Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2201

(09/2009)

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 et capacités des réseaux de prochaine génération de l'UIT-T

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
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
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
Réseaux futurs	Y.2600–Y.2699
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999

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

Recommandation UIT-T Y.2201

Spécifications et capacités des réseaux de prochaine génération de l'UIT-T

Résumé

La Recommandation UIT-T Y.2201 contient les spécifications de haut niveau relatives aux services et aux capacités d'un réseau de prochaine génération (NGN, next generation network).

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T Y.2201	2007-04-27	13
2.0	ITU-T Y.2201	2009-09-12	13

Mots clés

Activateur de service, administration et maintenance (OAM), adressage, authentification, autorisation, capacités, comptabilité, confidentialité, environnement de service ouvert, exploitation, gestion, gestion des identités, identification, interfonctionnement, interopérabilité, mobilité, multidiffusion, nommage, numérotage, perception du contexte, politique, prise en charge du protocole Internet-version 6 (IPv6), profil, qualité de service, réseau d'entreprise, réseau NGN, sécurité, spécifications relatives aux capacités, taxation, télévision utilisant le protocole Internet (TVIP).

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/.

TABLE DES MATIÈRES

Recommandation UIT-T Y.2201

Spécifications et capacités des réseaux de prochaine génération de l'UIT-T

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 (NGN, *next generation network*).

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 2 [b-UIT-T Y-Sup.7].

Ces spécifications sont essentiellement données dans 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 donner des spécifications plus détaillées.

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) arbitraire de services pris en charge par les réseaux NGN et de capacités spécifiées dans la présente Recommandation.

NOTE 1 – Le texte repris de [UIT-T Y.2201] est indiqué en caractères bleus. L'Appendice I recense les principales différences en termes de spécifications de haut niveau et de capacités entre la présente Recommandation et [UIT-T Y.2201].

NOTE 2 – Il est aussi nécessaire d'examiner comment un réseau NGN pourrait contribuer à l'économie d'énergie. Des études portant sur cette question sont en cours au sein de la Commission d'études 5 de l'UIT-T. Elles sont fondées sur les conclusions du Groupe spécialisé de l'UIT-T sur les TIC et les changements climatiques. Les spécifications concernant les aspects d'économie d'énergie doivent faire l'objet d'un complément d'étude dans la présente Recommandation. S'agissant des conclusions du Groupe spécialisé de l'UIT-T sur les TIC et les changements climatiques, veuillez vous reporter au document [b-ITU-T Climate].

2 Références

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 (2008), *Plan d'identification international pour les réseaux publics et les abonnements.*

[UIT-T G.711] Recommandation UIT-T G.711 (1988), *Modulation par impulsions et codage (MIC) des fréquences vocales.*

[UIT-T G.722] Recommandation UIT-T G.722 (1988), *Codage audiofréquence à 7 kHz à un débit inférieur ou égal à 64 kbit/s.*

[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).*

[UIT-T G.729] Recommandation UIT-T G.729 (2007), *Codage de la parole à 8 kbit/s par prédiction linéaire avec excitation par séquences codées à structure algébrique conjuguée.*

[UIT-T G.729.1] Recommandation UIT-T G.729.1 (2006), *Codeur intégré à débit variable basé sur le vocodeur G.729: Codeur à flux binaire modulable à large bande à 8-32 kbit/s interopérable avec le codeur G.729.*

[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 H.263] Recommandation UIT-T H.263 (2005), *Codage vidéo pour communications à faible débit.*

[UIT-T H.264] Recommandation UIT-T H.264 (2005), *Codage vidéo évolué pour les services audiovisuels génériques.*

[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 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), *Spécifications relatives à la fonctionnalité d'exploitation et de maintenance pour les réseaux MPLS.*

[UIT-T Y.1730] Recommandation UIT-T Y.1730 (2004), *Spécifications relatives aux fonctions d'exploitation, d'administration et de maintenance dans les réseaux à base Ethernet et les services Ethernet.*

[UIT-T Y.1901] Recommandation UIT-T Y.1901 (2009), *Exigences pour la prise en charge des services de TVIP.*

[UIT-T Y.2001] Recommandation UIT-T Y.2001 (2004), *Aperçu général des réseaux de prochaine génération.*

[UIT-T Y.2012] Recommandation UIT-T Y.2012 (2006), *Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1.*

[UIT-T Y.2051] Recommandation UIT-T Y.2051 (2008), *Présentation générale des réseaux de prochaine génération utilisant le protocole IPv6.*

[UIT-T Y.2091] Recommandation UIT-T Y.2091 (2008), *Termes et définitions pour les réseaux de prochaine génération.*

[UIT-T Y.2111] Recommandation UIT-T Y.2111 (2008), *Fonctions de commande de ressource et d'admission dans les réseaux de prochaine génération.*

[UIT-T Y.2201] Recommandation UIT-T Y.2201 (2007), *Spécifications des réseaux de prochaine génération de version 1.*

[UIT-T Y.2212] Recommandation UIT-T Y.2212 (2008), *Spécifications des services de gestion de la fourniture.*

[UIT-T Y.2213] Recommandation UIT-T Y.2213 (2008), *Exigences et capacités liées aux services NGN concernant les aspects réseau des applications et services utilisant une identification par étiquette.*

[UIT-T Y.2215] Recommandation UIT-T Y.2215 (2009), *Spécifications et cadre pour la prise en charge de services VPN dans les réseaux NGN, y compris l'environnement mobile.*

[UIT-T Y.2233] Recommandation UIT-T Y.2233 (2008), *Spécifications et cadre général d'offre des capacités de comptabilité et de taxation dans les NGN.*

[UIT-T Y.2234] Recommandation UIT-T Y.2234 (2008), *Capacités d'environnement de service ouvert pour les applications NGN.*

[UIT-T Y.2236] Recommandation UIT-T Y.2236 (2009), *Cadre destiné à la prise en charge par les réseaux de prochaine génération des services en mode multidiffusion.*

[UIT-T Y.2701] Recommandation UIT-T Y.2701 (2007), *Prescriptions de sécurité des réseaux de prochaine génération de version 1.*

[UIT-T Y.2720] Recommandation UIT-T Y.2720 (2009), *Cadre de gestion d'identité des réseaux NGN.*

[UIT-T Z.100] Recommandation UIT-T Z.100 (2007), *SDL: langage de description et de spécification.*

[ETSI TS 126.071] ETSI TS 126.071 V6.0.0 (2004-12), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); AMR speech Codec; General description (3 GPP TS 26.071 version 6.0.0 Release 6).*

[TIA-127-C] TIA Standard-127-C (2007), *Enhanced Variable Rate Codec, Speech Service Options 3, 68, and 70 for Wideband Spread Spectrum Digital Systems.*

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).

NOTE – L'équipement du réseau privé appartient à une entreprise ou est exploité pour son compte, et est interconnecté de manière à assurer la fourniture de services de télécommunication à un groupe donné d'utilisateurs appartenant à cette entreprise.

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]: utilisateur effectif d'un produit ou d'un service proposé par l'entreprise. Il est "consommateur" du produit ou du service. Voir également la définition d'abonné.

3.1.9 entité [UIT-T Y.2720]: tout type d'élément qui a une existence séparée et distincte et peut être identifié de manière unique. Dans le contexte de la gestion des identités (IdM, *identity management*), il peut s'agir d'abonnés, d'utilisateurs, d'éléments de réseaux, de réseaux, d'applications logicielles, de services et de systèmes. Une entité peut avoir plusieurs identificateurs.

3.1.10 fédération [UIT-T Y.2720]: création d'une relation entre deux entités ou plus ou une association composée d'un nombre quelconque de fournisseurs de services et de fournisseurs d'identités.

3.1.11 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.

3.1.12 réseau de rattachement [UIT-T Q.1706]: réseau auquel est normalement rattaché un utilisateur de mobile, ou fournisseur de réseau auquel est associé l'utilisateur de mobile, et où sont gérées les informations de l'abonnement de l'utilisateur.

3.1.13 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).

3.1.14 identité [UIT-T Y.2720]: information sur une entité qui suffit à l'identifier dans un contexte donné.

3.1.15 gestion d'identité [UIT-T Y.2720]: ensemble de fonctions et de fonctionnalités (par exemple, l'administration, la gestion et la tenue à jour, la découverte, l'échange de communication, la corrélation et les liens, l'application des politiques, l'authentification et les assertions) utilisées pour:

– garantir les informations d'identité (par exemple, les identificateurs, les justificatifs d'identité, les attributs);
– garantir l'identité d'une entité (par exemple les utilisateurs/abonnés, les groupes, les dispositifs d'utilisateur, les organismes, les fournisseurs de réseaux et de services, les éléments et objets de réseaux et les objets virtuels); et
– permettre des applications commerciales et liées à la sécurité.

3.1.16 fournisseur d'identités [UIT-T Y.2720]: entité qui crée, maintient et gère des informations d'identité sécurisées pour d'autres entités (par exemple utilisateurs/abonnés, organismes et systèmes) et propose des services fondés sur l'identité basés sur une relation de confiance, commerciale ou d'autres natures.

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

3.1.18 réseaux de prochaine génération utilisant le protocole IPv6 [UIT-T Y.2051]: réseaux NGN qui prennent en charge l'adressage, les protocoles de routage et les services associés au protocole IPv6. Un réseau NGN utilisant le protocole IPv6 doit reconnaître et traiter les en-têtes et les options IPv6, en employant diverses technologies de transport sous-jacentes dans la strate de transport.

3.1.19 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 domiciliaire 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".

3.1.20 gestion de la mobilité [UIT-T Q.1706]: ensemble des fonctions utilisées pour assurer la mobilité. Ces fonctions comprennent l'authentification, l'autorisation, la mise à jour de la localisation, la pagination, le téléchargement des informations d'utilisateur, etc.

3.1.21 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.

3.1.22 information personnellement identifiable [UIT-T Y.2720]: information relative à une personne vivante, qui permet son identification (y compris une information qui, combinée à d'autres informations, permet d'identifier une personne même si seule, elle ne permet pas d'identifier la personne avec certitude).

3.1.23 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 de la capacité du réseau à assurer les services définis dans le profil de service de l'utilisateur.

3.1.24 présence [UIT-T Y.2720]: ensemble d'attributs qui caractérise une entité en relation avec le statut actuel.

3.1.25 réseau public [b-UIT-T I.570]: réseau qui assure la fourniture de services au grand public.

NOTE – Cette définition n'incorpore pas les aspects juridiques ou réglementaires et ne concerne en rien la propriété.

3.1.26 itinérance [UIT-T Q.1706]: Il s'agit de la capacité des utilisateurs d'accéder à des services, suivant leur profil, tout en se déplaçant à l'extérieur du réseau de rattachement auquel ils sont abonnés, c'est-à-dire en utilisant un point d'accès d'un réseau visité. Pour ce faire, il faut que les utilisateurs puissent avoir accès au réseau visité, qu'il existe une interface entre ce dernier et le réseau de rattachement ainsi qu'un accord d'itinérance entre les deux opérateurs de réseaux.

3.1.27 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.

3.1.28 service (Supplément 1 aux Recommandations UIT-T de la série Z.): ensemble de fonctions et de ressources offertes à un utilisateur par un fournisseur de services.

3.1.29 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.

3.1.30 abonné [UIT-T M.3050.1]: l'abonné conclut des contrats pour obtenir des services et paie ces services.

3.1.31 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.

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

3.1.33 réseau visité [UIT-T Q.1706]: réseau situé à l'extérieur d'un réseau de rattachement fournissant un service à un utilisateur mobile; le sens de cette expression vaut d'un point de vue plus commercial que géographique.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 communication entrante: communication émanant d'un utilisateur de réseau public à destination d'un utilisateur de réseau d'entreprise.

3.2.2 communication sortante: communication émanant d'un utilisateur de réseau d'entreprise à destination d'un utilisateur de réseau public.

3.2.3 jonction d'entreprise: connexion d'un réseau d'entreprise de prochaine génération (NGCN, *next generation corporate network*) à un réseau de prochaine génération (NGN, *next generation network*).

3.2.4 application de jonction d'entreprise: application NGN qui offre des capacités de communication de transit entre réseaux d'entreprise de prochaine génération (NGCN) ou des capacités de communication entrante, de réseaux NGN vers les réseaux NGCN, et/ou des capacités de communication sortante, des réseaux NGCN vers les réseaux NGN.

NOTE – S'agissant des réseaux NGCN, une application de jonction d'entreprise peut aussi leur fournir des services supplémentaires, venant s'ajouter aux capacités de base que sont les capacités de communication entrante, de communication sortante ou de communication de transit.

3.2.5 perception du contexte: capacité permettant, lors d'une télécommunication ou d'une procédure, de définir une action suivante ou d'influer sur elle, en renvoyant au statut des entités pertinentes qui forment un environnement cohérent en tant que contexte.

3.2.6 identificateur d'utilisateur de réseau d'entreprise: élément permettant d'identifier un utilisateur de réseau d'entreprise, lors de communications entrant dans un réseau NGN, en sortant ou transitant par lui, et indiquant soit un utilisateur de réseau d'entreprise d'origine soit une identité de cible susceptible d'être acheminée à l'échelle mondiale.

3.2.7 communication d'entreprise: toute communication qui:

1) émane d'un réseau d'entreprise de prochaine génération (NGCN); ou
2) aboutit dans un réseau NGCN; ou
3) émane d'un réseau NGN pour le compte d'une entreprise; ou
4) aboutit dans un réseau NGN pour le compte d'une entreprise;

et est soumise à des accords spéciaux entre l'opérateur de réseau NGN et l'entreprise.

3.2.8 capacités de communication d'entreprise: toute capacité hébergée dans un réseau d'entreprise de prochaine génération (NGCN) ou dans un réseau NGN, qui permet et/ou enrichit une communication d'entreprise.

NOTE – L'application de jonction d'entreprise, les services hébergés destinés aux entreprises et les lignes louées virtuelles sont des exemples de capacités de communication d'entreprise hébergées dans un réseau NGN.

3.2.9 services d'entreprise hébergés (HES, *hosted enterprise services*): application NGN permettant aux réseaux NGN d'héberger toutes les capacités de communication d'entreprise entrantes et/ou sortantes destinées aux utilisateurs d'entreprise qui sont directement reliés à un réseau NGN et ont contracté un abonnement à cette application dans le réseau NGN.

NOTE – Cette solution est couramment désignée sous le nom de solution IP-Centrex.

3.2.10 réseau d'entreprise de prochaine génération (NGCN, *next generation corporate network*): réseau d'entreprise autonome, conçu pour tirer profit des solutions de communication IP émergentes et pouvant avoir ses propres applications et fourniture de services.

NOTE – Aux fins de la présente Recommandation, il incombe au réseau d'entreprise de fournir une interface IP à un réseau NGN.

3.2.11 site NGCN: partie distincte d'un réseau d'entreprise de prochaine génération (NGCN).

NOTE – Un site NGCN peut correspondre à une partie d'un réseau NGCN, liée à un emplacement géographique particulier. Lorsqu'un site NGCN dessert plusieurs emplacements géographiques, tous les emplacements desservis par lui auront accès à un réseau NGN donné, en vertu de l'accord concernant la connectivité du site NGCN avec ce réseau NGN. La communication entre différents sites NGCN appartenant au même réseau NGCN peut, mais non nécessairement, passer à travers leur(s) réseau(x) NGN respectif(s). De telles communications peuvent par exemple être acheminées par le(s) réseau(x) NGN uniquement au cours de période de trafic dense ou de panne d'équipement dans le réseau NGCN. Un site NGCN peut avoir

accès à son réseau NGN soit directement, soit via un autre réseau NGN qui offre une capacité de transit. Un réseau NGCN peut avoir des sites NGCN dans différents pays.

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

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

3.2.14 trafic de réseau privé: trafic envoyé ou reçu d'un réseau NGN pour traitement conformément à un ensemble convenu de règles propres à une entreprise ou à un groupe d'entreprises étroitement liées.

3.2.15 trafic de réseau public: trafic envoyé ou reçu d'un réseau NGN pour traitement conformément aux règles normales pour les réseaux NGN.

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

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

3.2.18 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.

3.2.19 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.)).

