement de défaut dans un réseau de couche serveur donné ne provoquera pas le déclenchement de plusieurs alarmes ni la mise en œuvre de mesures correctrices inutiles dans un réseau de couche client de niveau supérieur. Les réseaux de couche client prendront en charge la suppression d'alarmes pour les défauts émanant d'une couche serveur dont la présence a été signalée par des moyens d'indication de défaut vers l'avant. Ils prendront en charge la capacité d'indication de défaut vers l'avant [UIT-T Y.1710], [UIT-T Y.1730].
- 15) Dans un réseau multicouche, les fonctions OAM d'un réseau de couche donné ne dépendront pas d'un réseau de couche inférieure ou supérieure spécifique. Ce point est critique d'un point de vue architectural pour s'assurer qu'un réseau de couche peut fait l'objet d'une évolution, être ajouté ou supprimé sans incidence sur d'autres réseaux de couche.

- 16) Dans un réseau multicouche, les fonctions OAM d'un réseau de couche donné seront suffisamment indépendantes de tout plan de commande pour que des modifications touchant un plan de commande n'entraînent pas la modification des fonctions OAM du plan d'utilisateur. Le point est critique d'un point de vue architectural pour s'assurer que le plan d'utilisateur et le plan de commande peuvent évoluer sans incidence de l'un sur l'autre.
- 17) Les fonctions OAM prendront en charge plusieurs environnements de fournisseur de services/fournisseur de réseaux.
- 18) Lorsque des services NGN sont fournis dans plusieurs environnements de services/de réseaux, il faut pouvoir détecter/indiquer le fournisseur de services/de réseaux responsable du défaut de telle sorte qu'une action rapide puisse être entreprise. En outre, le fournisseur de services/de réseaux qui fournit le service à l'utilisateur sera informé du dérangement de service, même si le dérangement et le point de détection sont situés dans le réseau d'un autre fournisseur de services.
- 19) Un réseau NGN possédera des mécanismes permettant de vérifier que les flux OAM de fournisseurs de services/de réseaux, qui sont destinés à un usage interne à ces fournisseurs, sont confinés dans les réseaux de ces fournisseurs et ne "fuient" pas vers des clients ou vers d'autres fournisseurs de services/de réseaux.
- 20) Pour réaliser des fonctions OAM dans des réseaux hybrides, de telle sorte que des services puissent être fournis à travers un conduit de bout en bout associant des réseaux NGN et des réseaux non NGN, il faut que les fonctions OAM soient prises en charge dans les scénarios d'interfonctionnement (§ 6.7.3)
- 21) Pour permettre la gestion indépendante d'une portion de réseau sous la responsabilité d'un fournisseur et pouvoir définir une flexibilité d'entités de maintenance, il faudra pouvoir prendre en charge les fonctions OAM "de segment" et les fonctions OAM "de bout en bout".

NOTE – Par segment, on entend une partie d'une connexion de bout en bout définie à des fins d'exploitation et de maintenance.
- 22) L'enregistrement des indisponibilités de service pour mesurer la performance et la disponibilité sera pris en charge.
- 23) Les informations fournies par les fonctions OAM seront gérées de manière à fournir au personnel de maintenance les indications appropriées pour maintenir la qualité du niveau de service offert aux clients [UIT-T I.610].
- 24) Des capacités de surveillance de la performance seront prises en charge.

6.16 Capacité de survie

Des fonctions de capacité de survie sont nécessaires pour obtenir des réseaux très fiables.

6.16.1 Spécifications de commutation de protection

Un réseau NGN prendra en charge des capacités de commutation de protection pour mettre en œuvre des fonctions de capacité de survie rapides et déterministes pour tous les conduits de trafic.

Les spécifications générales applicables à la commutation de protection de transport NGN sont les suivantes:

- 1) des capacités permettant d'empêcher qu'un défaut de couche supérieure n'entraîne la commutation de protection d'une couche inférieure seront prises en charge;
- 2) lorsque plusieurs couches interviennent dans la commutation de protection, les couches inférieures seront prioritaires par rapport aux couches supérieures (on parle de stratégie d'escalade intercouches);
- 3) les commutations de protection 1+1 et 1: n devraient être assurées;

- 4) les ressources de protection de transport non utilisées peuvent servir à acheminer le trafic de "meilleur effort";
- 5) les incidences de la commutation de protection sur la performance de réseau (temps de transmission additionnel, variation du temps de transmission, erreurs binaires, pertes de paquets, etc.) devraient être aussi faibles que possible;
- 6) les fonctions de commande d'opérateur (telles que les commandes de verrouillage de protection, de commutation forcée et de commutation manuelle) seront prises en charge.

On trouvera des spécifications détaillées relatives à des technologies spécifiques dans diverses Recommandations ([UIT-T G.808.1] par exemple).

6.16.2 Spécifications de reroutage

Lorsqu'un incident grave ou un événement particulier se produit, il peut y avoir, dans le pire des cas, dégradation ou défaillance du réseau. Des capacités telles que le reroutage (moyennant dégradation éventuelle de la performance ou de la qualité de service) et des mécanismes de contrôle de trafic sont donc requis.

NOTE – Ces capacités peuvent également être considérées comme faisant partie des fonctions d'intégrité du réseau.

Les spécifications générales de reroutage dans un réseau NGN sont les suivantes:

- 1) lorsque plusieurs couches participent au reroutage, les couches inférieures pourraient avoir priorité sur les couches supérieures (stratégie d'escalade intercouches);
- 2) le mécanisme de reroutage sera capable de trouver un trajet de remplacement en un temps acceptable;
- 3) les incidences de la commutation de protection sur la performance de réseau (temps de transmission additionnel, variation du temps de transmission, erreurs binaires, pertes de paquets, etc.) devraient être aussi faibles que possible;
- 4) le réseau NGN n'exclura pas la possibilité d'une commande par l'opérateur;
- 5) une nouvelle optimisation du réseau sera possible, si nécessaire, après rétablissement du flux de trafic dégradé;
- 6) après élimination d'un dérangement ou suppression de conditions dégradées, les niveaux de performance et de qualité de service existants avant l'apparition du dérangement ou des conditions dégradées seront rétablis.

6.16.3 Spécifications de résilience de service

Les conditions de résilience dépendent du service considéré et seront donc décrites au cas par cas pour chaque service.

Les spécifications générales de résilience de service (SR, *service resiliency*) sont les suivantes:

- 1) le réseau NGN pourra attribuer de façon indépendante différents niveaux de résilience de service à différents services;
- 2) le réseau NGN pourra attribuer de façon indépendante différents niveaux de résilience de service à différents services en fonction du flux considéré;
- 3) le réseau NGN prendra en charge la capacité de résilience, suivant le niveau de résilience de service attribué, et retrouvera le niveau de qualité de service qu'il connaissait avant l'événement de défaillance;
- 4) l'équipement terminal pourrait signaler facultativement les niveaux de résilience de service au réseau NGN;
- 5) le réseau NGN pourra attribuer une résilience de service et de la prendre en charge entre le point d'entrée et le point de sortie du réseau de fournisseur de services;

- 6) le réseau NGN pourra faire la distinction entre les flux à capacité de résilience de service du plan d'utilisateur et les flux à capacité de résilience de service du plan de commande;
- 7) le réseau NGN prendra en charge de notifier à l'application/l'utilisateur que le niveau de résilience de service requis ne peut pas être atteint par le réseau NGN.

6.17 Gestion

Les capacités de gestion de réseau NGN prennent en charge des domaines de gestion couvrant la planification, l'installation, l'exploitation, l'administration, la maintenance et la fourniture de réseaux et de services. L'objectif de haut niveau est la mise à disposition de réseaux viables et rentables.

Les capacités de gestion de réseau NGN prennent également en charge la surveillance et la commande de services et de composantes de transport NGN via la communication d'informations de gestion à travers des interfaces entre des composantes et des services de gestion NGN, entre des systèmes de gestion de prise en charge de réseaux NGN et enfin entre des composantes NGN et des personnes travaillant pour les fournisseurs de services ou de réseaux.

Les capacités de gestion de réseau NGN prennent en charge les objectifs de réseau NGN en:

- 1) fournissant la capacité à gérer, tout au long de leur cycle de vie, les composantes NGN, tant physiques que logiques. Il faut pour cela des ressources au niveau de la strate de transport et de la strate de service, des fonctions de transport d'accès, des composantes d'interconnexion et des réseaux et des terminaux d'utilisateur;
- 2) fournissant la capacité à gérer des composantes de service NGN indépendamment des composantes de transport NGN sous-jacentes et en permettant à des organisations fournissant des services NGN (qui pourraient émaner de plusieurs fournisseurs de services) de proposer aux clients des offres de service distinctes;
- 3) fournissant des capacités de gestion permettant aux organisations qui fournissent des services NGN de proposer aux utilisateurs la capacité de personnaliser les services d'utilisateur et de créer de nouveaux services à partir des capacités NGN (émanant éventuellement de fournisseurs de services différents);
- 4) fournissant les capacités de gestion permettant aux organisations offrant des services NGN de les améliorer, y compris via le libre-service de l'utilisateur (fourniture de service, signalement des dérangements, rapports de facturation en ligne, par exemple);
- 5) développant une architecture de gestion et des services de gestion permettant aux fournisseurs de services de réduire les délais de conception, de création et de fourniture de nouveaux services;
- 6) prenant en charge la sécurité des informations de gestion, y compris les informations de client et d'utilisateur;
- 7) prenant en charge l'accès aux services de gestion en tout lieu et à tout instant pour tout organisation ou individu habilité;
- 8) prenant en charge les réseaux de commerce électronique sur la base des concepts des rôles commerciaux (client, fournisseur de services, fournisseur complémentaire, intermédiaire, fournisseur (par exemple fournisseur d'équipements)) [UIT-T Y.110] [UIT-T M.3050.0];
- 9) permettant à une entreprise et/ou à un individu d'adopter plusieurs rôles dans différents réseaux ou plusieurs rôles dans un réseau particulier (par exemple un rôle de fournisseur de services "au détail" et un rôle de fournisseur de services "en gros") [M.3050];
- 10) prenant en charge des processus interentreprises entre des organisations fournissant des services et des capacités NGN;
- 11) permettant la gestion de réseaux hybrides comprenant des ressources NGN et des ressources non NGN;

- 12) intégrant une vue abstraite des ressources (de réseau, de calcul et d'application), qui cache la complexité et la multiplicité des techniques et des domaines.