3.2.20 identité d'utilisateur: type de mot de passe, d'image ou de pseudonyme associé à un utilisateur, attribué et échangé entre opérateurs et 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:

AMR multidébit adaptatif (*adaptive multi-rate*)

ANI interface de réseau d'application (*application network interface*)

API interface de programmation d'application (*application programming interface*)

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

B2B inter-entreprise (*business-to-business*)

CC contenu de communication (*content of communication*)

CD disque compact (*compact disk*)

cPVR enregistreur vidéo personnel client (*client personal video recorder*)

DECT NG nouvelle génération de communications numériques sans fil améliorées (*digital enhanced cordless telecommunications new generation*)

DNS système de noms de domaine (*domain name system*)

DTMF multifréquence à deux tonalités (*dual tone multi-frequency*)

EAN notification d'alerte et d'urgence (*emergency alert notification*)

ENUM mappage des numéros téléphoniques (*telephone number mapping*)

ETS service de télécommunication d'urgence (*emergency telecommunications service*)

EVRC codec à débit variable amélioré (*enhanced variable rate codec*)

HES service d'entreprise hébergé (*hosted enterprise services*)

HTML langage de balisage hypertexte (*hyper text markup language*)

IdM gestion des identités (*identity management*)

IEPS plan international de priorité en période de crise (*international emergency preference scheme*)

IM messagerie instantanée (*instant messaging*)

IMS sous-système multimédia utilisant le protocole Internet (*Internet Protocol multimedia subsystem*)

IN réseau intelligent (*intelligent network*)

IP protocole Internet (*Internet protocol*)

IPv4 protocole Internet-version 4 (*Internet protocol version 4*)

IPv6 protocole Internet-version 6 (*Internet protocol version 6*)

IRI informations liées à l'interception (*intercept related information*)

LDAP protocole rapide d'accès à l'annuaire (*lightweight directory access protocol*)

LEA organisme d'application des lois (*law enforcement agencies*)

MMS service de messagerie multimédia (*multimedia messaging service*)

MPLS commutation multiprotocole par étiquette (*multi-protocol label switching*)

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

NAPT traduction d'adresse de réseau et de port (*network address and port translation*)

NAT traduction d'adresse de réseau (*network address translation*)

NB bande étroite (*narrow band*)

NGCN réseau d'entreprise de prochaine génération (*next generation corporate network*)

NGN réseau de prochaine génération (*next generation network*)

NNA numérotage, nommage et adressage (*numbering, naming and addressing*)

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

nPVR enregistreur vidéo personnel réseau (*network personal video recorder*)

OAM exploitation, administration et maintenance (*operations, administration and maintenance*)

OIP présentation de l'identité d'origine (*originating identity presentation*)

OMA Open Mobile Alliance

OS système d'exploitation (*operating system*)

OSA accès ouvert aux services (*open service access*)

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

PBX autocommutateur privé (*private branch eXchange*)

PC ordinateur personnel (*personal computer*)

PDA assistant numérique personnel (*personal digital assistant*)

PII	informations personnellement identifiables (*personally identifiable information*)
PNP	plan de numérotage privé (*private numbering plan*)
POTS	service téléphonique ordinaire (*plain old telephone service*)
PSAP	point de réponse de sécurité publique (*public safety answering point*)
QoE	qualité d'expérience (*quality of experience*)
QoS	qualité de service
QoSM	mesure de la qualité de service (*quality of service measurement*)
RACF	fonctions de commande de ressource et d'admission (*resource and admission control functions*)
RNIS	réseau numérique à intégration de services
RTPC	réseau téléphonique public commuté
SIP	protocole d'ouverture de session (*session initiation protocol*)
SLA	accord de niveau de service (*service level agreement*)
SMS	service de messages courts (*short message service*)
SR	résilience de service (*service resiliency*)
TDR	télécommunications pour les secours en cas de catastrophe (*telecommunications for disaster relief*)
TE	équipement terminal (*terminal equipment*)
TIP	présentation de l'identité de terminaison (*termination identity presentation*)
TVIP	télévision utilisant le protocole Internet
UC	communication non sollicitée (*unsolicited communication*)
UDDI	découverte, description et intégration universelles (*universal discovery, description and integration*)
UMTS	système universel de télécommunications mobiles (*universal mobile telecommunications system*)
UNI	interface utilisateur réseau (*user-to-network interface*)
URI	identificateur uniforme de ressources (*uniform resource identifier*)
USN	réseau de capteurs ubiquitaires (*ubiquitous sensor network*)
VoD	vidéo à la demande (*video on demand*)
VoIP	protocole de transmission de la voix par Internet (*voice over Internet protocol*)
VPN	réseau privé virtuel (*virtual private network*)
WB	large bande (*wide-band*)
Wi-Fi	fidélité sans fil (*wireless fidelity*)
xDSL	divers types de ligne d'abonné numérique (*various types of digital subscriber lines*)

5 Conventions

Dans la présente Recommandation:

Les mots clés "doit" et "doivent" indiquent une spécification qui doit être strictement appliquée et dont il est interdit de s'écarter si la conformité avec la présente Recommandation est revendiquée.

Les mots clés "est interdit" et "sont interdit(e)s" indiquent une spécification qui doit être strictement appliquée et dont il est interdit de s'écarter si la conformité avec la présente Recommandation est revendiquée.

Les mots clés "est recommandé" et "sont recommandé(e)s" indiquent une spécification qui est recommandée mais qui n'est pas absolument requise. Cette spécification ne doit donc pas être invoquée pour revendiquer la conformité.

Les mots clés "n'est pas recommandé" et "ne sont pas recommandé(e)s" indiquent une spécification qui n'est pas recommandée mais qui n'est pas nommément interdite. La conformité avec cette spécification peut toujours être revendiquée même lorsque la spécification est invoquée.

Les mots clés "peut éventuellement" et "peuvent éventuellement" indiquent une spécification en option qui est admissible, sans impliquer une quelconque recommandation. Ces mots n'impliquent pas que la mise en œuvre du vendeur doit incorporer l'option et que la caractéristique peut éventuellement être activée par l'opérateur du réseau/le fournisseur de service. Ils signifient plutôt que le vendeur peut éventuellement incorporer la caractéristique et que la conformité avec cette spécification peut toujours être revendiquée.

Aux fins de la présente Recommandation, les mots "réseau d'entreprise" et "réseau de société" sont interchangeables.

6 Transport

6.1 Connectivité de transport

La strate de transport d'un réseau NGN [UIT-T Y.2012] doit utiliser 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 (xDLS, 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 doit prendre en charge les modes de communication suivants:

– point à point;
– point à multipoint;
– multipoint à multipoint;
– multipoint à point.

6.3 Composants du réseau de transport

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

1) Un réseau NGN doit prendre en charge les diverses technologies des fonctions de transport vers un réseau d'accès et un réseau central.

2) Toutes les fonctions de transport d'accès de réseau NGN doivent pouvoir assurer une connectivité IP entre les fonctions d'utilisateur final et les fonctions de transport vers un réseau central.

3) Un réseau NGN doit ne pas exclure la prise en charge d'aucun réseau d'utilisateur présentant un certain niveau de complexité de configuration.

6.4 Rattachement au réseau

Les spécifications suivantes concernant le rattachement au réseau s'appliquent:

1) Un réseau NGN doit prendre 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).

2) Le profil d'utilisateur doit garder les données d'authentification d'accès de l'utilisateur et les informations relatives à la configuration requise d'accès au réseau.

3) Un réseau NGN doit prendre 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 doit attribuer les ressources conformément aux services à fournir.

4) Lorsque plusieurs réseaux d'accès sont reliés à un seul réseau central NGN, un réseau d'accès doit pouvoir authentifier/autoriser l'accès d'un utilisateur en itinérance à ce réseau à partir d'un autre réseau d'accès.

5) Pour garantir la disponibilité des services d'itinérance, les procédures de rattachement du réseau d'accès NGN doivent prendre 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-IETF RFC 2486]).

6.5 Prise en charge du protocole IPv6

Le protocole IPv6 permet de prendre en charge non seulement les extensions de l'espace d'adresse IP mais aussi diverses caractéristiques évoluées qui influent sur les fonctions NGN et les entités fonctionnelles pertinentes. Cela veut dire que le protocole IPv6 est aussi plus souple, s'agissant de l'introduction de nouvelles applications ou de nouveaux services en employant la combinaison des en-têtes d'extension et des options.

Aussi, le présent paragraphe recense-t-il les spécifications générales d'un réseau NGN utilisant le protocole IPv6, sur lesquelles les caractéristiques IPv6 influent. Il est admis qu'un réseau NGN utilisant le protocole IPv6 doit satisfaire aux spécifications suivantes:

– un réseau NGN utilisant le protocole IPv6 doit prendre en charge les en-têtes d'extension et les options IPv6;

– un réseau NGN utilisant le protocole IPv6 doit accueillir les systèmes d'adressage IPv6.

6.5.1 Rattachement multiple d'un réseau NGN utilisant le protocole IPv6

– Un réseau NGN utilisant le protocole IPv6 doit prendre en charge les capacités d'accès multiple pour un utilisateur, y compris les capacités d'accès aux réseaux d'accès employant des technologies différentes (par exemple, réseau mobile, Wi-Fi).

– Un terminal d'utilisateur doit avoir de multiples connexions avec de multiples interfaces de réseau et/ou avec de multiples adresses IPv6.

– Il est recommandé qu'un terminal d'utilisateur employant le rattachement multiple avec le protocole IPv6 acquière (ou récupère) dynamiquement des adresses IPv6 supplémentaires.

– Il est recommandé qu'un terminal d'utilisateur employant le rattachement multiple avec le protocole IPv6 acquière (ou récupère) dynamiquement une ou des interfaces de réseau supplémentaires.

– Un réseau NGN utilisant le protocole IPv6 doit acquérir (ou récupérer) dynamiquement des préfixes IPv6 supplémentaires.

6.5.2 Signalisation dans un réseau NGN utilisant le protocole IPv6

1) Un réseau NGN utilisant le protocole IPv6 doit prendre en charge l'interfonctionnement en matière de signalisation avec d'autres réseaux (par exemple, les réseaux NGN utilisant le protocole IPv4).

2) Un réseau NGN utilisant le protocole IPv6 doit prendre en charge les modifications requises pour une minimalisation de la signalisation dans les protocoles de signalisation employés dans les réseaux NGN utilisant le protocole IPv4.

6.5.3 Passage au protocole IPv6 dans un réseau NGN

Un réseau NGN doit prendre en charge la fonction de passage au protocole IPv6, s'agissant des fonctions de transport vers les réseaux d'accès et les réseaux centraux.

6.6 Prise en charge de la multidiffusion

Ces capacités permettent aux applications de fournir des contenus à plusieurs utilisateurs en même temps.

Non seulement les capacités de monodiffusion mais aussi les capacités de multidiffusion doivent être prises en charge pour que l'utilisation des ressources de réseau et la fourniture de données modulables soient efficaces.

Les spécifications suivantes s'appliquent à un réseau NGN:

1) Il doit offrir des capacités de multidiffusion dans un seul domaine NGN.

2) Il est recommandé qu'il offre des capacités de multidiffusion dans plusieurs domaines NGN.

3) Un réseau NGN doit offrir des capacités de fourniture de données en mode multidiffusion.

4) Un réseau NGN doit offrir des capacités de commande de service en mode multidiffusion.

5) Un réseau NGN doit prendre en charge les capacités de gestion de groupes en mode multidiffusion.

6) Un réseau NGN doit prendre en charge les mécanismes de sécurité pour la multidiffusion.

7) Un réseau NGN doit prendre en charge le nomadisme pour les communications en mode multidiffusion.

8) Il est recommandé qu'un réseau NGN prenne en charge les capacités prédéfinies de qualité de service, applicables à l'ensemble d'un groupe en mode multidiffusion.

9) Il est recommandé qu'un réseau NGN prenne en charge une mobilité sans heurts pour les communications en mode multidiffusion.

10) Un réseau NGN peut éventuellement assurer la fiabilité des capacités de multidiffusion.

NOTE – Pour plus de détails, voir [UIT-T Y.2236].

7 Prise en charge des services et des applications

7.1 Environnement de service ouvert

7.1.1 Spécifications générales pour un 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 actuels 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, il est recommandé que la réutilisabilité et la portabilité des logiciels ainsi que l'utilisation de logiciels commerciaux soient prises en charge pour assurer un développement au meilleur rapport.

Ci-après sont indiqués 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 doit fonctionner 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 doivent être 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 doit être 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 doivent accéder 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 doit permettre aux applications et aux services de n'avoir aucune connaissance des technologies et des terminaux utilisés.

5) Transparence du protocole: la transparence du protocole doit être 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 doit satisfaire aux spécifications générales de sécurité des réseaux NGN spécifiées au § 10.

NOTE – Des spécifications supplémentaires de prise en charge d'un environnement de service ouvert sont données dans [UIT-T Y.2234].

7.2 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.

NOTE – L'Appendice II contient un exemple de mappage de services choisis à des activateurs de service choisis.

7.2.1 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 il est recommandé que les communications au sein du groupe soient protégées vis-à-vis des autres utilisateurs. Il est recommandé qu'un réseau NGN gère de tels groupes et assure 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 doit fournir une capacité permettant la création de groupes dans la strate de transport;

2) un réseau NG doit fournir 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 doit gérer des groupes et fournir des communications de groupe sûres.

7.2.2 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 aussi 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 éventuellement 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 aussi extraire ces informations des applications au nom des utilisateurs.

2) Les informations gérées par la capacité de gestion des informations personnelles doivent être protégées contre les opérations non autorisées d'accès, d'extraction, de manipulation, etc.

3) Il est recommandé que la capacité de gestion des informations personnelles prenne en charge différents contextes de communication.

7.2.3 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 doit prendre en charge les services de messagerie accessibles par terminaux fixes et ceux accessibles par terminaux mobiles;

2) la capacité de gestion de messages NGN doit prendre en charge les services de messagerie en temps réel et les services de messagerie en différé.

NOTE – La capacité de gestion de groupes peut aussi 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).

7.2.4 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 doivent permettre aux utilisateurs d'être tant fournisseurs d'informations de présence (ils sont alors appelés "entités de présence" [b-ETSI TR 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 doit fournir 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 doit fournir une capacité permettant de recueillir des informations relatives à la localisation de l'entité de présence conformément à la réglementation et à la législation nationales.
3) Un réseau NGN doit fournir une capacité permettant de recueillir des informations concernant le contenu multimédia de l'entité de présence.
4) Un réseau NGN doit fournir une capacité permettant d'agréger des informations relatives à la présence émanant des entités de présence multiples.

Diffusion des informations de présence

5) Un réseau NGN doit fournir 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.
6) Un réseau NGN doit fournir une capacité permettant de distribuer des informations relatives au contenu multimédia de l'entité de présence.
7) Un réseau NGN doit fournir une capacité permettant d'envoyer des notifications en vrac à des entités de présence multiples.
8) Un réseau NGN doit distribuer des informations relatives à la présence en fonction du temps d'expiration (durée) qui peut être un moment précis dans le temps ou une période de validité.

Gestion des informations de présence

9) Un réseau NGN doit assurer la gestion des informations de présence en offrant un ensemble de capacités pour gérer les informations de présence collectées.
10) Le contrôle d'accès aux informations de présence (à l'aide des capacités de diffusion des informations de présence) doit être géré conformément aux spécifications relatives à la confidentialité de l'entité de présence et aux règles d'accès.
11) Les capacités de gestion des informations de présence doivent permettre à la capacité de diffusion de ne fournir qu'une partie des informations de présence en fonction de ce qui est demandé.
12) Les capacités de gestion des informations de présence doivent permettre 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).

7.2.5 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. Il est recommandé que la prise en charge d'applications et de services fondés sur la connaissance de l'emplacement soit 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 doit fournir 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 doit fournir 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 doivent être respectées par les services et les applications fournisseurs de localisation.
4) La capacité de gestion de l'emplacement doit permettre de fournir des informations d'emplacement conformément aux informations contenues dans les profils d'utilisateur/de dispositif.

7.2.6 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 doit prendre 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.

7.2.7 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 doit prendre en charge la mise à niveau des dispositifs;

2) un réseau NGN doit prendre en charge l'autoconfiguration des dispositifs;

3) un réseau NGN doit prendre 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 éventuellement fournir des fonctions permettant l'enregistrement, la gestion et la mise à jour des informations de dispositif;

5) la gestion de dispositif peut éventuellement 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 doit être sûre et toujours effectuée par une entité habilitée conformément à la législation nationale.

NOTE 1 – Il est recommandé que la gestion de dispositif permette l'installation des préférences et des applications d'utilisateur.

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

7.2.8 Gestion de session

Un réseau NGN doit fournir 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 doivent être 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 doit 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 doit prendre en charge des sessions pour divers types de média (voix, vidéo, texte);

4) une commande d'admission de session fondée sur des niveaux définis de qualité de service et de sécurité doit être prise en charge;

5) les mécanismes de commande d'admission de session doivent prendre 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 doit y mettre fin dès lors qu'un des utilisateurs le demande. Le réseau peut éventuellement mettre fin à une session à tout moment (par exemple si des conditions de défaillance apparaissent);

7) lorsqu'une session compte plus de deux participants, le réseau peut éventuellement y mettre fin, à tout moment, dès lors qu'un des utilisateurs le demande. Le réseau peut éventuellement y mettre fin à un moment quelconque (par exemple en cas de défaillance).

7.2.9 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 NGN doit assurer 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;

Il est recommandé qu'un réseau NGN assure 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 peuvent présenter des capacités limitées de prise en charge des applications fondées sur le web.

7.2.10 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 des bases de données et gestion de documents web.

Il est recommandé qu'un réseau NGN prenne 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 doit être indépendant des protocoles de transport;
2) des données de réseau arbitraires doivent être prises en charge;
3) il est recommandé que le mécanisme de synchronisation des données prenne en compte les limitations de ressource des terminaux.

7.3 Perception du contexte

La perception du contexte est la capacité permettant de définir une action suivante lors d'une télécommunication ou d'une procédure ou d'influer sur elle, en renvoyant au statut des entités pertinentes qui forment un environnement cohérent en tant que contexte. Le statut des différentes entités et leur regroupement en fonction de leur statut sont traités comme des informations de contexte. Des informations de contexte sont par exemple celles ayant trait à la connectivité de l'abonné, à l'emplacement de marchandises remarquées dans un système de distribution et à l'état du trafic dans un réseau.

Soit les rôles clés suivants:

- **Générateur de contexte**: il produit des informations de contexte et permet d'y accéder. Il peut être incorporé au réseau NGN ou être en dehors de celui-ci.
- **Demandeur de contexte**: il demande des informations de contexte et s'y réfère. Il peut être incorporé au réseau NGN ou être en dehors de celui-ci.
- **Distributeur de contexte**: il recueille, distribue, traite et éventuellement emmagasine les informations de contexte, agissant comme médiateur entre le générateur et le demandeur de contexte.

Lorsque les rôles ci-dessus sont joués par un réseau NGN, il est recommandé que celui-ci garantisse:

1) La sécurité des informations de contexte du point de vue du générateur de contexte:
   - Il faut que le(s) demandeur(s) d'informations de contexte n'y accèdent que lorsque le générateur de contexte l'autorise. Cette politique doit être appliquée aussi longtemps que les informations de contexte sont présentes dans le réseau NGN.
   - Le suivi involontaire d'un générateur de contexte doit être interdit.

     NOTE – Cette spécification suppose l'existence d'informations de contexte provenant d'un générateur de contexte, qui sont accessibles à différents demandeurs de contexte à des fins diverses. Il ne doit s'agir que d'utilisation volontaire. Par exemple, même si un générateur de contexte autorise l'accès à son historique de vente de livres à un utilisateur (pour obtenir des informations sur de nouvelles parutions éventuelles), il est interdit que cette information soit

accessible par d'autres applications, telles que la diffusion d'annonces pour des billets de cinéma, des CD musicaux ou des vêtements de sport.

- Les informations de contexte ne doivent pas faire l'objet de fuites ou d'abus au cours d'un processus de distribution dans un réseau NGN.
- Les informations de contexte emmagasinées dans une base de données dans un réseau NGN ne doivent pas faire l'objet de fuites ou d'abus.

2) La fiabilité des informations de contexte du point de vue du demandeur de contexte:

- Il est recommandé que les informations de contexte soient transférées de façon transparente au demandeur de contexte, sans modification aucune.
- Il est recommandé que les nouvelles informations de contexte soient transférées au demandeur de contexte.
- Il est souhaitable que les anciennes informations de contexte soient automatiquement abandonnées.
- Des informations de contexte factices doivent ne pas être produites ni être ouvertes.

3) La conservation d'une utilisation simple des informations de contexte du point de vue du demandeur de contexte ou du fournisseur d'application:

- Il est recommandé que le format de données et la sémantique des informations de contexte soient normalisés afin que les divers demandeurs de contexte ou fournisseurs d'application puissent les employer.
- Il est recommandé que les informations de contexte puissent aisément être recherchées par le demandeur de contexte, s'il en est autorisé.
- Il est recommandé que les informations de contexte puissent être utilisées par le demandeur de contexte à tout moment, s'il en est autorisé.
- Les informations de contexte primaires peuvent éventuellement être converties en informations de contexte appropriées afin qu'un fournisseur d'application puisse aisément développer une application en employant les informations de contexte converties.
- Le distributeur de contexte peut éventuellement être en mesure de sélectionner automatiquement les éléments et les données de service parmi de nombreuses autres possibilités afin qu'un développeur d'application d'une tierce partie puisse aisément développer une application en employant les informations de contexte.

4) Le transfert des informations de contexte en temps réel et sur demande lorsque le demandeur de contexte le souhaite.

5) L'échelonnabilité pour le distributeur de contexte:

- Il est recommandé de traiter d'importantes quantités d'informations de contexte afin d'éviter une fausse inférence sur la base d'informations de contexte limitées.
- Il est recommandé que le distributeur de contexte fasse preuve de souplesse en maniant les divers types d'informations de contexte et en prenant en charge les diverses applications.

6) La distribution efficace des informations de contexte.

8 Routage

Un réseau NGN doit fournir 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 doit prendre en charge les mécanismes de routage les plus appropriés pour les fournisseurs NGN. Il doit prendre 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.

4) le routage, sur la base des séries de numéros UIT-T E.164.

Il est recommandé qu'un réseau NGN prenne en charge:

5) le routage, en tenant compte du contexte (par exemple le routage fondé sur la présence, l'emplacement et les informations personnelles).

NOTE – Le § 7.3 contient d'autres informations sur la perception du contexte.

9 Qualité de service

Un réseau NGN doit prendre 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 doit prendre en charge plusieurs niveaux de qualité de service, qui peuvent être négociés entre l'utilisateur et le fournisseur et/ou entre les fournisseurs. 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.

9.1 Spécifications générales de qualité de service

Un réseau NGN doit satisfaire 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, tandis que d'autres ne le peuvent pas).

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 [UIT-T Y.2111].

5) Prendre en charge la commande de ressource 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 [UIT-T Y.2111].

7) Prendre en charge les spécifications de qualité de service induites par l'application.

8) Vérifier de bout en bout la disponibilité des ressources de transport [UIT-T Y.2111].

9) Prendre en charge la différenciation de la qualité de service pour diverses catégories de circulation de paquets, y compris les flux de types paquet et les désignations des utilisateurs [UIT-T Y.2111].

10) Autoriser les demandes concernant la qualité de service et ne répondre qu'aux demandes autorisées [UIT-T Y.2111].

11) Prendre en charge la commande dynamique de traduction d'adresse de réseau et de port (NAPT, network address port translation) à l'extrémité proche et la sélection du mode de fonctionnement avec coupe-feu [UIT-T Y.2111].

12) Prendre en charge la traversée de la traduction de l'adresse (NAT, network address translation) de réseau jusqu'à l'extrémité distante [UIT-T Y.2111].

13) Assurer la commande de ressource et d'admission pour la multidiffusion en vue de prendre en charge la télévision utilisant le protocole Internet (TVIP) [UIT-T Y.2111], par exemple.

14) Assurer la commande de ressource et d'admission en vue de prendre en charge le nomadisme [UIT-T Y.2111].

9.2 Classes de qualité de service de réseau

1) Il est recommandé qu'un réseau NGN prenne en compte la performance du réseau au niveau de la strate de transport.

2) Il est recommandé qu'un réseau NGN prenne en charge les classes de qualité de service de réseau NGN fondées sur [UIT-T Y.1541].

9.3 Priorité de service/d'application

Pour assurer la priorité de service/d'application, il est recommandé qu'un réseau NGN prenne 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, NNI et ANI;

3) les mécanismes d'activation de priorité déclenchant l'action prioritaire voulue.

9.4 Contrôle de la qualité de service

Il est recommandé qu'un réseau NGN prenne 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 est recommandé qu'il soit 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;

7) des méthodes de commande de l'admission fondées sur les ressources, utilisant par exemple des informations relatives aux mesures de la performance.

9.5 Signalisation de la qualité de service

Il est recommandé qu'un réseau NGN utilise 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.

9.6 Performance

Un réseau NGN doit mesurer et gérer la performance pour garantir le niveau de qualité de service.

A cette fin, il est recommandé que les mesures de performance de réseau et leur gestion permettent:

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.

9.7 Gestion du traitement et du 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, il est recommandé qu'un réseau NGN propose 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.

Il est recommandé qu'un réseau NGN dispose 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.

10 Identification et sécurité

NOTE – L'emploi du mot "identité" dans la présente section n'a pas une signification absolue. Il n'est en particulier pas une validation positive d'une personne.

10.1 Spécifications générales

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

NOTE 1 – Les mécanismes d'authentification et d'autorisation spécifiques ne relèvent pas de la présente Recommandation.

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 2 – Parfois, l'expression "fournisseur de services" a été utilisée pour faire référence au fournisseur de services de la strate de transport. Dans la présente section, 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.

Ci-après sont indiquées les spécifications générales relatives aux capacités d'identification, d'authentification et d'autorisation.

1) Un réseau NGN doit prendre 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) Un réseau NGN doit identifier 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 doit permettre d'effectuer séparément les processus d'identification, d'authentification et d'autorisation pour les utilisateurs et pour les équipements terminaux.

4) Un réseau NGN doit permettre de vérifier l'association entre l'utilisateur et l'équipement terminal de l'utilisateur pour certains services spécifiques.

5) Il est recommandé que les processus d'authentification, d'autorisation et de comptabilité effectués par le fournisseur de réseaux NGN et par le fournisseur de services soient des processus sûrs.

6) Un fournisseur de services doit fournir 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 doit fournir 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 doit prendre 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 doit fournir 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 doit 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 doit prendre 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) doivent être administrés par l'opérateur de réseau approprié.

13) L'identificateur privé et l'identificateur public d'un utilisateur NGN des ressources de la strate de service (identificateurs utilisés pour l'authentification, l'autorisation et le routage) doivent être 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 doivent être masqués pour les autres utilisateurs.

15) Les identificateurs publics d'utilisateur NGN d'un utilisateur de services peuvent éventuellement 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 identificateurs d'utilisateur public et privé.

17) Comme un utilisateur donné peut utiliser plusieurs identificateurs d'utilisateur privés via une seule procédure d'abonnement, le réseau NGN doit prendre en charge les identificateurs privés multiples d'utilisateur par une procédure d'abonnement unique.

18) Un réseau NGN peut éventuellement authentifier et autoriser un même utilisateur pour plusieurs services ("guichet unique").

NOTE 3 – 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 mais est souhaitée si les technologies actuelles le permettent.

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

10.2 Spécifications d'identification

Les réseaux NGN 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 doit offrir à l'utilisateur la capacité d'identifier les fournisseurs NGN (au niveau de chaque strate) lorsqu'une relation directe existe.

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

1) Existence de plusieurs identificateurs d'utilisateur

Un utilisateur de réseau NGN pouvant avoir un ou plusieurs identificateurs publics et privés, le réseau NGN doit pouvoir les différencier (par exemple à des fins d'utilisation personnelle ou professionnelle).

2) Portabilité de l'identificateur

Un réseau NGN doit fournir des capacités assurant une fonctionnalité équivalente à la portabilité du numéro dans un environnement RTPC.

3) Indépendance de l'identificateur

Il est recommandé que l'identificateur d'utilisateur public soit attribué 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 éventuellement être assurée grâce à des fonctions d'interfonctionnement appropriées.

4) Prise en charge des attributs d'identificateur

Des informations d'attribut d'identificateur privé (telles que la durée de vie de cet identificateur pour l'utilisateur, pour l'abonné, pour le réseau utilisé, etc.) peuvent éventuellement être associées à un identificateur 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 éventuellement être associées à un identificateur d'utilisateur par un fournisseur d'attributs (réseau, utilisateur principal, utilisateur final par exemple).

6) Autorisation d'attribut sélective

Un réseau NGN doit prendre en charge l'autorisation sélective d'informations d'attribut d'identité privée par un fournisseur d'attributs (durée de vie de l'identificateur par exemple).

7) Prise en charge de la programmation par abonné

Il est recommandé qu'un réseau NGN prenne 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 doit prendre en charge un lien dynamique entre l'identificateur d'utilisateur public et l'identité d'équipement terminal pour certains services.

9) Associations à plusieurs terminaux

Un réseau NGN doit autoriser 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 doit prendre 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.

11) Administration des identificateurs d'utilisateur public

Un identificateur d'utilisateur public doit être administré par l'opérateur de réseau et doit ne pas pouvoir être modifié par l'utilisateur.

12) Authenticité des identificateurs d'utilisateur public

L'opérateur de réseau doit garantir l'authenticité d'un identificateur d'utilisateur public présenté pour une session entrante à un utilisateur, la communication se faisant entièrement à travers un réseau sécurisé.

10.3 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, un réseau 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, un réseau NGN doit aussi offrir à un utilisateur la capacité d'authentifier et d'identifier un fournisseur de service.

Il est recommandé qu'un réseau NGN assure 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 doit permettre l'utilisation de divers mécanismes d'authentification de réseau adaptés aux technologies de réseau d'accès sous-jacentes.
2) Il est recommandé que le mécanisme d'authentification de service vise à être indépendant des technologies de réseau d'accès NGN et reste cohérent.
3) Un réseau NGN doit demander à un utilisateur/un équipement terminal de fournir des informations d'authentification d'une manière explicite ou implicite.
4) Il est recommandé qu'un réseau NGN prenne 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 doit être prise en charge.
6) Il est recommandé qu'un réseau NGN fournisse des capacités d'authentification réciproque entre un fournisseur de services et un utilisateur.
7) Il est recommandé qu'un réseau NGN fournisse des capacités d'authentification réciproque entre le fournisseur de réseau de transport et l'utilisateur.

10.4 Spécifications d'autorisation

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

1) Un réseau NGN doit fournir 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) Il est recommandé que l'autorisation d'accès aux services vise à être indépendante des technologies de réseau d'accès NGN.
3) Il est recommandé que la capacité d'autorisation prenne en charge les scénarios de mobilité des réseaux NGN lorsque cela est possible.