Les prescriptions détaillées de gestion NGN ne relèvent pas du domaine d'application de la présente Recommandation et sont fournies dans des Recommandations traitant spécifiquement de questions de gestion, telles que [UIT-T M.3060].

NOTE – Voir également les spécifications du § 6.10 ("Comptabilité et taxation").

6.18 Environnement de service ouvert

Les capacités d'environnement de service ouvert découlent des capacités générales d'un réseau NGN et permettent la prise en charge et l'établissement d'un environnement de création et de fourniture de service amélioré, flexible et ouvert dans la strate de service.

La mise en œuvre de nouvelles fonctionnalités dans les réseaux actuelles peut être limitée ou impossible en raison des capacités des équipements installés. La fourniture de logiciels permettant l'implémentation de nouvelles fonctionnalités est principalement réservée aux fournisseurs d'équipements, puisque les interfaces de programmation d'application (API) sont généralement de type propriétaire (c'est-à-dire pas de type ouvert).

Un réseau NGN doit offrir de nouvelles capacités et prend en charge une large gamme de nouveaux services, notamment des services à fonctionnalités évoluées et complexes. Les fournisseurs d'applications et de services tiers incitant au développement d'applications et de capacités nouvelles accessibles via des interfaces ouvertes et normalisées, la coopération entre fournisseurs de réseaux et de services pour le développement d'interfaces de réseau d'application (ANI) normalisés est de plus en plus nécessaire. De plus, la réutilisabilité et la portabilité des logiciels ainsi que l'utilisation de logiciels commerciaux devraient être prises en charge pour assurer un développement au meilleur rapport.

On trouvera ci-après quelques avantages généraux d'un environnement de service ouvert:

- les applications et les capacités peuvent être facilement développées par des fournisseurs de réseaux et par des parties tiers;
- on peut rendre les capacités portables et/ou réutilisables entre les réseaux;
- des applications ANI ouvertes et normalisées permettront des interactions entre des entités et des applications NGN (pour la création de service par exemple).

Dans un environnement de service ouvert, chaque capacité fonctionnera de manière indépendante ou avec d'autres capacités pour la mise en œuvre d'applications. Chaque capacité assure l'ensemble des fonctions de service appropriées au profit de l'entité demandeuse (par exemple une partie tiers). Les applications pouvant être fournies dans différents réseaux, les capacités doivent pouvoir fonctionner indépendamment des technologies de réseau sous-jacentes.

Un réseau NGN doit satisfaire aux spécifications générales d'environnement de service ouvert suivantes:

- 1) indépendance par rapport aux fournisseurs de réseaux de transport: les fonctionnalités, l'exploitation et la gestion des applications et des services seront indépendantes de l'infrastructure et des technologies des fournisseurs du réseau de transport sous-jacent;
- 2) indépendance par rapport aux fabricants: un environnement de service ouvert multifournisseur sera pris en charge, une large gamme de services et d'applications étant alors fournie aux utilisateurs dans un environnement concurrentiel;
- 3) transparence de l'emplacement: dans un environnement distribué, les fournisseurs de services accéderont aux capacités depuis un emplacement quelconque, quel que soit l'emplacement physique réel de ces capacités;

- 4) transparence du réseau: l'environnement de service ouvert permettra aux applications et aux services de n'avoir aucune connaissance des technologies et des terminaux utilisés;
- 5) transparence du protocole: la transparence du protocole sera obtenue à l'aide d'outils normalisés ouverts d'interface de programmation de protocole, afin de réaliser un processus de commande de service indépendant, et de masquer les détails techniques complexes du réseau par rapport à l'environnement de service ouvert;
- 6) un accès sûr aux capacités d'environnement de service ouvert satisfera aux spécifications générales de sécurité des réseaux NGN spécifiées au § 6.13.

On décrit dans les paragraphes ci-après les capacités d'environnement de service ouvert.

6.18.1 Coordination de service

Les spécifications de coordination de service d'un environnement de service ouvert sont les suivantes:

- 1) Un réseau NGN permettra de coordonner les applications et les services aux capacités.
- 2) Il convient de suivre l'évolution des capacités ou des composantes de service NGN émanant de divers fournisseurs de services et de suivre l'évolution de la relation entre ces capacités ou ces composantes de services.
- 3) Des informations sur les changements d'état des capacités ou des composantes de service (par exemple suite à une mise à niveau) devraient être mises à la disposition des applications et des services.

6.18.2 Interfonctionnement avec des environnements de création de service

- 1) Un environnement de service ouvert NGN permettra l'interfonctionnement entre des environnements de création de service et des entités de réseau pour la création et la fourniture d'applications et de services.
- 2) Un réseau NGN de version 1 devrait prendre en charge les trois classes suivantes d'environnements de création de service:
 - environnement de création de service ouvert: l'accès OSA/Parlay, Parlay X et l'architecture de gestion d'objets OMA (*object management architecture*) sont des exemples de cette classe d'environnement utilisant des interfaces ANI;
 - environnement de création de service fondé sur des sous-systèmes multimédias IP [UIT-T Q.1741.X];
 - environnement de création de service fondé sur des réseaux intelligents: le protocole d'application de réseau intelligent INAP (*intelligent network application protocol*), les applications personnalisées pour une logique améliorée de réseau mobile CAMEL (*customized application for network enhanced logic*) et le réseau intelligent hertzien WIN (*wireless intelligent network*) sont des exemples de protocoles d'interface appropriés pour cette classe d'environnement.

6.18.3 Découverte de services

La découverte de services est souvent la première étape pour découvrir des capacités et/ou des services et des applications. Une capacité de découverte de services est essentielle dans plusieurs scénarios (dans les scénarios de mobilité par exemple (pour localiser des services dans le réseau visité)) ou pour permettre un accès aux services indépendant du dispositif d'utilisateur.

Par exemple, lorsque cette capacité est implémentée dans des services Web, on peut utiliser les registres de services web publics (registre UDDI (découverte, description et intégration universelles par exemple)) pour implémenter la découverte de services et permettre l'accès aux services.

Les spécifications de découverte de services sont les suivantes:

- 1) un réseau NGN prendra en charge une capacité de découverte de services pour permettre aux utilisateurs et à leurs dispositifs de découvrir des services les intéressant quelles que soient les technologies de réseau sous-jacentes;
- 2) les mécanismes de découverte de services seront indépendants des technologies de réseau sous-jacentes pour pouvoir prendre en charge des technologies de réseau hétérogènes et changeantes;
- 3) la capacité de découverte de services permettra aux utilisateurs de découvrir des services intéressants tant du point de vue humain que du point de vue dispositif:
 - les services intéressants du point de vue utilisateur peuvent être directement utilisés par des utilisateurs. On peut citer à titre d'exemple les services d'annuaire, les services de traduction et les installations partagées (informations de prise en charge des technologies de l'information par exemple);
 - les services intéressants du point de vue dispositif peuvent faire l'objet d'un accès direct par des dispositifs (combinés mobiles ou ordinateurs personnels portables par exemple). On peut citer à titre d'exemple les imprimantes, les dispositifs de sauvegarde, les graveurs de CD/DVD, les serveurs d'authentification et les serveurs d'attribution d'adresses IP. Les services intéressant les dispositifs et les informations de réseau peuvent ne pas être directement utilisables par des utilisateurs;
- 4) les mécanismes de découverte de services ne devraient pas être limités uniquement aux technologies client-serveur traditionnelles.
NOTE – On peut mettre en œuvre la découverte de services en utilisant des technologies homologue à homologue ou en associant des technologies client-serveur et homologue à homologue.
- 5) la capacité de découverte de services devrait prendre en charge divers critères d'évaluation (emplacement et coûts par exemple) pour présenter le degré d'adaptabilité approprié;
- 6) la capacité de découverte de services prendra en charge des mécanismes appropriés assurant la sécurité et la confidentialité;
- 7) la capacité de découverte de services prendra en compte des considérations d'échelonnabilité (l'utilisation de mécanismes de radiodiffusion devrait par exemple être évitée).