10.5 Gestion des identités

1) Un réseau NGN doit prendre en charge une démarche structurée, s'agissant de la gestion d'une ou des identités (IdM, *identity management*) (y compris les informations associées telles que les identificateurs, les attributs, les assertions et la politique) d'entités telles que les suivantes:
   a) Utilisateurs/groupes.
   b) Organismes/fédérations/entreprises/fournisseurs de services.
   c) Dispositifs/éléments de réseau/systèmes.
   d) Objets (processus d'application, contenu, données).
2) Un réseau NGN doit prendre en charge les capacités de gestion IdM afin de:
   a) Sécuriser la gestion du cycle de vie (par exemple immatriculation, validation, révocation) d'une identité ou des identités d'entité.
   b) Sécuriser la découverte et l'échange d'informations associées à une identité ou aux identités d'entité. Sont inclus la découverte et l'échange d'informations sur les identités qui sont situées dans un domaine de réseau NGN ou dans différents domaines de réseau NGN.
3) Un réseau NGN doit prendre en charge les capacités permettant de faire respecter la politique applicable associée à une identité d'entité ou à des informations sur l'identité.
4) Un réseau NGN doit prendre en charge les capacités communes de gestion IdM à employer par de multiples services et applications, notamment:
   a) Les services de communication en temps réel (par exemple voix sur IP (VoIP), télévision linéaire et services de messagerie en temps réel).
   b) Les autres services de communication (par exemple les transactions utilisant le web).
5) Un réseau NGN doit prendre en charge les capacités de gestion IdM permettant l'assertion anonyme des informations sur les identités (par exemple les identificateurs et les attributs), soumises à la politique applicable.
6) Un réseau NGN doit prendre en charge les capacités de gestion IdM permettant l'interfonctionnement entre éléments de réseau dans un domaine NGN (c'est-à-dire Intranet) et dans différents domaines NGN ou fédérations. Cela exige:
   a) L'emploi d'interfaces normalisées pour l'échange d'informations de gestion IdM.
   b) L'emploi de mécanismes normalisés (par exemple protocoles, structures de données et schémas) pour l'échange de données de gestion IdM.
7) Un réseau NGN doit prendre en charge les capacités de gestion IdM admettant des utilisateurs terminaux disposant de facilités d'utilisation, telles que:
   a) L'accès unique à de multiples services et applications et leur interruption unique.
   b) La convergence fixe et mobile.
   c) Le contrôle et la protection des informations personnellement identifiables (PII, personally identifiable information).
8) Un réseau NGN doit prendre en charge les capacités de gestion IdM afin d'assurer la sécurité des services et des applications.
9) Un réseau NGN doit prendre en charge la sécurité des capacités, fonctions, données et communications de gestion IdM.

10.6 Spécifications de sécurité

Les réseaux NGN doivent prendre 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 doit respecter 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 doit la garantir en ne révélant des informations que lorsqu'une autorisation valable est fournie;
9) protection pour réduire au minimum les effets des attaques contre le réseau, de l'intérieur ou de l'extérieur.

10.7 Protection d'infrastructure critique

Il est recommandé que les fournisseurs de services aient 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 § 10.6.

11 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, la fourniture de réseaux et la fourniture 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 organismes 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 organismes 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 organismes 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 organisme 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") [UIT-T M.3050.0];
10) prenant en charge des processus interentreprises entre des organismes 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 spécifications 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 § 16.2 ("Comptabilité et taxation").

12 Traitement 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, on distingue deux types de mobilité: la mobilité personnelle et la mobilité du terminal [UIT-T Q.1706].

Dans un réseau NGN, 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.

Dans un réseau NGN, 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.

Ci-après sont indiquées des spécifications générales de gestion de la mobilité axées sur la prise en charge des besoins des clients.

Les réseaux NGN 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 limités de réseaux des fournisseurs;
4) la prise en charge de la gestion de l'abonnement itinérant, de l'identification 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;
8) la prise en charge de la gestion de la mobilité à l'aide du protocole IP ou, au moins, bien harmonisée avec la technologie IP en vue d'un fonctionnement efficace et intégré.

Pour les services auxquels la mobilité convient, il est recommandé qu'un réseau NGN:

– prenne en charge la continuité des services au cours de scénarios dans un réseau d'accès ou entre réseaux d'accès. La continuité des services s'applique notamment dans les cas suivants:
  a) mobilité du terminal;
  b) mobilité de la personne.

NOTE 1 – Les niveaux de mise en œuvre de la continuité des services peuvent différer selon le scénario, en fonction de conditions, telles les restrictions imposées par les technologies d'accès et le niveau de service pris en charge par le fournisseur de services ou de réseau.

NOTE 2 – La continuité des services pour les scénarios dans un réseau central doit faire l'objet d'un complément d'étude.

Pour les services vocaux, un réseau NGN doit prendre en charge la continuité des services en cas de mobilité du terminal.

Un réseau NGN doit offrir des capacités permettant la prise en charge de la continuité des services, en tenant compte des conditions de réseau (par exemple le nombre de sessions d'utilisateur, les cas de mobilité et la largeur de bande consommée) et des exigences des utilisateurs.

Il est recommandé qu'un réseau NGN permette une certaine adaptation afin de prendre en charge la continuité des services lorsque les exigences des utilisateurs ne concordent pas avec les conditions de réseau. Cette adaptation peut inclure une négociation ou une renégociation de la qualité de service du réseau et/ou des paramètres du terminal (par exemple, le changement ou l'adaptation du codec).

NOTE 3 – Voir [UIT-T Q.1706] pour plus de détails sur les spécifications relatives à la gestion de la mobilité pour les réseaux NGN.

13 Gestion des profils

13.1 Gestion du 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 éventuellement disposer de fonctions d'échange de données entre elles.

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

1) Un profil d'utilisateur doit exister pour chaque utilisateur chez un fournisseur correspondant. Ce profil peut éventuellement comprendre plusieurs composantes.
2) Les composantes peuvent éventuellement être réparties entre le réseau de rattachement et l'environnement du fournisseur de services. Les critères de confidentialité et de protection des données doivent être respectés.
3) Dans le domaine du réseau de rattachement, les composantes peuvent éventuellement être réparties entre plusieurs entités.
4) Dans le réseau de rattachement, il doit exister 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 doit être sous le contrôle du réseau de rattachement.
5) Les services, les applications et les autres entités NGN doivent 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 doivent être respectés.
6) Il doit 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 classifier les données qu'un tel profil peut contenir, un classement par catégories (informations générales sur l'utilisateur, informations spécifiques sur le service, etc.) peut éventuellement 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.

13.2 Gestion du 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. Les profils de dispositif peuvent comprendre des informations sur le transport et des informations sur le service. Ils peuvent être stockés dans des bases de données distinctes situées dans la strate de service et dans la strate de transport et peuvent éventuellement 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 éventuellement exister pour chaque équipement d'utilisateur. Il peut éventuellement comprendre plusieurs "composantes";

2) ces composantes peuvent éventuellement être réparties entre le réseau de rattachement et/ou les fournisseurs de services;

3) dans le réseau de rattachement, les composantes peuvent éventuellement être réparties entre plusieurs entités;

4) dans le réseau de rattachement, il doit y avoir 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 éventuellement 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 doit exister 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 sur le dispositif, informations propres au service, etc.) peut éventuellement 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.

14 Traitement des médias

14.1 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.

Un réseau NGN doit prendre 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 pour les réseaux NGN 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);
– la conversion de média (par exemple pour la prise en charge de services texte-parole, parole-texte et télécopie-courrier électronique);
– 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.

Les capacités supplémentaires de ressources de média pour les réseaux NGN comprennent:

– le téléchargement de données de média (par exemple, clips vidéo/audio, images);
– les flux de médias (par exemple, la vidéo à la demande);
– le transfert transparent;
– le stockage et la fourniture de données de médias distribuées (copies multiples de données de média, extraits multiples de données de médias);
– l'adressage dynamique de données de média (localisant les données de média existantes sur le lieu de stockage correct afin que l'utilisateur puisse y accéder en temps réel).

14.2 Spécifications pour les codecs

14.2.1 Généralités

Les spécifications générales applicables aux codecs pour un réseau NGN sont les suivantes:

1) Le transcodage doit être évité toutes les fois où cela est possible.
2) Un réseau NGN doit prendre 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 doit prendre en charge la négociation de bout en bout des codecs de texte, tels que ceux actuellement spécifiés dans les Recommandations de l'UIT-T.

Il est recommandé qu'un réseau NGN possède les caractéristiques suivantes:

1) fonctionnement auto-adaptable selon les variations de la qualité de service;
2) prise en charge des effets des changements du niveau de service sur le fonctionnement des codecs;
3) compatibilité avec les codecs RTPC/RNIS;
4) découverte/interrogation des paramètres de codec;
5) sélection/négociation et renégociation en cours de session des paramètres de codec.

14.2.2 Codecs audio

Soit les classes de codecs audio suivantes:

a) "codecs audio à bande étroite" pour la gamme des fréquences audio de 300 Hz à 3 400 Hz;
b) "codecs audio à large bande" pour la gamme des fréquences audio de 50 Hz à 7 000 Hz;
c) "codecs audio à bande extra-large" pour la gamme des fréquences audio de 50 Hz à 14 000 Hz;
d) "codecs audio à bande complète" pour la gamme des fréquences audio de 20 Hz à environ 20 000 Hz, avec des capacités associées de canaux multiples (mono, stéréo, etc.).

Afin de permettre son interfonctionnement avec d'autres réseaux (le RTPC, les réseaux mobiles ou d'autres réseaux NGN par exemple), un réseau NGN doit pouvoir recevoir et présenter des données vocales à codage [UIT-T G.711] lorsqu'il est interconnecté à un autre réseau. 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, il est recommandé d'utiliser des échantillons de 10 ms pour la mise en paquets des données vocales à codage 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 éventuelles 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 1 – 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, il n'est pas imposé de spécification dans la présente Recommandation concernant la valeur devant être choisie.

NOTE 2 – Ce qui précède ne constitue ni une spécification relative aux codecs devant être pris en charge par les terminaux, ni une obligation pour les réseaux NGN de prendre en charge le transcodage audio entre codecs arbitraires et le codec [UIT-T G.711].

En outre, la prise en charge des codecs audio suivants est recommandée:

– Multidébit adaptatif (AMR, *adaptative multi-rate*) [ETSI TS 126.071]: Afin de prendre en charge les terminaux 3GPP (Projet de partenariat de troisième génération) et de faciliter l'interfonctionnement avec les réseaux 3GPP.
– UIT-T G.729A [UIT-T G.729]: Afin de faciliter l'interfonctionnement avec les réseaux VoIP existants et de prendre en charge les terminaux VoIP existants.
– Codec à débit variable amélioré (EVRC, *enhanced variable rate codec*)/codec EVRC à large bande (EVRC-B, *EVRC broadband*) [TIA-127-C]: Afin de prendre en charge les terminaux 3GPP2 et de faciliter l'interfonctionnement avec les réseaux 3GPP2.

14.2.3 Codecs audio à large bande

14.2.3.1 Généralités

Le § 14.2.1 doit prévaloir sur le présent paragraphe afin de réduire le transcodage et d'améliorer tant l'interopérabilité à large bande que la qualité de bout en bout.

Les codecs audio à large bande sont une capacité en option qui peut être prise en charge par:

– les entités en bordure du réseau NGN (par exemple l'équipement terminal) qui possèdent une capacité audio à large bande;

– l'équipement de réseau au départ et à l'arrivée du flux média IP dans le réseau NGN à contenu audio à large bande.

Les terminaux fournissant des capacités audio à large bande doivent aussi posséder une capacité à bande étroite et satisfaire au § 14.2.2.

L'équipement de réseau fournissant des capacités audio à large bande doit aussi posséder une capacité à bande étroite et satisfaire au § 14.2.2.

Le transcodage audio peut éventuellement être effectué dans le but d'assurer l'interfonctionnement des services de bout en bout, mais il est recommandé de l'éviter dans la mesure du possible.

14.2.3.2 Codecs audio à large bande dans les terminaux

Il est recommandé que les terminaux au départ et à l'arrivée de flux média IP de bout en bout dans les réseaux NGN, prenant en charge la capacité audio à large bande, fournissent un ou plusieurs des codecs audio suivants à large bande:

– UIT-T G.722 [ITU-T G.722];

NOTE 1 – Requis pour l'équipement d'utilisateur de nouvelle génération de communications numériques sans fil améliorées (DECT NG, digital enhanced cordless telecommunications new generation), utilisé dans certains équipements d'utilisateur VoIP et/ou ancien.

– AMR-WB/UIT-T G.722.2 [ITU-T G.722.2];

NOTE 2 – Requis pour l'équipement d'utilisateur 3GPP et/ou l'équipement d'utilisateur avec une mobilité conforme à l'accès 3GPP.

– UIT-T G.729.1 [ITU-T G.729.1];

NOTE 3 – Utilisé dans certains équipements d'utilisateur DECT NG, dans certains équipements d'utilisateur VoIP et/ou ancien.

– EVRC-WB [TIA-127-C];

NOTE 4 – Requis pour l'équipement d'utilisateur 3GPP2 et/ou l'équipement d'utilisateur avec une mobilité conforme à l'accès 3GPP2.

NOTE 5 – Les terminaux peuvent éventuellement fournir, outre les codecs susmentionnés, d'autres codecs.

NOTE 6 – A titre d'exception, il est recommandé que les terminaux fournissant un ou plusieurs codecs audio à large bande, aucun d'entre eux ne figurant dans la liste ci-dessus, (par exemple, les terminaux existants/anciens) soient autorisés dans les réseaux NGN. L'interopérabilité audio à large bande de tels terminaux peut éventuellement être limitée.

14.2.3.3 Codecs audio à large bande dans les réseaux

Il est recommandé que l'équipement de réseau au départ et à l'arrivée de flux média IP de bout en bout dans les réseaux NGN, prenant en charge la capacité audio à large bande, fournissent les codecs audio suivants à large bande:

– UIT-T G.722 [UIT-T G.722];

NOTE 1 – Pour prendre en charge l'équipement d'utilisateur DECT NG, certains équipements d'utilisateur VoIP et/ou ancien et/ou l'interfonctionnement avec d'autres réseaux.

– AMR-WB/UIT-T G.722.2 [ITU-T G.722.2];

NOTE 2 – Pour prendre en charge l'équipement d'utilisateur 3GPP, l'équipement d'utilisateur avec une mobilité conforme à l'accès 3GPP et/ou l'interfonctionnement avec les réseaux 3GPP.

– UIT-T G.729.1[UIT-T G.729.1];

NOTE 3 – Le cas échéant, pour prendre en charge l'équipement d'utilisateur DECT NG, l'équipement d'utilisateur VoIP et/ou ancien et/ou l'interfonctionnement avec certains réseaux VoIP et anciens.

– EVRC-WB [TIA-127-C];

NOTE 4 – Le cas échéant, pour prendre en charge l'équipement d'utilisateur 3GPP2, l'équipement d'utilisateur avec une mobilité conforme à l'accès 3GPP2 et/ou l'interfonctionnement avec les réseaux 3GPP2.

14.2.4 Codecs vidéo

Afin d'assurer l'interfonctionnement pour les services de communication vidéo entre les réseaux NGN et d'autres réseaux, il est recommandé de prendre en charge les codecs de profil 0 UIT-T H.263 [UIT-T H.263] et de profil de base UIT-T H.264 [UIT-T H.264].

NOTE – Ce qui précède ne constitue ni une spécification relative aux codecs vidéo devant être pris en charge par les terminaux ni une obligation pour les réseaux NGN de prendre en charge le transcodage vidéo entre codecs arbitraires et le codec UIT-T H.263 ou UIT-T H.264.

15 Gestion de contenu

Il est recommandé qu'un réseau NGN offre des capacités de gestion de contenu afin de pouvoir gérer les diverses et importantes ressources de contenu.

NOTE 1 – Les objets soumis à la gestion de contenu sont généralement classés comme contenus d'entreprise (par exemple documents d'entreprise), contenus de services web (par exemple fichiers HTML, images), contenus de services TVIP (par exemple données de flux de taille relativement importante). La gestion de contenu dans les réseaux NGN offre la possibilité de gérer le cycle de vie du contenu (de sa création, en passant par l'édition, l'approbation, la publication et la maintenance jusqu'à l'archivage). En outre, la gestion de contenu offre la possibilité de prendre en charge les processus d'entreprise à entreprise conformément à leurs contrats.

NOTE 2 – S'agissant des services TVIP, les spécifications détaillées relatives à la gestion de contenu sont contenues dans le § 14.1.

NOTE 3 – Les capacités de gestion de contenu comprennent, mais la liste n'est pas exhaustive:

– L'acquisition du contenu, l'agrégation et l'importation de contenus/de métadonnées en provenance de multiples sources extérieures.

– La validation et la vérification du format du contenu/des métadonnées ainsi que la définition de la relation entre le contenu et ses métadonnées.

– Le classement du contenu en fonction des diverses normes de classement.

– La manipulation du contenu et des métadonnées (par exemple l'ajout, la modification, la recherche, le traitement relatif au droit d'auteur, l'adaptation).

NOTE 4 – L'adaptation du contenu inclut la capacité de transformation du contenu afin d'adapter celui-ci aux capacités du dispositif et/ou aux contraintes de réseau.

– La distribution du contenu dans un réseau NGN a lieu conformément à l'attribution des ressources de fourniture de contenu, aux restrictions en matière de publication de contenu, etc.

– Le contrôle et la vérification du contenu ont lieu (par exemple le contrôle de l'état du contenu et/ou du résultat d'une manipulation du contenu, l'analyse du contenu et les statistiques).

16 Exploitation et fourniture

16.1 Spécifications relatives au numérotage, au nommage et à l'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 doivent être 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 est 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.

1) Les modes d'attribution d'adresse fixes et dynamiques doivent être pris en charge.
2) Des capacités de numérotage, d'adressage et de nommage peuvent éventuellement 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 doit être 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).

NOTE – Ces registres pourraient être des répertoires UIT-T X.500 dont l'accès est spécifié dans [b-UIT-T X.511].

16.1.1 Numérotage

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

1) Les mécanismes d'adressage doivent prendre en charge la capacité à différencier le plan de numérotation des plans de numérotage et d'adressage.
2) Les mécanismes d'adressage doivent prendre en charge la capacité à traduire une séquence de numérotation en une valeur du plan de numérotage et d'adressage.
3) Un réseau NGN doit prendre en charge le numérotage UIT-T E.164 (numéros mondiaux).
4) Il est recommandé qu'un réseau NGN permette l'utilisation d'un numérotage non UIT-T E.164 (numéros locaux).
5) Il est recommandé qu'un réseau NGN permette l'utilisation de numéros courts dans les plans de numérotation nationaux.
6) Il n'est pas recommandé qu'un réseau NGN empêche l'utilisation de numéros privés et de numéros d'entreprise (voir § 17).
7) En cas d'utilisation de numéros non UIT-T E.164 (numéros locaux) ou de séquences de numérotation, le mécanisme d'adressage du réseau NGN doit déterminer le cadre de validité des numéros locaux.
8) Un réseau NGN doit prendre en charge les numéros internationaux UIT-T E.164.
9) Un réseau NGN doit prendre en charge les numéros nationaux UIT-T E.164.
10) Un réseau NGN doit prendre en charge les codes courts (numéros non UIT-T E.164) dans les plans de numérotation nationaux.
11) Un réseau NGN doit prendre en charge les numéros privés (par exemple, les numéros propres à un service et les numéros d'entreprise) (voir § 17.1 et 17.2).

12) En cas d'utilisation de numéros UIT-T E.164 nationaux ou de codes courts ou de numéros privés, le mécanisme d'adressage du réseau NGN doit déterminer le cadre de validité des numéros.

13) Un réseau NGN doit prendre 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 qu'il est recommandé de traiter comme tels dans les procédures de routage.

16.1.2 Mécanismes de numérotage, de nommage et d'adressage

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

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

2) Les opérateurs de réseaux NGN peuvent éventuellement 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 doit prendre 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 UIT-T 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. Pour les identificateurs URI de téléphonie:

- les numéros internationaux UIT-T E.164 doivent être pris en charge;
- les numéros nationaux UIT-T E.164 et les codes courts doivent être pris en charge.

4) Pour certains scénarios de service (par exemple l'interfonctionnement avec le réseau RTPC/RNIS), un réseau NGN doit prendre en charge l'établissement de communications multimédias IP (pour l'émission et pour la réception) en utilisant le numérotage UIT-T E.164 avec prise en charge de type ENUM si nécessaire.

5) Les mécanismes de numérotage et d'adressage doivent prendre en charge les types de service monodiffusion et multidiffusion.

6) Il est recommandé que les mécanismes de numérotage et d'adressage prennent en charge les types de service radiodiffusion.

7) D'autres mécanismes de numérotage, de nommage et d'adressage peuvent éventuellement être pris en charge.

NOTE 3 – D'autres mécanismes de numérotage, de nommage et d'adressage, tels que ceux des noms distinctifs comme spécifiés dans [b-UIT-T X.501], doivent faire l'objet d'un complément d'étude.

16.1.3 Résolution du numéro/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: Il est recommandé qu'un réseau NGN soit 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 doivent ne pas être entravées par l'existence d'une défaillance en un point (utilisation par exemple de mécanismes de résolution distribués).

3) Sécurité: Des mesures de sécurité doivent être associées aux capacités de résolution de nom/de numéro/d'adresse.

NOTE – Ces capacités peuvent éventuellement faire intervenir des bases de données prenant en charge les services de répertoire qui sont internes ou externes au réseau NGN (par exemple une base de données DNS Internet, LDAP [b-ITU-T X.511]). 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.

16.1.4 Interfonctionnement du numérotage, du nommage et de l'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 doit prendre en charge plusieurs scénarios d'interfonctionnement d'adresses de la strate de transport en minimisant l'incidence sur le 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 doivent être utilisées pour prendre en charge les différences de format d'adresse, tant dans la strate de transport que dans la strate de service, en minimisant l'incidence sur le service fourni aux utilisateurs.

16.2 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 doivent prendre 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 celles utilisées pour des services prépayés (taxation en ligne).
2) Des mécanismes ouverts doivent être disponibles pour la gestion de la taxation.
3) Différentes politiques de taxation doivent être 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 doivent prendre en charge les services ayant une fonctionnalité de multidiffusion.
5) Un réseau NGN doit accepter 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.
6) Un réseau NGN doit prendre en charge les interfaces et les protocoles entre les éléments de réseau et les éléments de comptabilité et entre les éléments de comptabilité et les éléments de taxation afin de recueillir et de transporter les données sur l'utilisation des ressources (par exemple les mesures de comptabilité et relevés d'informations de taxation (CIR – *charging information records*). Ces interfaces et protocoles doivent être conformes avec [UIT-T Y.2233].

7) Un réseau NGN doit prendre en charge les fonctionnalités de gestion pour un fonctionnement sans heurts des éléments fonctionnels de comptabilité et de taxation [UIT-T Y.2233].

8) Il est recommandé qu'un réseau NGN prenne en charge la fonctionnalité de comptabilité et de taxation liée au flux pour divers services NGN (par exemple l'utilisation des ressources pour le flux unidirectionnel, pour le flux bidirectionnel, pour la session). Une telle fonctionnalité doit être précise, fiable et adaptable.

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

16.3 Spécifications relatives à l'exploitation, à l'administration et à la 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 doivent assurer des fonctions OAM dans la strate de service et dans la strate de transport.

Les services de réseau NGN doivent disposer de leurs propres capacités OAM pour être fiables et respecter les spécifications des accords SLA.

NOTE 1 – Les capacités OAM décrites dans le présent paragraphe complètent les capacités de gestion décrites au § 11.

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 doit être prise en charge.

2) Les fonctions OAM doivent être utilisées pour des applications point à point, point à multipoint et multipoint à multipoint.

3) Les fonctions OAM doivent être efficacement adaptables à des réseaux de grande taille.

4) La capacité à détecter des dérangements, des défauts et des défaillances doit être 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 doit être 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 doit être 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) doit être prise en charge.

8) Le trafic OAM doit être acheminé dans le même conduit que le trafic d'utilisateur.

9) Les anomalies suivantes doivent être 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 doivent être compatibles avec les versions antérieures. Un réseau NGN doit être capable d'activer des fonctions OAM de façon transparente sans perturber le trafic d'utilisateur ou provoquer des actions inutiles.

11) Les fonctions OAM doivent être 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) doivent être 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 doit pas provoquer le déclenchement de plusieurs alarmes ni la mise en œuvre de mesures correctrices inutiles dans un réseau de couche client de niveau supérieur. Il est recommandé que les réseaux de couche client prennent 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 doivent prendre 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 doivent ne pas dépendre 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 doivent être 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 doivent prendre 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 doit être 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 doit posséder 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 (§ 18.3)

21) Pour permettre la gestion indépendante d'une portion de réseau sous la responsabilité d'un fournisseur et la définition flexible d'entités de maintenance, il faut prendre en charge les fonctions OAM "de segment" et les fonctions OAM "de bout en bout".

NOTE 2 – 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 doit être pris en charge.

23) Les informations fournies par les fonctions OAM doivent être 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 doivent être prises en charge.

16.4 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 la commande 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 tout 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 (§ 9) peuvent être considérées comme faisant partie de l'ensemble global des capacités de gestion des politiques.

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

1) les capacités de gestion des politiques doivent être prises en charge pour garantir l'accès aux services, la fourniture et la gestion de ces derniers;

2) les capacités de gestion des politiques doivent s'appliquer à certains services et dans certains domaines de fournisseur ou entre plusieurs domaines de fournisseur;

3) les capacités de gestion des politiques doivent rejeter ou ne pas répondre à des demandes non autorisées et répondre à des demandes autorisées.

16.5 Spécifications relatives à la capacité de survie

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

16.5.1 Commutation de protection

Un réseau NGN doit prendre 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 doivent être prises en charge;
2) lorsque plusieurs couches interviennent dans la commutation de protection, les couches inférieures doivent être prioritaires par rapport aux couches supérieures (on parle de stratégie d'escalade intercouches);
3) il est recommandé d'assurer les commutations de protection 1+1 et 1: n;
4) les ressources de protection de transport non utilisées peuvent éventuellement servir à acheminer le trafic de "meilleur effort";
5) il est recommandé que 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.) soient 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) doivent être prises en charge.

Ci-après sont indiquées des spécifications détaillées relatives à des technologies spécifiques dans diverses Recommandations ([UIT-T G.808.1] par exemple).

16.5.2 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 peuvent éventuellement avoir priorité sur les couches supérieures (stratégie d'escalade intercouches);
2) le mécanisme de reroutage doit être capable de trouver un trajet de remplacement en un temps acceptable;
3) il est recommandé que 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.) soient aussi faibles que possible;
4) un réseau NGN ne doit pas exclure la possibilité d'une commande par l'opérateur;
5) une nouvelle optimisation du réseau doit être 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 doivent être rétablis.

16.5.3 Résilience de service

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

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

1) un réseau NGN doit attribuer de façon indépendante différents niveaux de résilience de service à différents services;
2) un réseau NGN doit attribuer de façon indépendante différents niveaux de résilience de service à différents services en fonction du flux considéré;
3) un réseau NGN doit prendre en charge la capacité de résilience, suivant le niveau de résilience de service attribué, et doit retrouver le niveau de qualité de service qu'il connaissait avant l'événement de défaillance;
4) l'équipement terminal peut signaler éventuellement les niveaux de résilience de service au réseau NGN;
5) un réseau NGN doit 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) un réseau NGN doit 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) un réseau NGN doit prendre en charge la capacité permettant de notifier à l'application/l'utilisateur que le niveau de résilience de service requis ne peut pas être atteint par le réseau NGN.

17 Réseaux d'utilisateur notamment les réseaux d'entreprise

17.1 Spécifications générales applicables aux NGN concernant l'accès via des réseaux d'utilisateur

Les spécifications générales applicables aux réseaux NGN concernant l'accès via les réseaux d'utilisateur sont les suivantes:

1) Un réseau NGN ne doit pas exclure les solutions d'accès via un réseau d'utilisateur vers un réseau NGN 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. Il n'est pas nécessaire que ces adresses puissent être acheminées dans le réseau NGN.
2) Les solutions d'accès au réseau NGN via un réseau d'utilisateur doivent avoir une incidence minimale sur les déploiements de réseaux d'utilisateur existants.
3) Les solutions d'accès au réseau NGN via un réseau d'utilisateur doivent prendre 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 (via des réseaux de rattachement et des réseaux d'entreprise).

Il est recommandé que les réseaux NGN autorisent 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 – Il n'est pas prévu d'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.

17.2 Spécifications générales concernant les réseaux d'utilisateur

Les spécifications de haut niveau concernant les réseaux d'utilisateur reliés aux réseaux NGN sont les suivantes:

– Il est recommandé que les réseaux d'utilisateur reliés aux réseaux NGN assurent l'accès de l'utilisateur:
  1) aux services fournis par les réseaux NGN;
  2) aux services fournis au sein des réseaux d'utilisateur eux-mêmes (localement et via les réseaux NGN interconnectés);
  3) aux services accessibles aux entreprises et aux utilisateurs à domicile.

– Il est recommandé que les réseaux d'utilisateur reliés aux réseaux NGN prennent en charge:
  1) la sécurité, la gestion et la qualité de service pour les réseaux de rattachement;
  2) la fourniture de l'équipement et la configuration des services (terminaux d'utilisateur, passerelles de réseaux d'utilisateur), y compris l'accès distant.

17.3 Réseaux d'entreprise

17.3.1 Introduction

Dans ce paragraphe sont données les spécifications de haut niveau pour les communications d'entreprise afin que soient pris en charge:

1) la connexion et l'interfonctionnement des capacités de communication d'entreprise (hébergées soit dans un réseau d'entreprise de prochaine génération (NGCN, *next generation corporate network*), soit dans un réseau NGN) avec un réseau NGN;
2) la connexion et l'interfonctionnement des capacités de communication d'entreprise avec d'autres capacités de communication d'entreprise (hébergées soit dans un réseau NGCN, soit dans un réseau NGN);
3) la connexion et l'interfonctionnement des capacités de communication d'entreprise avec d'autres capacités de communication d'entreprise situées dans le RNIS ou le RTPC ou reliées à eux;
4) les services d'entreprise hébergés dans un réseau NGN.

NOTE 1 – Dans la présente Recommandation sont données des spécifications applicables aux réseaux, assurant la prise en charge de la connexion directe d'un réseau NGCN à un réseau NGN, ainsi que des spécifications applicables aux réseaux pour la communication entre les capacités hébergées dans un réseau NGCN (y compris l'équipement d'utilisateur) et les autres capacités hébergées dans un réseau NGCN de la même entreprise via un réseau NGN (par exemple géographiquement distant).

NOTE 2 – Il est supposé que les spécifications existantes anciennes applicables aux services s'appliquent en cas de rattachement d'anciens autocommutateurs privés (PBX, *private branch exchange*) aux réseaux NGN.

17.3.2 Types de trafic d'entreprise

Le trafic généré ou reçu pour le compte d'un réseau NGCN peut être:

– soit le trafic envoyé au réseau NGN pour traitement conformément aux règles normales du réseau NGN. Ce type de trafic est nommé trafic de réseau public,

– soit le trafic envoyé au réseau NGN pour traitement conformément à un ensemble convenu de règles propres à une entreprise. Ce type de trafic est nommé trafic de réseau privé. Le trafic de réseau privé est normalement envoyé au sein d'une entreprise unique, mais il peut aussi se faire entre deux entreprises s'il n'est pas interdit pour des motifs réglementaires.

  NOTE – Un réseau d'entreprise peut éventuellement distinguer les communications de réseau privé au départ d'un réseau NGN des communications de réseau privé au départ de l'entreprise; cette question sort du cadre de la présente Recommandation.

Un réseau NGN doit distinguer le trafic de réseau public du trafic de réseau privé.

Un réseau NGN doit distinguer le trafic de réseau privé d'une entreprise de celui d'une autre entreprise.

Le trafic de réseau privé peut éventuellement nécessiter un traitement différent dans le réseau NGN, comparé à celui du trafic de réseau public.

Sauf lorsque la réglementation et la législation nationales ne le permettent pas, un réseau NGN doit traiter le trafic entre entreprises comme un trafic de réseau public. Dans ces cas, dans le cadre des capacités offertes à l'entreprise, le réseau NGN peut éventuellement fournir les capacités des communications sortantes/entrantes pour le compte de chaque entreprise.

S'agissant du trafic de réseau privé, un réseau NGN doit être transparent aux yeux des mécanismes de signalisation, sauf lorsqu'il existe un besoin spécifique d'intervention du réseau NGN afin que le service demandé par les clients de l'entreprise puisse être fourni.

17.3.3 Capacités de communication d'entreprise

Un réseau NGN doit permettre l'utilisation de tout média utilisant le protocole IP au cours d'une communication d'entreprise soumise à la disponibilité des ressources et aux accords contractuels.

Sauf s'il existe une autorisation par l'intermédiaire d'un accord explicite avec le réseau NGCN (par signalisation ou par contrat) ou si des prescriptions juridiques établies doivent être satisfaites, un réseau NGN doit ne pas intervenir, s'agissant du média qui est transporté dans ledit réseau NGN.