6.18.4 Enregistrement de services

Cette capacité permet l'enregistrement d'autres capacités, services et applications dans des annuaires de l'environnement de service ouvert accessibles à des capacités, des services et des applications. Par exemple, la capacité d'enregistrement peut être implémentée dans un service Web lorsque l'on souhaite que ce service bénéficie d'une "exposition": les services web peuvent être enregistrés dans des "registres" de services web publics (un registre est un annuaire particulier qui non seulement dirige les utilisateurs vers une ressource mais leur permet également d'enregistrer des services en son sein).

Les spécifications d'enregistrement de services sont les suivantes:

- 1) l'environnement de service ouvert permettra de gérer l'enregistrement des capacités, des services et des applications. Les technologies choisies permettront de proposer des fonctions d'enregistrement et de suppression d'enregistrement de services, notamment pour la configuration, l'activation et la publication.

6.18.5 Prise en charge du développement pour les services

La prise en charge du développement pour les services est un aspect essentiel de la chaîne de fourniture de services, tant chez le fournisseur de services que chez les parties tiers qui élargissent l'ensemble de capacités et l'offre de services globale. La collecte et la publication des données figurent parmi les besoins des développeurs, qui souhaitent de plus pouvoir articuler et spécifier ces besoins et identifier les interfaces de développement des services.

Un réseau NGN devrait permettre la prise en charge d'un développement efficace pour:

- 1) la construction d'applications et de services;
- 2) la mise à l'essai d'applications et de services (suivi pas à pas et correction d'erreurs par exemple);
- 3) le déploiement d'applications et de services;
- 4) la suppression d'applications et de services.

La prise en charge du développement devrait comprendre les points suivants:

- 1) la réutilisabilité et l'interchangeabilité des composantes (logicielles);
- 2) la capacité à associer les composantes en gérant les interfaces et à utiliser une sémantique cohérente de mécanismes/données partagés entre ces composantes;
- 3) la prise en charge du cycle de vie complet des composantes (installation, configuration, administration, publication, mise à jour de la version, maintenance et suppression);
- 4) la prise en charge d'une conception d'application indépendante du mode de fourniture pour permettre la mise en œuvre d'applications sans nécessité d'une nouvelle conception pour chaque scénario de développement;
- 5) le suivi des dépendances entre les composantes.

6.19 Gestion des profils

6.19.1 Profil d'utilisateur

Un profil d'utilisateur est un ensemble d'informations stockées relatives à un utilisateur (ou à un abonné). Dans un environnement de réseau NGN, la gestion des attributs du profil d'utilisateur est particulièrement importante puisque les informations d'utilisateur sont requises pour implémenter un certain nombre de capacités, notamment l'authentification, l'autorisation, la mobilité, la localisation, la taxation, etc. Le profil d'utilisateur comprend des informations sur le transport et des informations sur le service. Les profils d'utilisateur peuvent être stockés dans des bases de données distinctes situées dans la strate de service et dans la strate de transport, pouvant disposer de fonctions d'échange de données entre elles.

Les spécifications générales applicables au profil d'utilisateur sont les suivantes:

- 1) Un profil d'utilisateur existera pour chaque utilisateur chez un fournisseur correspondant. Ce profil pourra comprendre plusieurs composantes.
- 2) Les composantes peuvent être réparties entre le réseau de rattachement et l'environnement du fournisseur de services. Les critères de confidentialité et de protection des données seront respectés.
- 3) Dans le domaine du réseau de rattachement, les composantes peuvent être réparties entre plusieurs entités.
- 4) Dans le réseau de rattachement, il existera une fonctionnalité capable de localiser les composantes du profil d'utilisateur, permettant ainsi aux services et applications de ne pas avoir à connaître l'emplacement réel des composantes. Cette fonction sera sous le contrôle du réseau de rattachement.

- 5) Les services, les applications et les autres entités NGN devront pouvoir extraire le profil d'utilisateur en tout ou partie (selon les besoins) en une seule transaction. Les critères de confidentialité et de protection de données seront respectés.
- 6) Il devra exister des moyens efficaces d'extraire différentes composantes du profil d'utilisateur dans un délai acceptable par des services en temps réel.

NOTE – Bien que la gestion d'un profil d'utilisateur ne vise pas à classer les données qu'un tel profil peut contenir, un classement par catégories (informations générales sur l'utilisateur, informations spécifiques sur le service, etc.) peut être appliqué.

Le détail des spécifications relatives au profil d'utilisateur, à son utilisation et à sa gestion devrait figurer dans une ou plusieurs futures Recommandations de l'UIT-T.

6.19.2 Profil de dispositif

Un profil de dispositif est un ensemble d'informations stockées relatives à un équipement d'utilisateur. Dans un environnement de réseau NGN, la gestion des attributs du profil de dispositif est également une question importante puisque des données sur le dispositif sont requises avec le "profil d'utilisateur; pour un certain nombre de capacités, en particulier l'authentification, l'autorisation, la mobilité, la localisation, la taxation etc. Le profil de dispositif peut comprendre des informations sur le transport et des informations sur le service. Les profils de dispositif peuvent être stockés dans des bases de données distinctes situées dans la strate de service et dans la strate de transport et peuvent disposer de fonctions d'échange de données.

NOTE 1 – Ces informations peuvent inclure des attributs d'identification du terminal, tels son adresse et son nom, des attributs statiques (tels que les flux de média et les protocoles pris en charge), des détails sur l'écran (taille en pixels, résolution des couleurs, temps de réponse, etc.), le débit de transmission, la largeur de bande et la puissance de traitement, et des attributs évoluant dynamiquement tels que l'utilisateur du terminal, la position géographique, les applications en cours sur le terminal.

On peut utiliser les profils de dispositif aux fins suivantes:

- suivre la trace des dispositifs volés ou usurpés;
- déterminer le type et le niveau de service susceptibles d'être fournis à l'utilisateur (en fonction des capacités du dispositif);
- déterminer la qualité de service requise pour une connexion entre des terminaux (en fonction des capacités du dispositif).

Les spécifications applicables aux profils de dispositif sont les suivantes:

- 1) un profil de dispositif peut exister pour chaque équipement d'utilisateur. Il peut comprendre plusieurs "composantes";
- 2) ces composantes peuvent être réparties entre le réseau de rattachement et/ou les fournisseurs de services.
- 3) dans le réseau de rattachement, les composantes peuvent être réparties entre plusieurs entités;
- 4) dans le réseau de rattachement, il faudra une fonctionnalité capable de localiser les composantes du profil de dispositif, permettant aux applications et services d'ignorer la localisation effective des composantes. Cette fonctionnalité doit être sous le contrôle du réseau de rattachement;
- 5) sur accord de l'utilisateur, les services, les applications et les autres entités NGN doivent pouvoir extraire tout ou partie du profil du dispositif (selon les besoins) en une transaction; les critères de confidentialité et de protection des données doivent être remplis;

- 6) il existera des moyens efficaces d'extraire différentes composantes du profil de dispositif dans un délai acceptable par les services en temps réel.

NOTE 2 – Bien que la gestion d'un profil de dispositif ne vise pas à classer les données qu'un tel profil peut contenir, un classement par catégories (informations générales le dispositif, informations spécifiques sur le service, etc.) peut être appliqué.

Le détail des spécifications relatives au profil du dispositif, à son utilisation et à sa gestion devrait figurer dans une ou plusieurs futures Recommandations de l'UIT-T.

6.20 Gestion des politiques

La gestion des politiques peut être utilisée dans les réseaux NGN aux fins suivantes:

- 1) assurer la cohérence des services en cas d'utilisation d'une variété de technologies de réseau d'accès et de réseau central. Cette spécification peut également s'appliquer lorsqu'il existe plusieurs réseaux de fournisseurs de services;

NOTE 1 – La politique appliquée à chaque réseau dépend des technologies de réseau et peut être spécifique à chaque technologie de réseau.

- 2) assurer le contrôle d'admission par rapport à l'utilisation des capacités de réseau et des ressources de réseau par les services et les applications;

- 3) enregistrer des informations décrivant l'utilisation de ressources de réseau;

NOTE 2 – Ceci peut être vu comme la fonction générant des informations susceptibles d'être utilisées par d'autres capacités de réseau (fonctions de comptabilité et taxation par exemple).

- 4) ne pas fournir aux services et aux applications des détails complexes sur l'implémentation du réseau de transport.

NOTE 3 – Le mécanisme de contrôle des politiques peut servir à répondre aux besoins des applications tant en n'ayant aucune connaissance des technologies de réseau déployées.

De nombreuses mesures favorables aux services NGN peuvent être prises en matière de gestion des politiques dans les principaux domaines d'application cités plus haut dans le respect des spécifications de connectivité, de qualité de service et de sécurité. La gestion des politiques peut par exemple porter sur les points suivants:

- la fourniture de services;
- la configuration de services;
- l'autorisation (c'est-à-dire les droits);
- la mise en œuvre de service;
- la comptabilité et la taxation.

La gestion des politiques peut faire appel à des règles de politique pour fournir des résultats fiables, cohérents et déterministes appelés décisions politiques. Le degré de complexité de ces règles est proportionnel à l'utilisation que l'on souhaite en faire.

NOTE 4 – Les capacités de gestion de la qualité de service telles que le contrôle de ressources et d'admission (§ 6.9) peuvent être considérées comme faisant partie de l'ensemble global de gestion des politiques.

Les spécifications générales de gestion des politiques pour les réseaux NGN de version 1 sont les suivantes:

- 1) les capacités de gestion des politiques seront prises en charge pour garantir l'accès aux services, la fourniture et la gestion de ces derniers;
- 2) les capacités de gestion des politiques s'appliqueront à certains services et dans certains domaines de fournisseur ou entre plusieurs domaines de fournisseur;
- 3) les capacités de gestion des politiques rejeteront ou ne répondront pas à des demandes non autorisées et répondront à des demandes autorisées.

6.21 Activateurs de service

La catégorie "activateurs de service" regroupe des capacités qui donnent les caractéristiques de services et d'applications spécifiques ou évoluées et/ou qui permettent l'accès aux informations spécifiques fournies par ces capacités et/ou la gestion de ces informations.

6.21.1 Gestion de groupes

Cette capacité fournit des fonctionnalités relatives à une gestion sûre et efficace de groupes d'entités de réseau (terminaux, utilisateurs, nœuds de réseau, etc.). Elle peut être utilisée par des applications et des services à différentes fins: applications VPN, distribution de contenus vidéo, gestion de dispositifs, fourniture et gestion, de transport et de service, services d'urgence (notification à une communauté), etc.

La gestion de groupes est par exemple obligatoire dans le cas type d'un service VPN fourni par un fournisseur. On doit définir dans le cas d'un réseau VPN, un groupe fermé à l'aide d'une liste d'utilisateurs de service et les communications au sein du groupe doivent être protégées vis-à-vis des autres utilisateurs. Un réseau NGN devrait gérer de tels groupes et assurer des communications de groupe sûres.

La distribution simultanée de contenus vidéo par multidiffusion depuis une source vers plusieurs utilisateurs d'un groupe est un autre exemple de gestion de groupes. Pour une telle application, la capacité de gestion de groupes est également d'une importance cruciale. Les spécifications de gestion de groupes sont les suivantes:

- 1) un réseau NGN fournira une capacité permettant la création de groupes dans la strate de transport;
- 2) un réseau NGN fournira une capacité permettant la création d'un groupe de services et/ou de groupes propres à un service (strate de service);
- 3) un réseau NGN gèrera des groupes et fournir des communications de groupe sûres.

6.21.2 Gestion d'informations personnelles

Cette capacité permet de gérer des informations statiques ou dynamiques propres à l'application considérée (informations relatives à l'utilisateur et au contexte de communication). On peut citer comme exemples d'informations spécifiques d'application les informations de contact d'utilisateur, les conditions d'accès à l'application (mots de passe, etc.), les paramètres par défaut de l'application, les préférences de largeur de bande/de qualité de service (par exemple par rapport aux réseaux d'accès disponibles), les préférences de média, les données spécifiées d'utilisateur, etc. Fournies par les applications (services de notification et d'informations par exemple) conformément à des préférences d'utilisateur prédéfinies et à des attributs de politique (entre différents dispositifs mobiles et types de réseau d'accès), ces informations peuvent être stockées et gérées au nom des utilisateurs par la capacité de gestion des informations personnelles. La capacité de gestion des informations personnelles, agissant en tant que mandataire de l'utilisateur pour des applications, peut également extraire ces informations des applications pour le compte des utilisateurs.

Les spécifications relatives à la capacité de gestion des informations personnelles sont les suivantes:

- 1) Une capacité de gestion des informations personnelles peut être fournie. Elle peut permettre de stocker et de gérer au nom des utilisateurs des informations statiques ou dynamiques propres à l'application considérée; elle peut également extraire ces informations des applications au nom des utilisateurs.
- 2) Les informations gérées par la capacité de gestion des informations personnelles seront protégées contre les opérations non autorisées d'accès, d'extraction, de manipulation, etc.
- 3) La capacité de gestion des informations personnelles devrait prendre en charge différents contextes de communication.

6.21.3 Gestion des messages

Dans les réseaux actuels, certains services sont pris en charge dans deux types d'environnement (filaire ou hertzien) et d'autres seulement dans un seul. Par exemple, le service de messages courts (SMS, *short message service*) a été conçu pour un environnement hertzien (bien qu'on puisse à présent l'utiliser dans certains réseaux fixes) et la messagerie instantanée (IM, *instant messaging*) a été conçue pour un environnement filaire (même si certains réseaux mobiles ont mis en œuvre des services IM). Les attentes liées aux divers services diffèrent également en ce sens que certains services sont conçus pour une utilisation perçue comme en "temps réel" alors que d'autres servent de "boîte aux lettres" pour le stockage de messages en vue de leur fourniture ultérieure.

La capacité de gestion des messages fournit des fonctionnalités pour les services fondés sur les messages. Ces fonctionnalités comprennent la commande de service de messagerie en temps réel ou pas en temps réel. La messagerie instantanée et la conversation textuelle ("Chat") sont des exemples de messagerie en temps réel, la messagerie électronique, le service de messages courts (SMS) et le service de messagerie multimédia (MMS, *multimedia messaging service*) étant des exemples de services pas en temps réel.

Les spécifications générales sont les suivantes:

- 1) la capacité de gestion des messages de réseau NGN prendra en charge les services de messagerie accessibles par terminaux fixes et ceux accessibles par terminaux mobiles;
- 2) la capacité de gestion de messages NGN prendra en charge les services de messagerie en temps réel et les services de messagerie par en temps réel.

NOTE – La capacité de gestion de groupes peut également être nécessaire pour prendre en charge des services de messagerie.

Il existe en outre des spécifications d'utilisateur relatives à la capacité de gestion des messages qui permettent de configurer les services de messagerie (sélection, filtrage, formatage, gestion de groupes et traitement (isolement des gros volumes de télécommunications non sollicités par exemple)).

6.21.4 Prise en charge de la multidiffusion

Cette capacité permet à des applications de fournir des contenus à plusieurs utilisateurs simultanément à l'aide de mécanismes de multidiffusion.

Outre l'unidiffusion, la multidiffusion devrait être prise en charge pour une utilisation efficace des ressources de réseau.

La strate de transport et la strate de service devraient fournir les capacités nécessaires à la fourniture de services de radiodiffusion/multidiffusion.

Les spécifications générales sont les suivantes:

- 1) un réseau NGN prendra en charge des capacités de multidiffusion pour fournir des données de façon efficace et modulable;
- 2) un réseau NGN devrait fournir des capacités permettant d'assurer des services de radiodiffusion/multidiffusion dans un seul réseau NGN ou dans plusieurs réseaux NGN.

6.21.5 Présence

La capacité de présence (service) donne l'accès à des informations de présence et indique sa disponibilité à des utilisateurs ou à des services. Il s'agit d'un ensemble d'attributs caractérisant les propriétés à l'instant considéré (état, emplacement, etc.) d'une entité.

On entend ici par entité tout dispositif, service, application, etc., capable de fournir des informations de présence. Par disponibilité, on entend la capacité et la volonté d'une entité à communiquer en se fondant sur diverses propriétés et politiques associées à cette entité (heure, capacités de dispositif,

préférences et capacités de média, etc.). Les termes présence et disponibilité sont presque toujours utilisés ensemble pour fournir un ensemble complet d'informations de présence.

Les réseaux NGN permettront aux utilisateurs d'être tant fournisseurs d'informations de présence (ils sont alors appelés "entités de présence" [b-121.905]) que demandeurs de telles informations (ils sont alors les "observateurs").

Les informations de présence sont fournies par trois groupements de capacités. Les spécifications associées à chaque groupement sont décrites ci-après.

Collecte des informations de présence

- 1) Un réseau NGN fournira une capacité permettant de recueillir les informations décrivant l'état de connectivité de l'entité de présence avec la permission de l'utilisateur (par exemple le ou les dispositifs utilisés par un utilisateur).
- 2) Un réseau NGN fournira une capacité permettant de recueillir des informations relatives à la localisation de l'entité de présence conformément à la législation nationale.

Diffusion des informations de présence

- 3) Un réseau NGN fournira une capacité permettant à une entité (par exemple un utilisateur) d'être informé de l'état à l'instant considéré de l'entité de présence. Cette capacité peut également permettre à un autre service d'accéder aux informations de présence des utilisateurs, sous réserve de la permission de l'utilisateur.

Gestion des informations de présence

- 4) Un réseau NGN permettra la gestion des informations de présence en offrant un ensemble de capacités pour gérer les informations de présence collectées.
- 5) Le contrôle d'accès aux informations de présence (à l'aide des capacités de diffusion des informations de présence) sera géré conformément aux spécifications relatives à la confidentialité de l'entité de présence et aux règles d'accès.
- 6) Les capacités de gestion des informations de présence permettront à la capacité de diffusion de ne fournir qu'une partie des informations de présence en fonction de ce qui est demandé.
- 7) Les capacités de gestion des informations de présence permettront de collecter les demandes émanant de certaines entités qui souhaitent recevoir des informations de présence relatives à d'autres entités. Elle permet également à l'entité de présence de déterminer la diffusion de ses informations de présence (par exemple accepter ou rejeter les demandes d'informations de présence en fonction de l'observateur considéré).

6.21.6 Gestion de l'emplacement

La gestion de l'emplacement est une capacité utile à des applications et à des services qui ont besoin d'informations sur l'emplacement des utilisateurs et des dispositifs dans les réseaux. L'emplacement des utilisateurs et des dispositifs dans les réseaux peut être lié à leur position physique; la connaissance du contexte local et de la pertinence des informations permettent d'améliorer la qualité des applications.