NOTE 1 – Le transcodage, la traduction et la transition sont des exemples de motifs d'intervention autorisée. Le choix par défaut de la non-intervention vise à éviter une dégradation injustifiée de la performance (en particulier pour les données de télémesure en temps réel, pour les données audio et vidéo bidirectionnelles) et à garantir la confidentialité attribuée du média.

Il est recommandé qu'un réseau NGN autorise qu'il se charge du transport de la signalisation tandis que le transport du média se fait via d'autres réseaux.

NOTE 2 – Par exemple, s'agissant de la communication entre deux réseaux d'entreprise, le réseau NGN peut être impliqué dans la signalisation (pour aider au routage de la première entreprise vers la deuxième entreprise), tandis que le média peut circuler directement à travers d'autres réseaux IP.

Un réseau NGN peut éventuellement offrir les capacités suivantes à une entreprise:

a) Une ligne louée virtuelle, où les sites de réseau NGCN sont interconnectés par l'intermédiaire du réseau NGN. Aucune capacité supplémentaire n'est fournie par le réseau NGN.

b) Une application de jonction d'entreprise, le réseau NGN hébergeant les capacités de communication de transit entre les réseaux NGCN, les capacités de communication entrante, du réseau NGN vers le réseau NGCN, les capacités de communication sortante, du réseau NGCN vers le réseau NGN. Outre les capacités de base susmentionnées, une telle application peut éventuellement aussi héberger des capacités supplémentaires pour le réseau NGCN. En général, aucun équipement terminal de réseau d'entreprise n'est directement relié à un réseau NGN.

c) L'hébergement de services d'entreprise (HES, hosted enterprise services), le réseau NGN hébergeant les capacités de communication d'entreprise entrante et/ou sortante pour les utilisateurs de communication d'entreprise qui sont directement reliés à un réseau NGN et ont contracté un abonnement à ces services dans ce réseau NGN.

17.3.4 Gestion de l'emplacement

Un réseau NGN doit fournir à un réseau NGCN des informations sur l'emplacement géographique d'un utilisateur de réseau NGCN. Cette indication peut être soumise à des spécifications relatives à la confidentialité.

NOTE 1 – Un réseau NGCN peut utiliser les informations sur l'emplacement géographique, par exemple, pour offrir des services en fonction de l'emplacement à l'utilisateur du réseau NGCN.

NOTE 2 – La source des informations sur l'emplacement géographique peut être un réseau NGN ou un utilisateur NGCN.

17.3.5 Signalisation

Un réseau NGN doit offrir une signalisation normalisée en vue d'assurer l'interface avec un réseau NGCN.

17.3.6 Routage

17.3.6.1 Routage vers un utilisateur de réseau NGCN

Un réseau NGN doit prendre en charge le routage vers les utilisateurs de réseau NGCN qui n'ont pas contracté d'abonnement à un service NGN, mais peuvent être joints par un site NGCN pour lequel il existe un accord de jonction d'entreprise avec un réseau NGN.

NOTE – Dans le cas où, pour un site NGCN, il existe un abonnement aux services NGN, il n'est pas nécessaire que les utilisateurs du réseau NGCN contractent individuellement un abonnement aux services NGN, puisque ceux-ci appartiennent au réseau NGCN et sont gérés par lui. Cette spécification permet que ces utilisateurs de réseau d'entreprise puissent être joints directement à partir de la partie publique du réseau NGN au moyen d'une adresse publique.

17.3.6.2 Routage employant les séries de numéros

Afin de pouvoir assurer l'acheminement vers les utilisateurs de réseau d'entreprise dans un réseau NGCN, il est recommandé que le réseau NGN ne prenne en charge le routage que pour une série de numéros spécifique [UIT-T E.164], attribuée à ce réseau NGCN.

17.3.7 Contrôle de la qualité de service

Le réseau NGN doit prendre en charge le contrôle d'admission de la communication pour chaque site NGCN.

NOTE 1 – Le fournisseur de réseau NGN définit l'ensemble de règles ou de politiques qu'il est recommandé d'appliquer dans ce cas, et il est recommandé que le fournisseur de réseau NGCN puisse configurer la capacité conformément à ces règles et politiques.

Il faut pouvoir fixer les seuils suivants pour chacune des directions (communications entrantes et sortantes):

1) le nombre maximal de communications simultanées orientées session;

2) le nombre maximal de flux simultanés par communication.

Les communications excédentaires peuvent être acceptées ou rejetées.

NOTE 2 – L'entreprise peut choisir des valeurs pour le contrôle d'admission des communications, qui correspondent à l'accord de niveau de service (SLA – service level agreement) entre l'entreprise et le fournisseur de réseau NGN. Si tel est le cas, les communications entrantes excédentaires qui sont acceptées peuvent être soumises à des règles de taxation spécifiques.

17.3.8 Identification

17.3.8.1 Identification de site NGCN

Un réseau NGN doit prendre en charge l'identification d'un site NGCN, pour authentification et autorisation.

NOTE 1 – L'identification d'un site NGCN est nécessaire pour que le réseau NGN puisse déterminer le site NGCN dont émane la communication.

NOTE 2 – Un réseau NGCN peut éventuellement comporter plusieurs sites NGCN et donc plusieurs identificateurs de site NGCN y associés.

17.3.8.2 Identification d'utilisateur de réseau d'entreprise

En plus des spécifications relatives au nommage, au numérotage et à l'adressage au § 16, le réseau NGN doit fournir la capacité permettant l'identification des utilisateurs de réseau NGCN de manière unique. Les identificateurs d'utilisateur de réseau NGCN sont attribués par un réseau NGCN.

NOTE 1 – Cela n'exclut pas les scénarios où un organisme, agissant déjà en tant que fournisseur de réseau NGN dans un autre rôle, administre le réseau NGCN d'une entreprise pour le compte de cette entreprise.

NOTE 2 – La spécification ci-dessus assure que, pour les communications émanant d'un utilisateur de réseau NGCN à destination d'un utilisateur de réseau NGN, le service de présentation de l'identité d'origine (*originating identity presentation* – OIP) de l'utilisateur de réseau NGN peut présenter l'identificateur correct de l'utilisateur de réseau NGCN appelant.

NOTE 3 – La spécification ci-dessus assure que, pour les communications émanant d'un utilisateur de réseau NGN à destination d'un utilisateur de réseau NGCN, le service de présentation de l'identité de terminaison (*termination identity presentation* – TIP) de l'utilisateur de réseau NGN peut présenter l'identificateur correct de l'utilisateur de réseau NGCN appelé.

NOTE 4 – La spécification ci-dessus assure que les utilisateurs de réseau NGN peuvent appeler les utilisateurs de réseau NGCN ayant des identificateurs qui font partie de l'ensemble d'identificateurs mis à disposition de ce réseau NGCN, dans le cadre d'un accord de jonction d'entreprise pour ledit réseau NGCN.

Il n'est pas recommandé qu'un réseau NGN empêche un réseau NGCN d'attribuer de nouveaux identificateurs d'utilisateur dans son domaine sans l'accord préalable dudit réseau NGN.

Il est recommandé qu'un réseau NGN prenne en charge les identificateurs d'utilisateur de réseau NGCN qui correspondent aux numéros UIT-T E.164.

Il n'est pas recommandé qu'un réseau NGN empêche un réseau NGCN de modifier la correspondance entre les identificateurs d'utilisateur dans son domaine et les numéros UIT-T E.164 sans l'accord préalable dudit réseau NGN.

NOTE 5 – Cela implique que, pour une communication émanant du RTPC/RNIS à destination du réseau NGCN, le réseau NGN devrait pouvoir déterminer que le numéro appelé UIT-T E.164 appartient au domaine du réseau NGCN et donc acheminer la communication vers le réseau NGCN en indiquant comme destination soit le numéro appelé UIT-T E.164 soit un identificateur NGCN découvert, obtenu à partir d'informations publiées par le réseau NGCN (par exemple, le système de noms de domaine (DNS, *domain name system*)).

Il est recommandé qu'un réseau NGN prenne en charge les identificateurs d'utilisateur de réseau NGCN qui ne correspondent pas aux numéros UIT-T E.164.

NOTE 6 – Même si les identificateurs d'utilisateur de réseau NGCN qui ne correspondent pas aux numéros UIT-T E.164 ne sont pas directement joignables à partir du RTPC/RNIS, ils devraient être joignables par d'autres utilisateurs de réseaux NGCN ou NGN.

Il n'est pas recommandé qu'un réseau NGN empêche l'acheminement des identificateurs d'utilisateur appelant ou connecté à destination du réseau NGCN, s'ils sont disponibles et en l'absence de spécifications relatives à la confidentialité ou de spécifications réglementaires qui interdisent un tel acheminement.

Il n'est pas recommandé qu'un réseau NGN empêche l'application de la confidentialité aux identificateurs d'utilisateur appelant ou connecté dans un réseau NGCN de façon permanente ou à chaque communication, de manière que ces identificateurs ne soient pas divulgués à d'autres parties.

NOTE 7 – Cela veut dire qu'un réseau NGN ne doit pas procéder dans ces circonstances à l'acheminement vers d'autres parties soit d'un identificateur fourni par le réseau NGCN (et marqué comme étant privé) soit d'un identificateur par défaut que le réseau NGN attribue au réseau NGCN.

17.3.9 Authentification

L'authentification, s'agissant de la connexion d'un réseau NGCN à un réseau NGN, doit être conforme aux spécifications données dans le présent paragraphe et au § 10.3.

17.3.10 Sécurité

La sécurité, s'agissant de la connexion d'un réseau NGCN à un réseau NGN, doit être conforme aux spécifications données au § 10.

17.3.11 Gestion de la mobilité

Dans le présent paragraphe sont données les spécifications relatives à l'itinérance, dans le contexte des communications d'entreprise.

S'agissant de l'itinérance dans le contexte des communications d'entreprise, il est recommandé que le nomadisme soit pris en charge tant pour la mobilité des terminaux que pour la mobilité des personnes.

En particulier, il est recommandé qu'un utilisateur de réseau NGCN puisse s'enregistrer et recevoir des services de son réseau NGCN alors qu'il se déplace:

a) vers un autre site NGCN du même réseau NGCN, interconnecté par un réseau NGN;

b) vers un réseau NGN auquel le réseau NGCN est directement connecté;

c) vers un réseau NGN auquel le réseau NGCN est indirectement connecté via un autre NGN.

En dehors des capacités d'itinérance offertes aux utilisateurs de réseau NGN dans le présent paragraphe, il est recommandé que, sous réserve d'un accord avec le réseau NGCN, un utilisateur de réseau NGN puisse s'enregistrer et recevoir des services de son réseau NGN alors qu'il se déplace:

a) vers un réseau NGCN connecté au réseau NGN;

b) vers un réseau NGCN indirectement connecté au réseau NGN.

17.3.12 Comptabilité

Une entreprise peut comptabiliser le trafic de ses capacités de communication d'entreprise, qu'elles soient hébergées dans un réseau NGCN ou dans un réseau NGN.

Pour le trafic de réseau public, les spécifications de [UIT-T Y.2201] et [UIT-T Y.2233] s'appliquent.

Pour le trafic de réseau public encore, l'entreprise et le fournisseur de réseau NGN doivent être en mesure de s'identifier mutuellement à travers une interface d'interconnexion quelconque, notamment une interface intraréseau NGN avec les capacités de communication d'entreprise hébergées.

Pour le trafic de réseau privé, les entreprises concernées doivent être en mesure de s'identifier mutuellement à travers une interface d'interconnexion quelconque entre ses capacités de communication d'entreprise.

Toute capacité de communication d'entreprise hébergée dans un réseau NGN doit pouvoir comptabiliser le trafic de réseau privé vers l'entreprise, comme le fait le fournisseur de réseau NGN pour son propre trafic.

En outre, pour le trafic de réseau privé, l'entreprise et le fournisseur de réseau NGN doivent être en mesure de s'identifier mutuellement à travers une interface d'interconnexion quelconque.

18 Interconnexion et interfonctionnement

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

18.1 Spécifications relatives à l'interconnexion

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

– "L'interconnexion orientée connectivité": 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 UIT-T G.711 sur interconnexion IP. Les niveaux d'interopérabilité définis dépendent du service, de la qualité de service ou de la sécurité, etc.

  NOTE 3 – Seule l'interconnexion orientée services satisfait pleinement aux spécifications relatives l'interopérabilité des réseaux NGN.

Les spécifications d'interconnexion sont les suivantes:

1) Le type interconnexion orientée connectivité entre réseaux NGN doit être pris en charge.

   Il faut prendre en charge ce type d'interconnexion entre réseaux NGN utilisant différentes versions du protocole IP.

2) Le type interconnexion orientée service entre réseaux NGN doit être pris en charge.

   Il faut prendre en charge ce type d'interconnexion entre réseaux NGN utilisant différentes versions du protocole IP.

3) L'interconnexion orientée service entre les réseaux NGN et NGCN doit être prise en charge, lorsque le réseau NGN fournit des services d'entreprise hébergés.

   Il faut prendre en charge ce type d'interconnexion entre réseaux NGN et NGCN utilisant différentes versions du protocole IP.

18.1.1 Interconnexion orientée service entre les réseaux NGN utilisant un sous-système multimédia IP

Les spécifications relatives à l'interconnexion orientée service entre les réseaux NGN utilisant un sous-système multimédia IP (IMS, *IP multimedia subsystem*) sont les suivantes:

1) La liaison logique d'interconnexion entre les fournisseurs de réseau NGN doit "avoir connaissance" des services NGN spécifiques. Il peut s'agir d'une liaison physique ou logique qui achemine tant les données que les porteurs de signalisation. Le réseau NGN doit offrir une interface normalisée d'interconnexion avec un autre réseau NGN.

2) Il faut contrôler les ressources de la liaison d'interconnexion afin de prendre en compte les caractéristiques des données et des porteurs de signalisation des différents services.

3) Les caractéristiques de sécurité et de comptabilité doivent être prises en compte.

D'autres spécifications détaillées relatives à l'interconnexion orientée service doivent faire l'objet d'un complément d'étude (notamment dans les domaines de la signalisation, des codecs, du routage, de la sécurité, de la taxation et de la comptabilité, des ressources, de la qualité de service et des accords SLA).

18.2 Spécifications relatives à l'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 doivent interopérer;

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

18.3 Spécifications relatives à l'interfonctionnement

Les réseaux NGN doivent interfonctionner avec différents types de réseaux pour la fourniture de certains services. Les services identifiés pour l'interfonctionnement doivent opérer de façon transparente à travers l'infrastructure fournie par un ou plusieurs fournisseurs de services. Les réseaux NGN 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 doit pouvoir interfonctionner avec d'autres réseaux non NGN;

– il est recommandé qu'un réseau NGN prenne 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).

18.3.1 Interfonctionnement avec le réseau RTPC/RNIS

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

1) l'interfonctionnement entre le réseau RTPC/RNIS et des services d'émulation du réseau RTPC/RNIS. Il doit assurer 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 doit prendre 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 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.

18.3.2 Interfonctionnement avec d'autres réseaux

1) Un réseau NGN doit fournir 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 spécifications d'interfonctionnement avec le réseau RTPC/RNIS.

   Un réseau NGN doit fournir la capacité d'une interconnexion orientée connectivité avec des réseaux non NGN mais IP.

   Un réseau NGN doit fournir la capacité d'une interconnexion orientée connectivité avec des réseaux non NGN mais IP employant différentes versions de protocole IP.

   Il doit ne pas exclure la capacité d'une interconnexion orientée service avec des réseaux non NGN mais IP.

   Si le réseau interconnecté fournit toutes les capacités d'interfonctionnement, comme on l'a identifié au § 18.3, 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.

2) Un réseau NGN doit ne pas exclure délibérément l'interconnexion avec des réseaux non NGN mais IP.

NOTE – Les spécifications de sécurité sont données au § 10.6.