Les mécanismes permettant de déterminer et de faire état des informations de localisation dépendent souvent de la technologie des réseaux d'accès. La prise en charge d'applications et de services fondés sur la connaissance de l'emplacement devrait donc être mise en œuvre pour chaque technologie de réseau d'accès.

Les spécifications suivantes sont applicables à la gestion de l'emplacement:

- 1) Un réseau NGN fournira une capacité de gestion de l'emplacement pour déterminer et faire état des informations sur l'emplacement des utilisateurs et des dispositifs dans le réseau.

- 2) Un réseau NGN fournira des capacités additionnelles pour garantir l'exactitude et l'authenticité des informations d'emplacement utilisées par les applications et les services afin d'éviter l'utilisation d'informations de localisation frauduleuses ou fausses et ses conséquences néfastes.
- 3) Les conditions de confidentialité seront respectées par les services et les applications fournisseurs de localisation.
- 4) La capacité de gestion de l'emplacement permettra de fournir des informations d'emplacement conformément aux informations contenues dans les profils d'utilisateur/de dispositif.

6.21.7 Poussée

La capacité de poussée permet de transmettre des données d'un émetteur à un récepteur sans demande préalable du récepteur (utilisation par exemple d'un mécanisme de poussée fondé sur l'utilisation du protocole SIP).

Si l'utilisateur a généralement la capacité de configurer des services de poussée choisis parmi une gamme de services proposés par des fournisseurs de services, le récepteur n'a pas à émettre de demande spécifique mais une demande générale quant aux données à envoyer. Les données peuvent être envoyées périodiquement ou après déclenchement d'une invocation unique fonction de l'application.

Le mécanisme de poussée peut par exemple être utilisé pour indiquer la disponibilité d'un message MMS.

Les spécifications de poussée sont les suivantes:

- 1) un réseau NGN prendra en charge une capacité de poussée conformément à la législation nationale.

NOTE – L'invocation d'un service de poussée peut nécessiter l'accord de l'utilisateur.

6.21.8 Gestion de dispositif

La gestion de dispositif active les capacités de réseau permettant de gérer et de contrôler les dispositifs. Les capacités de gestion de dispositif peuvent être utilisées aux fins suivantes:

- gestion de la configuration matérielle/logicielle (informations sur l'équipement, capacités média, version logicielle);
- mises à niveau de logiciels à distance, avec ou sans intervention de l'utilisateur pour exemple pour des corrections d'erreur, une mise à jour de caractéristiques, le service d'exploitation, un micrologiciel, des applications client);
- diagnostic de dérangement distant.

Les spécifications générales relatives à la gestion de dispositif sont les suivantes:

- 1) un réseau NGN prendra en charge la mise à niveau des dispositifs;
- 2) un réseau NGN prendra en charge l'autoconfiguration des dispositifs;
- 3) un réseau NGN prendra en charge la mise en commun des informations de connexion de dispositifs conformément à la législation nationale (adresse IP et emplacement par exemple);
- 4) la gestion de dispositif peut fournir des fonctions permettant l'enregistrement, la gestion et la mise à jour des informations de dispositif;
- 5) la gestion de dispositif peut fournir des fonctions permettant de vérifier à distance l'état du dispositif, notamment les modifications d'état et les mises à niveau, et de générer des comptes rendus de diagnostic;

- 6) la procédure de gestion de dispositif sera sûre et toujours effectuée par une entité habilitée conformément à la législation nationale.

NOTE 1 – La gestion de dispositif devrait permettre l'installation des préférences et des applications d'utilisateur.

NOTE 2 – L'invocation de services de gestion de dispositif nécessitera normalement un accord d'utilisateur.

6.21.9 Gestion de session

Un réseau NGN fournira des capacités de démarrage, de gestion et de terminaison de l'identificateur de service de bout en bout qui, par exemple, fait intervenir plusieurs parties, un groupe de points d'extrémité associés à ces parties et une description des connexions multimédias entre ces points. Ces capacités de gestion de session seront fournies dans des environnements de réseau fixe et dans des environnements mobile pour prendre en compte diverses spécifications de services, en utilisant les serveurs d'application appropriés pour l'exploitation du service considéré.

Les fonctions de gestion de session sont les suivantes:

- établissement d'une session;
- présentation de l'identificateur pour l'appelant et pour l'appelé d'une session;
- suppression de l'identificateur pour l'appelant et pour l'appelé d'une session;
- fourniture et suppression des informations facultatives fournies par l'utilisateur (image, vidéo ou texte fourni durant l'établissement d'une session par exemple);
- gestion d'une session entrante par l'appelé;
- négociation de capacité d'une session entrante;
- acceptation, non-prise en compte, redirection ou rejet d'une session entrante;
- négociation de média et de composantes de média durant l'établissement d'une session;
- gestion d'une session entrante;
- modification de média et de composantes de média durant une session en cours;
- suspension et reprise d'une session en cours;
- fin d'une session;
- terminaison de session commandée par le réseau.

Les spécifications de gestion de session sont les suivantes:

- 1) la gestion de session devra pouvoir mettre en œuvre les serveurs d'application appropriés pour l'exploitation du service considéré;
- 2) l'utilisateur doit pouvoir invoquer une ou plusieurs sessions et activer des applications multimédias concurrentes dans chaque session;
- 3) la gestion de session prendra en charge des sessions pour divers types de média;
- 4) une commande d'admission de session fondée sur des niveaux définis de qualité de service et de sécurité sera prise en charge;
- 5) les mécanismes de commande d'admission de session prendront en charge plusieurs types de service (voix, texte et vidéo par exemple);
- 6) lorsqu'une session ne compte qu'un ou deux participants, le réseau y mettra fin dès lors qu'un des utilisateurs le demande. Le réseau peut mettre fin à une session à tout moment (par exemple si des conditions de défaillance apparaissent);
- 7) lorsqu'une session ne compte qu'un ou deux participants, le réseau doit y mettre fin dès lors qu'un des utilisateurs le demande. Le réseau peut mettre fin à une session à tout moment (par exemple si des conditions de défaillance apparaissent).

6.21.10 Prise en charge des applications fondées sur le Web

Les capacités de prise en charge des applications fondées sur le Web permettent d'améliorer l'utilisation des capacités de dispositif et des caractéristiques de réseau pour les applications fondées sur le Web.

Les capacités de prise en charge des applications fondées sur le Web fournissent aux utilisateurs un environnement Web cohérent qui s'étend à plusieurs environnements de réseau et plusieurs dispositifs (ordinateurs personnels, ordinateurs portables, assistants numériques personnels, téléphones cellulaires, etc.).

La prise en charge des applications fondées sur le Web suppose la prise en compte des interactions suivantes:

- (application) serveur à serveur;
- serveur à terminal;
- terminal à serveur;
- terminal à terminal (ou homologue à homologue).

Un réseau assurera la prise en charge des applications fondées sur le Web en respectant les points suivants:

- 1) interopérabilité entre les environnements de réseau filaire et les environnements de réseau hertzien;
- 2) accès sûr à des applications;
- 3) nomadisme;
- 4) faible temps de réponse et utilisation efficace de la largeur de bande;

Le réseau NGN doit assurer la prise en charge des applications fondées sur le Web en respectant les points suivants:

- 5) réutilisation des technologies existantes et des composantes NGN (par exemple l'authentification) pour la fourniture d'applications fondées sur le Web;
- 6) réutilisation des outils de création et d'intégration;
- 7) pas de perturbation pour l'utilisateur en cas de passage d'un réseau à un autre;
- 8) prise en charge des techniques de composition de service;
- 9) échelonnabilité des applications fondées sur le Web;
- 10) maintien de la fiabilité des réseaux NGN.

NOTE – Les réseaux NGN de version 1 peuvent présenter des capacités limitées de prise en charge des applications fondées sur le web.

6.21.11 Synchronisation de données

On définit la synchronisation de données comme la mise en équivalence de deux ensembles de données. Cette capacité permet de synchroniser des données de réseau provenant de différents terminaux ordinateurs de poche, téléphones mobiles, ordinateurs portables et ordinateurs de bureau par exemple. Les applications suivantes sont susceptibles d'utiliser la capacité de synchronisation de données: gestion de calendrier ou d'informations de contact, gestion de données d'entreprise stockées dans de bases de données et gestion de documents Web.

Un réseau NGN doit prendre en charge un synchronisateur de données avec les capacités suivantes:

- 1) synchronisation des données de réseau avec les terminaux prenant en charge cette capacité;
- 2) synchronisation d'un terminal avec des données de réseau appropriées;
- 3) synchronisation des données de réseau entre terminaux.

Si un synchronisateur de données est pris en charge, les spécifications suivantes s'appliqueront:

- 1) le synchronisateur de données sera indépendant des protocoles de transport;
- 2) des données de réseau arbitraires seront prises en charge;
- 3) le mécanisme de synchronisation des données devra prendre en compte les limitations de ressource des terminaux.

6.22 Emulation et simulation de réseau RTPC/RNIS

L'évolution des réseaux vers des réseaux NGN dépend des choix des fournisseurs et de leurs besoins. Le mode d'évolution choisi par les fournisseurs de réseaux dépendra de leurs ressources réelles, de leurs plans d'activités et de leurs stratégies. Les opérateurs peuvent donc choisir des technologies et des calendriers différents.

Pendant la période de transition d'un réseau RTPC/RNIS vers un réseau NGN, le réseau NGN présentera les capacités suivantes:

- 1) capacités d'émulation de réseau RTPC/RNIS;
- 2) capacités de simulation de réseau RTPC/RNIS.

Les spécifications associées à ces capacités sont décrites ci-après.

6.22.1 Spécifications d'émulation de réseau RTPC/RNIS

6.22.1.1 Spécifications générales relatives à l'émulation de réseau RTPC/RNIS

Un réseau NGN devra fournir un service d'émulation RTPC/RNIS avec un niveau de service offrant des capacités égales ou supérieures à celles offertes par les réseaux à commutation de circuits.

6.22.1.2 Spécifications de terminal pour l'émulation de réseau RTPC/RNIS

Un réseau NGN prendra en charge les terminaux traditionnels (par exemple les téléphones RTPC classiques, les textophones, les télécopieurs et autres types de terminaux RTPC/RNIS existants) qui ne lui sont pas rattachés par une interface UNI NGN, mais par une interface UNI de type RTPC/RNIS.

NOTE – L'émulation de tous les services RTPC/RNIS peut ne pas être possible et la prise en charge des services peut être limitée à certains types de terminal (terminaux d'origine ou équipements d'utilisateur se comportant comme des terminaux d'origine).

6.22.1.3 Spécifications de service pour l'émulation de réseau RTPC/RNIS

Les spécifications de service pour l'émulation de réseau RTPC/RNIS sont les suivantes:

- 1) un réseau NGN prendra en charge la capacité des fournisseurs de services à émuler un ou plusieurs de leurs services RTPC/RNIS;
- 2) un réseau NGN prendra en charge les définitions de capacités héritées des spécifications de réseau RTPC/RNIS existantes.

NOTE – Un déploiement de réseau NGN spécifique n'a pas besoin de prendre en compte l'ensemble des capacités et interfaces présentes dans un réseau RTPC/RNIS.

6.22.2 Spécifications de simulation de réseau RTPC/RNIS

6.22.2.1 Spécifications générales pour la simulation de réseau RTPC/RNIS

Un réseau NGN prendra en charge les services de simulation de réseau RTPC/RNIS donnant à l'utilisateur un ressenti d'utilisation de type réseau RTPC/RNIS.

6.22.2.2 Spécifications de terminal pour la simulation de réseau RTPC/RNIS

Un réseau NGN prendra en charge les terminaux non traditionnels pour les services de simulation RTPC/RNIS. Il peut également prendre en charge des dispositifs d'adaptation pour permettre la connexion des terminaux traditionnels au réseau NGN (téléphones classiques, textophones et télécopieurs).

6.22.2.3 Spécifications de service pour la simulation de réseau RTPC/RNIS

Les spécifications de service pour la simulation de réseau RTPC/RNIS sont les suivantes:

- 1) un réseau NGN prendra des capacités de service de type RTPC/RNIS en utilisant le mécanisme de contrôle de session sur interfaces et infrastructure IP;
- 2) un réseau NGN devrait assurer à un fournisseur de services la capacité de simuler des services RTPC/RNIS;
- 3) un réseau NGN ne sera pas tenu de fournir des services identiques à ceux d'un réseau RTPC/RNIS.

NOTE – On suppose que les services de simulation de réseau RTPC/RNIS n'utilisent pas les modèles d'appel ou les protocoles de signalisation de réseau RTPC/RNIS.

6.23 Aspects touchant aux intérêts publics

Un réseau NGN fournira des capacités de prise en charge des services d'intérêt public requis conformément aux traités internationaux et aux réglementations ou aux lois d'administrations nationales ou régionales. Ces services d'intérêt public peuvent comprendre, entre autres, les services décrits dans les paragraphes ci-après.

6.23.1 Interception légale

- 1) Un fournisseur de transport NGN ou de services NGN respectera les spécifications d'interception légale. Un réseau NGN fournira donc des mécanismes rendant l'interception légale possible lorsqu'une telle possibilité est requise par les règlements ou la loi d'un pays dans leur zone d'application.
- 2) Les mécanismes d'interception légale doivent permettre à des organismes chargés de l'application des lois (LEA, *law enforcement agency*) d'accéder au contenu de communication et aux informations d'interception (IRI, *intercept related information*), conformément aux spécifications des administrations et des traités internationaux.

Les spécifications applicables dépendent de l'environnement réglementaire de chaque pays puisque la nature de l'interception légale est fonction des lois et usages nationaux/régionaux.

6.23.2 Identification de communications malveillantes

Un réseau NGN aura la capacité d'identifier la source d'une communication malveillante, par exemple en obtenant l'identificateur du terminal impliqué ou l'emplacement de l'émetteur de la communication.

6.23.3 Arrivée en masse de télécommunications non sollicitées

Un réseau NGN fournira des capacités empêchant l'arrivée en masse de télécommunications non sollicitées.

6.23.4 Télécommunications d'urgence

Les télécommunications d'urgence (en particulier la prise en charge de l'alerte rapide) peuvent se décliner comme suit:

- télécommunications d'un particulier à un organisme (appels à des fournisseurs de services d'urgence par exemple);

- télécommunications d'un organisme à un autre organisme (télécommunications pour les secours en cas de catastrophe (TDR, *telecommunications for disaster relief*) par exemple);
- télécommunications d'un organisme à un particulier (services de notification à une communauté par exemple).

NOTE – Les télécommunications de type TDR et ETS peuvent se faire non seulement d'organisme à organisme, mais également d'organisme à particulier.

[UIT-T Y.1271], [UIT-T E.106] et [UIT-T E.107] traitent respectivement des points suivants: "*Cadres généraux applicables aux spécifications et aux capacités de réseau pour la prise en charge des télécommunications d'urgence sur les réseaux à commutation de circuits et à commutation de paquets en cours d'évolution*", "*Plan international de priorité en période de crise destiné aux opérations de secours en cas de catastrophe*", "*Service de télécommunications d'urgence (ETS) et cadre d'interconnexion pour applications nationales du service ETS*".

Un réseau NGN mettra les capacités de réseau à la disposition des applications d'alerte rapide, par exemple pour fournir des informations d'emplacement géographique afin que les messages d'alerte ne soient envoyés qu'à ceux qui risqueraient d'être touchés par une catastrophe imminente.

Pour prendre en charge les télécommunications d'urgence et l'alerte rapide, un réseau NGN doit présenter une grande robustesse opérationnelle et une grande disponibilité.

Un réseau NGN doit:

- 1) comprendre des capacités de niveau de strate de service et strate de transport permettant la prise en charge des télécommunications d'urgence à l'aide de mécanismes de priorités/de préférences. La commande d'appel/de session des télécommunications d'urgence et le trafic de prise en charge des télécommunications d'urgence bénéficieront d'un traitement prioritaire dans les situations d'encombrement/de défaillance;
- 2) assurer au besoin l'interfonctionnement et le mappage des mécanismes de priorité entre les diverses composantes du réseau NGN (par exemple entre le réseau d'accès et le réseau central ou entre la strate de service et la strate de transport) et entre les réseaux NGN (par exemple entre deux réseaux centraux de fournisseurs de services) pour garantir des télécommunications prioritaires/préférentielles de bout en bout appropriées;
- 3) prendre en charge les services de télécommunications existants, notamment un service équivalant à l'ensemble des services de télécommunications d'urgence RTPC/RNIS existants, même lorsqu'une ou plusieurs des entités de communication sont rattachées à un réseau NGN et qu'une ou plusieurs autres entités sont rattachées à un réseau RTPC/RNIS;
- 4) permettre la prise en charge de nouveaux moyens de télécommunications d'urgence (messagerie instantanée par exemple) dans de futurs déploiements par des organismes (fournisseurs de services d'urgence par exemple);
- 5) assurer un interfonctionnement transparent des télécommunications d'urgence à travers tous les réseaux publics au sein d'un domaine (d'urgence) administratif;
- 6) assurer le routage des télécommunications d'urgence vers les organismes appropriées;
- 7) assurer le routage des télécommunications d'urgence d'un organisme à des particuliers;
- 8) assurer, lorsque cela est possible, la continuité des télécommunications d'urgence entre un organisme et un particulier jusqu'à ce que l'organisme mette fin à la session, même si le particulier a peut-être raccroché;
- 9) fournir à l'organisme des informations sur l'emplacement géographique et l'identificateur du particulier conformément aux prescriptions réglementaires nationales ou régionales. Lorsque la réglementation ou la loi l'exige, l'organisme peut acquérir de telles informations même si le particulier a demandé leur non-divulgateion;

- 10) fournir la capacité d'un accès authentifié ou non authentifié aux services de télécommunications d'urgence conformément aux prescriptions réglementaires nationales ou régionales. Par exemple, un réseau NGN fournira la capacité d'authentifier l'accès d'utilisateurs aux télécommunications ETS/TDR;
- 11) prendre en charge le fait que les télécommunications d'urgence n'ont pas à faire l'objet de certaines fonctions de gestion de réseau restrictives;
- 12) prendre en charge les télécommunications d'urgence à l'aide de plusieurs médias différents si cela est prescrit (par la réglementation ou la loi par exemple). L'utilisation de la vidéo, du texte et de la voix, l'association de ces médias ainsi que l'utilisation de différentes formes de messagerie sont essentielles pour les télécommunications avec les services d'urgence dans le cas de personnes handicapées;
- 13) fournir des capacités pour garantir que seuls les messages d'alerte rapide autorisés sont distribués;
- 14) fournir des capacités pour empêcher la diffusion de messages de type alerte rapide non ciblés et inutiles.