18.4 Non-divulgation d'informations à travers des interfaces NNI et ANI

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

– d'empêcher la divulgation d'informations internes ou d'informations relatives aux utilisateurs de service à d'autres entités via des interfaces NNI;

– d'empêcher la divulgation d'informations internes sur les réseaux ou d'informations relatives aux utilisateurs du réseau à d'autres entités via des interfaces NNI;

– d'empêcher la divulgation d'informations internes ou d'informations relatives aux utilisateurs de service à d'autres entités via des interfaces ANI;

– d'empêcher la divulgation d'informations internes sur les réseaux ou d'informations relatives aux utilisateurs du réseau à d'autres entités via des interfaces ANI.

18.5 Echange interfournisseurs d'informations sur les utilisateurs

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

19 Spécifications propres aux services

19.1 Emulation 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 susceptible d'être choisi éventuellement par les fournisseurs de réseaux peut dépendre 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 doit présenter 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.

19.1.1 Généralités

Un réseau NGN doit fournir au moins 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.

19.1.2 Terminal

Un réseau NGN doit prendre 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).

19.1.3 Service

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

1) un réseau NGN doit prendre en charge la capacité des fournisseurs de services à émuler un ou plusieurs de leurs services RTPC/RNIS;

2) un réseau NGN doit prendre 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.

19.2 Services conversationnels multimédia en temps réel notamment la simulation de réseau RTPC/RNIS

19.2.1 Généralités

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

19.2.2 Terminal

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

19.2.3 Service

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

1) un réseau NGN doit prendre des capacités de service de type RTPC/RNIS en utilisant le mécanisme de contrôle de session sur interfaces et infrastructure IP;
2) il est recommandé qu'un réseau NGN assure à un fournisseur de services la capacité de simuler des services RTPC/RNIS;
3) un réseau NGN ne doit pas être 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.

19.3 Services de télévision utilisant le protocole Internet

Lorsqu'un réseau NGN fournit des services TVIP, la description suivante s'applique.

Les spécifications pour les réseaux NGN, relatives à la prise en charge des services TVIP, qui sont contenues dans la présente Recommandation, sont des spécifications de haut niveau.

Afin que les réseaux NGN prennent en charge les services TVIP, leurs capacités prennent en principe en charge les spécifications décrites dans [UIT-T Y.1901], étant entendu que, dans ces spécifications, les mots "l'architecture TVIP" sont remplacés par "l'environnement NGN". Des considérations spécifiques, comme celles de savoir quelles capacités spécifiques de réseau NGN prennent en charge les spécifications formulées dans [UIT-T Y.1901] et celles de savoir si celles-ci s'appliquent de la même manière à tous les services ou applications TVIP, doivent faire l'objet d'un complément d'étude.

19.3.1 Fourniture de services

L'architecture des réseaux NGN doit prendre en charge les mécanismes destinés aux services TVIP à la demande (y compris la vidéo à la demande (VoD, *video on demand*) avec distribution sélective [ITU-T Y.1901]), les services de diffusion de retransmission [ITU-T Y.1901] (y compris la télévision linéaire [ITU-T Y.1901]), et les services interactifs. Il est recommandé que l'architecture de réseau NGN prenne en charge des mécanismes destinés au service enregistreur vidéo personnel client (cPVR, *client personal video recorder*) [ITU-T Y.1901] et au service enregistreur vidéo personnel réseau (nPVR, *network personal video recorder*) [ITU-T Y.1901]. La prise en charge de la fonctionnalité mode d'enrichissement [ITU-T Y.1901] est recommandée pour la mise en œuvre de certains services TVIP.

Il est recommandé que l'architecture de réseau NGN prenne en charge les mécanismes au moyen desquels les utilisateurs finaux peuvent mettre les contenus qu'ils ont produits/créés à la disposition d'autres utilisateurs finaux.

L'architecture de réseau NGN doit donner à l'utilisateur final la possibilité de choisir une langue préférée (audio, sous-titres [ITU-T Y.1901], légendes [ITU-T Y.1901], contenus supplémentaires [ITU-T Y.1901] et descriptions audio [ITU-T Y.1901]) parmi les diverses langues que le fournisseur de contenus a prédéfinies et que le fournisseur de services a acheminées.

NOTE – D'autres informations concernant les "services à la demande" peuvent être consultées dans [b-UIT-T Y.Sup.5].

19.3.2 Transport et mobilité

Pour la prise en charge des services TVIP, les spécifications relatives au transport au § 6, y compris la prise en charge de la multidiffusion, sont applicables.

Pour la prise en charge des services TVIP, les spécifications relatives au traitement de la mobilité au § 12 sont applicables.

19.3.3 Activateurs de services

L'architecture de réseau NGN doit prendre en charge les capacités de découverte et de sélection, ainsi que la capacité de navigation pour les contenus et les services TVIP.

Il est recommandé que l'architecture de réseau NGN prenne en charge le suivi des informations sur l'audience tout en protégeant la confidentialité de l'utilisateur comme requis.

Il est recommandé que l'architecture de réseau NGN permette la collecte de statistiques sur l'utilisation des contenus et le traçage des contenus.

Il est recommandé que l'architecture de réseau NGN dispose d'un moyen pour permettre aux contenus de n'être vus que par l'audience appropriée, en fonction de zones géographiques spécifiées, de l'évaluation parentale et de groupes spécifiés. L'architecture de réseau NGN doit en particulier prendre en charge des mécanismes permettant de bloquer la transmission de contenus à des zones géographiques spécifiées lorsque des prescriptions d'occultation sont applicables.

19.3.4 Intergiciels et métadonnées

L'architecture de réseau NGN doit ne pas exclure une quelconque utilisation d'intergiciels et de métadonnées pour les services TVIP.

19.3.5 Qualité de service

Les réseaux qui prennent en charge les services TVIP doivent prendre en charge les classes de qualité de service IP et satisfaire aux spécifications associées relatives à la performance, spécifiées dans [UIT-T Y.1541]. Cela inclut le maintien du contrôle précis quant au temps de la synchronisation, par exemple la synchronisation labiale. Il est recommandé que l'architecture de réseau NGN prenne en charge un moyen de donner les temps de changement de canaux [UIT-T Y.1901] avec une qualité d'expérience (QoE, *quality of experience*) suffisante.

Le réseau NGN doit disposer d'un cadre qui identifie les composantes et les points de mesure (y compris le dispositif de l'utilisateur final) pour la mesure de la qualité de service (QoSM).

19.3.6 Sécurité

L'architecture de réseau NGN doit prendre en charge la protection des services et des contenus.

19.3.7 Gestion

Il est recommandé que l'architecture de réseau NGN prenne en charge la mise à niveau et le téléchargement (distants) de logiciels pour les dispositifs TVIP.

19.3.8 Média

L'architecture de réseau NGN doit ne pas exclure toute utilisation des formats vidéo et audio (y compris les résolutions vidéo, les formats vidéo, les taux d'échantillonnage audio et les profondeurs de bit audio) spécifiés pour les services TVIP.

L'architecture de réseau NGN doit ne pas exclure toute utilisation des codecs vidéo et audio spécifiées pour les services TVIP.

Le transcodage pendant la fourniture des contenus TVIP dans l'architecture de réseau NGN doit être évité dans la mesure du possible.

19.3.9 Taxation

L'architecture de réseau NGN doit prendre en charge les mécanismes de collecte de données à des fins de comptabilité et de rapport, de règlement entre partenaires et de conciliation avec l'utilisation des utilisateurs finals, tels que les abonnements, les achats et les transactions en ce qui concerne les services. Le but est de prendre en charge des options de taxation telles que celle du paiement à la séance [UIT-T Y.1901].

19.3.10 Aspects concernant les terminaux

Un dispositif terminal prenant en charge les services TVIP doit être en mesure de sélectionner, de recevoir et de restituer les multiples informations audio, vidéo ainsi que les informations associées de contrôle.

Il est recommandé que l'architecture de réseau NGN prenne en charge de telles capacités de terminal et les capte pour adapter la fourniture de services.

19.3.11 Interfonctionnement

Les spécifications relatives à la prise en charge de l'interfonctionnement entre les services TVIP doivent faire l'objet d'un complément d'étude.

19.3.12 Intérêts publics

L'architecture de réseau NGN doit prendre en charge les dispositifs terminaux pour les services TVIP, qui sont constamment à l'écoute de messages de notification d'alerte et d'urgence (EAN, *emergency alert notification*).

L'architecture de réseau NGN doit prendre en charge la mise à disposition de caractéristiques facilitant l'accessibilité (légendes, sous-titres, informations audio descriptives et flux vidéo multiple tels que celui de la langue des signes) et leur synchronisation avec le contenu principal pendant une visualisation en lecture normale.

Il est recommandé que l'architecture de réseau NGN prenne en charge la transmission de vidéo ou de données de qualité suffisante pour que soit perçue l'interprétation en langue des signes et que la lecture sur les lèvres puisse notamment se faire. Cela exige la transmission d'un nombre suffisant de trames par seconde et une résolution spatiale suffisante pour reproduire les détails des mains, du visage, des lèvres, des yeux et du corps de la personne exécutant les signes [b-UIT-T H.Sup.1].

19.4 Services d'entreprise

19.4.1 Service de ligne louée virtuelle

Aucune spécification propre à ce service n'est établie dans la présente Recommandation.

19.4.2 Application de jonction d'entreprise

Aucune spécification propre à ce service n'est établie dans la présente Recommandation.

19.4.3 Services d'entreprise hébergés

Lorsqu'un réseau NGN fournit des services d'entreprise hébergés, il doit:

– prendre en charge les communications des entreprises qui regroupent tant des utilisateurs pris en charge par les réseaux NGCN que des utilisateurs pris en charge par les services d'entreprise hébergés (HES, *hosted enterprise services*), notamment des communications entre un utilisateur pris en charge par un réseau NGCN et un utilisateur pris en charge par un service HES;

– permettre à un utilisateur d'entreprise de se déplacer entre un site de réseau NGCN et un site pris en charge par un service HES, sans que les partenaires de la communication soient nécessairement conscients de ce changement;

– permettre à un utilisateur d'entreprise de déplacer son terminal entre un site de réseau NGCN et un site pris en charge par un service HES, avec un minimum de reconfiguration.

19.5 Applications et services utilisant une identification par étiquette

Lorsqu'un réseau NGN fournit des applications et des services utilisant une identification par étiquette, [UIT-T Y.2213] énonce les spécifications correspondantes pour chaque service.

19.6 Services de gestion de la fourniture

Lorsqu'un réseau NGN fournit des services de gestion de la fourniture, [UIT-T Y.2212] énonce les spécifications correspondantes pour chaque service.

19.7 Services de surveillance visuelle

Un service de surveillance visuelle de terminal à terminal permet à un terminal de recevoir et de surveiller les informations multimédia produites par l'autre terminal (source) et permet le contrôle distant du dispositif source.

Un service de surveillance visuelle de serveur à terminal permet à plusieurs terminaux de recevoir et de surveiller les mêmes informations multimédia produites par un serveur source unique.

Un service de surveillance visuelle de terminal à serveur permet à un serveur de recueillir de multiples morceaux ou un morceau agrégé d'information multimédia produits par plusieurs terminaux (sources).

Lorsqu'un réseau NGN fournit des services de surveillance visuelle, il doit prendre en charge:

– les services de surveillance visuelle de terminal à terminal (notamment de terminal unique à terminal unique et de terminal unique à terminaux multiples) (par exemple le service de surveillance visuelle destiné à la supervision de la sécurité domestique);
– les services de surveillance visuelle de serveur à terminal (notamment de serveur unique à terminal unique et de serveur unique à terminaux multiples) (par exemple le service de surveillance visuelle destiné à la supervision du trafic public).

Les spécifications pour les services de surveillance visuelle de terminal à serveur doivent faire l'objet d'un complément d'étude.

19.7.1 Service de surveillance visuelle de serveur à terminal

Un réseau NGN doit prendre en charge les capacités de découverte et de sélection, ainsi que la capacité de navigation pour les services de surveillance visuelle de serveur à terminal.

Il est recommandé qu'un réseau NGN permette la collecte de statistiques sur l'utilisation des contenus et le traçage des contenus.

Il est recommandé qu'un réseau NGN dispose d'un moyen pour permettre aux contenus de n'être vus que par l'audience appropriée, en fonction de zones géographiques spécifiées, de l'évaluation parentale et de groupes spécifiés. Un réseau NGN doit en particulier prendre en charge des mécanismes permettant de bloquer la transmission de contenus à des zones géographiques spécifiées lorsque des prescriptions d'occultation sont applicables.

Un réseau NGN doit assurer la protection des services et des contenus.

Il est recommandé qu'un réseau NGN prenne en charge la mise à niveau et le téléchargement (distants) de logiciels pour les dispositifs de surveillance visuelle de serveur à terminal.

19.7.2 Service de surveillance visuelle de terminal à terminal

Afin de prendre en charge les services de surveillance visuelle de terminal à terminal, un réseau NGN doit appliquer les spécifications données dans les paragraphes suivants.

19.7.2.1 Traitement des sessions

Un réseau NGN doit prendre en charge le contrôle d'admission aux sessions à l'aide d'informations liées à la surveillance visuelle.

Un réseau NGN doit prendre en charge le traitement des sessions à l'aide d'informations liées à la surveillance visuelle (par exemple des données propres au service telles que le contrôle à distance).

19.7.2.2 Routage

Un réseau NGN doit prendre en charge le routage en tenant compte des capacités des terminaux d'origine/de destination (par exemple la prise en charge de média).

19.7.2.3 Codecs

L'architecture de réseau NGN doit permettre toute utilisation des codecs vidéo et audio spécifiés pour les services de surveillance visuelle.

Le transcodage pendant l'acheminement des informations de surveillance visuelle dans l'architecture de réseau NGN doit être évité dans la mesure du possible.

19.8 Applications et services de réseaux ubiquitaires de capteurs (USN, *ubiquitous sensor network*)

Les spécifications propres aux services doivent faire l'objet d'un complément d'étude.

19.9 Services des centres de communication multimédia

Les spécifications propres aux services doivent faire l'objet d'un complément d'étude.

19.10 Services VPN dans les réseaux NGN

Lorsqu'un réseau NGN fournit des services VPN, [UIT-T Y.2215] énonce les spécifications correspondantes pour chaque service.

20 Aspects touchant aux intérêts publics

Un réseau NGN doit fournir 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 présents paragraphes.

20.1 Interception légale

1) Un fournisseur de transport NGN ou de services NGN doit respecter les spécifications d'interception légale. Un réseau NGN doit donc fournir 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.

20.2 Identification de communications malveillantes

Un réseau NGN doit disposer de 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.

20.2.1 Identification de communications malveillantes pour l'entreprise

Une communication identifiée comme faisant partie du trafic de réseau public doit être traitée conformément aux spécifications relatives à l'identification de communications malveillantes du réseau NGN.

L'identification de communications malveillantes faisant partie du trafic de réseau privé sort du cadre de la présente Recommandation. Un réseau NGN doit ne pas traiter de telles communications. Cela s'applique aussi à une capacité de réseau NGCN hébergée.

NOTE – Des prescriptions réglementaires distinctes peuvent s'appliquer pour le trafic de réseau privé.

20.3 Communications non sollicitées

Un réseau NGN doit fournir des capacités empêchant les communications non sollicitées.

Un réseau NGN doit fournir la possibilité de traiter les tentatives de communication détectées et marquées et y réagir (par exemple, en redirigeant la communication vers une boîte aux lettres, une boîte de messagerie vocale ou une poubelle).

Il est recommandé qu'un réseau NGN fournisse des mécanismes permettant de lutter contre les communications non sollicitées (par les listes blanche/noire, le système de réputation, le masquage des adresses, le filtrage des contenus).

NOTE 1 – Pour plus d'informations sur ces mécanismes, veuillez vous reporter à [b-UIT-T X.1244].

Il est recommandé qu'un réseau NGN fournisse un mécanisme permettant le signalement des communications non sollicitées par les utilisateurs de réseau NGN.

Il est recommandé qu'un réseau NGN fournisse un mécanisme permettant la vérification des rapports établis par les utilisateurs de réseau NGN.

Il est recommandé qu'un réseau NGN:

- fournisse la capacité permettant à un utilisateur victime de communications non sollicitées de demander le marquage (l'évaluation) des communications non sollicitées;
- fournisse la capacité permettant à utilisateur victime de communications non sollicitées de rectifier le marquage des communications non sollicitées.