6.23.5 Présentation et confidentialité de l'identificateur d'utilisateur

- 1) un réseau NGN aura la capacité de présenter l'identificateur de l'appelant.
- 2) un réseau NGN aura la capacité de présenter l'identificateur de l'appelé.
- 3) un réseau NGN aura la capacité de supprimer la présentation de l'identificateur de l'appelant.
- 4) un réseau NGN aura la capacité de supprimer la présentation de l'identificateur de l'appelé.

NOTE – Les spécifications de prise en charge des télécommunications d'urgence peuvent prévaloir sur les spécifications de suppression.

6.23.6 Sélection de fournisseur de réseaux ou de service

Un réseau NGN prendra en charge la capacité à sélectionner un fournisseur, si cela est prescrit (par la réglementation ou la loi par exemple).

6.23.7 Utilisateurs handicapés

Les utilisateurs handicapés ont généralement besoin de disposer de moyens de commande et d'utilisation des terminaux et de services suivant différents voies et modes, convenant à diverses capacités et préférences. Ces spécifications sont prises en compte de manière optimale grâce à une conception adaptée des terminaux et des services.

- 1) Un réseau NGN fournira les moyens nécessaires à l'invocation de services de relais. Les services de relais opèrent une traduction entre divers modes de télécommunication intéressant les personnes handicapées (langage des signes, lecture labiale, texte, voix par exemple). L'invocation de relais de services peut être fondée sur les préférences d'utilisateur, la résolution d'adresse ou les commandes d'utilisateur.
- 2) Un réseau NGN aura la capacité de permettre l'invocation des services de relais par l'une des parties lors de télécommunications d'urgence.

NOTE 1 – Le paragraphe 6.23.4 traite d'autres besoins d'utilisateurs handicapés relatifs aux services de télécommunications d'urgence.

NOTE 2 – Voir également dans la bibliographie [b-UIT-T TP.TACL] et [b-UIT-T F.790].

6.23.8 Portabilité du numéro

La portabilité du numéro est une capacité de réseau RTPC/RNIS.

La capacité équivalente dans un réseau NGN est la portabilité de l'identificateur (§ 6.12.2). L'émulation de réseau RTPC/RNIS ne donne lieu à aucune nouvelle spécification de prise en

compte de la portabilité de numéro parce que les services émulsés héritent de caractéristiques associées au réseau RTPC/RNIS (voir le § 6.22.1.3).

6.23.9 Dégroupage de services

De nombreuses juridictions nationales imposent aux fournisseurs de services de "dégrouper" leurs offres pour permettre aux clients de faire un choix entre plusieurs fournisseurs pour divers services et pour permettre aux fournisseurs de proposer aux clients des offres de services concurrentielles.

Lorsque cela est prescrit (par la réglementation ou la loi par exemple), un réseau NGN prendra en charge les mécanismes de dégroupage de services.

6.24 Protection d'infrastructure critique

Les fournisseurs de services devraient avoir la capacité de protéger leurs infrastructures NGN contre des attaques malveillantes telles que le déni de service, l'écoute illicite, l'usurpation d'identité, l'altération de messages (modification, retard, suppression, insertion, répétition, reroutage, routage incorrect ou réordonnancement de messages), la répudiation ou la falsification. La protection peut englober la prévention, la détection, le rétablissement après attaques ainsi que des mesures empêchant les interruptions de service.

Les spécifications de sécurité sont indiquées au § 6.13.

6.25 Non-divulgation d'informations à travers des interfaces NNI

Lorsque cela est prescrit (par la réglementation, la loi ou les prescriptions nationales ou régionales par exemple), un réseau NGN aura les capacités permettant:

- aux fournisseurs de services d'empêcher la divulgation d'informations internes ou d'informations relatives aux utilisateurs de service à d'autres entités via des interfaces NNI;
- aux fournisseurs de réseau d'empêcher la divulgation d'informations internes sur les réseaux ou d'informations relatives aux utilisateurs du réseau via des interfaces NNI.

6.26 Echange interfournisseurs d'informations sur les utilisateurs

Lorsque cela est prescrit (par la réglementation ou la loi par exemple), un réseau NGN prendra en charge des mécanismes d'échange d'informations sur les utilisateurs entre des réseaux NGN à des fins d'interopérabilité de service.

Appendice I

Mappage entre des services et des activateurs de service

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

Le présent appendice donne un exemple de mappage entre des services sélectionnés et des activateurs de service sélectionnés (paragraphe 6.21). Ce mappage ne vise pas à l'exhaustivité et ne correspond pas à des spécifications de prise en charge.

Tableau I.1 – Exemple de mappage entre des services et des activateurs de service

Services\ Activateurs de service	Présence	Gestion de l'empla- cement	Gestion de groupes	Gestion des messages	Prise en charge de la multi- diffusion	Poussée	Gestion de session
Services vocaux conversationnels en temps réel							X
Texte en temps réel							X
Services de messagerie	X		X	X			X
Poussée pour parler sur réseau NGN	X		X				X
Services multimédias interactifs point à point			X				X
Services de communication interactifs exploités en commun		X	X				X
Services de fourniture de contenu		X				X	
Services de type poussée		X				X	
Services de radiodiffusion/de multidiffusion					X		
Services hébergés et de transit pour les entreprises			X				X
Services d'informations	X	X				X	

Tableau I.1 – Exemple de mappage entre des services et des activateurs de service

Services\ Activateurs de service	Présence	Gestion de l'emplacement	Gestion de groupes	Gestion des messages	Prise en charge de la multi- diffusion	Poussée	Gestion de session
Services de présence et de notification générale	X	X	X				
Services OSA 3GPP version 6 et 3GPP2 version A	X	X	X	X	X	X	X
Applications d'extraction de données	X					X	
Services VPN			X		X		

Bibliographie

Les documents indiqués ci-après contiennent des informations dont le lecteur de la présente Recommandation pourrait tirer parti. Ils donnent des informations complémentaires sur des questions traitées dans la présente Recommandation mais ne sont pas indispensables à la compréhension de cette dernière.

Recommandations UIT

- [b-UIT-R M.1645] Recommandation UIT-R M.1645 (2003), *Cadre et objectifs d'ensemble du développement futur des IMT-2000 et des systèmes postérieurs aux IMT-2000.*
- [b-UIT-T E.351] Recommandation UIT-T E.351 (2000), *Acheminement des connexions multimédias à travers des réseaux TDM, ATM ou IP.*
- [b-UIT-T F.703] Recommandation UIT-T F.703 (2000), *Services conversationnels multimédias.*
- [b-UIT-T F.724] Recommandation UIT-T F.724 (2005), *Description et spécifications des services visiophoniques sur réseaux IP.*
- [b-UIT-T F.733] Recommandation UIT-T F.733 (2005), *Description et spécifications des services de conférence multimédia dans les réseaux IP.*
- [b-UIT-T F.741] Recommandation UIT-T F.741 (2005), *Description et spécifications des services audiovisuels à la carte.*
- [b-UIT-T F.742] Recommandation UIT-T F.742 (2005), *Description et spécifications des services de télé-apprentissage.*
- [b-UIT-T F.790] Recommandation UIT-T F.790 (2007), *Lignes directives relatives à l'accessibilité des télécommunications pour les personnes âgées et les handicapés.*
- [b-UIT-T G.722.2] Recommandation UIT-T G.722.2 (2003), *Codage vocal à large bande à 16 kbit/s environ par codage adaptatif multidébit à large bande (AMR-WB).*
- [b-UIT-T G.729] Recommandation UIT-T G.729 (1996), *Codage de la parole à 8 kbit/s par prédiction linéaire avec excitation par séquences codées à structure algébrique conjuguée.*
- [b-UIT-T G.729A] Recommandation UIT-T G.729 Annexe A (1996), *Version simplifiée du codec vocal CS-ACELP à 8 kbit/s.*
- [b-UIT-T G.780] Recommandation UIT-T G.780/Y.1351 (2004), *Termes et définitions des réseaux à hiérarchie numérique synchrone (SDH).*
- [b-UIT-T G.799.1] Recommandation UIT-T G.799.1/Y.1451.1 (2004), *Spécifications des fonctionnalités et des interfaces des équipements de réseau de transport RTGC pour l'interconnexion des réseaux RTGC et IP.*
- [b-UIT-T G.805] Recommandation UIT-T G.805 (2000), *Architecture fonctionnelle générique des réseaux de transport.*
- [b-UIT-T G.809] Recommandation UIT-T G.809 (2003), *Architecture fonctionnelle des réseaux de couche sans connexion.*
- [b-UIT-T G.1000] Recommandation UIT-T G.1000 (2001), *Qualité de service des communications: cadre et définitions.*

- [b-UIT-T G.1010] Recommandation UIT-T G.1010 (2001), *Catégories de qualité de service multimédia pour l'utilisateur final.*
- [b-UIT-T H.263] Recommandation UIT-T H.263 (2005), *Codage vidéo pour communications à faible débit.*
- [b-UIT-T H.264] Recommandation UIT-T H.264 (2005), *Codage vidéo évolué pour les services audiovisuels génériques.*
- [b-UIT-T H.510] Recommandation UIT-T H.510 (2002), *Mobilité pour systèmes et services multimédias H.323.*
- [b-UIT-T H-suppl1] Supplément 1 aux Recommandations de la série H (1999), *Profil d'application – Utilisation des vidéocommunications à faible débit pour les conversations en temps réel par langage signé et lecture labiale.*
- [b-UIT-T I.230] Recommandation UIT-T I.230 (1988), *Définition des catégories de services supports.*
- [b-UIT-T I.250] Recommandation UIT-T I.250 (1988), *Définition des services supplémentaires.*
- [b-UIT-T M.3017] Recommandation UIT-T M.3017 (2003), *Cadre général de la gestion intégrée des réseaux hybrides circuits et paquets.*
- [b-UIT-T Q.833.1] Recommandation UIT-T Q.833.1 (2001), *Ligne d'abonné numérique asymétrique – Gestion des éléments de réseau: modèle CMIP.*
- [b-UIT-T Q.1200] Recommandation UIT-T Q.1200 (1997), *Organisation générale de la série de Recommandations relatives au réseau intelligent.*
- [b-UIT-T Q.1236] Recommandation UIT-T Q.1236 (1999), *Ensemble de capacités 3 du réseau intelligent – Spécifications et méthodologie du modèle d'information de gestion.*
- [b-UIT-T Q.1702] Recommandation UIT-T Q.1702 (2002), *Aspects réseau au-delà des systèmes IMT-2000 – Vision à long terme.*
- [b-UIT-T Q.1742.4] Recommandation UIT-T Q.1742.4 (2005), *Références IMT-2000 (approuvées au 30 juin 2004) au réseau central évolué ANSI-41 avec réseau d'accès cdma2000.*
- [b-UIT-T Q.1761] Recommandation UIT-T Q.1761 (2004), *Convergence des systèmes fixes et des systèmes IMT-2000 existants: principes et prescriptions.*
- [b-UIT-T T.140] Recommandation UIT-T T.140 (1998), *Protocole de conversation en mode texte pour application multimédia.*
- [b-UIT-T Y.1411] Recommandation UIT-T Y.1411 (2003), *Interfonctionnement des réseaux ATM et MPLS – Interfonctionnement dans le plan utilisateur en mode cellule.*
- [b-UIT-T Y.2111] Recommandation UIT-T Y.2111, *Fonctions de contrôle des ressources et d'admission dans les réseaux de prochaine génération.*
- [b-UIT-T Y-Sup.1] Supplément 1 aux Recommandations de la série Y.2000, *Domaine d'application des réseaux de prochaine génération de version 1.*

Lignes directrices de l'UIT-T

- [b-UIT-T TP.TACL] papier technique *Accessibility checklist for use in UIT-T standardization work* (2006) (disponible sur www.itu.int/ITUStudyGroups/com16/accessibility/docs/tacl.pdf)

Spécifications techniques de l'IETF

- [b-101.331] ETSI TS 101 331 V1.2.1 (2006-06), *Requirements of Law Enforcement Agencies*.
- [b-102.71] 3GPP TS 22.071 3rd Generation Partnership Project; Technical specification Group Services and System Aspects; *Location Services (LCS); Service description; Stage 1* (Release 1999).
- [b-121.905] ETSI TR 121 905 V7.3.0 (2007-03), *Vocabulary for 3GPP Specifications*.
- [b-122.057] ETSI TS 122 057 V6.0.0 (2005-01), *Mobile Execution Environment (MExE) service description; Stage 1*.
- [b-122.127] ETSI TS 122 127 V7.1.0 (2006-03), *Service requirement for the Open Services Access (OSA); Stage 1*.
- [b-122.140] ETSI TS 122 140 V6.7.0 (2005-03), *Multimedia Messaging Service (MMS); Stage 1*.
- [b-122.146] ETSI TS 122 146 V7.2.0 (2006-09), *Multimedia Broadcast/Multicast Service (MBMS); Stage 1*.
- [b-122.174] ETSI TS 122 174 V6.2.0 (2005-01), *Push service; Stage 1*.
- [b-122.240] ETSI TS 122 240 V6.5.0 (2005-01), *Service requirements for 3GPP Generic User Profile (GUP); Stage 1*.
- [b-122.250] ETSI TS 122 250 V6.0.0 (2005-01), *IP Multimedia Subsystem (IMS) Group Management; Stage 1*.
- [b-122.708] ETSI TS 122 078 V7.6.0 (2005-12), *Customized Applications for Mobile network Enhanced Logic (CAMEL); Service description*.
- [b-123.141] ETSI TS 123 141 V7.2.0 (2006-09), *Presence service; Architecture and functional description; Stage 2*.
- [b-123.228] ETSI TS 123 228 V7.7.0 (2007-03), *IP Multimedia Subsystem (IMS); Stage 2*.
- [b-126.235] ETSI TS 126 235 V6.4.0 (2005-03), *Packet switched conversational multimedia applications; Default codecs*.
- [b-133.106] ETSI TS 133 106 V7.0.1 (2006-01), *Lawful interception requirements*.
- [b-142.033] ETSI TS 142 033 V7.0.0 (2007-06), *Lawful interception – Stage 1*.
- [b-181.005] ETSI TS 181 005 V1.1.1 (2006-03), *Services and Capabilities Requirements*.

Normes de l'Institut national américain de normalisation (ANSI)

- [b-JSTD025] ANSI J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance (CALEA)*.
- [b-T1.678] ANSI ATIS 1000678-2006, *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks*.
- [b-T1.724] ANSI T1.724-2004, *UMTS Handover Interface for Lawful Interception, March, 2004*.
- [b-TIA-1066] TIA-1066 (2006), *Lawfully Authorized Surveillance (LAES) for cdma2000 Voice Over IP (VoIP)*.

- [b-TIA-1072] TIA-1072 (2006), *LAES for cdma2000 push-to-talk over cellular*.
- [b-TIA-1016-A] *Source-Controlled Variable-Rate Multimode Wideband Speech Codec (VMR-WB), Service Options 62 and 63 for Spread Spectrum Systems (TIA-1016-A-2006)*.
- [b-TIA-127-A] *Enhanced Variable Rate Codec Speech Service Option 3 for Wideband Spread Spectrum Digital Systems (ANSI/TIA-127-A-2004)*.

Spécifications de l'IETF

- [b-RFC 2486] IETF RFC 2486 (1999), *The Network Access Identifier*.
- [b-RFC 4594] IETF RFC 4594 (2006), *Configuration guidelines for DiffServ Service Classes*.

Spécifications de l'Open Mobile Alliance

- [b-OMA-DS] OMA Data Synchronization V1.2 – **Status:** Approved Enabler – **Release Date:** 2006-07-10.
- [b-OMA-DM] OMA Device Management V1.2 – **Status:** Approved Enabler – **Release Date:** 2007-02-09.
- [b-OMA-OSE] OMA Service Environment V1.0 – **Status:** Candidate Release – **Release Date:** 2007-03-13.
- [b-OMA-PoC] OMA Push to talk over Cellular V1.0.1 – **Status:** Approved Enabler – **Release Date:** 2006-11-28.
- [b-OMA-PS] OMA Presence Simple V1.0.1 – **Status:** Approved Enabler – **Release Date:** 2006-11-28.
- [b-OMA-WS] OMA Web Services V1.1 – **Status:** Approved Enabler – **Release Date:** 2006-03-28.
- [b-OMA-XML] OMA XML Document Management V1.0.1 – **Status:** Approved Enabler – **Release Date:** 2006-11-28.
- [b-OMA-LS] OMA Mobile Location Service V1.1 – **Status:** Candidate Enabler – **Release Date:** 2006-10-20.
- [b-OMA-XDM] OMA XML Document Management V1.0.1 – **Status:** Approved Enabler – **Release Date:** 2006-11-28.
- [b-OMA-Push] OMA Push V2.1 – **Status:** Candidate Enabler – **Release Date:** 2005-11-22.

Accès ouvert aux services (OSA)

- [b-OSA-Parlay-X] *Open Service Access (OSA), Parlay X Web Services, Parts 1-14, ETSI ES 202 391-[1-14] V1.1.1 (2006-12)*.
- [b-OSA-Parlay-4] *Open Service Access (OSA), Application Programming Interface (API), Parts 1-14, ETSI ES 202 915-[1-14] V1.3.1 (2006-12)*.
- [b-OSA-Parlay-5] *Open Service Access (OSA), Application Programming Interface (API), Parts 1-15, ETSI ES 203 915-[1-15] V1.1.1 (2007-01)*.

Services de réseau intelligent

- [b-TIA-771] TIA/EIA/IS 771-1 (1999), *Wireless Intelligent Network – Addendum 1 (2001)*.
- [b-TIA-873] TIA/EIA 873.002 (2003), *All IP Core Network Multimedia Domain – IP Multimedia Subsystem – Stage-2*.

Spécifications UDDI

[b-UDDI] UDDI Specification Technical committee, *UDDI Specification*,
Version 3.0.2

Spécifications SOA

[b-OASIS-SOA] *OASIS, Reference Model for Service Oriented Architecture 1.0*, Committee
Specification 1. 2 August 2006.

SÉRIES DES RECOMMANDATIONS UIT-T

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