NOTE 2 – Pour plus d'informations sur le marquage des communications non sollicitées, veuillez vous reporter à [b-ETSI TS 187.009].

20.4 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: "cadre(s)général(aux) 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 doit mettre 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 doivent bénéficier 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 peut avoir raccroché.

9) Fournir à l'organisme des informations sur l'emplacement géographique et l'identificateur du particulier conformément aux spécifications 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-divulgation.

10) Fournir la capacité d'un accès authentifié ou non authentifié aux services de télécommunications d'urgence conformément aux spécifications réglementaires nationales ou régionales. Par exemple, un réseau NGN doit fournir 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.

20.4.1 Télécommunications d'urgence pour une entreprise

Tant le trafic de réseau public que le trafic de réseau privé peuvent éventuellement acheminer les télécommunications d'urgence pour une entreprise.

1) Une télécommunication d'urgence pour une entreprise identifiée comme faisant partie du trafic de réseau public doit être traitée conformément aux spécifications relatives aux télécommunications d'urgence des réseaux NGN.

2) En cas d'une télécommunication d'urgence, faisant partie du trafic de réseau public, pour une entreprise, un réseau NGN doit transmettre les informations sur l'emplacement géographique reçues d'un réseau NGCN et éventuellement les utiliser pour leur acheminement aux autorités appropriées. Cela peut être soumis tant aux prescriptions relatives à la confidentialité qu'aux prescriptions réglementaires.

3) L'acheminement des communications identifiées comme étant des télécommunications d'urgence faisant partie du trafic de réseau privé sort du cadre des documents sur les réseaux NGN. Un réseau NGN doit ne pas traiter de telles communications. Cela s'applique aussi à une capacité de réseau NGCN hébergée.

4) Conformément à la réglementation et à la législation nationales, dans les plans de numérotage privés utilisés au sein d'une entreprise, les numéros d'urgence nationaux peuvent éventuellement être réutilisés à d'autres fins et un numéro différent peut éventuellement être utilisé pour désigner une télécommunication d'urgence.

5) Conformément à la réglementation et à la législation nationales, lorsqu'une entreprise exploite un point de réponse de sécurité publique (PSAP, *public safety answering point*) privé, un réseau NGN peut éventuellement prendre en charge l'acheminement pour une entreprise des télécommunications d'urgence, faisant partie du trafic de réseau public, vers le point PSAP privé (ou vers l'un des points PSAP privés) ou vers un point PSAP public, en fonction des circonstances. Par exemple, pour un appelant physiquement présent sur un site d'entreprise particulier, l'acheminement pour ce site vers un point PSAP privé peut être requis, tandis que pour des appelants physiquement présents ailleurs, l'acheminement vers un point PSAP public peut être requis.

20.5 Présentation et confidentialité de l'identificateur d'utilisateur

1) Un réseau NGN doit avoir la capacité de présenter l'identificateur de l'appelant.

2) Un réseau NGN doit avoir la capacité de présenter l'identificateur de l'appelé.

3) Un réseau NGN doit avoir la capacité de supprimer la présentation de l'identificateur de l'appelant.

4) Un réseau NGN doit avoir 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.

20.6 Sélection de fournisseur de réseaux ou de service

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

20.7 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 doit fournir 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 doit avoir la capacité de permettre l'invocation des services de relais par l'une des parties lors de télécommunications d'urgence.

NOTE 1 – Le § 20.4 traite d'autres besoins d'utilisateurs handicapés relatifs aux services de télécommunications d'urgence.

NOTE 2 – Voir également [b-ITU-T Accessibility] et [b-UIT-T F.790].

20.8 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 (§ 10.2). 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 émulés héritent de caractéristiques associées au réseau RTPC/RNIS (voir le § 19.1.3).

20.9 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 doit prendre en charge les mécanismes de dégroupage de services.

20.10 Rejet des communications anonymes

Un réseau NGN doit fournir un mécanisme permettant à un utilisateur de rejeter une communication entrante lorsque l'appelant est anonyme.

20.10.1 Rejet des communications anonymes pour une entreprise

Une communication identifiée comme faisant partie du trafic de réseau public doit être traitée conformément aux spécifications du réseau NGN relatives au rejet des communications anonymes.

Les spécifications destinées au traitement des communications anonymes faisant partie du trafic de réseau privé sortent du cadre de la présente Recommandation. Un réseau NGN doit ne pas traiter de telles communications. Cela s'applique aussi à une capacité de réseau NGCN hébergée.

NOTE – Des prescriptions réglementaires distinctes peuvent éventuellement s'appliquer au trafic de réseau privé.

Appendice I

Principales différences en termes de spécifications de haut niveau et de capacités entre la présente version de la Recommandation UIT-T Y.2202 (Y.2201 Rév.1) et la version précédente de la Recommandation Y.2201 (2007)

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

Dans le présent Appendice sont énumérées les principales différences en termes de spécifications de haut niveau et de capacités entre la présente Recommandation et la Recommandation UIT-T Y.2201 (04/07) [UIT-T Y.2201].

NOTE – L'achèvement du présent Appendice doit faire l'objet d'un complément d'étude.

Capacité UIT-T Y.2201 Rév.1	**Paragraphe dans la présente Recommandation**	**Paragraphe dans la Recommandation UIT-T Y.2201 (2007) (s'il y a lieu)**	**Améliorations par rapport à la Recommandation UIT-T Y.2201 (2007)**	**Nouvelle capacité**
OAM			Aucune	–
Mobilité			Prise en charge du transfert	–
Perception de contexte		–	–	X

Appendice II

Mappage entre services et activateurs de service

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

NOTE – L'achèvement du présent Appendice doit faire l'objet d'un complément d'étude.

Le présent Appendice donne un exemple de mappage entre des services sélectionnés et des activateurs de service sélectionnés (§ 7.2). Ce mappage ne vise pas à l'exhaustivité et ne correspond pas à des spécifications de prise en charge.

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

Services/ Activateurs de service	Présence	Gestion des emplacements	Gestion des groupes	Gestion des messages	Prise en charge de la multi-diffusion	Poussée	Gestion des sessions	Gestion des informations personnelles	Gestion des dispositifs	Prise en charge des applications utilisant le Web	Synchronisation des données
Services vocaux conversationnels en temps réel							X				
Services conversationnels multimédia 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				

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

Services/ Activateurs de service	Présence	Gestion des emplacements	Gestion des groupes	Gestion des messages	Prise en charge de la multi-diffusion	Poussée	Gestion des sessions	Gestion des informations personnelles	Gestion des dispositifs	Prise en charge des applications utilisant le Web	Synchronisation des données
Services multimédias interactifs point à point			X				X				
Services de communication interactifs exploités en commun		X	X				X				
Services de type poussée		X				X					
Services de radiodiffusion/de multidiffusion					X						
Services d'informations	X	X				X					
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						
Applications et services utilisant					X				X		

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

Services/ Activateurs de service	Présence	Gestion des emplacements	Gestion des groupes	Gestion des messages	Prise en charge de la multi-diffusion	Poussée	Gestion des sessions	Gestion des informations personnelles	Gestion des dispositifs	Prise en charge des applications utilisant le Web	Synchronisation des données
l'identification par étiquette											
Surveillance visuelle							X		X		
Services TVIP											
Services d'entreprise: services de ligne louée virtuelle											
Services d'entreprise: application de jonction d'entreprise											
Services d'entreprise: services hébergés pour entreprises											
Services de gestion de la fourniture											

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-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.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.510] Recommandation UIT-T H.510 (2002), *Mobilité pour systèmes et services multimédias H.323.*

[b-UIT-T H-Sup.1] Supplément 1 aux Recommandations UIT-T 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 I.570] Recommandation UIT-T I.570 (1993), *Interfonctionnement entre des RNIS publics et des RNIS privés.*

[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.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).*

[b-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).*

[b-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.*

[b-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.*

[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 X.501] Recommandation UIT-T X.501 (2008), ISO/CEI 9594-2:2008, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles.*

[b-UIT-T X.509] Recommandation UIT-T X.509 (2008), ISO/CEI 9594-8:2008, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*

[b-UIT-T X.511] Recommandation UIT-T X.511 (2008), ISO/CEI 9594-3:2008, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: définition du service abstrait.*

[b-UIT-T X.1244] Recommandation UIT-T X.1244 (2008), *Aspects généraux de la lutte contre le pollupostage dans les applications multimédias sur les réseaux IP.*

[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.2052] Recommandation UIT-T Y.2052 (2008), *Cadre du rattachement multiple dans les réseaux de prochaine génération utilisant le protocole IPv6.*

[b-UIT-T Y.2053] Recommandation UIT-T Y.2053 (2008), *Caractéristiques fonctionnelles du passage au protocole IPv6 dans les réseaux de prochaine génération.*

[b-UIT-T Y.2054] Recommandation UIT-T Y.2054 (2008), Cadre de prise en charge de la signalisation pour les réseaux de prochaine génération utilisant le protocole IPv6.

[b-UIT-T Y-Sup.1] Supplément 1 aux Recommandations UIT-T de la série Y.2000 (2006), Recommandations UIT-T de la série Y.2000 – *Supplément sur le domaine d'application des réseaux de prochaine génération de version 1*.

[b-UIT-T Y-Sup.5] Supplément 5 aux Recommandations UIT-T de la série Y.1900 (2008), Recommandations UIT-T de la série Y.1900, *Supplément sur les cas d'utilisation des services de TVIP.*

[b-UIT-T Y-Sup.7] Supplément 7 aux Recommandations UIT-T de la série Y (2008), Recommandations UIT-T de la série Y.2000, *Supplément sur le domaine d'application des réseaux NGN de version 2*.

[b-ITU-T Climate] ITU-T ICTs and Climate Change (2009), *Deliverable 2: Gap Analysis and Standards Roadmap.*

[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.*

Lignes directrices de l'UIT-T

[b-ITU-T Accessibility] Document technique UIT-T (2006), *FSTP-TACL Telecommunications Accessibility Checklist.*

Spécifications techniques de l'ETSI

[b-ETSI TR 121 905] ETSI TR 121 905 V7.3.0 (2007), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications*.

[b-ETSI TS 101 331] ETSI TS 101 331 V1.2.1 (2006), *Lawful Interception (LI); Requirements of Law Enforcement Agencies*.

[b-ETSI TS 122 057] ETSI TS 122 057 V6.0.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Mobile Execution Environment (MExE) service description; Stage 1*.

[b-ETSI TS 122 071] ETSI TS 122 071 V3.5.0 (2004), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Location Services (LCS); Stage 1*.

[b-ETSI TS 122 078] ETSI TS 122 078 V7.6.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Customized Applications for Mobile network Enhanced Logic (CAMEL); Service description*.

[b-ETSI TS 122 127] ETSI TS 122 127 V7.1.0 (2006), *Universal Mobile Telecommunications System (UMTS); Service requirement for the Open Services Access (OSA); Stage 1*.

[b-ETSI TS 122 140] ETSI TS 122 140 V6.7.0 (2005), *Universal Mobile Telecommunications System (UMTS); Multimedia Messaging Service (MMS); Stage 1*.

[b-ETSI TS 122 146] ETSI TS 122 146 V7.2.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Multimedia Broadcast/Multicast Service (MBMS); Stage 1*.

[b-ETSI TS 122 174] ETSI TS 122 174 V6.2.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Push service; Stage 1*.

[b-ETSI TS 122 240] ETSI TS 122 240 V6.5.0 (2005), *Universal Mobile Telecommunications System (UMTS); Service requirements for 3GPP Generic User Profile (GUP); Stage 1*.

[b-ETSI TS 122 250] ETSI TS 122 250 V6.0.0 (2005), *Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS) Group Management; Stage 1*.

[b-ETSI TS 123 141] ETSI TS 123 141 V7.2.0 (2006), *Universal Mobile Telecommunications System (UMTS); Presence service; Architecture and functional description; Stage 2*.

[b-ETSI TS 123 228] ETSI TS 123 228 V7.7.0 (2007), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2*.

[b-ETSI TS 126 235] ETSI TS 126 235 V6.4.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Packet switched conversational multimedia applications; Default codecs*.

[b-ETSI TS 133 106] ETSI TS 133 106 V7.0.1 (2006), *Universal Mobile Telecommunications System (UMTS); Lawful interception requirements*.

[b-ETSI TS 142 033] ETSI TS 142 033 V7.0.0 (2007), *Digital cellular telecommunications system (Phase 2+); Lawful Interception; Stage 1*.

[b-ETSI TS 181 005] ETSI TS 181 005 V2.4.1 (2007), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements*.

[b-ETSI TS 181 019] ETSI TS 181 019 V2.0.0 (2007), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business Communication Requirements*.

[b-ETSI TS 187 009] ETSI TS 187 009 V2.1.1 (2008), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN*.

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

[b-ANSI-J-STD-025] ANSI-J-STD-025-A-2003, *Lawfully Authorized Electronic Surveillance (CALEA)*.

[b-ATIS 1000678] ATIS 1000678-2006, *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 2*.

[b-T1.724] ANSI T1.724-2004, *UMTS Handover Interface for Lawful Interception*.

[b-TIA-127-A] TIA-127-A (2004), *Enhanced Variable Rate Codec Speech Option 3 for Wideband Spread Spectrum Digital Systems*.

[b-TIA-1016-A] TIA-1016-A (2006), *Source-Controlled Variable-Rate Multimode Wideband Speech Codec (VMR-WB) – Service Options 62 and 63 for Spread Spectrum Systems*.

[b-TIA-1066] TIA-1066 (2006), *LAES for cdma2000 VoIP*.

[b-TIA-1072] TIA-1072 (2006), *LAES for cdma2000 push-to-talk over cellular*.

Spécifications de l'IETF

[b-IETF RFC 2486] IETF RFC 2486 (1999), *The Network Access Identifier*.

[b-IETF RFC 4594] IETF RFC 4594 (2006), *Configuration Guidelines for DiffServ Service Classes*.

Spécifications de l'Open Mobile Alliance

[b-OMA-DS] OMA specification (2006), *Data Synchronization V1.2*.

[b-OMA-DM] OMA specification (2007), *Device Management V1.2*.

[b-OMA-OSE] OMA specification (2007), *Service Environment V1.0*.

[b-OMA-PoC] OMA specification (2006), *Push to talk over Cellular V1.0.1*.

[b-OMA-PS] OMA specification (2006), *Presence Simple V1.0.1*.

[b-OMA-WS] OMA specification (2006), *Web Services V1.1*.

[b-OMA-XML] OMA specification (2006), *XML Document Management*.

[b-OMA-LS] OMA specification (2006), *Mobile Location Service V1.1*.

[b-OMA-XDM] OMA specification (2006), *XML Document Management V1.0.1*.

[b-OMA-Push] OMA specification (2005), *Push V2.1*.

Accès ouvert aux services (OSA)

[b-OSA-Parlay-X] ETSI ES 202 391-x (2006), *Open Service Access (OSA), Parlay X Web Services, Parts 1-14*.

[b-OSA-Parlay-4] ETSI ES 202 915-x V1.3.1 (2006), *Open Service Access (OSA); Application Programming Interface (API); Parts 1-14 (Parlay 4)*.

[b-OSA-Parlay-5] ETSI ES 203 915-x V1.1.1 (2007), *Open Service Access (OSA); Application Programming Interface (API); Parts 1-15 (Parlay 5)*.

Services de réseau intelligent

[b-TIA/EIA/IS-771-1] TIA/EIA/IS 771-1 (1999), *Wireless Intelligent Network – Addendum 1 (2001)*.

[b-TIA-873.002] TIA-873.002 (2003), *All IP Core Network Multimedia Domain – IP Multimedia Subsystem – Stage-2 (2003)*.

Spécifications UDDI

[b-OASIS-UDDI] OASIS specification (2004), *UDDI Version 3.0.2*.

Spécifications SOA

[b-OASIS-SOA] OASIS specification (2006), *Reference Model for Service Oriented Architecture 1.0*.

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	Terminaux et méthodes d'évaluation subjectives et objectives
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

Imprimé en Suisse
Genève, 2010